

# **International Conference for Data Protection and Privacy Commissioners**



## **Working Group on International Enforcement Cooperation**

*Final report – published October 2019*

# Table of contents

- Table of contents..... 2
- Foreword..... 3
- Executive summary ..... 4
- Introduction..... 6
  - Background ..... 6
  - Overview of the group and its work..... 6
  - Documentation presented to the Conference ..... 8
- Workstream 1: Practical Tools for Enhancing Enforcement Cooperation ..... 9
  - Workstream 1.1: Repository of enforcement cooperation tools and initiatives..... 9
  - Workstream 1.2: Secure Space and associated tools on the permanent ICDPPC Website .....13
    - 1.2.1 First scenario .....16
    - 1.2.2 Second scenario .....17
- Workstream 2: Legal Solutions for Enhancing Enforcement Cooperation .....18
  - Workstream 2.1: Schedule 2 to the GCBECA .....18
    - 2.1.1 Work to date on the GCBECA .....18
    - 2.1.2 State of the debate on development of Schedule Two .....19
    - 2.1.3 Recommendations for future steps .....20
  - Workstream 2.2: Model Clauses and Agreements .....20
    - 2.2.1 Results of the questionnaire.....21
    - 2.2.2 Observations .....21
    - 2.2.3 Recommendations .....22
  - Workstream 2.3: Mutual Legal Assistance Treaty .....22
    - 2.3.1 Introduction.....22
    - 2.3.2 Benefits of an international treaty .....23
    - 2.3.3 Practical experiences + timeline .....24
    - 2.3.4 Feasibility viewed by ICDPPC members .....25
    - 2.3.5 Recommendations on future steps .....26
- Conclusions .....27
  - Way forward .....28
- Annexes: GCBECA Schedule Two and the Questionnaire relating to Workstream 2.2 .....29

## Foreword

The co-chairs of the Working Group on International Enforcement Cooperation (“the Working Group”) – James Dipple-Johnstone of the UK Information Commissioner’s Office (ICO), and Marianne Niessink of the Autoriteit Persoonsgegevens (Netherlands Data Protection Authority, NL DPA) – are pleased to present this report to the 41<sup>st</sup> International Conference of Data Protection and Privacy Commissioners in Tirana, Albania.

During the two years execution of its mandate, the Working Group has worked together closely and intensively in the search for potential solutions that may facilitate a broader scope of enforcement cooperation in the realm of privacy and data protection.

This report represents the output of the work done and details the coming into being of the Working Group, its mandate, terms of reference and its workplan. It discusses the aims of the separate workstreams the work was divided into, the progress made and the final output. It then makes recommendations and suggestions for further steps and ways forward, which are given more concrete substance in a proposed resolution that accompanies this report. This *Draft Resolution on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement (2019)* (the “Resolution”) is to be presented at the International Conference of Data Protection and Privacy Commissioners (“ICDPPC” or “Conference”) for discussion and consideration of eventual adoption.

All attendees of the Tirana Conference are warmly invited and encouraged to take note of this report and the proposed Draft Resolution as well as to consider co-sponsoring the Resolution. Should any questions arise about this report or the work done by the Working Group, the co-chairs remain available for queries. Any queries can be sent to the Secretariat of the Working Group, which is facilitated by the Netherlands Data Protection Authority, at: [internationaal@autoriteitpersoonsgegevens.nl](mailto:internationaal@autoriteitpersoonsgegevens.nl).

Finally, the co-chairs would like to thank all the members of the Working Group for their active involvement and continued engagement with the Working Group and with international enforcement cooperation, as well as for their invaluable input and contributions that lead to fruitful discussions and new insights. The co-chairs also wish to highlight the much-appreciated contributions of the rapporteurs and would like to express their firm gratitude.

## Executive summary

In giving effect to its mandate, the Working Group has divided its work into two workstreams. The first workstream (“Workstream 1”) proposes practical solutions for enforcement cooperation, the second workstream (“Workstream 2”) proposes legal solutions.

**In Workstream 1**, the Working Group explored two practical solutions for enforcement cooperation, the first of which is the design and implementation of a permanent repository on the ICDPPC website that links to enforcement cooperation resources. The repository is aimed to go live in the run up to the 41<sup>st</sup> Conference. For this solution, the Working Group proposes the presentation of a Resolution to the 41<sup>st</sup> Conference in which commitment is pronounced towards promoting and maintaining the repository.

The work on the second practical solution involved research on an Authorities Database, possibly embedded in a member-only accessible secure space on the website. For this solution the Working Group proposes that steps are taken towards a public, non-secure database first, however, should the Future of the Conference Working Group recommend that a secure space can be implemented swiftly and easily, the recommendation is to incorporate the database into this secure space so as to avoid duplication of work.

