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 (Full unabridged version)

October 2017

Contents

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

1. 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 (2017)**

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[1];

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

[1] 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).

WORKSTREAM ONE

The Key Principles

5. Summary of Key Legislative Principles

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 free flow of data around the world, privacy enforcement authorities 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 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,

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.

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[2]*.*

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.

[2] As OECD Recommendation 13 recognises "Member countries and their Privacy Enforcement Authorities should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross border aspects arising out of the enforcement of Laws Protecting Privacy. Such cooperation may be facilitated by appropriate bilateral or multilateral enforcement arrangements".

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[3] ("PEAs") in cases involving the processing of personal information in multiple jurisdictions.

The protection of personal information[4] 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 privacy enforcement authorities 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.

[3] 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.
[4] 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".[5]

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".[6] 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[7]) 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.

[5] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Part Five, Guideline 21, 1980.
[6] OECD Recommendation on cross-border co-operation in the enforcement of laws protecting privacy, 2007.
[7] 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[8], 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.

[8] 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[9].

***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 free flow of data around the world, privacy enforcement authorities 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 authority can be used by the recipient authority in pursuit of actions in its own jurisdiction.

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

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[10]. 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[11] to achieve many of the aims being taken forward by this work[12].

***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,

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

[10] 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.
[11] 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.
[12] OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007), paragraph 21

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[13]. 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

[13] 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 Enforcement Cooperation,[14] 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),

[14] 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[15].

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.

[15] 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[16]. 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

[16] 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.[17] 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

[17] 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[18].

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

[18] 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[19].

- 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).

[19] 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,[20] 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.

[20] 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')[21] 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

[21] 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)[22]
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:

[22] 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)[23]

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.

[23] 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[24]

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

[24] 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 2.2: Reports on individual networks' available tools and resources

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

Asia-Pacific Economic Cooperation (Data Privacy Subgroup)
Available Tools and Resources

General Information

What is the organization: The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. APEC's members[25] aim to create greater prosperity for the people of the region by promoting balanced, inclusive, sustainable, innovative and secure growth and by accelerating regional economic integration.

APEC has an Electronic Commerce Steering Group (ECSG) which at the same time has a Data Privacy Subgroup (DPS). The DPS was created in 2004 in order to contribute to the development of a governance that guarantees the confidence of the consumers in the information flows for e-commerce (on a region with several policies of data protection).

Tools and Resources

Overview: in order to develop a regional privacy governance based on the information flow, the DPS issue a Privacy Framework[26] (updated in November 2016). The framework contains 9 guiding principles for the members to design national approaches to Personal Data Protection. In the same way, the framework seeks improve the creation of a regional mechanisms to promote and strength the personal privacy, as well as to maintain the continuity of information flows between the members and the other trading partners.

One of these mechanisms is the APEC Cross Border Privacy Rules System (CBPR)[27]. The document is the basis for cooperation between privacy authorities of APEC economies and is a set of rules and policies for personal data protection

[25] APEC's 21 member economies are Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Viet Nam.
[26] Available at: http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf
[27] Available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

(mainly self-regulatory schemes) implemented by data controllers and organizations who transfer data to third parties outside their territory. The rules must be validated by a third party.

Members may participate in the CBPR expressing their interest by an application and with the approval of the DPS.

For this, the members must comply certain requirements, for instance be part of the APEC Cross-Border Privacy Enforcement Arrangement (CPEA) [28]. This multilateral arrangement provides the first mechanism in the APEC region for Privacy Enforcement Authorities (PEAs) to share information and provide assistance for cross-border data privacy enforcement. The CPEA signifies the ongoing commitment within APEC to increase the protection of cross-border flows of personal information and is a significant step in the effective implementation of the APEC Privacy Framework.

The aims of the CPEA are:

- Facilitate the exchange of information between PEAs;
- Provide mechanisms to promote effective cross-border cooperation between authorities for the application of privacy laws;
- Encourage information exchange and privacy research cooperation, as well as enforcement of laws with privacy protection authorities who are not members of APEC.

Moreover, in order to ensure a high degree of transparency during the implementation of the Privacy Framework, the members have published their Individual Data Privacy Action Plan[29], which contains the most relevant provisions of its legislation on the personal data protection.

In August 2015, the Data Processing Supervisor's Privacy Recognition System (PRP)[30] was approved. The aim of this system is to assist in Law enforcement those responsible for the processing of personal information.

The documents issued by the Privacy Subgroup, as well as by the Electronic Commerce Group, are available in a database[31].

[28] Available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx
[29] Available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/link.aspx?_id=CB717EE6184848D396F31DBB814E5C90&_z=z
[30] Available at: http://www.apec.org/~/media/Files/Groups/ECSG/2015/APEC%20PRP%20Rules%20and%20Guidelines.pdf
[31] Available at: http://publications.apec.org/index.php?m=a&cat_id=15

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

Asia Pacific Privacy Authorities
Available Tools and Resources

General Information

What is the organization: the principal forum for privacy and data protection authorities in the Asia Pacific region.

Primary activities of the organization are to promote:

- The formation of partnerships
- The exchange of ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints.

Tools and Resources

Overview: there are very few tools per se available on APPA's website. The type of international cooperation carried out by APPA members is limited to the exchange or information and best practices through international conferences.[32] The website does contain some resources consisting of a series of common administrative practices that have been agreed to by APPA members (i.e., best practices) and a framework to assist organizations carry out successful for secondments.

Common administrative practices on the following topics:

- Case Note Citation
- Case Note Dissemination
- Recommended Common Core Questions for Community Attitude Surveys

Staff exchanges:

- APPA Secondment Framework: advises on how to set up successful secondments.

[32] For example, prior to an international conference, DPAs are encouraged to complete a "jurisdiction/country report" in which they highlight the top three issues of interest since the last conference. The results are then grouped thematically and then discussed at the conference by the attendees. Another example are the data breach notification reports which are circulated amongst members for their interest and information.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

Central and Eastern European Data Protection Authorities (CEEDPA)
Available Tools and Resources

General Information

The network:

The network of Central and Eastern European Data Protection Authorities (CEEDPA) consists of 20 Data Protection Supervisory Authorities. These are:

Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Czech Republic, Croatia, Georgia, Hungary, Kosovo, Lithuania, Moldova, Montenegro, Poland, Latvia, Macedonia, Romania, Russian Federation, Slovakia, Serbia, Ukraine

The CEEDPA network was founded in Warsawa on 17th Dec 2001, where a "Final Declaration" on close cooperation was adopted.

Objective/Motivation of establishing the CEEDPA was to jointly meet concerns with regard to the notions that:

- Personal data protection problems in Central and Eastern Europe countries are our common problems in the new democracies;
- During performing our duties we meet particular problems which result very often from an incomprehension or trivializing of personal data protection problems by the controllers;
- Many problems result from a particular practice of data controller witch is unknown in the others European countries;
- Many new tasks arise from closer co-operation with the Council of Europe and with European Union in order to harmonise data protection legislation around Europe;

Three further resolutions have been adopted by CEEDPA members:

2005 Declaration on future cooperation

2008 Declaration on the equal treatment of all national languages of EU member states

2008 Declaration on future cooperation

Tools and Resources

Main forum of CEEDPA members is the annual meeting. In 2016 it took place in Sarajevo. The upcoming 20th meeting of CEEDPA authorities will be hosted by the new member of Georgia in its capital city of Tbilisi. (17th/18th May 2017).

This is in line with the latest (2008) Declaration on future cooperation, where members committed themselves to also

- elaborate common solutions

- organise ad hoc working meetings to discuss data protection issues with aspects specific to Central and Eastern European (CEE) countries.

- intensify cooperation and take joint actions with regard to the cases of data processing of special importance to CEE countries

- develop educational and awareness-raising activity of our data protection authorities carried out within the framework of information campaigns or in relation to Data Protection Day,

- to seek to participate in cross-border projects funded by the European Union, with the objective of and guaranteeing the rights of our citizens and increasing the level of data protection in our countries, among others by improving the qualifications of the employees of our Data Protection Authorities.

The most important tool and source of information seems to be the CEEDPA network website at www.ceecprivacy.org, which is hosted by GIODO, the DPA of Poland.

It includes separate sub-section under the headlines of "Legal instruments", "Annual Reports", "Forum", "News", "Internet & Privacy", "Contacts" and "Links".

However, the degree of information included in each sub-section varies and does not always include information with regard to CEEDPA member DPAs. The "Forum" is open to registered users (therefore it cannot be assessed how it is being used). The "News" sub-section mainly mentions brief reports on Annual Meetings. Under "Internet & Privacy" two guidance papers can be found (Polish Guidelines on the Protection of Privacy in the Internet, Hungarian recommendation on certain issues of handling data in connection with the Internet), but the link to the first document did not work and the second document is dated 1 Feb 2001. The "contacts" functionality allows to select whether all or specific CEEDPA members only shall receive a message.

Specific tools for exchanging information or cooperation, such as common forms, are not visible on the website.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

Council of Europe – Convention 108 – T-PD Committee
Available Tools and Resources

General Information

Council of Europe – Convention 108:
The "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)", which was opened for signature on 28 January 1981 (therefore this date has been chosen to be the annual "Data Protection Day" in Europe), was the first legally binding international instrument in the field of data protection. Under this Convention the parties are required to take the necessary steps in their domestic legislation to apply the data protection principles laid down in the Convention in order to ensure respect in their respective territories for the fundamental right of personal data protection. The process of modernizing Convention 108 should be finished soon.

An Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181) was opened for signature on 8 November 2001. It requires Parties to set up supervisory authorities and to enable these to exercise their functions in complete independence in order to have implemented an important element for effective protection oversight.

Currently, there are 50 Parties to the Convention (47 Council of Europe Member States, plus Uruguay, Mauritius, Senegal).

T-PD-Committee:
Established by Article 18 of Convention 108, the Consultative Committee (T-PD) consists of representatives of Parties to the Convention and by observers from other States (members or non-members) and international organizations.
The T-PD is responsible for interpreting the provisions and for improving the implementation of the Convention.

Tools and Resources

The T-PD fulfills its overall task by having drafted and adopting reports, opinions and guidelines on specific topics, such as data transfers to third states or biometrics.

The T-PD exists in two different formats:
- the Plenary, which meets once every year, usually in late June, convening all Parties and Observers to Convention 108,

- the Bureau, which meets – in addition to the Plenary – three times a year, convening the Chair (Italy), deputy Chair and a limited number (four) of CoE member states; all of them elected by the T-PD Plenary; however, bureau meetings are open to representatives of other CoE member states, if they wish to attend.

Usually, the Bureau holds discussions on specific topics, decides about mandates to external experts for drafting opinions or guidelines, reviews such draft documents and prepares decisions or recommendations to be adopted by the Plenary of T-PD.
The work of the Chair is being supported by a Secretariat provided by the Council of Europe and manned by its staff.

Main resource of information or tools provided to T-PD Parties is the website https://www.coe.int/en/web/data-protection
It includes a plethora of reports, agendas, guidelines, opinions and recommendations and other deliverables of the work done by the T-PD. The website is searchable by selecting a specific year. The latest example for guidelines adopted by the T-PD is the document "T-PD (2017) Big Data Guidelines", which can be found and downloaded at: https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.

A repository of data protection related legal Council of Europe documents can be found at https://www.coe.int/en/web/data-protection/legal-instruments. This includes:

- Council of Europe Treaties
- Resolutions of the Parliamentary Assembly
- Resolutions of the Ministers of Justice
- Declarations of the Committee of Ministers
- Recommendations of the Committee of Ministers

This is amended by a subsection "National Information" providing links to each Convention 108 Party and by another subsection on relevant case law of the European Court of Human Rights.

Most notably is a "Handbook on European data protection law", which has been published in 2014 jointly by the T-PD and the FRA (Fundamental Rights Agency of the European Union) and will be updated in 2018. It is available in 22 different languages and can be downloaded at: http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law
The handbook aims at making legal practitioners who are not experts in the field of data protection familiar with this area of law. It provides an overview of applicable legal frameworks of the Council of Europe as well as the European Union.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

Common Thread Network
Available Tools and Resources

Aim of review

To identify what tools or initiatives each network makes available to its members, that could foster or facilitate enforcement cooperation and that may: (i) be already available to privacy enforcement authorities; or (ii) serve as an example for future implementation by the privacy enforcement community.

Details

The **Common Thread Network** (CTN) is still a young network, established only in 2014. It aims to build a further a common approach to respecting citizens' privacy, to promote and build capacity in the sharing of knowledge and good practices for effective data protection.

The CTN has members from across the Commonwealth – currently from 14 jurisdictions and new members are in the process of being confirmed from a further three jurisdictions from Africa and Asia.

Therefore, it has started to share resources and know-how on a number of issues via its network. It does this through a variety of means:

- The new website is one among many features which the Common Thread Network intends to use to foster a common approach and create synergies among Commonwealth nations to uphold individuals' privacy and data protection rights.
- The CTN holds quarterly teleconferences among members to foster collaboration and exchange know-how and expertise.
- The Network allows members to participate in certain large conferences/events organised by the Commonwealth umbrella agencies such as the Commonwealth Telecommunications Organisation. This helps to spread the CTN's enforcement cooperation message to other types of regulator and the private sector who are network members to these agencies.
- The CTN also collaborates with other networks such as the Global Privacy Enforcement Network (GPEN) to exchange knowledge on relevant enforcement-related activities. This happens through nominating a dedicated member to liaise between the Common Thread Network and the GPEN, who can report back at regular intervals, usually at the quarterly teleconferences for CTN.

- The CTN gets involved in promoting its members enforcement and regulatory role at the level of Heads of State too which has a top-down effect on improving the political status of regulatory authorities' cooperation in networks. It did just this in 2015 when it encouraged Heads of State to resolve in their Governmental Meeting Communiqué statement to encourage the development of practical networks that facilitate the sharing of information and building of capacity in these areas. The Communique included this resolution which was seen as a very useful step by the regulatory community.
- The Common Thread Network issued a statement on the occasion of Data Privacy Day 2017 to raise awareness of the role of data protection authorities' enforcement role in the Network. The statement also spoke of the Network members' role more generally in upholding people's data protection and privacy rights which was targeted at both with individuals themselves and with organisations and businesses that handle personal information.

Further information:

More information at: https://commonthreadnetwork.org/

Analysis completed by the ICO, responsible for the Secretariat for the Common Thread Network

International.team@ico.org.uk

June 2017

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

The Global Alliance of National Human Rights Institutions[33] Available Tools and Resources

General Information

What is the organization: the international association of NHRIs, established in 1993 to promote and strengthen NHRIs in accordance with the Paris Principles on National Institutions[34] as well as provide leadership in the promotion and protection of human rights.