**Workstream 2** focussed on potential future enforcement cooperation projects. It investigated three possible legal solutions for international enforcement cooperation split into three sub-streams.

**Workstream 2.1** concerns the possible expansion of the existing Global Cross-Border Enforcement Cooperation GCBECA via the addition of an optional but legally binding “Schedule 2.” The Working Group, however, recommends that the schedule requires additional revision. Recommended future steps include a mapping exercise to find out which provisions cause difficulties to different members and what kind of arrangements would best suit members’ needs.

**Workstream 2.2** considered the possibility of producing a set of model contract clauses or model bilateral or multilateral agreements to be used by authorities that wish to cooperate. The Working Group circulated a questionnaire that sought to clarify the differences between the varied jurisdictions and the requirements they pose on international cooperation. It was found that many respondents did not have the capacity to enter into legally binding agreements; hence, model clauses would not necessarily contribute to facilitating easier cooperation. The Working Group suggests that focus is placed on the proposals made under Workstream 1 and that after completion of the website, a mapping exercise could be undertaken to identify the legal impediments related to enforcement cooperation.

**Workstream 2.3** considered the feasibility of negotiating an international mutual legal assistance treaty in the context of privacy enforcement cooperation. Though it found that the benefits are potentially substantial, the negotiation of such treaty is a long-term effort that requires a carefully coordinated approach and stamina in both financial and time/capacity terms to create the necessary political momentum. Additionally, it was found that there are insufficient grounds to conclude that the Conference members are ready to approach their governments for the exploration of the negotiation of an international treaty in this field. The Working Group recommends that the work in this area is paused in favour of Workstream 2.2.

The main recommendations of the Working Group are the following:

- To pause the Working Group after the completion of its mandate in October 2019;

- To propose to the Conference the creation of a permanent Working Group on International Enforcement Cooperation; and
- To present for discussion and eventual adoption to the 41st Conference in Tirana, Albania a resolution that expresses commitment to supporting, maintaining and promoting the repository on the Conference website, that recommends a way forward for an Authorities Database, and that invites the Conference members to take note of the work done by the Working Group in the context of Workstream 2 and to use the output at national level for further work as each member deems appropriate to their needs.

# Introduction

## Background

International enforcement cooperation has been a key priority for the Conference for a long time. 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 data protection and privacy authorities to maintain pace with new challenges that are increasingly of a global nature and relevance.

Building on the 2014 and 2016 Resolutions on International Enforcement Cooperation, the Conference adopted a Resolution on exploring future options for International Enforcement Cooperation in 2017, prepared by the ICDPPC Group of Experts on Legal and Practical Solutions for Cooperation ("the 2017 Group of Experts").<sup>1</sup> In this resolution, the Conference accepted the Key Principles for Cooperation developed by the 2017 Group of Experts,<sup>2</sup> the amendments to the Global Cross Border Enforcement Cooperation GCBECA as suggested by the 2017 Group of Experts,<sup>3</sup> and took note of its exploratory work regarding tools and initiatives currently available for privacy enforcement cooperation.<sup>4</sup>

Furthermore, the Conference mandated:

*'[...] 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).'<sup>5</sup>*

The Working Group was created on the basis of this Resolution and in 2018, the Working Group presented its progress at the 40<sup>th</sup> Conference in Brussels. As mandated, this final report presents the work of the Working Group to the 41<sup>st</sup> Conference in Tirana and proposes recommendations for future work.

## Overview of the group and its work

The call for members of the Working Group was issued in early 2018. Twenty-one ICDPPC members from all over the world designated senior legal, policy or enforcement experts to take part in the Working Group. The members are regionally diverse and the Working Group consists of representatives from Albania, Argentina, Belgium, Burkina Faso, Canada (Federal), Catalonia,

---

<sup>1</sup> 39<sup>th</sup> International Conference of Data Protection and Privacy Commissioners, Resolution on exploring future options for International Enforcement Cooperation, Hong Kong: 2017.

<sup>2</sup> ICDPPC Group of Experts on Legal and Practical Solutions for Cooperation 2016-2017, Final Report presented to the 39<sup>th</sup> Conference of the ICDPPC in Hong Kong, August 2017, page 15.

<sup>3</sup> Final Report 2017, page 34.

<sup>4</sup> Final Report 2017, page 52 and beyond. These initiatives concern: compiling a comprehensive authorities database; creating a repository for sharing best practices; devising a cross-sectoral information sharing platform; developing a cross-border multi-jurisdictional complaint tool; creating teams of case handlers, and, lastly; devising model bilateral or multilateral cooperation tools. Moreover, the 2017 Group of Experts discerned three possible approaches to devising model bilateral or multilateral cooperation tools: developing a Mutual Legal Assistance (MLA-) Treaty, developing a model agreement or set of model clauses, or further encouraging increased participation in the existing ICDPPC GCBECA.