Primary activities of the organization:

- Undertakes accreditation of NHRIs in accordance with the Paris Principles.
- Promotes the role of NHRIs within the United Nations (UN) as well as with States and other international agencies.
- Facilitates and supports NHRI engagement with the UN Human Rights Council, Treaty Bodies and Special Rapporteurs.
- Encourages cooperation and information sharing among NHRIs, including through an annual meeting and biennial conference.
- Offers capacity building for NHRIs in collaboration with the Office of the High Commissioner for Human Rights (OHCR)
- Assists NHRIs under threat.
- Can assist government to establish NHRIs.

Tools and Resources[35]

Overview: most of the tools and resources can be broken down into two categories, (1) those aimed at promoting and enhancing NHRI cooperation and interaction with international organizations, mostly UN human rights bodies, and (2) promote cooperation amongst NHRIs through the sharing of information and best practices.

General tools consist of the ICC website (hosted by the OHCHR) and a directory/rolodex page (listing all members/regional networks, including contact persons and details for each member/network).

[33] Formerly known as the International Coordinating Committee of National Human Rights Institutions ("ICC")
[34] The Paris Principles are a set of international standards which frame and guide the work of NHRIs. They were drafted at an international NHRIs workshop in Paris in 1991 and subsequently adopted by the United Nations General Assembly in 1993.
[35] Note: the following is a sample of the types of tools available through this network, rather than the full list. The full list of tools is available upon request.

Procedural tools to assist in enhancing cooperation with international bodies, including the following:

- OHCHR: UNDP-OHCHR Toolkit for Collaboration with NHRIs
- Treaty Bodies: Handbook for NHRIs on Treaty Bodies; and Conclusions of the International Roundtable on the Role of NHRIs and Treaty Bodies.
- Special Procedures: Discussion Paper on NHRI interactions with Special Procedures.
- The Human Rights Council: Human Rights Council Universal Periodic Review Calendar.
- Regional bodies: Mapping Survey on Complaints Handling Systems of African NHRIs; and Guidelines on Implementation of decisions of Regional Human Rights Organs.

Accreditation tools consisting of the Paris Principles (the international benchmark according to which NHRIs are accredited, adopted by UNGA in 1993), general Observations on interpretative issues regarding the Paris Principles and the Handbook on accreditation of NHRI in EU.

Substantive/thematic tools relating to a number of human rights issues that NHRIS actively collaborate on addressing. These resources tend to be developed by regional bodies of the ICC (such as the Asia Pacific Forum) of the international bodies (i.e., OHCHR). Some of these resources include the International Human Rights System Manual (APF publication); Preventing Torture: an operational guide for NHRIs (APF, APT and OHCHR publication); Promoting and Protecting the Rights of Migrant Workers (APF publication); and New Detention Monitoring Tool (APF publication).

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

Global Privacy Enforcement Network
Available Tools and Resources

General Information

What is the organization: an informal network of privacy enforcement authorities that was created in 2010 and now consist of 64 members from 47 jurisdictions around the world. Its aim is to foster cross-border cooperation among privacy authorities and strengthen personal privacy protection in a global context.

Primary activities of the organization:

- Exchange information about relevant issues, trends and experiences.
- Encouraging training opportunities and sharing of enforcement knowhow, expertise and good practice.
- Promoting dialogue with organizations having a role in privacy enforcement.
- Creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral cooperation.
- Undertaking or supporting various specific activities as outlined in the GPEN Action Plan.

Tools and Resources

Overview: The vast majority of tools offered by GPEN are found on its website.

Much of the tools are centred on **information sharing**

- Documents library where members can share findings, guidance and other public non-confidential information of interest.
- Discussion forum where members can engage in online discussion with other members (e.g., requesting interest in or advice/position on specific issues – non-confidential)
- GPEN Alert which is a separate secure portal where participants can share confidential information regarding potential or ongoing investigations.
- News/Events Calendar where relevant items can be flagged by members.

There are also several **databases** that centre on information sharing:

- Privacy Authority Pages which provides information regarding the jurisdiction, legislation, etc. about member authorities.
- International Privacy Law Library which link to worldly and relevant findings for various jurisdictions

Contact tools are also found on the GPEN website:

- Enforcement Contacts List – a list of designated enforcement contacts for GPEN/APEC/OECD authorities.
- Ability to contact individual users or all members via email contact functionality (user profiles, available to member users, can also provide telephone or mailing contact info)
- Opportunities Board where member authorities post training, secondment and other career opportunities that may be available to GPEN member users

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

The International Association of Privacy Professionals (IAPP)
Available Tools and Resources

General Information

What is the organization: The International Association of Privacy Professionals (IAPP) is the world's largest global information privacy community. The IAPP is a resource for professionals who want to develop and advance their careers by helping their organizations successfully manage these risks and protect their data. In fact, we're the world's largest and most comprehensive global information privacy community.

The IAPP is responsible for developing and launching the only globally recognized credentialing programs in information privacy: the Certified Information Privacy Professional (CIPP)[36], the Certified Information Privacy Manager (CIPM)[37] and the Certified Information Privacy Technologist (CIPT)[38]. The CIPP, CIPM and CIPT are the leading privacy certifications for thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.

Due to the great number of professionals of the privacy, the Association has created two regional chapters in which thematic meetings are organized (IAPP Europe and IAPP Asia)[39].

The CIPP helps organizations around the world bolster compliance and risk mitigation practices, and arms practitioners with the insight needed to add more value to their businesses. The CIPM certificates the leaders in privacy program administration and that one person got the goods to establish, maintain and manage a privacy program across all stages of its lifecycle. The CIPT is focused in shows the knowledge to build the organization's privacy structures from the ground up.

[36] Available at: https://iapp.org/certify/cipp/
[37] Available at: https://iapp.org/certify/cipm/
[38] Available at: https://iapp.org/certify/cipt/
[39] Available at: https://iapp.org/conferences/

Tools and Resources

Overview: In addition to face-to-face activities, the Association offers online courses[40], privacy training classes[41], books to encourage learning and research on privacy[42] and online conferences[43].

Furthermore, the IAPP has a virtual database[44] where you can find various materials produced by the Association itself or by third parties specialized in the subject, such as tools for privacy impact assessment or DPO's Toolkits.

The website includes a glossary[45] and an area exclusively for data protection authorities[46].

[40] Available at: https://iapp.org/train/online-training/
[41] Available at: https://iapp.org/train/training-classes/
[42] Available at: https://iapp.org/train/books/
[43] Available at: https://iapp.org/conferences
[44] Available at: https://iapp.org/resources/
[45] Available at: https://iapp.org/resources/glossary/
[46] Available at: https://iapp.org/resources/dpa/

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

International Conference of Data Protection and Privacy Commissioners
Available Tools and Resources

General Information

What is the organization: a global forum for data protection authorities that was established in 1979.

Primary activities of the organization are to provide leadership at the international level in data protection by connecting the efforts of 115 data protection and privacy authorities around the world.

Tools and Resources

Overview: most of the cooperative tools available on the ICDPPC website are information-based although the body does organize a number of activities that go towards promoting enforcement cooperation.

The principle **framework for cooperation** is the Global Cross Border Enforcement Cooperation Arrangement (the "Arrangement"), which is an informal MOU, is the ICDPPC's main vehicle for promoting enforcement cooperation between its members.

The principle **reference guide** for cooperation is the Enforcement Cooperation Handbook, which is a living document that is meant to provide guidance to authorities wishing to engage in enforcement cooperation, whether pursuant to the Arrangement or otherwise.

Several **databases** are available on the ICDPPC website:

- The Contacts database: covers members, observers, alumni and privacy media contacts including office address, contact information for the authority head(s), and identifying a communications-related contact person although these are for use by the Secretariat.
- A public list of members, observers and Participants to the Arrangement, including links to their websites and social media accounts.
- International Privacy Law Library, which is the largest freely accessible and searchable collection of privacy law materials in the world.

Numerous **information tools** are found on the ICDPPC's website:

- A repository of adopted resolutions, declarations and communiques.

- A repository of working group reports.
- A repository of committee documents.
- A newsletter.
- News from members.
- A repository of information and contact details for regional, linguistic/cultural, specialized and miscellaneous networks.
- A repository of resources that are available through other networks.

ICDPPC members also undertake a number of **activities** to promote enforcement cooperation, including:

- Organizing annual conferences.
- Holding enforcement cooperation meetings.
- The website includes an events calendar.

Finally, the ICDPPC carries out **accreditation** of its members.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

International Consumer Protection Enforcement Network (ICPEN)
Available Tools and Resources

ICPEN is a network of consumer protection authorities from over 60 jurisdictions. ICPEN members share information about cross-border commercial activities affecting consumers and encourage international enforcement cooperation among consumer protection agencies. ICPEN generally meets twice a year, operates the website www.icpen.org, provides best practices training workshops, and delivers year-round work through several steering groups and working groups. ICPEN members from 36 countries participate in ICPEN's econsumer.gov, international consumer complaint database and website. The current **members** are:

Angola, Australia, Austria, Azerbaijan, Barbados, Belgium, Canada, Chile, China, Costa Rica, Cyprus, Czech Republic, Denmark, Dominican Republic, Egypt, El Salvador, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Korea, Kenya, Kosovo, Latvia, Lithuania, Luxembourg, Malta, Mexico, Mongolia, the Netherlands, New Zealand, Nigeria, Norway, Panama, Papua New Guinea, Poland, Portugal, Peru, Philippines, Seychelles, Slovakia, Spain, Suriname, Sweden, Switzerland, Turkey, United Kingdom, United States, Vietnam, Zambia.

Before becoming a member, an agency must participate for two years as a **partner organization**. The three current partners are: Sri Lanka, United Arab Emirates and the Kingdom of Saudi Arabia.

ICPEN has four **Observers**: European Commission, Iberoamerican Forum of Consumer Protection Agencies (FIAGCC), OECD, UNCTAD.

The Network operates under a rotating **presidency**, currently held by the German Federal Ministry of Justice and Consumer Protection until 30 June 2017.
President Elect – Turkey, Directorate General of Consumer Protection and Market Surveillance
President Elect (2018-2019) – Zambia, Competition and Consumer Protection Commission
Current Secretariat – Belgium

The **Advisory Group** is composed of the current, former, and future Presidents and nominated representatives from within the membership seeking geographical representation and rotating participation of different member organizations. The current members of the advisory group are from the following

countries: Australia, Belgium, Canada, Chile, Germany, Italy, New Zealand, Panama, Turkey, UK, US, Zambia.

Three **Steering Groups** (SGs) facilitate achievement in the three core objectives of 1) Intelligence (2) Best Practices and 3) Enforcement. SGs assist members in determining whether new proposals fit within ICPEN's objectives; provide direction on projects and activities; and assist the Presidency and Advisory Group in advancing the core strategies of ICPEN.

ICPEN Strategic Objectives (2017-2020)

1. To generate and share information and intelligence on consumer protection issues.
2. To share best practice in legislative and enforcement approaches to consumer protection.
3. To take action to combat cross-border breaches of consumer protection laws.
4. To identify and promote measures for effective consumer protection enforcement.
5. To promote and encourage wider participation, coordinated work, communication and cooperation with other consumer protection enforcement organisations.
6. To facilitate cross-border remedies.

ICPEN Core Strategies

To achieve its objectives ICPEN focuses on the following three core strategies:

1. To *co-ordinate and co-operate* on consumer protection enforcement matters.
2. To *share information and intelligence* on consumer protection trends and risks.
3. To *share best practice informatio*n about key consumer protection laws, enforcement powers and regulatory approaches to consumer protection.

Econsumer.gov

Econsumer.gov is a joint effort to gather and share cross-border e-commerce complaints of consumer protection agencies from 36countries. 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.

Econsumer.gov members: Australia; Belgium; Bulgaria, Canada; Chile; Costa Rica; Denmark; Dominican Republic; Egypt; Estonia; Finland; Greece; Hungary;

Ireland; Israel; Italy; Japan; Kenya; Latvia; Lithuania; Mexico; Netherlands; New Zealand; Nigeria; Norway: Philippines; Poland; South Korea; Spain; Suriname, Sweden; Switzerland; Turkey; United Kingdom; United States; Zambia

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

OECD Working Party on Security and Privacy in the Digital Economy (WPSPDE)

Available Tools and Resources

General Information

What is the organization: The Working Party on Security and Privacy in the Digital Economy (WPSPDE) of the Organization for Economic Cooperation and Development (OECD) develops public policy analysis and high level recommendations to help governments and other stakeholders ensure that digital security and privacy protection foster the development of the digital economy.

Moreover, the WPSPDE:

- Addresses information security and privacy as complementary issues that are essential for the sustainability of the Internet economy as a platform for economic and social prosperity.
- Is a platform where policy makers monitor trends, share experience, and analyse the impact of technology on information security and privacy policy making.
- Develops and monitors the implementation of several non-binding legal instruments (soft law) adopted by the OECD Council by consensus.
- Maintains an active network of experts from government, business, civil society and the Internet technical community.

The WPSPDE gathers policy experts from OECD member and partner governments as well as business, civil society and the Internet technical community to share experience on better approaches to security and privacy in an open and globally interconnected environment. The SPDE reports to the Committee on Digital Economy Policy (CDEP) which itself reports to the OECD Council.

Tools and Resources

Overview: in the official web site of the WPSPDE[47] are several informational resources, including Council Recommendations and reports about different privacy topics and events.

[47] Available at: http://oe.cd/spde

The resources are stored by year of elaboration and subject[48].

The WPSPDE has a repository of Information Security and Privacy Policy[49]:

1. Privacy[50].
2. Security[51].
3. Digital identity and online authentication[52].
4. Issues related to consumers[53].

[48] Available at: http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm
[49] Available at: http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm
[50] Available at: http://www.oecd.org/internet/ieconomy/privacy.htm
[51] Available at: http://www.oecd.org/sti/ieconomy/security.htm
[52] Available at: http://www.oecd.org/internet/ieconomy/digitalidentitymanagementandelectronicauthentication.htm
[53] Available at: http://www.oecd.org/sti/consumer/

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

PHAEDRA ("Improving Practical and Helpful Cooperation Between Data Protection Authorities")
Available Tools and Resources

General Information

The Project:

The PHAEDRA Project was launched in 2013 and continued in two separate phases until January 2017. It was carried out by a consortium consisting of Trilateral Research and Consulting, DPA Poland (GIODO) and University Jaume I of Castellon, Spain, and it was co-funded by the European Commission under its Fundamental Rights and Citizenship Programme.