<sup>5</sup> Resolution on exploring future options for International Enforcement Cooperation, Hong Kong: 2017, paragraph 5.

European Data Protection Supervisor ("EDPS"), France, Germany (Federal), Ghana, Gibraltar, Hong Kong, Mexico, Morocco, the Netherlands, the Philippines, Switzerland, Turkey, United Kingdom, the United States (Federal) and Uruguay.

The first teleconference of the Working Group took place on 26 April 2018. During this call, the Information Commissioner's Office (UK DPA) and the Netherlands Data Protection Authority (NL DPA) were elected co-chairs. The Dutch Data Protection Authority agreed to act as the Administration Team for the Working Group. The co-chairs connected with the Global Privacy Enforcement Network (GPEN) to set up an online space on the GPEN website to share information between the members, however, the majority of communication was completed via e-mail or teleconference. The Working Group also adopted its own Terms of Reference to help steer the work.

After the first teleconference, the co-chairs proposed to divide the scope of the mandate into two separate workstreams; one to propose practical solutions for better cooperation and knowledge-sharing on the topic, and one to work on legal solutions to frame international enforcement cooperation. The participants shared oral and written statements on this proposal, which – after multiple rounds of feedback – were included in a work plan, which was adopted on 13 July 2018.

- **Workstream 1: Practical solutions for better cooperation**

Under Workstream 1, the Working Group has worked on practical solutions to improve communication and collaboration amongst ICDPPC members. This included exploring the creation of an authority database (including relevant information about the different authorities, clarification of the legal frameworks and legal room for cooperation) and a separate repository for sharing non-confidential information and resources relevant to enforcement cooperation. In the first place, this workstream has been dedicated to researching the feasibility of these options, and secondly, has worked towards practical implementation of several of the most viable options.

- **Workstream 2: Legal solutions for better cooperation**

In Workstream 2, the Working Group has focused on three separate topics: the possibility of a legally binding and enforceable schedule to the existing Global Cross Border Enforcement Cooperation GCBECA, the possibility of creating model clauses to be used in Members' cooperation agreements, and – finally – exploring the feasibility of the Conference promoting a Mutual Legal Assistance Treaty (MLAT) for furthering cooperation on data protection and privacy.

In Workstream 1, Canada and the Netherlands acted as rapporteurs, with the help of the United Kingdom in their role as Secretariat to the Executive Committee and webmasters of the ICDPPC website. Besides the team of rapporteurs, Catalonia, EDPS, France, Germany, Ghana, Hong Kong, Switzerland and the United States were involved. In Workstream 2.1, Belgium acted as rapporteur. In Workstream 2.2, the United Kingdom and Gibraltar spearheaded the work, and Workstream 2.3 was concluded with the Netherlands as rapporteur. Besides this team of rapporteurs, Argentina, Canada, Catalonia, EDPS, France, Mexico, Turkey and the United States were involved.

Those working on the respective workstreams each convened a series of teleconferences which culminated in a face-to-face meeting in The Hague in February 2019, where the first results were presented and the members decided on the final directions for the respective workstreams. The Working Group conferred with the ICDPPC's Executive Committee by letter of 18 March 2019 about these decisions.

The Executive Committee was consulted to:

- a) raise awareness that further potential exists for better understanding the enforcement tool needs of the ICDPPC members;
- b) discuss the lack of desire among conference members to develop some recommendations for content into a Mutual Legal Assistance Treaty, at least at this time, given that this has relevance for the Policy Strategy that is currently under development by the Conference; and
- c) pursue exploration of developing practical enforcement cooperation resources, which are also useful for policy analysis, for example by populating a repository with useful resources on the ICDPPC website, and an Authorities' Database enabling identification of each member's ability to cooperate on enforcement matters. Such exploration would be pursued with the Data Metrics Working Group to use the Conference census to source information.

The Executive Committee agreed with the proposals and noted the conclusions for any relevance to the ICDPPC Policy Strategy.

In finalizing the work for the Working Group, the co-chairs consulted with the ICDPCC Working Group on the Future of the Conference concerning the feasibility of certain web-based options identified in Workstream 1. Additionally, the Working Group reached out to the ICDPPC Working Group on Data Protection Metrics to discuss the possibilities of using the ICDPPC Census to further the work. Both Working Groups are still deliberating on how to best shape this proposed cooperation. The co-chairs also consulted with the Working Group members on a draft resolution to be sent to the Conference in Tirana (2019) and issued a call for co-sponsors.

The co-chairs finalized the work in August 2019.

## 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) **Resolution on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement**

With this report, the co-chairs recommend the Resolution and the Working Group's documents to the 41<sup>st</sup> Conference in Tirana October 2019.

The co-chairs:

<b>James Dipple-Johnstone</b> Co-chair, Deputy Commissioner of the Information Commissioner's Office (United Kingdom)	<b>Marianne Niessink</b> Co-chair, Director of Policy, Strategy and International Affairs, Autoriteit Persoonsgegevens (the Netherlands)
<b>James Moss</b> Deputy co-chair to James Dipple-Johnstone, Director of Regulatory Enforcement, Information Commissioner's Office (United Kingdom)	



## Workstream 1: Practical Tools for Enhancing Enforcement Cooperation

As already remarked, the Working Group has, to best suit and give effect to its mandate, divided its work into two separate workstreams. Workstream 1 builds on the recommendations made by the 2017 Group of Experts and aims to seek **practical rather than legal** solutions for improved enforcement cooperation.<sup>6</sup> In addition to the recommendations made by the Group of Experts, which the Working Group used as starting point, the Working Group identified the desire to search for additional practical enforcement cooperation tools. The general objectives of Workstream 1 are firstly, to research the **feasibility** of the recommended and identified options and, secondly, to work towards **practical implementation** of several of the most viable options.

To better streamline the work, the Working Group decided to subdivide Workstream 1 into two subworkstreams. Workstream 1.1 focusses on the design and implementation, on the ICDPPC website, of an easily accessible **repository** that links to Enforcement Cooperation related resources. Workstream 1.2 focusses on evaluating and recommending options for the creation of a comprehensive **Authorities' Database**, thereby also exploring options for embedding such a database in a **secure space** for information sharing amongst members on the ICDPPC website. Such a secure space could additionally include a document library and a discussion forum.

The ICDPPC Members from Canada and the Netherlands acted as rapporteurs for Workstream 1, aided by the United Kingdom in their role as Secretariat to the Executive Committee and webmasters of the ICDPPC website. Besides the team of rapporteurs and Secretariat, ICDPPC Members from Catalonia, France, Germany, Ghana, Hong Kong, Switzerland, the United States and the EDPS were involved in much of the work.

### Workstream 1.1: Repository of enforcement cooperation tools and initiatives

In its Final Report, the 2017 Group of Experts recommended 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."<sup>7</sup> This recommendation was made after having conducted a survey, from which the conclusion was drawn that there is a need for more and better enforcement cooperation tools. In the resolution adopted at the 39<sup>th</sup> Conference in Hong Kong, it was underlined that such cooperation tools may further improve effective cross-border cooperation, by sharing information and best practices.<sup>8</sup>

Taking on the recommendation to create an easily accessible repository, the Working Group examined the feasibility of the creation of such a repository with a view to realise the practical implementation of such a repository before the Conference in Tirana. The Working Group thereby directed special attention to the challenges identified by the Group of Experts along with its recommendations, namely the need to increase awareness of these tools, and to make them easily and intuitively accessible. The Working Group therefore focussed its Workstream 1.1 efforts on

---

<sup>6</sup> Final Report 2017, page 47.

<sup>7</sup> Ibid.

<sup>8</sup> Resolution on exploring future options for International Enforcement Cooperation, Hong Kong: 2017, pages 2 and 3.

answering the following questions, taking into account the consequences that the answers may have for the requirements for and specifications of the repository:

- *What type of **information** is to be included in the repository?*
- *In what manner should the information included in the repository be **organised**?*
- *What **form and architecture** for the repository are desirable?*
- *What **additional features** is the repository desired to have?*
- *In what manner should the **input** for the repository be provided?*
- *In what manner should the **future and upkeep** of the repository be organised and ensured?*
- *In what manner should the repository be **promoted**?*
- *In what manner should the repository be implemented and what is the timeframe for such **implementation**?*

Taking into account the input from several telephone conferences and a face-to-face meeting in February 2019 in The Hague (NL), the Working Group agreed for the repository to have the following specifics.