Main persons involved were – inter alia – David Wright, Paul de Hert (both Trilateral Research), Urszula Goral, Piotr Drobek, Pawel Makowski, Beata Batorowicz (all of GIODO) and Artemi Rallo Lombarte (former Head of DPA Spain, University Jaume I).

The principal objective of the PHAEDRA project Phase 1 was to help improve practical co-operation and co-ordination between DPAs, privacy commissioners and privacy enforcement authorities, especially in regard to the enforcement of privacy laws. The consortium recognised that many DPAs face constraints, by way of human and/or budgetary shortages, institutional and legislative rules and other factors.

The PHAEDRA project Phase 2 was focused on practical aspects of European DPA co-operation: Practical challenges to co-operation between DPAs, which might result from both non-legal (technical, cultural, economic or other) and legal barriers to co-operation. Primarily, the project was to focus on the non-legal issues (technical, practical) which impact co-operation (trust building, best practices, practices for case handling, including information exchange). Phase 2 also aimed to identify the relevant legal challenges, and proposed solutions to overcome them: identifying the challenges to effective cooperation between European DPAs; analyzing the existing practices of co-operation; and identifying best practices and other solutions to co-operation.

Tools and Resources

According to the objective of the project a broad range of "deliverables" were presented, discussed with key stakeholders at various workshops and finally published. The deliverables are still available on the **PHAEDRA Project website** at http://www.phaedra-project.eu/deliverables-2/ and include:

PHAEDRA Phase 1 (2013-2015) deliverables:

- Deliverable 1:David Barnard-Wills & David Wright, Co-ordination and co-operation between Data Protection Authorities
- Deliverable 2.1: Paul de Hert, Gertjan Boulet, A Compass towards best elements for cooperation between data protection authorities
- Deliverable 2.2: Paul de Hert, Gertjan Boulet, Legal reflections for further improving cooperation between data protection authorities
- Deliverables 3.1 and 3.2: David Wright, David Barnard-Wills, Inga Kroener, Contact list of Data Protection Authorities (DPAs) and collaboration with GPEN and the ICDPPC working group (restricted to Projects´ members).
- Deliverable 3.4: Beata Batorowicz, PHAEDRA workshops and final conference
- Deliverable 4: David Wright, David Barnard-Wills, Inga Kroener, Findings and recommendations
- Deliverable 5: Artemi Rallo, Rosario-Garcia Mahamut, Dissemination activities

PHAEDRA Phase 2 (2015-2017) deliverables:

- Deliverable D1: Barnard-Wills, David and David Wright, Authorities' views on the impact of the data protection framework reform on their co-operation in the EU
- Deliverable D2.1: Galetta, Antonella, Dariusz Kloza and Paul De Hert, Cooperation among data privacy supervisory authorities by analogy: lessons from parallel European mechanisms
- Deliverable D2.2: Barnard-Wills, David and Vagelis Papakonstantinou, Best Practices for cooperation between EU DPAs
- Deliverable D3.1: Papakonstantinou, Vagelis, Cristina Pauner Chulvi, Andres Cuella and David Barnard-Wills, European and national legal challenges when applying the new General Data Protection Regulation provisions on co-operation
- Deliverable D4.1: Barnard-Wills, David, Vagelis Papakonstantinou, Cristina Pauner and José Díaz Lafuente, Recommendations for improving practical cooperation between European Data Protection Authorities
- Deliverable D4.2: Pauner, Cristina and Jorge Viguri, A report on a repository of European DPAs' leading decisions with cross-border implications
- Deliverable D4.3: Pauner, Cristina and Jorge Viguri, A report on the PHAEDRA II blog
- Deliverable D4.4: Saffell, Jacek and Paweł Makowski, A report on PHAEDRA II events

There seems to be a substantial area of overlay of issues discussed in the PHAEDRA Project with rather similar issues covered by the International Conference´s Expert Group or the former International Enforcement Cooperation Working Group (IEC WG).

However, a more detailed analysis of the PHAEDRA Project deliverables would overextend the scope of this brief review. It could be worth considering to get in touch with representatives of GIODO (DPA Poland) to learn more about the outcome of the Project or to have particularly useful deliverables identified or recommended.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

The Ibero-American Data Protection Network

Available Tools and Resources

General Information

The organization: The Ibero-American Data Protection Network (RIPD) was established in 2003 as a consequence of an agreement signed in the Ibero – American Data Protection Symposium which took place in La Antigua, Guatemala, from June 1st to June 6th 2003, attended by representatives from 14 Ibero-American countries.

Primary activities of the organization: The RIPD was established as a forum for the promotion of the right to data protection in the Ibero-American community. At an early stage, its activity was mainly aimed at promoting the legal and institutional development of the protection of personal data in the Ibero-American countries.

As most Ibero-American countries have now adopted specific laws and implemented data protection authorities, the work of the network, without abandoning this line, has entered a phase in which its main activity is directed to promote, maintain and strengthen a close and permanent exchange of information, experience and knowledge among the network members in the development of common instruments and involving coordinated/joint activities.

Tools and Resources

Overview: the RIPD's website contains several tools and resources to assist with and promote international cooperation. They can be classified into four categories, following the website's main menu: (1) legislation, (2) activities, (3) documents, and (4) useful links.

There is a section titled **"Legislation"**, which includes links to the most important legislation of every Ibero-American country (except for Cuba). The legislation displayed for each country includes: the Constitution (if the right to data protection is incorporated in the constitution of the corresponding country), general legislation and sectoral legislation.

In the **"Activities"** section, the RIPD's website contains information of the different activities carried out by the network for the fulfillment of its objectives. These activities are classified in three main groups: Symposiums, Seminars and Workshops.

Once in a year, a General Assembly is held where every network member attends. This meeting takes the name of Symposium. The RIPD's website includes all the information delivered in every symposium as from the RIPD's origin.

Seminars are meetings held by the RIPD to promote the exchange of experiences and, in this way, deepen the analysis and knowledge of those issues of greater relevance. The website contains information of seminars held as from 2007.

Workshops are meetings held by the RIPD addressed to those network members that do not have their own data protection legislation or those that have a poorly developed legislation on the matter. The website contains information related to workshops held in 2014 and 2016.

The **"Documents"** section includes: general documents, RIPD annual reports, RIPD action plan 2015-2017 and other documents of interest. Among the "general documents", the RIPD has published its statements ("*declaraciones"*). In most statements the network members commit to promote the strengthening of the RIPD by making existing cooperation mechanisms stronger, intensifying the dialogue among countries and increasing the cooperation between data protection authorities. (e.g. XI Symposium Statement – 2013).

Among "other documents of interest" there are some documents specifically related to international cooperation and enforcement. Particularly, there is one resolution titled "Resolution on International Enforcement Coordination", adopted in the 35th International Conference of Data Protection and Privacy Commissioners held in 2013 in Warsaw, which resolves to further encourage efforts to bring about more effective coordination of cross-border investigation and enforcement in appropriate cases, and among other things, it stresses out the importance to encourage privacy enforcement authorities to look for concrete opportunities to cooperate in particular investigations with cross-border aspects. Another noteworthy resolution is the "Resolution on International Enforcement Cooperation", adopted in the 38th International Conference of Data Protection and Privacy Commissioners held in 2016 in Marrakesh, which is also aimed to achieve more effective cooperation in cross-border investigation and enforcement in appropriate cases, and among other things, it resolves to mandate a new Working Group of experts to develop a proposal for key principles in legislation that facilitate greater enforcement cooperation between members.

The **"Useful Links"** section includes links to the websites of the data protection authorities of all RIPD member states. It also includes links to some European institutions and other organizations that could be related to the protection of personal data.

In June 2017, the RIPD made available a new "**Corpus Iurus**" online Platform. The tool that stores and allows the search of documents relevant to personal data protection (i.e. normative, jurisdictional, quasi-jurisdictional documents and any others considered relevant standards or benchmarks, at the national level as well the international, for the protection of personal data, privacy, private life, habeas data action and other related terms).

Data Protection Standards for the Ibero-American States ("*Estándares de Protección de Datos Personales para los Estados Iberoamericanos"*):

These standards, adopted by the RIPD in June 2017, are general guidelines for countries that still do not have a regulation on data protection or for countries that do have a regulation, but need to modernize or update its existing legislation. Its main aim is to favor the adoption of a unified regulatory framework to provide an adequate level of protection of personal data and, at the same time, guarantee commercial and economic development of the region.

The Data Protection Standards for the Ibero-American States highlight, as one of its main purposes, the importance to strengthen international cooperation among data protection authorities of Ibero-American states as well as with other non-regional data protection authorities and international organisms. The standards include a section which specifically lists some international cooperation mechanisms to be adopted by Ibero-American states, which in essence, are designed to strengthen the dialogue and favor the exchange of information and research assistance among them.

Association francophone des autorités de protection des données personnelles (AFAPDP)
Available Tools and Resources

General Information[54]

The AFAPDP was created in 2007 and brings together the personal data protection authorities of 19 states of the French-speaking world.

The main objectives of AFAPDP are:
• promote the right to the protection of personal data and privacy in the French-speaking world;
• build the capacity of AFAPDP members and facilitate cooperation between them;
• strengthen the influence of Francophone authorities' vision and expertise internationally.

The association organizes each year a Conference in the French language bringing together all of its members, in the margins of which is held its General Assembly. These meetings are forums for reflection, fostering an open and inclusive dialogue between authorities, public authorities and civil society.

Tools and Resources

Overview: A lot of information is available on the AFAPDP website.

AFAPDP facilitates the exchange of information between its members, including by keeping them up to date via its website:
• a directory of its members;
• a table summarizing the state of data protection in the French-speaking world;
• a directory of national laws relating to the protection of personal data within the French-speaking area as well as the relevant international texts.

The AFAPDP General Secretariat is also available to AFAPDP members to respond to their requests: technical questions, sharing of good practices

[54] Original text provided to the Group of Experts by AFAPDP in French. The French original follows this entry and readers should use the French version for reference of the original.

and networking with other members or experts, for example.
Training sessions are regularly organized for the agents of the authorities. These courses take place in face-to-face capacity or remotely (long-distance learning). AFAPDP strives to offer training that takes into account the cultural and legal diversity of its members. The training materials are available on a dedicated area of the AFAPDP website.

AFAPDP also proposes, to States that do not yet have a personal data protection law and are considering adopting such a law, to make available the expertise of its members to support this process.

Association francophone des autorités de protection des données personnelles (AFAPDP)
Available Tools and Resources

General Information[55]

L'AFAPDP a été créée en 2007 et rassemble les autorités de protection des données personnelles de 19 Etats de l'espace francophone.

Les grands objectifs de l'AFAPDP sont de :

- promouvoir le droit à la protection des données personnelles et à la vie privée dans l'espace francophone ;
- renforcer les capacités des membres de l'AFAPDP et faciliter la coopération entre eux ;
- renforcer le rayonnement de la vision et de l'expertise francophones à l'international.

L'association organise chaque année une Conférence francophone réunissant l'ensemble de ses membres, en marge de laquelle se tient son Assemblée générale. Ces réunions constituent des *fora* de réflexion favorisant un dialogue ouvert et inclusif entre autorités, pouvoirs publics et société civile.

Tools and Resources

Overview: De nombreuses informations sont disponibles sur le site internet de l'AFAPDP[56].

L'AFAPDP facilite l'échange d'informations entre ses membres, notamment en tenant à jour sur son site internet :

- un annuaire de ses membres;
- un tableau récapitulant l'état de la protection des données dans l'espace francophone;
- un répertoire des lois nationales relatives à la protection des données personnelles au sein de l'espace francophone ainsi que les textes internationaux pertinents.

Le secrétariat général de l'AFAPDP se tient par ailleurs à la disposition des membres de l'AFAPDP pour répondre à leurs demandes : questions techniques, partage de bonnes pratiques et mise en relation avec d'autres membres ou experts, par exemple.
Des formations sont régulièrement organisées à destination des agents des autorités. Ces formations ont lieu en présentiel ou à distance. L'AFAPDP s'efforce

[55] Original text provided to the Group of Experts by AFAPDP in French. The English translation precedes this entry but this entry is the version to reference for queries.
[56] www.afapdp.org

de proposer des formations prenant en compte les diversités culturelle et juridique de ses membres. Les supports de ces formations sont mis à disposition sur un espace dédié du site internet de l'AFAPDP.

L'AFAPDP propose en outre, aux Etats qui ne sont pas encore dotés d'une loi de protection des données personnelles et envisagent de se doter d'une telle loi, de mettre à disposition l'expertise de ses membres pour accompagner ce processus.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

The Unsolicited Communications Enforcement Network (UCENet)
Available Tools and Resources

Formally the London Action Plan (LAP) – www.ucenet.org

Membership

Executive Committee: Dutch Authority for Consumers and Markets, New Zealand Department of Internal Affairs, Australian Communications and Media Authority, Canadian Radio-Television and Telecommunications Commission, US Federal Trade Commission, Korean Internet and Security Agency, UK Information Commissioner's Office.

Other members include other privacy authorities (such as the Canadian Office of the Privacy Commissioner), other telecoms authorities (such as UK Ofcom), consumer protection authorities (such as the UK Competition and Markets Authority) and a number of authorities with other responsibilities (such as the Australian Children's Commissioner and the Malaysian Cyber Security authority). There are also a number of private sector members involved in anti-spam work, including consultants and technology companies.

Aim of the network

The aim of the network is to coordinate and promote international enforcement cooperation and activities targeting unlawful spam and related problems.

Background and structure

The network was created in 2004 when government and public agencies from 27 countries responsible for enforcing laws concerning spam met in London to discuss international spam enforcement cooperation.

The activities of the group are split into four working groups:

- Intelligence;
- Enforcement;
- Communications; and
- Training.

Working groups

1. Intelligence

UCENet aims to facilitate the exchange of information across jurisdictions. This information may consist of operational information to aid enforcement, and more general expertise.

An intelligence contact group is being established, with the first conference call taking place shortly.

This group is establishing a contact list for intelligence sharing between UCENet members. Similar work has been undertaken to identify contact points within GPEN previously. This contact list will lead to an updated membership list being made available on the UCENet website, which may be a useful resource for data protection authorities.

The group has also committed to identifying relevant data feeds. This is sources of potentially useful information, including those (such as complaint databases or honeypots) which are non-public. Whilst identified, these sources will not necessarily be accessible to other members. This work has not started yet.

UCENet is also planning its first Sweep in 2017, based on the ICPEN and GPEN Sweeps. This will focus on affiliate marketing. This work is open to members of other networks via the ICDPPC or GPEN.

2. Enforcement

UCENet seeks to encourage cooperation on cases and initiatives through(1) training relevant officials, (2) sharing and enhancing methodology and processes for information sharing, and (3) developing technology to improve the network's ability to detect, intercept, and deter illegal telemarketing or spam across borders.

UCENet has also established a Memorandum of Understanding on cooperation. The Memorandum seeks to encourage a framework to facilitate the exchange of information between the Members while recognising the legal, policy, and administrative limits on the authority and jurisdiction of each Member to disclose such information.

This Memorandum is similar in many ways to the International Arrangement pursued under ICDPPC.

Members include:

- ACM (the Netherlands)
- the ACMA (Australia)
- CRTC and OPC (Canada)

- ICO and NTSIT (United Kingdom)
- KISA (Korea)
- FTC and the FCC (United States of America)
- Department of Internal Affairs (New Zealand)
- National Consumer Commission (South Africa)

3. Communications

Work is ongoing to produce an accurate membership list, and this will be posted to the UCENet website. UCENet has a core of active members, however some are inactive, and so this project seeks to identify these. Work is also ongoing to expand the membership. This includes via promotion of the network, such as through engaging in the GPEN Network of Networks initiative.

4. **Training**

Work is ongoing to develop a consistent training programme based on member requirements. Surveys have been conducted to gauge interest in particular topics. Sessions will be recorded where possible and included in a restricted area on the UCENet website.

Within this area there is also a plan to identify an 'inventory of experts'. The objective of this project is to assist the member organisations in increasing their awareness of what expertise is currently available within the UCENet community, create opportunities for dialogue, knowledge and expertise sharing among experts on methodologies, approaches, technologies, applications and other aspects related to unsolicited communication compliance and enforcement. This project will also lead to increase awareness and common understanding on methodologies, approaches, technologies, and best practices to enhance regulatory, compliance and enforcement activities, as well as collaboration. The deliverable for this project will be a list of key experts within each of the member organizations.

Access to these tools for data protection authorities

- Some authorities with the relevant areas of responsibility may wish to join UCENet.
- UCENet participates in the GPEN Network of Networks initiative to make sure each network is briefed on the activities of the other.
- Additional members of the privacy community may want to participate in the UCENet Annual Events alongside those that already do (eg ICO, OPC, FTC).
- Data protection authorities may want to participate in the UCENet Sweep activity.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.2

The UN Office on Drugs and Crime (UNODC)
Available Tools and Resources

General Information

What is the organization: the UN body responsible for the global fight against illicit drugs and international crime, established in 1997 through a merger between the UN Drug Control Programme and the Centre for International Crime Prevention.

Primary activities of the organization: mandated to assist members in combatting illicit drugs international crime and terrorism. Its work focuses on:

- Field-based technical cooperation projects to enhance Member States' capacity.
- Research and analytical work to increase knowledge and understanding of drugs and crime issues and expand the evidence base for policy/operational decisions.
- Normative work to assist States in ratifying/implementing relevant international treaties, the development of relevant domestic legislation, and the provision of secretariat and substantive services to the treaty-based and governing bodies.

Tools and Resources[57]

Overview: the UNODC's website contains a plethora of tools to assist with and promote international cooperation. They can be broken down into the following categories: (1) model laws, (2) databases (various types and topics, including a directory of authorities and contact details), (3) numerous procedural manuals and handbooks meant to guide authorities in international cooperation (including best practices), and (4) a number of substantive manuals and handbooks.

The main **reference guide** is the UNODC Services and Tools – Practical solutions to global threats to justice, security and health (i.e., an overview of the tools and services available through the UNODC)

There are numerous **model laws** that are available, including a Model Law on International Cooperation as well as numerous others addressing substantive topics such as the following: Model Legislative Provisions against Organized Crime; Model Law against Trafficking in Persons; and Model Laws on Money-Laundering and Financing Terrorism (for common and civil law jurisdictions).

[57] Note: the following is a sample of the types of tools available through this network, rather than the full list. The full list of tools is available upon request.

There are five **databases** set up with differing purposes. The principle one, Sharing Electronic Resources and Laws on Crime (SHERLOC) is a knowledge management portal that facilitates the dissemination of information regarding the implementation of the Convention/Protocols and itself includes databases on legislation and case law, as well as a directory of competent national authorities. Two other noteworthy ones are the Government Office Case Management System, which support agencies in the conduct and management of investigations (inlc. collection/dissemination of intelligence), and the Legal Library, which is a repository of legislation adopted by state members to give effect to drug control conventions and the Organized Crime Convention.[58]

There are numerous **procedural manuals, handbooks and best practices**. Four of them focus on enhancing international cooperation: (1) the Digest of Organized Crime, which provides guidance on implementing the conventions through case studies as well as examples of best practices and international cooperation; (2) the Manual on Mutual Legal Assistance and Extradition, which is a guide to facilitate the drafting, transmission and execution of extradition and MLA requests pursuant to arts. 16 and 18 of the *Organized Crime Convention* where the Convention is used as the basis for a request;[59] (3) the Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime;[60] and (4) the Extradition and Mutual Legal Assistance Casework Guidelines. The remaining ones consist of best practices in such areas as the use of electronic surveillance in the investigation of serious organized crime, as well as criminal intelligence manuals.

Finally, there are a number of **thematic/substantive manuals**, handbooks and best practices, including the Handbook on Identity-related Crime; the Issue Paper on Combating Transnational Organized Crime Committed at Sea Issue Paper; and the Counter-Kidnapping Manual.

[58] The other two databases are the Cybercrime repository, a repository on legislation and lessons learned, and the Human Trafficking Case Law Database, a repository of information related to documented instances of the crime (incl. nationality, traffic routes, verdicts, et. al.).
[59] The Manual includes the following additional tools: general checklist for requesting mutual legal assistance; supplemental checklist for specific types of mutual legal assistance requests; sample cover note for an outgoing mutual legal assistance request, acknowledgment of receipt of an incoming request and sample authentication certificate; checklist for the contents of an outgoing extradition; checklist for outgoing extradition requests – casework planning; and a list of UN human rights instruments that apply to MLA and extradition matters.
[60] The Manual includes the following additional tools: Checklist – Considerations for preservation or seizure of assets; A model for a net worth calculation; Sample freezing order; Model product; Sample account monitoring order; and Sample guidelines on considering an asset manager or receiver application.

11. Task 2.3 - Summary Report on Additional Frameworks

Introduction

This section is the first of two parts of section 2.3 on Additional Frameworks. This is the summary and a section with more details on specific frameworks follows thereafter (page 98 onwards).

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[61]. 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:

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

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

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[62]. In the case of the UN-based

[62] 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.

international human rights law ("IHRL") regime, only one treaty explicitly 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.

12. Task 2.3: Report Background on Treaties and Frameworks

Convention on Cybercrime (the "CoC")

General

What: the treaty's main objective, set out in the Preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime. The CoC is overseen by the Council of Europe.[63] In 2001 the CoC was drawn up by the Counsel of Europe with the active participation of several "observer states" (non-member States). The treaty is open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States. Fifty five State Parties are now obliged to cooperate pursuant to the CoC.[64]

The CoC aims principally at:

- Harmonising the **domestic (substantive) criminal law elements of offences** and connected provisions in the area of cyber-crime;[65]
- Providing for **domestic procedural law powers**, necessary for the *investigation* and *prosecution* of such offences as well as other offences committed by means of a computer system or *evidence* in relation to which is in electronic form;[66]
- Setting up a fast and **effective regime of international cooperation**;

1) The Scope of Investigative Measures

In general: State Parties are obliged to take legislative and other measures as may be necessary to establish the powers and procedures, for the purpose of the criminal investigations or proceedings (as specified in Article 14 of the CoC).[67]

The CoC furthermore sets out a number of specific powers for the competent authority (Art 16 – 21 CoC), for instance to request for:

- the expedited *preservation* of *stored computer data*;
- the expedited *preservation* and partial *disclosure of traffic data*;

[63] The purpose of the present Convention is "to supplement applicable multilateral of bilateral treaties or arrangements as between the parties, including provisions of '*The European Convention on Extradiction* (..), '*The European Convention on Mutual Assistance in Criminal Matters*' (..), '*the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters'* (..), (Art. 39 CoC).
[64] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
[65] Furthermore, the CoC calls for adequate (domestic) legal sanctions (and other measures), and determines how 'corporate liability' should be established, in case of an offence. See: 'Chapter II: Measures to be taken at the national level. Section I. Substantive Criminal Law.'
[66] See: 'Chapter II: Measures to be taken at the national level. Section II. Procedural Law.'
[67] The powers and procedures apply to a.) criminal offences detailed in Section I (Substancive Criminal Law) as b.) committed by means of a computer system and c.) the collection of evidence in electronic form of a criminal offence (Art. 14 (2)).

- a *production order* (the order to submit specified information stored on a computer or to provide information relating such a service),
- *access* to *computer data* (search and seizure);
- *real-time collection* of traffic- and content data, and interception of content data;
- respect the confidential character of the investigation by a service provider, about the fact that the powers, mentioned above, are executed;[68]

The CoC also specifically permits **proactive disclosure of information** - obtained within the framework of its own investigations - **between State Parties**, when they believe that the information might assist in concluding inquiries and/or proceedings, or lead to a formal MLA request pursuant to the CoC (Art. 26).

To encourage and facilitate cooperation, the CoC sets out a **detailed framework for enforcement cooperation**, including that every State Party:

- Shall designate a *central authority* or *authorities* responsible mutual assistance (Art. 27 (2.a));
- Can request another State Party for *seizure or disclosure of preserved traffic data*, stored by means of a computer system, located in the territory of that other Party (Art 29 (1)) or to disclose preserved traffic data (Art. 30);
- Can request another State Party to *access stored computer data* (Art. 31);
- Provides mutual assistance to each other in case of *real time collection of traffic data and / or recording of content data*, in their territory, with respect to criminal offences (Art. 33 and 34);

In addition, the CoC contains specific provision for **transborder access** to **stored computer data** which does not require mutual assistance (with consent of another State Party or when the data is publicly available - open source (Art. 32)).

Furthermore, the CoC provides a framework in case of mutual assistance requests **in the absence of applicable international agreements** (Art. 27 (1)). When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation between State Parties, the CoC provides such an arrangement (see also: Art. 27 (2 – 9).

[68] In sub 2 of these provisions domestic legal boundaries and differences are acknowledged by adding that when a State Party cannot adopt the measures as referred to, it may instead adopt legislative and other measures as may be necessary to ensure the collection of the specified data, through the application of technical means on that territory.

2) Scope of Proceedings for Cooperation

The overarching context for cooperation pursuant to the CoC is **domestic criminal law** and procedures although it does also address, to a certain degree, some of the **underlying administrative matters** relating to extradition (Art. 24) and/or MLA more broadly.

3) How the Sharing of Personal Data is Addressed

The OCC does not specifically address personal data as such, although it is inherent that some of the cooperation amongst State Parties will involve the sharing and use of personal information given the nature of criminal proceedings (be it at the law enforcement, judicial or other levels).

Regarding confidentiality more generally, the CoC addresses two different positions.
1. Confidentiality in case of 'spontaneous information' (Art. 26 (2), which can be requested by the Providing State Party, and subject to his conditions);
2. Confidentiality in case of absence of applicable international agreements
Art. 27 (8) provides the arrangement that the requesting Party may request the confidentiality of the mere fact that the request was made, and Art. 28 sets out conditions for the supply of information by the requested party.

4) How Applicable Law is Addressed

The OCC is built on the premise that the cooperation between State Parties is done as follows (Art. 23 – general principles relating to international cooperation).

"The parties shall cooperate in accordance with the provisions of this Chapter and trough application of relevant international instruments on international cooperation on criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws, to the widest extend possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence."

Furthermore, each party must adopt legislative and other measures to establish jurisdiction (as set out in Art. 22 (1)).[69] When more than one party claims

[69] Art. 22: "Each party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of the Convention, when the offence is committed: a. on its territory; or b.) on board of a ship flying the flag of that Party; or c.) on board an aircraft registered under the laws of that Party; or d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside of the jurisdiction of any State; (…)"

jurisdiction over an alleged offence, established in accordance with the CoC, the State Parties involved, shall consult with a view to determine the most appropriate jurisdiction (Art. 22 (5)).

5) The Method of Implementation

The CoC requests each State Party to take the necessary legislative measure to ensure the implementation of its obligations under this Convention, as specified in several articles.

6) Other Relevant Aspects

The CoC requests a **24/7 network** (Art. 35 (1)) to ensure speedy assistance among the Signatory Parties (Art.35). Therefore each State Party shall designate a point of contact, with the aim of providing the following assistance:
a) provision of technical advice;
b) preservation of data;
c) collection of evidence, the provision of legal information, and locating of suspects

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

International Covenant on Civil and Political Rights – ICCPR

(incl. Optional Protocols on: establishing an individual complaints mechanism; and abolishing the death penalty)

General / Content of ICCPR

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the UN in 1966 (entering in force 1976). It commits its parties to respect the civil and political rights of individuals, including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial. As of May 2017, the Covenant has 169 parties and six more signatories without ratification.

The ICCPR is part of the system of the UN Human Rights legislation, in addition to the International Bill of Human Rights, the Universal Declaration of Human Rights, and the International Covenant on Economic, Social and Cultural Rights.

In the context of privacy and data protection, Article 17 is most important; it says:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
2. *Everyone has the right to the protection of the law against such interference or attacks.*

In addition, General Comment No. 16 to the ICCPR provides further specification on data protection requirements under Article 17. It states, among other things, that

- the collection and storage of personal information on computers, in data bases or other devices, whether by public or private bodies, must be regulated by law;
- states must take effective measures to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it;
- uses of this information for purposes incompatible with the Covenant must be prevented;
- individuals should have the right to determine what information is being held about them and for what purposes and to request rectification or elimination of incorrect information;
- any "interference" with these rights must only take place on the basis of law which must comply with the Covenant.

These requirements are supplemented by the storing body's duty of transparency with regard to data processing, in particular as regards the provision of information, rectification and elimination as essential data protection principles.

The ICCPR allows the adoption of additional protocols on specific subjects. Two such additional protocols currently exist: one on the establishment of an individual complaint mechanism (with, as of May 2017, 116 Parties) and another one on abolishing death penalty (with, as of May 2017, 84 Parties).