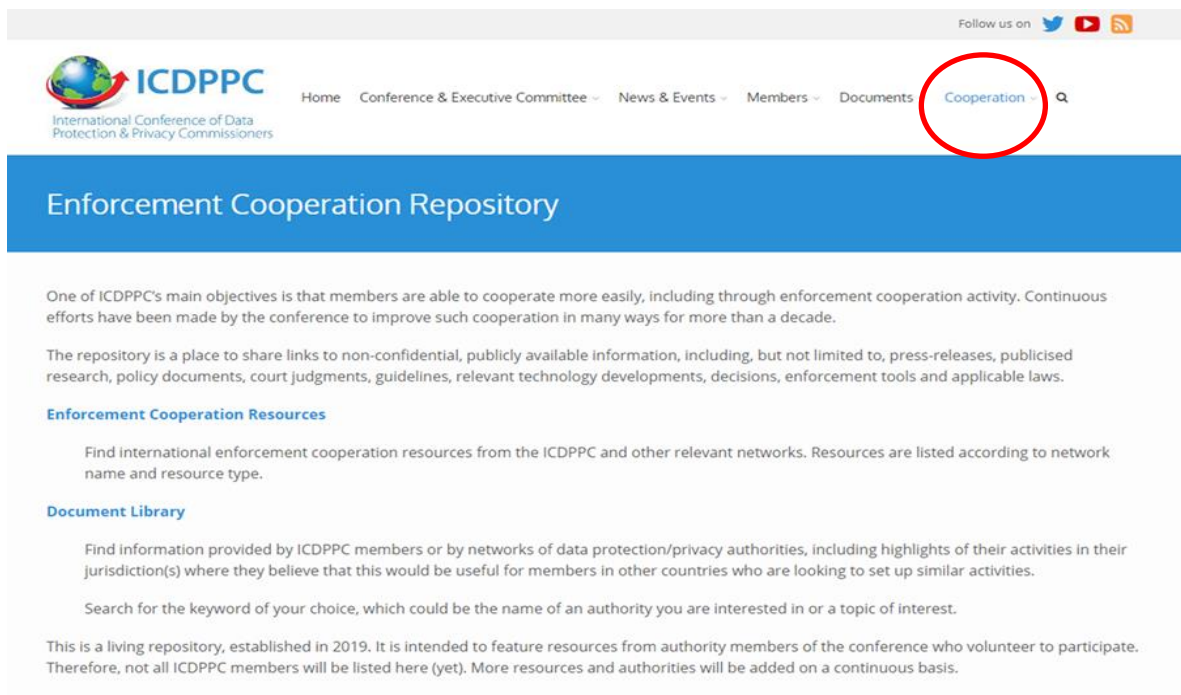
- A 'tab' is to be placed on the ICDPPC website, named "Enforcement Cooperation".
- Clicking on this tab is to direct to a 'landing page' that includes a short description highlighting and promoting Enforcement Cooperation, relevant Enforcement Cooperation quotes from different ICDPPC Members, and links to relevant Enforcement Cooperation resolutions.
- The repository is to be a library with two distinct sections:
  - One is to be a place for members to share links to **non-confidential, publicly available information**, including, but not limited to, press-releases, publicised research, policy documents, court judgments, guidelines, relevant technology developments, decisions, enforcement tools and applicable laws. The information to be shared in this section is relevant to Enforcement Cooperation but may also be relevant to policy development, and does not necessarily have to be limited to documents created by ICDPPC members.
  - The other is to be a place that provides links to resources and tools associated with various privacy and data protection related networks, such as – importantly – the Conference. One example of such resource could be the ICDPPC Enforcement Cooperation Handbook.
- The links and information included in the repository should ideally be organised taking into account these two types of libraries, namely according to both network and to member contributions. That means that, firstly, the "Enforcement Cooperation" drop-down tab will direct towards two sub-options: "Enforcement Cooperation Resources" and "Document Library". The sub-tab "Enforcement Cooperation Resources" will subsequently direct to the available resource links associated with different networks. The sub-tab "Document Library" will direct towards the library with links that were contributed by members.
- The repository is to take the form of a **database** that only provides **links** to the documents or information. No documents are to be uploaded on the repository itself to prevent hosting difficulties and reduce costs associated with hosting. The repository will be publicly accessible.
- The Working Group agreed that the inclusion of a possibility to subscribe to **RSS-feed**, to inform members of any new updates or contributions to the repository, would be useful. It was agreed that the frequency of the updates will be monthly so as not to overburden recipients, and no updates will be sent out if no new contributions are made to the repository. The addition of the RSS-feed was, however subject to a feasibility check which the ICO carried out and concluded that a basic RSS-feed function was in fact integrated into the website already although it was unclear how many users it currently had. Therefore, keeping the current arrangement was feasible, as currently, there is a low number of articles posted

on the website. But if the number of published articles increased then the Conference could then look at more advanced RSS solutions which allow users to filter by topic, author and so on.