The 35th International Conference of Data Protection and Privacy Commissioners (Warsaw 2013) called upon governments to negotiate and adopt another Additional Protocol on the subject of data and privacy protection; the content of this Additional Protocol could be supported by the "International Standards on the Protection of Personal Data and Privacy" (Madrid Resolution 2009), which was adopted by the 31st International Conference of Data Protection and Privacy Commissioners.

1) The Scope of Investigative Measures / Reporting

The ICCPR is monitored by the UN Human Rights Committee (a separate body and not to be mixed up with the United Nations Human Rights Council or UN Human Rights High Commissioner), which consists of 18 experts nominated by UN Member States. It regularly reviews reports of States parties on how the rights are being implemented. States must report initially one year after acceding to the Covenant and then whenever the Committee requests (usually every four years). The Committee normally meets in Geneva and usually holds three sessions per year.

2) Scope of Proceedings for Cooperation / Means of Cooperation / Remedies

<u>Among Parties to the Convention:</u>
A kind of dispute resolution mechanism has been introduced by Art. 41 of the ICCPR. However, it is limited to those Parties which have declared before that they "recognize the competence of the Committee to receive and consider communications to the effect that a State Party claims that another State Party is not fulfilling its obligations under the present Covenant". The Committee may then investigate the matter; it can call upon the Parties concerned, to supply any relevant information. On this basis, the Committee shall offer its "good offices" to the Parties concerned with a view to a friendly solution of the matter. There is no bindingness, Parties concerned are completely free to agree or to dismiss suggestion for solution tabled by the Committee. In any case, the outcome of

the Committee proceedings will be a report. Committee procedures may be supported by or delegated to an ad-hoc-Commission (5 members).

Individuals:
The First Optional Protocol establishes an individual complaints mechanism, allowing individuals to complain to the Human Rights Committee about violations of the Covenant. Specific conditions apply, e.g. complainants must have exhausted all domestic remedies, and anonymous complaints are not permitted. Parties agree to recognise the competence of the UN Human Rights Committee to consider complaints from individuals. The Committee must bring complaints to the attention of the relevant party, which must respond within six months. After that the Committee must forward its conclusions to the party and the complainant.

3) How the Sharing of Personal Data is Addressed

This is not particularly addressed by the ICCPR.

4) How Applicable Law is Addressed

The ICCPR obliges its Parties to "respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant,…" and to "to take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant." Accordingly, applicable law needs to be created or adapted to the provisions of the ICCPR.
Application of the ICCPR may not contravene the Charter of the United Nations.

5) The Method of Implementation

The ICCPR as well as Optional Protocols need to be ratified by State Parties. The ICCPR is open to all member states of the United Nations, whereas the Optional Protocols are open to ICCPR Parties. The instrument of accession and ratification shall be deposited with the Secretary-General of the United Nations. An accessing Party may also express concerns or reservations to specific provisions of the ICCPR or the Optional Protocols.

Changes to the ICCPR or Optional Protocols may be suggested by each Party. A dedicated conference will deal with such suggestions, if at least one third of all Parties support a conference. Eventually, consent of the United Nations General Assembly and two third of Parties will be necessary for any changes entering

into force. However, changes will be limited to those Parties, which have agreed to them before.

6) Other Relevant Aspects / Conclusion

The ICCPR provides generally a legal basis for anchoring data protection and privacy in International law by its Article 17 and the related General Comment Nr. 16.
In principle, an Optional Protocol amending Article 17 could be a legal tool in order to establish a specific international binding agreement for data and privacy protection, which could also include more detailed provisions on cooperation and responsibilities of Supervisory Authorities.

However, there are many obstacles to be overcome. The process of negotiating and drafting such a Protocol would most likely be very lengthy and uncertain. It could also result in watering down a desirable outcome, possibly even resulting in a state of affairs which might be worse than before. This is due to procedures necessary, i.e. negotiating with a multitude of rather different United Nations countries and the need to obtain a two-third majority of ICCPR Parties and a majority of the UN General Assembly.

Even if this hurdle would have been tackled successfully, the rules of an Optional Protocol on data and privacy protection would apply to signatory Parties only. This means that there is a great likelihood that some important or populous countries will not sign it; e.g. the ICCPR has not been ratified by states like the People´s Republic of China and Cuba or has not been signed by states like Malaysia, Singapore, the United Arab Emirates or Saudi-Arabia. Thus, the global outreach of such an Optional Protocol would be questionable or at least uncertain.

Another consideration, which should be taken into account, is the fact that violations against provisions of the ICCPR or its Optional Protocols cannot be enforced. The dispute resolution mechanisms provided for ICCPR Parties or for Individuals do not foresee any really effective means to enforce a specific decision or findings of an investigation on a Party.

Therefore and overall, it might be more worthwhile to continue the efforts for strengthening enforcement cooperation between existing Data Protection and Privacy Supervisory Authorities by further developing practical tools available to all and establishing closer working relationships based on mutual trust and commonality in aims and values.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

2003 Agreement on mutual legal assistance between the European Union and the United States of America

Gert Vermeulen
Privacy Commissioner at Belgian DPA
Full Professor International and European Criminal Law, Director Institute for International Research on Criminal Policy (IRCP), Department Chair Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University
Extraordinary Professor of Evidence Law, Faculty of Law, Maastricht University

Scope of investigative measures provided for

It concerns an 'umbrella agreement', supplementing possible bilateral MLA treaties between the US and individual EU MS (in which the core provisions on investigative measures are typically included), so that only forms of cooperation (listed below) have been regulated which do not commonly feature already in such bilateral treaties:

- Identification of bank information (Article 4)
- cooperation in joint investigation teams (Article 5)
- videoconferencing for taking testimonies of witnesses and experts abroad, or even investigative statements (Article 6)

Scope/character of proceedings: criminal matters, with cross-over to MLA with administrative authorities

- default scope: mutual legal assistance in criminal matters
- however: cross-over to MLA between authorities competent in criminal matters and administrative authorities (to the extent that the latter are investigating conduct with a view to a criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities, pursuant to their specific administrative or regulatory authority to undertake such investigation) (Article 8)

Sharing of personal data

The Agreement contains very elaborate provisions on data protection, purpose limitation and use conditions (Article 9) and a straightforward and clear article on confidentiality requested by the requesting state (Article 10)

The key dimensions of Article 9 (Limitations on use to protect personal and other data) are the following:

- detailed listing of the accepted purposes of use by the requesting state of any evidence or information obtained from the requested state

- possibility to impose additional use conditions (with control possibility)

- exclusion to have recourse to such additional use conditions as generic restrictions with respect to the legal standards of the requesting State for processing personal data: in other words, the 'adequacy' requirement vis-à-vis 3rd states (like, from an EU perspective, the US) was hereby circumvented

Article 10 (Requesting State's request for confidentiality):

"The requested State shall use its best efforts to keep confidential a request and its contents if such confidentiality is requested by the requesting State. If the request cannot be executed without breaching the requested confidentiality, the central authority of the requested State shall so inform the requesting State, which shall then determine whether the request should nevertheless be executed".

Applicable law

Entry into force governed by domestic law, phrased in a very open fashion (without explicitly requiring ratification):

"exchange [of] instruments indicating that they have completed their internal procedures [for the purpose of entry into force]" (Article 18)

In addition, there are several instances, relating to the taking of specific investigative measures or possible limitations of cooperation, where reference is made to applicable law:

- **Identification of bank information** (Article 4)
  - […]
  - 4. (a) Subject to subparagraph (b), a State may, pursuant to Article 15, limit its obligation to provide assistance under this Article to:
    (i) offences punishable under the laws of both the requested and requesting States;
    (ii) offences punishable by a penalty involving deprivation of liberty or a detention order of a maximum period of at least four years in the requesting State and at least two years in the requested State; or
    (iii) designated serious offences punishable under the laws of both the requested and requesting States.
    (b) A State which limits its obligation pursuant to subparagraph (a)(ii) or (iii) shall, at a minimum, enable identification of accounts associated with terrorist activity and the laundering of proceeds generated from a comprehensive range of serious criminal activities, punishable under the laws of both the requesting and requested States.
  - […]

- 6. The requested State shall respond to a request for production of the records concerning the accounts or transactions identified pursuant to this Article, in accordance with the provisions of the applicable mutual legal assistance treaty in force between the States concerned, or in the absence thereof, in accordance with the requirements of its domestic law.
- […]

- **Joint investigation teams** (Article 5)
  - […]
  - 4. Where the joint investigative team needs investigative measures to be taken in one of the States setting up the team, a member of the team of that State may request its own competent authorities to take those measures without the other States having to submit a request for mutual legal assistance. The required legal standard for obtaining the measure in that State shall be the standard applicable to its domestic investigative activities.

- **Video conferencing** (Article 6)
  - 1. The Contracting Parties shall take such measures as may be necessary to enable the use of video transmission technology between each Member State and the United States of America for taking testimony in a proceeding for which mutual legal assistance is available of a witness or expert located in a requested State, to the extent such assistance is not currently available. To the extent not specifically set forth in this Article, the modalities governing such procedure shall be as provided under the applicable mutual legal assistance treaty in force between the States concerned, or the law of the requested State, as applicable.
  - 2. Unless otherwise agreed by the requesting and requested States, the requesting State shall bear the costs associated with establishing and servicing the video transmission. Other costs arising in the course of providing assistance (including costs associated with travel of participants in the requested State) shall be borne in accordance with the applicable provisions of the mutual legal assistance treaty in force between the States concerned, or where there is no such treaty, as agreed upon by the requesting and requested States.
  - […]
  - 4. Without prejudice to any jurisdiction under the law of the requesting State, making an intentionally false statement or other misconduct of the witness or expert during the course of the video conference shall be punishable in the requested State in the same manner as if it had been committed in the course of its domestic proceedings.
  - […]
  - 6. This Article is without prejudice to application of provisions of bilateral mutual legal assistance agreements between Member States and the United States of America that require or permit the use of video conferencing

technology for purposes other than those described in paragraph 1, including for purposes of identification of persons or objects, or taking of investigative statements. Where not already provided for under applicable treaty or law, a State may permit the use of video conferencing technology in such instances. […]

- **Limitations on use to protect personal and other data** (Article 9)
  - […]
  - 4. A requested State may apply the use limitation provision of the applicable bilateral mutual legal assistance treaty in lieu of this Article, where doing so will result in less restriction on the use of information and evidence than provided for in this Article.
  - 5. Where a bilateral mutual legal assistance treaty in force between a Member State and the United States of America on the date of signature of this Agreement, permits limitation of the obligation to provide assistance with respect to certain tax offences, the Member State concerned may indicate, in its exchange of written instruments with the United States of America described in Article 3(2), that, with respect to such offences, it will continue to apply the use limitation provision of that treaty.

- **Non-derogation** (Article 13)
  - Subject to Article 4(5) and Article 9(2)(b), this Agreement is without prejudice to the invocation by the requested State of grounds for refusal of assistance available pursuant to a bilateral mutual legal assistance treaty, or, in the absence of a treaty, its applicable legal principles, including where execution of the request would prejudice its sovereignty, security, ordre public or other essential interests.

Method of implementation

Characterised by built-in flexibility (examples below):

- direct resolution between competent authorities of of legal, technical or logistical issues that may arise in the execution of videoconference hearings (Article 6.3),
- allowance of expedited, informal communications (Article 7)
- consultations in view of dispute resolution (Article 11)
- designation and notification of competent authorities by exchange of written instruments (Article 15)
- common review, addressing in particular practical implementation issues (Article 17), etc.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

Council of Europe Convention108

Gert Vermeulen
Privacy Commissioner at Belgian DPA
Full Professor International and European Criminal Law, Director Institute for International Research on Criminal Policy (IRCP), Department Chair Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University
Extraordinary Professor of Evidence Law, Faculty of Law, Maastricht University

Scope of investigative measures provided for

Convention 108 only provides a fairly basic and under-elaborate framework for mutual assistance between data protection authorities.

According to Article 13, parties agree to render each other mutual assistance in order to implement the convention (paragraph 1), in that a data protection authority shall, at the request of another state's data protection authority (paragraph 3):

a. furnish information on its law and administrative practice in the field of data protection;

b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

In essence, no investigative measures are specified at all. The notion "appropriate measures" flagrantly lacks precision, and refers back to domestic law. Unless states have enacted elaborate cooperation provisions in their domestic laws, cooperation therefore necessarily remains very limited.

Scope/character of proceedings: administrative

The scope is administrative cooperation between data protection authorities. The explanatory report (para 71) is explicit on the matter: "The main provisions of this chapter are based on the two recent European conventions relating to mutual assistance in *administrative* matters […]". The CoE keeps administrative cooperation conventions systemically separate from cooperation conventions in criminal matters, both on the level of mother conventions or thematic conventions. The reasons therefore are obvious, and have to do with purpose limitation as a core data protection issue.

Sharing of personal data not allowed | purpose limitation | confidentiality

Article 13, under 3.b of Convention 108 is explicit in prohibiting the exchange between data protection authorities of personal data in data files: "An authority designated by a Party shall at the request of an authority designated by another Party take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed." The explanatory report (para 76) adds: "With regard to factual information, paragraph 3.b specifies that States may not reveal to each other the contents of data contained in data files. This provision is an obvious data protection safeguard for the protection of the privacy of the people concerned".

Further, in Article 15, Convention 108 specifies clear rules concerning purpose limitation/specialty (paragraph 1) and confidentiality (paragraph 2):

1. *An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.*
2. *Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.*

Applicable law

As already stated above, assistance is limited to measures in conformity with the domestic law of the requested data protection authority (Article 13.3.b). Moreover, as indicated below, assistance requested may be refused where incompatible with the powers (under domestic law) of the requested data protection authority in the field of data protection.

Other substantive and relevant aspects

Specific grounds for refusal foreseen (Article 16):

- incompatibility of the requested assistance with the powers in the field of data protection of the authorities responsible for replying;
- incompatibility with the sovereignty, security or public policy (ordre public) of the requested party
- incompatibility with the rights and fundamental freedoms of persons under the jurisdiction of the requested party

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

International Human Rights Law Regime

General

What: the international human rights law ("IHRL") regime, consisting of United Nations (UN) based treaties (see **Annex I** for a list of treaties and the acronyms used throughout). The regime is promoted and its implementation is overseen by the Office of the High Commissioner for Human Rights ("OHCHR").[70] While touching on the IHRL generally, the focus of this research piece is on the *Convention against Torture* ("CAT") and its Optional Protocol ("OPCAT").[71] Whereas CAT establishes the international legal regime surrounding the prohibition of torture and associated acts, OPCAT supplements the regime by creating a coordinated international-domestic monitoring and inspection system for places where individuals are deprived of their liberty.[72]

1) The Scope of Investigative and other Cooperative Measures

The scope investigative measures under the IHRL regime is very narrow and essentially confined to CAT and OPCAT, as well as ICPPED. For the purposes of this research piece, fact finding missions in the form of site visits are considered a type of investigation, whether conducted by the Subcommittee or a NPM. CAT and OPCAT also provide for other forms of cooperation.

CAT requires State Parties to "afford one another the greatest measure of assistance in connection with criminal proceedings brought in respect of [torture …], including the supply of all evidence at their disposal necessary for the proceedings" (Sub. 9(1)).[73] CAT further maintains that "States Parties shall carry out their obligations under paragraph I of this article in conformity with any treaties on mutual judicial assistance that may exist between them" (Sub. 9(2)).

[70] The individual treaties are overseen by the respective committee (i.e. treaty body) that they create.
[71] CAT has 161 State Parties while OPCAT has 75 signatories and 83 State Parties.
[72] CAT established the Committee against Torture, which is mandated with, *inter alia*, receiving and investigating complaints by individuals. OPCAT establishes the Subcommittee on Prevention which is mandated with conducting fact finding missions in the form of unrestricted site visits, provide advice and recommendations to State Parties and national preventive mechanisms (NPMs), and cooperate with other organizations to strengthen international protections against torture. OPCAT also requires State Parties to designate at least one NPM, which are to be independent agencies with unrestricted access to information, individuals and sites where individuals are deprived of their liberty, and which cooperate with the Subcommittee.
[73] ICPPED has a similar requirement obliging State Parties to: "cooperate with each other and afford one another the greatest measure of mutual assistance with a view to assisting victims of enforced disappearance, and in searching for, locating and releasing disappeared persons and, in the event of death, in exhuming and identifying them and returning their remains" (Art. 15).

CRPD includes a provision specifically addressing international cooperation through which "State Parties recognize the importance of international cooperation and its promotion" to achieve the purposes of the Convention and are, as such, required to cooperate with each other as well as international or regional organizations and civil society. The suggested measures are: ensuring that developmental programs are accessible to persons with disabilities; facilitating capacity building through the exchange of information, experiences, training, and best practices; facilitate cooperation in research as well as access to scientific and technical information; and provide technical and economic assistance, including sharing accessible and assistive technologies, and technology transfers.

The broader IHRL regime provides for other forms of cooperation:[74]

- Information exchanges "in the field of preventive health care and of medical, psychological and functional treatment of disabled children" (CRC, Sub. 23(4)).[75]
- Measures "[…] relating to education, in particular with a view to contributing to the elimination of ignorance and illiteracy throughout the world and facilitating access to scientific and technical knowledge and modern teaching methods" (CRC, Sub. 28(3)).
- Measures to improve the living conditions for persons with disabilities is recognized as being important (CRPD, Preamble).
- Measures to progressively and fully achieve the economic, social and cultural rights of persons with disabilities (CRPD, Sub. 4(2))

Several treaty regimes require State Parties to cooperate with the committee they establish.[76] In this regard, OPCAT is unique in that if a State Party fails to cooperate with the Subcommittee in relation to site visits and/or its access powers, or take steps to improve a situation in light of recommendations from the Subcommittee, the Subcommittee can request that the Committee against Torture make a public statement on the matter (Sub. 16(4)). These same treaties further require that the treaty bodies cooperate with other UN bodies and other international organizations. OPCAT further mandates the Subcommittee to cooperate with other international, regional or national organizations.[77]

[74] With the exception of the ICRMW, only those treaties adopted after 1984 touch on or deal with international cooperation.
[75] This includes the "dissemination of and access to information concerning methods of rehabilitation, education and vocational services, with the aim of enabling States Parties to improve their capabilities and skills and to widen their experience in these areas."
[76] Namely, the *Refugee Convention* at Art. 35, CRPD at Art. 37, ICPPED at Sub. 26(9)), and OPCAT at Sub. 2(4).
[77] Namely CRPD at Art. 38, the ICPPED at Art. 28, and OPCAT at Sub. 11(1)(c).

2) Scope of Proceedings for Cooperation

The overarching context for cooperation pursuant to the IHRL regime is international treaty law and the domestic law of State Parties.[78]

In the case of CAT, the context for cooperation is primarily international criminal law and customary international law as well as domestic criminal law and procedures. The context for cooperation under the ICPPED is also international criminal law as well as domestic criminal law and procedures.

Cooperation under CAT and OPCAT occurs on several levels: State Party-to-State Party (in the case of cooperation for criminal or judicial proceedings under CAT); State Party-to-international organization (in the case of State Parties having to cooperate with the Committee and Subcommittee); State-to-international organization (in the case of NPMs collaborating with the Subcommittee); and within the State Party (in the case of State entities cooperating with NPMs).

3) How the Sharing of Personal Data is Addressed

With the exception of OPCAT, the IHRL regime is silent on the treatment of personal data in the context of international cooperation. Sub-article 21(2) maintains that "Confidential information collected by the [NPM] shall be privileged. No personal data shall be published without the express consent of the person concerned.

4) How Applicable Law is Addressed

The IHRL regime does not address this per se although it is built on the interplay between the domestic and international law.

Some treaties specifically indicate that they will not affect domestic legal provisions or other pieces of international law that are more conducive in achieving the purposes of the treaty.[79] OPCAT indicates that its provisions do not affect the obligations of State Parties pursuant to regional conventions establishing systems to visit places of detention (Art. 31)

OPCAT (Art. 32) and ICPPED (Art. 43) indicate that their provisions are without prejudice to international humanitarian law, i.e., the Geneva Conventions of 1949 and their 1977 Additional Protocols.

[78] This is the case whether the treaty obligations automatically become domestic law upon ratification as is the case with monist systems or must be included into domestic law through legislative action as is the case with dualists systems.
[79] See CEDAW at Art. 23, ICPPED at Art. 37.

5) The Method of Implementation

The IHRL regime does not address this per se. In ratifying a treaty, a State Party undertakes to take all necessary legislative measures to give effect to that treaty should it not automatically take legal effect upon ratification.[80]

6) Other Relevant Aspects

All of the IHRL treaties follow the same basic structure: they set out substantive rights and the undertakings of State Parties, the creation and mandate of the treaty body committee, and general governance matters such as the coming into force, amendments, and denunciations.

[80] Thus, a dualist State would require legislative action to give legal effect to the treaty in domestic law while a monist State would not. Some States would also bound by the *Vienna Convention on the Law of Treaties* in terms of implementing their treaty obligations under the IHRL regime.

ANNEX I
The Treaties Composing the IHRL Regime

The following are the treaties under the UN-based international human rights law regime that were examined for the purpose of this research piece:

- 1948 *Universal Declaration of Human Rights* ("UDHR") – not a treaty but has since been recognized as reflecting customary international law and thus binding on all States.

- 1948 *Convention on the Prevention and Punishment of the Crime of Genocide* ("CPCG")

- 1951 *Convention Relating to the Status of Refugees* ("CSR")

- 1965 *Convention on the Elimination of All Forms of Racial Discrimination* ("CERD")

- 1966 *International Covenant on Civil and Political Rights* ("ICCPR") – + 2 Optional Protocols

- 1966 *International Covenant on Economic, Social and Cultural Rights* ("ICESCR") – + 1 Optional Protocol

- 1979 *Convention on the Elimination of All Forms of Discrimination against Women* ("CEDAW") – + 1 Optional Protocol

- 1984 *Convention against Torture* ("CAT") – + 1 Optional Protocol

- 1989 *Convention on the Rights of the Child* ("CRC") – + 3 Optional Protocols

- 1990 *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families* ("ICRMW")

- 2006 *International Convention for the Protection of All Persons from Enforced Disappearance* ("ICPPED")

- 2007 *Convention on the Rights of Persons with Disabilities* ("CRPD") – + 1 Optional Protocol

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

International Organization of Securities Commissions

The International Organization of Securities Commissions (IOSCO) is the international body that brings together the world´s securities regulators. IOSCO develops, implements, and promotes adherence to internationally recognized standards for securities regulation. IOSCO was established in 1983. Its membership regulates more than 95% of the world's securities markets in more than 115 jurisdictions and includes all the major emerging markets. Most members participate in the IOSCO Multilateral Memorandum of Understanding, which has allowed members to request and share information about investigations and cases in thousands of matters.

IOSCO members have resolved:

- to cooperate in developing, implementing and promoting adherence to internationally recognized and consistent standards of regulation, oversight and enforcement in order to protect investors, maintain fair, efficient and transparent markets, and seek to address systemic risks;

- to enhance investor protection and promote investor confidence in the integrity of securities markets, through strengthened information exchange and cooperation in enforcement against misconduct and in supervision of markets and market intermediaries; and

- to exchange information at both global and regional levels on their respective experiences in order to assist the development of markets, strengthen market infrastructure and implement appropriate regulation.

IOSCO Membership

There are three categories of members: ordinary, associate and affiliate. In general, the ordinary members (125) are the national securities commissions in their respective jurisdictions. Associate members (25) are usually agencies or branches of government, other than the principal national securities regulator in their respective jurisdictions, that have some regulatory competence over securities markets or intergovernmental international organizations and other international standard-setting bodies, such as the IMF and the World Bank, with a mission related either to the development or the regulation of securities markets. Affiliate members (65) are self-regulatory organizations, stock exchanges, financial market infrastructures, investor protection funds and compensation funds, and other bodies with an appropriate interest in securities regulation.

The IOSCO Board

The IOSCO Board is the governing and standard-setting body of IOSCO, and is made up of 34 securities regulators. The IOSCO Board reviews the regulatory issues facing international securities markets and coordinates practical responses to those concerns. The policy work of IOSCO is conducted by eight policy committees.

IOSCO Multilateral Memorandum of Understanding:[81]

IOSCO members engage in information sharing and enforcement cooperation pursuant to the *Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information* (MMoU). It sets out specific requirements for the exchange of information, ensuring that no domestic banking secrecy, blocking laws or regulations prevent the provision of enforcement information among securities regulators. The MMoU includes provisions on:

- what information can be exchanged and how it is to be exchanged;
- the legal capacity to compel information;
- the types of information that can be compelled;
- the legal capacity for sharing information; and
- the permissible use of information.

Since its launch in 2002, the MMoU has provided a mechanism through which securities regulators share with each other essential investigative material, such as beneficial ownership information, and securities and derivatives transaction records, including bank and brokerage records.

As of March 2017, there were 112 signatories to the IOSCO MMoU. Sixteen others were listed on Appendix B, the list of members who have formally expressed their commitment to seek the legislative and administrative changes necessary for achieving MMoU compliance, and one member had not yet agreed to be listed on that Appendix

A large increase in the number of signatories over the last decade has led to a sharp upsurge in cross-border cooperation, enabling regulators to investigate a growing number of insider traders, fraudsters and other criminal offenders. The number of information requests made under the MMoU rose to 3,203 in 2015, from 3,080 the year before.

[81] https://www.iosco.org/about/?subsection=mmou

Enhanced MMOU[82]

Since the 2002 MMoU was established, there has been a significant increase in globalisation and the interconnectedness of financial markets, as well as advancements in technology that have changed the way that the securities and derivatives industry operates and how violations of securities and derivatives laws occur.

IOSCO has now established an Enhanced Multilateral Memorandum of Understanding ("EMMoU"). The additional key powers in the EMMoU include:

- To obtain and share audit work papers, communications and other information relating to the audit or review of financial statements,
- To compel physical attendance for testimony (by being able to apply a sanction in the event of non-compliance),
- To freeze assets if possible, or, if not, advise and provide information on how to freeze assets, at the request of another signatory.,
- To obtain and share existing Internet service provider (ISP) records (not including the content of communications) including with the assistance of a prosecutor, court or other authority, and to obtain the content of such communications from authorized entities.,
- To obtain and share existing telephone records (not including the content of communications) including with the assistance of a court, prosecutor or other authority, and to obtain the content of such communications from authorized entities.

[82] https://www.iosco.org/about/?subsection=emmou

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

Ibero-American Data Protection Network

Subgroup 2.3 further agreed that experts would review the above, considering the following substantive aspects (as appropriate, recognizing that not all frameworks relate specifically to enforcement cooperation):

First, we must consider that the Personal Data Protection Standards for Ibero-American States **will be adopted by Network's members on June 2017**. Therefore, it is possible that some of this content would change during the course of this month.

1. **The scope of investigative measures provided for**

The Ibero-American Standards do not include, in their content, investigative measures.

However, as this document highlights, the national legislation of the Ibero-American States (which is applicable on this matter) must grant to the supervisory authorities' **sufficient powers of: investigation, supervision, resolution, promotion, sanction**, as well as any other necessary powers to guarantee its enforcement and effectiveness.

2. **The scope of proceedings pursuant to which authorities may cooperate (e.g., administrative or civil vs. criminal)**.

The Ibero-American Standards do not regulate the specific proceedings pursuant to authorities´ cooperation.

However, the document states that the Ibero-American States may adopt international cooperation mechanisms which facilitate the application/implementation/enforcement of their national legislation, which may include, but are not limited to:

a. The establishment of mechanisms that strengthen international cooperation and assistance in the application/implementation of the respective national legislations on this subject.
b. Assistance among States through notifications and submission of complaints, assistance in investigations, and exchange of information.
c. The adoption of mechanisms which focus on the knowledge and the exchange of best practices and experiences regarding the protection of

personal data, as well as matters of jurisdictional conflicts involving third countries.

3. **How questions surrounding the sharing of personal data are addressed**.

The Ibero-American Standards state the following:

"**35. General rules for personal data transfers**

35.1.A data controller will be able to make international transfers of personal data under any of the following circumstances:

- **a.** When the recipient country of the personal data is recognized as a country with an adequate level of personal data protection by the transferring country. This in accordance with its national legislation applicable on this subject.
- **b.** When the transfer's data controller offers sufficient guarantees of the processing of personal data in the recipient country. Hence, proves the compliance of the minimum conditions established by the national legislation of each Ibero-American State which is applicable to this subject.
- **c.** When the transfer's data controller and the recipient country sign some contractual clauses or any other legal instrument(s), which demonstrate the scope of the processing of personal data, the responsibilities assumed by the parties and rights of data owners.
- **d.** When the transfer's data controller and the recipient country´s adopt a binding self-regulation scheme, in accordance with the provisions referred to the national legislation of the Ibero-American State applicable on this subject.
- **e.** The control authority of an Ibero-American State data controller of the transfer authorizes such a transfer, in compliance with the terms established by the applicable national legislation on this subject.
- **f.** When the territory of the data controller establishes the minimum conditions to guarantee and adequate level of personal data protection.