- In the same way, the Working Group favours the inclusion of an **advanced search option** to the repository. The inclusion of an advanced search option is subject to a feasibility check which the ICO agreed to carry out; this was subsequently found feasible, indeed recommended, in order to improve the user experience and monitor user behaviours more efficiently. An appropriate search plug-in was found and has been implemented.
- The **input** for the repository is to be contributed by members of the Conference. Contributed links are to be accompanied by a translated title and a short summary in English, which is to be provided by the contributing member. The input will be gathered for upload once per month.
- The repository is to be a **living** instrument. To that end, the Working Group deemed it necessary to create a small dedicated team or task force of two or three volunteer members of the Conference, who will be tasked with the management of the repository, reporting to the Executive Committee with any updates and the monitoring of member contributions to the repository, including the provided translated title and summary and to prevent duplication. In the time before such a task force is created, its tasks can be executed by the Secretariat of the Executive Committee, depending on available resources.
- Information surrounding the repository and links to interesting uploads can be provided through the ICDPPC newsletter, thereby **promoting** both Enforcement Cooperation and the repository.

The following screenshots reflect the extent to which the repository has been implemented at time of writing accessible via the new 'Cooperation' drop down menu (circled), much thanks to the invaluable efforts from the ICO Comms Team. Please be aware that much is still subject to change. The Working Group is looking forward to presenting a finished and polished product to the Conference in October.

Screenshot 1



The screenshot shows the ICDPPC website header with the logo and navigation menu. The 'Cooperation' menu item is circled in red. Below the header is a blue banner with the text 'Enforcement Cooperation Repository'. The main content area contains text about the repository's objectives and resources, including sections for 'Enforcement Cooperation Resources' and 'Document Library'.

Follow us on [Twitter](#) [YouTube](#) [RSS](#)

**ICDPPC**  
International Conference of Data Protection & Privacy Commissioners

Home Conference & Executive Committee News & Events Members Documents **Cooperation**

## Enforcement Cooperation Repository

One of ICDPPC's main objectives is that members are able to cooperate more easily, including through enforcement cooperation activity. Continuous efforts have been made by the conference to improve such cooperation in many ways for more than a decade.

The repository is a place to share links to non-confidential, publicly available information, including, but not limited to, press-releases, publicised research, policy documents, court judgments, guidelines, relevant technology developments, decisions, enforcement tools and applicable laws.

### Enforcement Cooperation Resources

Find international enforcement cooperation resources from the ICDPPC and other relevant networks. Resources are listed according to network name and resource type.




### Document Library


Find information provided by ICDPPC members or by networks of data protection/privacy authorities, including highlights of their activities in their jurisdiction(s) where they believe that this would be useful for members in other countries who are looking to set up similar activities.

Search for the keyword of your choice, which could be the name of an authority you are interested in or a topic of interest.

This is a living repository, established in 2019. It is intended to feature resources from authority members of the conference who volunteer to participate. Therefore, not all ICDPPC members will be listed here (yet). More resources and authorities will be added on a continuous basis.

Screenshot 2

Follow us on   



[Home](#)
[Conference & Executive Committee](#)
[News & Events](#)
[Members](#)
[Documents](#)
[Cooperation](#)

## Document Library




Enforcement cooperation repository / Document library


Find information provided by ICDPPC members or by networks of data protection/privacy authorities, including highlights of their activities in their jurisdictions. Search for the keyword of your choice, which could be the name of an authority you are interested in or a topic of interest.

Show  entries Search:

Network or Authority	Resource	Type of Resource	Description of Resource	Upload date
Catalan Data Protection Authority	<a href="#">Smart Cities</a>		This section includes, aware of the implication that the development of Smart Cities may have on the personal data and privacy rights, a Document for debate, a bibliography, and audio-visual materials to contribute to the debate regarding this issue.	29/8/2019
Mexico - National Institute for Transparency, Access to Information and Personal Data Protection (INAI)	<a href="#">Case "Access to clinical file"</a>	Enforcement Action	A procedure for imposing sanctions against a hospital was initiated because a data subject submitted a request for the protection of its rights. This, because the data controller did not respond to the data controller's request for access to a certified copy of the entire clinical record which was generated when she was admitted to the Hospital for the birth of her son.	29/8/2019
Mexico - National Institute for Transparency,	<a href="#">Case "Classification of personal data of the Interbank CLABE"</a>	Enforcement Action	Complaint was filed against a financial institution, since it improperly provided the complainant's standardized interbank key (CLABE), to a third party. Three fines were imposed which, in total, amounted to \$	29/8/2019

Screenshot 3

Follow us on   



[Home](#)
[Conference & Executive Committee](#)
[News & Events](#)
[Members](#)
[Documents](#)
[Cooperation](#)

## Enforcement Cooperation Resources

Enforcement cooperation repository / Enforcement cooperation resources

Find international enforcement cooperation resources from the ICDPPC and other relevant networks. Resources are listed according to network name and resource type.