35.2. The national legislation of Ibero-American States that is applicable on this subject may expressly **establish limits on international transfers** regarding of personal data categories on matters of public interest.

36. Recognition of proactive measures

36.1. The Ibero-American States´ national legislation on this subject must recognize and establish measures that promote a better enforcement of their legislation and cooperate to strengthen and raise the personal data protection

controls implemented by data controller, which may be found those referred to in this Chapter.

4. How the issue of applicable law is addressed

The Ibero-American Standards highlight that this document will be applicable to processing of personal data executed by:

- **a.** Data controllers established in the territory of the Ibero-American States.
- **b.** Data controllers that are not established in the territory of the Ibero-American States, when the processing of personal data activities will be related with supply of goods and services to Ibero-American States residents, as well, that they could be related to the control of their behavior.
- **c.** Data controllers that are not established in the territory of the Ibero-American States, bound to the national legislation of one the States (resulting from the conclusion of a contract or international law).
- **d.** Data controllers that are not established in the territory of the Ibero-American States, which use (or not) automated means settled in the territory of this State, in order to process personal data. Unless it will be only used for transit purposes.

Regarding the meaning of the Standards, the term *establishment* should be understood as the place of the central or principal administration of the data controller.

The Ibero-American Standards establish that Ibero-American national laws on this matter, could tie this prerogative in order to safeguard national security, public security, public health,as well as the protection of the rights and freedoms of third parties and issues of public interest.

Restrictions should be settled through legislative measures (established by law), in order to provide certainty to data owners about the nature and scope of these measures.

Any legislative measure, which limits the personal data protection, should contain at least:

- **a.** The purpose of treatment.
- **b.** The categories of personal data.
- **c.** The scope of the limitations established.
- **d.** Suitable safeguards in order to prevent illicit or disproportionate access or transfer.
- **e.** The determination of a data controller.

f. The deadlines for the retention of personal data.
g. The data owner's risks to their rights and freedoms.
h. The data owner's right to be informed regarding the restrictions.

The Standards highlight that legislative measures **must be necessary and proportional to a democratic society. Therefore, they must respect the rights and fundamental freedoms of data owners**.

Likewise, it establishes that the national legislation of the Ibero-American States **must establish the consequences on the security breaches** notifications, that made by data controller to the control authority, as well as the procedures and interventions in order to safeguard the owner's prerogatives and freedoms.

5. The method of implementation

The Ibero-American Standards do not provide an implementation method. Currently, it is planned that Standards will be **non-binding recommendations** for States parties.

Through the Standards, it is intended to establish parameters and good practices for all participants. The aim is that they will be to be adopted at national level, or maybe suit national documents, if there is already a legislation on the matter.

This is regardless of whether in the future, the authorities belonging to the members of the RIPD (according to its initials in Spanish) agree on the establishment of an method of implementation for this document.

Moreover, it is important to mention that the preamble of the Ibero-American Standards states:

"The parties have agreed to adopt the Standards as a top priority in the Ibero-American Community. This, in order to contribute to the issuance of regulatory initiatives for the personal data protection in the region (on those countries that do not yet have these regulations), or to serve as a reference for the updating of legislation, favoring the adoption of a harmonized regulatory framework that provides an adequate level of protection of people."

6. Any other substantive aspects deemed relevant to our Task

4.3. The Standards will not be applicable under the following circumstances :

a. When personal data be intended for family life's activities. For instance, the use of personal data in an environment of friendship, kinship or

close personal group and are not intended for commercial disclosure or use.

b. Information resulting from an anonymization process.

[…]

7.1. The Ibero-American States may, in their domestic legal framework, exempt the compliance of principles, duties and rights, in order to adjust personal data protection with any other fundamental rights and freedoms.

7.2. This exemption must require a weighting exercise in order to establish **necessity, suitability and proportionality** of any restriction, in accordance to the rules and criteria recognized by the Ibero-American States.

[…]

21. Security duty

21.1. Regardless of the type of treatment that data controller makes, the controller must **establish and maintain**, physical and technical measures in order to guarantee the confidentiality, integrity and availability of personal data.

21.2. In order to determine these measures, the data controller should consider the following factors:

a. The risk that personal data (and the value that can be obtained from it) may be treated by a third party that is not authorized for possession.

b. The technique's status.

c. Application costs.

d. The nature of the personal data processed, especially regarding sensitive personal data.

e. The scope and purpose of treatment.

f. Previous personal data transfers.

g. The number of data owners.

h. The potential consequences of infringement on the owners.

i. Previous breaches regarding the processing of personal data.

[…]

38. Privacy Officer

38.1. In the following cases, the data controller must designate a privacy officer or the equivalent:

a. When it is a public authority.

b. When personal data processing is carried out for systematic observation of the owner.

c. When it is processing personal data and it is probably that this involves a high level of risks which could potentially affect the right to the personal data protection of the owners. […]

42. System of penalties

42.1. The national legislation of the Ibero-American States must establish a regime that allows sanctioning the conduct that contravene the provisions in the corresponding national laws. This regime must indicate the boundaries and parameters which allows to ensure the sanctions, resulting by nature and seriousness of the breaches, as well as the measures implemented by data controller in order to guarantee the fulfillment of its obligations in the matter.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

The Unsolicited Communications Enforcement Network ("UCENet")

General

What: formed in 2004 and originally known as the London Action Plan UCENet is a network which promotes international spam enforcement cooperation and addresses spam related problems, such as online fraud and deception, phishing, and the dissemination of viruses. Both public bodies and private sector bodies can be members of UCENet. There are currently 47 regulatory and enforcement authority members from 29 countries participating in the network: predominantly data protection, telecommunications and consumer protection agencies. In addition, there are 27 private sector industry participants and 6 additional entities with observer status.

UCENet's current work is guided by the 2016-2018 Operational Plan of the London Action Plan (The "Operational Plan"). International enforcement cooperation is further supported by the LAP Memorandum of Understanding ("MOU")[83] which has been signed by 11 regulatory and enforcement authority members.

1) The Scope of Investigative and other Cooperative Measures

Before it became UCENet in September 2016, LAP adopted an Action Plan which does not directly address investigative measures per se. Rather, the LAP Action Plan seeks to promote other forms of enforcement cooperation, in particular information sharing. The Action Plan embodies the intention of participating public agencies "to develop better international spam enforcement cooperation" through the following methods:

- Designating a point of contact within each agency to further enforcement communications.
- Taking part in periodic conference calls and meetings to share information on such matters as cases, legislative and law enforcement developments, investigative techniques and enforcement strategies, obstacles to effective enforcement and how to overcome them, educational projects, and joint training.
- Encouraging dialogue between public sector agencies and the private sector to support compliance initiatives.

[83] Memorandum of Understanding among Public Authorities of the London Action Plan pertaining to Unlawful Telecommunications and Spam.

- Encourage and support the involvement of less developed countries in spam enforcement cooperation, including through technical assistance and capacity building.

The Action Plan has since been supplemented by the MOU and the Operational Plan, which establish a number of priorities that will result in the following additional cooperation tools once completed:

- Enhance intelligence collection, analysis and dissemination to assist in compliance and enforcement activities by creating (1) a key contact lists, (2) a registry of data feeds used by Members, and (3) an Intelligence Working Group.
- Maximize enforcement potential through (1) coordinated enforcement actions and (2) establish an MOU on information sharing and cooperation.
- Enhance capacity by training by way of (1) providing consistent training programmes, (2) recording training sessions, and (3) establishing an inventory of experts.

Some of UCENet's activities are also meant to promote and enhance enforcement cooperation, including (1) facilitating the coordination of compliance sweeps involving multiple authorities, (2) sharing information to identify risks and opportunities for enforcement action and/or prevention, (3) sharing effective intelligence and investigation techniques, (4) posting enforcement and compliance outcomes and initiatives, and (5) cooperating with other organizations or networks involved with related regulatory activities.

2) Scope of Proceedings for Cooperation

The overarching context for cooperation amongst Participants is domestic law and procedures relating to unsolicited communications. The MOU specifies that it does not require participating members to provide assistance or information to another member where the laws of the latter are penal in nature, although it does not preclude cooperation when matters are penal in nature. Cooperation is therefore not limited to regulatory or administrative law.

3) How the Sharing of Personal Data is Addressed

Neither the Action Plan nor the MOU specifically address the sharing of personal data per se. Rather, the Action Plan simply states "[…] that nothing in this Action Plan requires Participants to provide confidential or commercially sensitive information."

The MOU, although not specifically focused on personal information, addresses the sharing of information, including the confidential sort, much more extensively. To that effect, it confirms that members providing information will

only do so in a manner consistent with domestic laws, while recipients will maintain confidentiality unless required by their domestic law, in which case the recipient will notify the provider. Information can be provided subject to certain conditions and cannot be used for reasons beyond those for which the information was provided unless the recipient is otherwise required to fulfill a legislative request or judicial order.[84]

4) How Applicable Law is Addressed

The Action Plan is clear that any cooperation pursuant to the Plan is subject to domestic laws and the international obligations of participating members. The Action Plan is specific that "It is not intended to create any new legally binding obligations by or amongst Participants, and/or require continuing participation."

The MOU is equally clear that it is not binding in nature: rather it is a voluntary statement of intent and accordingly does not create any legally enforceable rights or impose legally binding obligations. Furthermore, the MOU does not modify or supersede any law in force applying to any participating member and does not create any expectations of cooperation, which would go beyond a member's legal authority.

5) The Method of Implementation

Neither the Action Plan nor the MOU specify the method of implementation. As an informal network, the documents are given effect once an authority signs on to become a participating member. In the case of the MOU, it became effective in December 2015 when the first two LAP member agencies signed it.

6) Other Relevant Aspects

Nil

[84] While the MOU maintains that despite confidentiality and limited use requirements, a recipient can use information obtained in connection with an investigation or criminal enforcement action to investigation, prosecution, or the prevention of violations of its domestic criminal law.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

United Nations Commission on International Trade Law ("UNCITRAL")

General

What: the core legal body of the United Nations ("UN") system in the field of international trade law which is mandated to further the progressive harmonization and unification of the law of international trade. This is achieved through, *inter alia*, the formulation of modern and harmonized rules on commercial transactions. UNCITRAL oversees the implementation of numerous conventions related to international trade, including commercial arbitration. It is a permanent commission of the UN General Assembly and is composed of 60 members elected from the Member States of the UN.

1) The Scope of Investigative or other Cooperative Measures

UNCITRAL is not involved in investigations nor do any of its treaties, model laws or rules deal with this. The organization and the trade system it oversees do, however, promote other cooperative measures, which largely consist of:

- Coordinating the work of organizations active in this field and encouraging cooperation among them.
- Coordinating and encouraging the cooperation of State Parties through:
  - Legal means:
    - The development of formal international treaty law.[85]
    - The development of model laws.[86]
  - Contractual means:
    - The development of rules (i.e., contractual texts).
  - Explanatory means:
    - Publishing legal/legislative interpretive guides and recommendations.
    - Publishing case law and enactments on uniform commercial law.
- Providing technical assistance.
- Promoting regional and national seminars on uniform commercial law.

[85] Binding treaties have been adopted for: international commercial arbitration and conciliation; international sale in addition to transport of goods; security interests; international payments; and electronic commerce.
[86] Model laws have been developed in all of the areas listed at footnote 1 in addition to insolvency as well as procurement and infrastructure development.

Enforcement cooperation with regards to international trade law is achieved through binding uniform rules on dispute resolution through arbitration and conciliation.

2) Scope of Proceedings for Cooperation

The overarching context for cooperation occurs on two levels:

1. Binding: international treaty law (public and private) and domestic law.

2. Non-binding: use of model laws and rules as well as legal and legislative guides to promote harmonious and uniform interpretations of international trade law.

3) How the Sharing of Personal Data is Addressed

None of the binding international treaties in this UN system address personal data and/or its transfer between State Parties or private sector organizations. Nor do its model laws or rules, including the Model Law on Electronic Commerce.[87] However, UNCITRAL's work, largely in promoting but not limited to electronic commerce, does address such matters as privacy, data protection and the handling of personal data:

- Working Group IV (Electronic Commerce): works on issues including identity management and trust services (see A/CN.9/WG.IV/WP.143).
- Publishing explanatory texts:
  - Recognizing and Preventing Commercial Fraud: Indicators of Commercial Fraud.
  - Promoting Confidence in Electronic Commerce: legal issues on international use of electronic authentication and signature methods.
- Holding seminars:
  - Colloquium on E-Commerce.[88]
  - Colloquium on Legal Issues Related to Identity Management and Trust Services.[89]

4) How Applicable Law is Addressed

[87] The Model Law and the *Convention on the Use of Electronic Communications in International Contracts* do, however, require reliable and appropriate methods to identify singers as conditions for the use of electronic signatures (Arts. 7 and 9 respectively). The Model Law also sets out rules for the issuance and use of the identity credentials required for the creation of certain electronic signatures (Arts. 8-12).
[88] 14-16 February 2011 (New York).
[89] 21-22 April 2016 (Vienna).

The UN international trade system is based on cooperation through the harmonization of the binding and non-binding rules that governs it. It is built on the premise that State Parties cooperate in the development of these rules, which in turn governs that international trade-related matters will be conducted in accordance to these rules, whether they be at the international level (i.e., treaties) or domestic (i.e., through the incorporation of these treaties and model laws into domestic law). The basis for cooperation is thus the interplay between the domestic and international legal spheres that are harmonized through the work of UNCITRAL.

5) The Method of Implementation

The international trade law system does not address this per se. In ratifying a treaty, a State Party undertakes to take all necessary legislative measures to give effect to that treaty should it not automatically take legal effect upon ratification.[90]

6) Other Relevant Aspects

Not applicable.

[90] Thus, a dualist State would require legislative action to give legal effect to the treaty in domestic law while a monist State would not. Some States would also bound by the Vienna Convention on the Law of Treaties in terms of implementing their treaty obligations under the UNCITRAL regime.

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

UN Convention against Transnational Organized Crime (the "UNTOC")

General

What: the international treaty focused on addressing transnational organized crime. It is overseen by the UN Office on Drugs and Crime ("UNODC"), who also oversees the implementation of the additional protocols to the UNTOC. The focus of this research piece is on the UNTOC along with the UNODC's Manual on Mutual Legal Assistance and Extradition the "Manual").[91] Over 160 State Parties are now obliged to cooperate pursuant to the UNTOC.