Show  entries Search:

Network or Authority	Resource	Type of Resource	Description of Resource
AFAPDP	<a href="#">Member List, and French data protection laws lists</a>	Authority Lists and Registries	
APEC	<a href="#">Cross-border Privacy Enforcement Arrangement</a>	Sharing Confidential Information	Regional arrangement that allows for the request for cooperation assistance by Asia-Pacific participants.
APPA	<a href="#">Member List</a>	Authority Lists and Registries	
APPA	<a href="#">Secondment Framework</a>	Enforcement Cooperation Training and Capacity Development	Provides guidance and templates to authorities wishing to implement a secondment from one data protection authority to another.

Finally, the Working Group acknowledged that, in order for the repository to be and remain a living instrument that is continually edited and updated, that is dynamic and effective in fulfilling its goals, and that hence contributes to the maximum of its potential to the achievements of the objectives of the Working Group and ultimately of the Conference, commitment from all ICDPPC Members is required towards maintaining the repository as a living instrument. The Working Group noted that, besides the commitment to keeping the repository alive, commitment to the structures that will be responsible for the management, maintenance and upkeep of the repository, along with reporting to the Executive Committee is also needed.

To those ends, the Working Group agreed to present and submit to the Conference a **resolution** expressing such commitment towards:

- **effectively maintaining** the repository;
- creating and supporting a small dedicated team or **task force** of two or three members of the Conference, who will be tasked with the maintenance of the repository, the monitoring of member contributions and the provided translated title and summary to the repository and with the prevention of duplication; and
- **promoting** the repository.

## **Workstream 1.2: Secure Space and associated tools on the permanent ICDPPC Website**

In its Final Report, the Group of Experts noted that the Marrakesh Resolution on International Enforcement Cooperation (2016) had mandated the ICDPPC Executive Committee to discuss the identification and creation of “**practical projects** that better coordinate the efforts towards global enforcement cooperation (p. 52).” Specifically, the Resolution mentioned “exploring the feasibility of networks’ cooperation on **population of a database** of each authority’s legal powers to cooperate, evidence-gathering requirements, definitions of personal data and confidential data, which can help Conference members to easily identify partner authorities in a case.”

In carrying out this mandate, the Group of Experts noted that various resources are available that list information on member authorities. However, the information listed in those sources is generally limited and no single available resource provides access to all information that may be relevant to the identification, evaluation and contact of potential enforcement cooperation partners. The Group of Experts recommended that, in further efforts towards developing and populating such a database, attention be paid to:

- the most efficient method of populating such a database and keeping it up-to-date;
- whether a wiki-format may be preferable to the standard database caretaker approach; and
- if a secure space requiring an account to log-in in order to access the database would be desirable.

In the Resolution adopted at the 2018 Conference in Brussels, noting the demand for the Conference to serve as an operational platform for **practical cooperation**, commitment was expressed towards studying “the development of a **secured online platform** for ICDPPC members only, dedicated to resources availability and knowledge sharing, including, but not limited to **directory of members**, repository of national and international data protection laws, Q&A forum, Working Groups and Executive Committee relevant documentation, dedicated research section, “hot topic”, “looking ahead” and “prospective” alerts.”

At the outset, the Working Group has defined the parameters of its work in Workstream 1.2. As to the Authorities Database, the Working Group noted in particular that, given the recommendations outlined in the Final Report, the database could include the following information:

- The authority **name**;
- A hyperlink to its **website**;
- **General information** about the authority such as office size and organizational structure.
- An enforcement **contact person**, including contact details (phone, email) (or potentially, general non-confidential contact information);
- Overview of members' **data protection regime**, including a link to relevant legislation and highlights of major provisions in the data protection laws;
- **Enforcement powers** – e.g.: evidence gathering (compelling testimony or production, search of premises); administrative fines; criminal sanctions; bring cases to court; awarding compensation to data subjects;
- Legal **authority to cooperate**, including the mechanism(s) pursuant to which they may cooperate, and any requirements for information sharing or assistance requests (e.g., limits on the sharing of personal data, confidentiality requirements, evidentiary requirements) and forms of investigation possible (joint investigation vs. information sharing); and
- Information regarding the scope of the **authority's jurisdiction** (geographically, substantively, public and/or private sector, administrative/criminal).

As to the parameters of the mandate regarding the secure space, the Working Group has confirmed at the outset that, as was acknowledged in the Resolution adopted at the 2018 Conference in Brussels, there is value in developing a secure space dedicated to sharing resources and knowledge between members, and to facilitating communication and cooperation between them. However, the Working Group has also noted that the **Working Group on the Future of the Conference** has taken up the task of studying the feasibility of development and implementation of a secured online platform for ICDPPC members. The Working Group on the Future of the Conference has, outside the scope of the Working Group on International Enforcement Cooperation, performed a cost-benefit analysis of the options available to implement a secure space in the context of considering the feasibility of its creation.