1) The Scope of Investigative Measures

In the context of formal mutual legal assistance (MLA), sub. 18(3) of the UNTOC sets out that State Parties can request the following broad range of cooperative investigative measures:

- Taking evidence or statements from persons.
- Effecting service of judicial documents.
- Executing searches and seizures, and freezing.
- Examining objects and sites.
- Providing information, evidentiary items and expert evaluations.
- Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records.
- Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes.
- Facilitating the voluntary appearance of persons in the requesting State Party
- Any other type of assistance that is not contrary to the domestic law of the requested State Party. [92]

The UNTOC also specifically permits proactive disclosure of information between State Parties when they believe that the information could assist in concluding inquiries and/or proceedings, or lead to a formal MLA request pursuant to the UNTOC (Sub. 18(4)).

[91] The Manual was created by the UNODC to serve as a guide to facilitate the drafting, transmission and execution of extradition and MLA requests pursuant to arts. 16 and 18 of the UNTOC in situations where the Convention is used as the basis for a request for assistance by a State Party.

[92] Where permitted under domestic law, State Parties are required to make available special investigative techniques such as controlled deliveries and electronic or other forms of surveillance (Art. 20). They are encouraged to enter into bilateral or multilateral arrangements to allow the use of such techniques or otherwise make use of them on a case-by-case basis.

To encourage and facilitate cooperation, the UNTOC maintains sets out a detailed framework for enforcement cooperation, including that State Parties:

- Are encouraged to enter into bilateral or multilateral agreements or arrangements to allow for joint investigations or otherwise carry them out on a case-by-case basis (Art. 19).
- Must take measures to enhance cooperation between law enforcement authorities through the sharing of information for investigative and evidentiary purposes, as well as providing factual, concrete help (Sub. 26(1)).
- Must "cooperate closely with one another" by establishing and enhancing lines of communication, in conducting inquiries, provide items or substances for analytical or investigative purposes, promote the exchange of personnel, to exchange information on specific means and methods used by organized criminal groups, and other measures to advance the UNTOC (Sub. 27(1)).
- Can transfer criminal proceedings to one another "for the prosecution of offences covered by" the UNTOC (Art. 21).
- Must assist one another in the planning and implementation of research and training programs to facilitate MLA and extraditions (Art. 29).
- Must make concrete efforts to enhance cooperation with as well as provide financial, material and technical assistance to developing countries for capacity building (Sub. 30(2)).

Finally, the Manual provides a number of examples of informal cooperative options prior to or short of making a formal MLA request: police-to police communications using liaison officers and, police-to-agency communications such as with INTERPOL, and consular communications (see paras. 151-156).

2) Scope of Proceedings for Cooperation

The overarching context for cooperation pursuant to the UNTOC is domestic criminal law and procedures although it does also address, to a certain degree, some of the underlying administrative matters relating to extradition and/or MLA more broadly. The UNTOC provides for cooperation on two levels. On the one hand, it harmonizes domestic legislation and overcomes potential problems surrounding dual criminality by requiring State Parties to implement certain specific Convention crimes (i.e., Arts. 5-8, and 23) into their domestic legislation. On the other hand, the UNTOC also encourages State Parties to cooperate in areas beyond the core Convention crimes.

3) How the Sharing of Personal Data is Addressed

The UNTOC does not specifically address personal data as such, although it is inherent that some of the cooperation amongst State Parties will involve the sharing and use of personal information given the nature of criminal proceedings (be it at the law enforcement, judicial or other levels).

Regarding confidentiality more generally, the MLA provisions maintain that a receiver State cannot transmit or use any information from the sending State for any purpose other than those set out in the request without prior consent of the sending State (Sub. 18(19)).[93]

4) How Applicable Law is Addressed

The UNTOC is built on the premise that the cooperation amongst State Parties is done in accordance with domestic law. Thus, a State Party requesting assistance does so within the confines of what is permissible under its domestic law and, conversely, the requested State Party provides assistance within the confines of what is permissible under its domestic law.[94] In this regard, the protection of sovereignty and the principle of non-interference in the domestic affairs of another State is built into the UNTOC (see Art. 4). The MLA portion of the UNTOC maintains that "a request shall be executed in accordance with the domestic law of the requested State party […]" (sub 18(17)).[95]

Finally, there are some cooperation provisions which assert that the UNTOC can be considered "the necessary and sufficient treaty basis" where a State Party requires that cooperation be carried out pursuant to a formal treaty (e.g. Subs. 13(6), 16(4), and 27(2)). Similarly, the provisions on MLA maintain that any such requests will be considered as being made pursuant to the UNTOC should a State Party not have an MLA treaty in place that it can otherwise rely on (see Sub. 18(7)).

---

[93] The provision on informal information sharing in the context of MLA requires the authority receiving the information to "comply with a request that said information remain confidential […] or with restrictions on its use" (sub. 18(5)). Sub. 18(20) maintains that the requesting State Party can request that the receiving authority "keep confidential the fact and substance of the request, except to the extent necessary to execute the request. In the context of combatting money laundering, the UNTOC maintains that information is to be shared "within the conditions prescribed by domestic law" (e.g. para. 7(1)(b)).

[94] Give the primacy of domestic law, the Manual encourages State Parties to approach MLA with flexibility and an understanding of the laws and legal traditions of the requested State Party. In this regard, State Parties are encouraged to consult foreign counterparts to confirm the requirements/nuances under the latter's domestic law.

[95] The Manual similarly confirms that "When a requested State takes action on a mutual legal assistance request, it does so acting under its own laws" (para. 196). Sub. 18(17) expands on this by maintaining that assistance "shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable […]."

5) The Method of Implementation

Sub-article 34(1) maintains that "each State Party shall take the necessary measures, […] in accordance with fundamental principles of its domestic law, to ensure the implementation of its obligations under this Convention." As explained in the Manual, this provision is worded as such in order to accommodate the differing legal traditions between State Parties, i.e. dualist vs. monist legal systems (see p. 9-10).

6) Other Relevant Aspects

The Manual suggests that INTERPOL "can be utilized in urgent circumstances as a communications conduit for [MLA] should the need arise."

Group of Experts on Legal and Practical Solutions for Cooperation
Task 2.3

U.S.-Canada Cooperation Agreement

In 1995 the U.S. and Canada signed a formal, binding "Agreement Between the Government of the United States of America and the Government of Canada Regarding the Application of Their Competition and Deceptive Marketing Practices Laws."[96]) The Agreement covers both competition and consumer protection matters, however, this note focuses mainly on the Article 7, the chapter on deceptive marketing laws and other provisions that are relevant to consumer protection cooperation.

The Agreement sets establishes a framework for cooperation and coordination with respect to enforcement of deceptive marketing practices laws.. The Agreement defines the relevant deceptive practices laws as specified sections of the Competition Act and the Federal Trade Commission Act. Art. 7(1). It requires the Director of Investigations and Research (the previous name of what is now the fair trading practices branch of the Competition Bureau) and the Federal Trade Commission to agree to

(a) use their best efforts to cooperate in the detection of deceptive marketing practices;
(b) inform each other as soon as practicable of investigations and proceedings involving deceptive marketing practices occurring or originating in the territory of the other party, or that affect consumers or markets in the territory of the other Party;
(c) share information relating to the enforcement of their deceptive marketing practices laws; and
(d) in appropriate cases, coordinate their enforcement against deceptive marketing practices with a transborder dimension.

Art. 7(3).

The provisions on confidentiality apply both to competition and consumer protection enforcement cooperation. In Article 10, the parties agree that neither is required to communicate information to the other Party if such communication is prohibited by the laws of the Party possessing the information or would be incompatible with that Party's important interests. The parties, to the fullest extent possible, are to maintain the confidentiality of any information communicated to it in confidence by the other Party under this Agreement. Each Party shall oppose, to the fullest extent possible consistent with that Party's laws, any application by a third party for disclosure of such confidential information.

[96] https://www.ftc.gov/policy/cooperation-agreements/us-canada-cooperation-agreement

Further, information communicated in confidence between the agencies is not to be communicated to third parties or to other agencies of the receiving agency's government, without the consent of the agency that provided the information. The receiving agency of a Party may, however, communicate such information to the Party's law enforcement officials for the purpose of enforcement of deceptive marketing practices laws. Finally, information communicated in confidence between the agencies in the context of deceptive marketing enforcement shall not be used for purposes other than enforcement of deceptive marketing practices laws, without the consent of the agency that provided the information.

Subsequent to the 1995 Agreement, the FTC and the Competition Bureau entered into an MOU on telemarketing fraud, designed to facilitate closer cooperation. That MOU, recognizing limitations on information sharing because of privacy and confidentiality laws in both countries, directs the participants to develop more effective methods of information sharing. In addition to the 1996 MOU, there are separate MOUS for regional U.S. – Canada partnerships on cross-border deceptive marketing practices.[97]

[97] Available here: https://www.ftc.gov/policy/international/international-cooperation-agreements

ANNEX

Other texts from the work of the Group of Experts

13. First round of comments from Conference members

Brief note accompanying changes to a) the Draft Resolution on exploring future options for International Enforcement Cooperation (2017) and b) the Document Package presented to the 39th Conference of the ICDPPC from the Group of Experts on Legal and Practical Solutions for Cooperation

07/09/2017 – first round of comments from Conference members

The Sponsors of the Draft Resolution on exploring future options for International Enforcement Cooperation (2017) received comments from **three** authority members of the Conference within the deadline for the first round of consideration of resolutions.

1) The Sponsors welcomed the confirmation of co-sponsorship of the INAI Mexico. The INAI did not wish to make any changes to the texts.
2) The Sponsors accepted the proposal from the Berlin Data Protection and Freedom of Information Commissioner to make a minor amendment to the first page of the recitals which the Sponsors agree helps clarify the status of individuals' rights.
3) The Sponsors also received some amendments to the Resolution from the Swiss Federal Data Protection and Information Commissioner. The Swiss Federal Member recommended including the text of the Global Cross-border Enforcement Cooperation Arrangement, as amended into a new Annex of the Resolution. The Sponsors accepted this.

   The Sponsors rejected an amendment from the Swiss Federal Member asking for the Principle 2 to be withdrawn from the set of the Key Principles set out in the Document Package of the work of the Group of Experts (now published on the closed session website) but proposed an alternative solution in the footnote to the Principles to provide clarification. The Swiss Federal Member considered that in certain situations the data protection authorities can be required to collaborate with other entities. The Sponsors explained in defence of their position that other members of the Group of Experts were relying on the inclusion of principle 2.

   The Sponsors clarified their ideas for dissemination and implementation of the Principles to governments/ legislators at national/ regional/ local level: the Principles do not need to be treated as a single set. Rather, individual members can choose to split the Principles up for use of merely a single Principle with their national government if they believe that this is the most appropriate approach for their national legal framework. There is no obligation placed upon the members of the conference as a result of this

Resolution to use all of the Principles, so if Principle 2 (or any of the other Principles) is not needed in one jurisdiction then it can be left out of the set presented to legislators. The Swiss Federal Member accepted the Sponsors' proposed compromise text for the footnote 9 of page 21 of the Explanatory Memorandum which is shown in track changes.

The Swiss Federal Member also asked for clarification of the Annex One of the Explanatory Memorandum to the Principles as some of the powers in the list do not in the Swiss Federal Member's view naturally seem to fall into the scope of the powers of the privacy enforcement authority (PEA). The Co-chairs proposed a clarification to be added to footnote 18 on p29 to take account of the Swiss proposal, which was agreed with the Swiss Federal Member.

The Swiss Federal Member also queried why the AFAPDP network has not been included in the final report of the Group of Experts work in workstream 2, task 2 (2.2). The Sponsors reassured the Swiss Federal Member that it was by no means their intention to overlook the network and they are working with the Swiss Federal Member on a report about AFAPDP similar to the other reports, to include in the final ICDPPC 2017 conference documentation.

14. Second round of comments from conference members

Brief note accompanying changes to a) the Draft Resolution on exploring future options for International Enforcement Cooperation (2017) and b) the Document Package presented to the 39th Conference of the ICDPPC from the Group of Experts on Legal and Practical Solutions for Cooperation

12/09/2017 – second round of comments from Conference members

The Sponsors of the Draft Resolution on exploring future options for International Enforcement Cooperation (2017) received comments from **one** authority member (from the European Data Protection Supervisor (EDPS)) of the Conference within the deadline for the second round of consideration of resolutions. These included some queries for clarification and amendments to the Resolution and the Document Package of the Group of Experts.

1) The Sponsors accepted the recommendation to include examples of other legislative frameworks for cooperation which exist, in addition to OECD which is already mentioned. But due to the different nature of the frameworks, and the keeping with previous resolutions on the broad theme of international enforcement cooperation, the Sponsors did not find it appropriate to amend the main body of the Resolution but instead to provide a footnote quoting merely a couple of examples from Council of Europe/EU, not excluding that there are more examples but it is inappropriate to list many such examples in such a text. One footnote quoting OECD was also deleted to avoid misinterpretation and two references to OECD Recommendation on cross-border co-operation in the enforcement of laws protecting privacy, 2007 were also corrected.

2) The EDPS also queried why a new working group was needed for the next stage of work, should this be mandated. The Co-chairs explained that the current Group of Experts' mandate is not extendable according to the Terms of Reference that it established. Moreover, one of the Co-chairs has indicated that it would not continue, and other members of the Group may wish to discontinue, while others may join. This would no longer be the same Group. In conclusion to that discussion, all agreed that there was no change needed to the text.

3) In the Group of Experts document package final report, the Co-chairs (Resolution Sponsors) agreed to clarify the term 'PEA' where it had not been explained.

4) Again in the final report, page 26, EDPS withdrew one amendment recommending reference to rights of individuals and prior information on

page 26. This followed discussions between EDPS and the Co-chairs who explained that there were already several other references to the positive impact that enforcement cooperation can have on individuals' rights, and the need for respect for existing legal requirements (which could include rights), e.g. including in paragraph 3 on the same page 26, under principle 5. Therefore, the agreement was to refrain from further amending the text.

5) Again in the final report (page 27) In the principle 5 section of the Explanatory Memorandum, one word 'appropriate' was added to clarify the text and promote legal certainty, following the EDPS query, that: '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).' However, the Co-chairs noted that they had taken a great effort to try and emphasise the need to create exemptions fitting to national needs/circumstances rather than one-size-fits-all approach throughout the text.

6) Finally in the Bibliography to the Document Package final report the reference to the OECD Recommendation on cross-border co-operation in the enforcement of laws protecting privacy, 2007 was corrected.

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.

16. 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).