Besides taking into account the work of the Future of the Conference Working Group on the development of a *new* secure space on the ICDPPC website, the Working Group also evaluated the possibility of working with the *existing* GPEN network on leveraging or amending tools that are already available via the GPEN website. In evaluating this option, the Working Group took into account that the possible benefit of having an ICDPPC secure space might be diminished given the already existing GPEN secure website, to which GPEN has, in certain circumstances, provided limited access to non-GPEN members, and the fact that GPEN is supportive of working with the ICDPPC. However, four arguments were discussed that led to the conclusion that, if at all, the creation of a separate ICDPPC secure space is preferable to using the GPEN-network:

- The value of the information in such a secure space goes beyond just enforcement cooperation and is possibly of interest to the entire ICDPPC;
- There are certain data protection or privacy authorities/commissioners that are members of GPEN but not of ICDPPC, which could bring up difficulties with exclusive use of the platform;
- The ICDPPC should be able to stand on its own; and
- The massive use of the GPEN-network by ICDPPC members could be burdensome for GPEN.

However, the Working Group noted that, in developing and implementing a recommended design for the Authorities Database, it may be desirable to include the Authorities Database in the secure space (which would be accessible via login). Even though the information to be included in the Authorities

Database mentioned above is not likely to be strictly confidential, the Working Group acknowledged that not all Conference members may feel comfortable in disclosing all of the abovementioned information on a publicly accessible website. In that sense, the choice whether the Authorities Database is to be publicly accessible or restricted-access only depends on the amount and sort of information that members are willing to share publicly.

In that regard, the Working Group has noted that the volume of confidential or otherwise not public information which must thus be shared through a secure connection, is relatively limited. In addition, and depending on the recommendations of the Future of the Conference Working Group regarding the secure space, the Working Group noted that it is likely that a non-publicly accessible secure space may be costly to build and to maintain. The Working Group has consequently favoured an approach in which steps towards a public, **non-secure Authorities Database** that builds upon existing member pages on the ICDPPC website are first explored, before moving towards a secure online environment. Having reached this conclusion, the Working Group also noted that, should the Working Group on the Future of the Conference recommend that a secure space for ICDPPC members can be implemented relatively swiftly and easily, it is not desirable to set up an additional Authorities Database that is publicly accessible given that this might result in duplication of work. Rather, after a secure space is implemented, the advantages of having more detailed information on all member authorities may merit the transfer of an Authorities Database in the public space into the restricted part of the website.

Hence, the Working Group presents two recommended scenarios. In the first scenario, the conclusion of the Working Group on the Future of the Conference would be that a secure space can be implemented relatively swiftly and easily, and consequently, the Authorities Database would be embedded in that secure space so as to avoid double work and to take full advantage of the restricted environment by expanding the information included in the Authorities Database to also include more detailed general and contact information. In the second scenario, the conclusion of the Working Group on the Future of the Conference is that a cautious approach is required towards the implementation of a secure space, and that consequently the Authorities Database merits remaining as a project for publicly available information, before more concrete steps are undertaken towards implementation of such secure space.

The following considerations apply to **both scenarios**. As it stands, the Conference website included two separate lists with information on members of the Conference, which the Working Group deemed not desirable.<sup>9</sup> Hence, the two lists should be **merged**, at least as a recommendation to the Secretariat for future work in a Conference **resolution**.

Building on this, the Working Group discussed the recommended content of the Authorities Database. Amongst others, the Working Group has considered to provide links to the websites of members, so as to ensure that there are no inaccuracies or discrepancies between the information displayed on the ICDPPC website and the website of members. However, since the websites of members do not, or only limitedly, provide enforcement cooperation information that is readily understandable for other members, considering amongst others a possible language barrier, it was decided to abandon this idea. As such, the Working Group agreed that the information to be included in the Authorities Database is **'tombstone information'** (in other words, headline information, i.e. an organisation's main identifiers, such as organisation name, website, etc.) on each member of the Conference.

---

<sup>9</sup> I.e. <https://icdppc.org/participation-in-the-conference/members-online/>; and <https://icdppc.org/participation-in-the-conference/list-of-accredited-members/>



As to the population and maintenance of the content in the Authorities Database, three options were considered:

- The information in the Authorities Database is updated by the Executive Committee Secretariat. The Working Group abandoned this possibility, as it would involve a lot of work for the Executive Committee Secretariat.
- The information in the Authorities Database is updated by the members themselves, who get the necessary credentials to do so. The Working Group decided not to run with this possibility, as it carries certain drawbacks concerning the required IT-infrastructure and information security.
- The information in the Authorities Database is drawn from the information gathered through the census questionnaire, which takes place every three years. The Working Group noted that a disadvantage to this possibility is that the information displayed may not remain correct and would thus only be a snapshot at a certain point in time.

The Working Group deemed the third option, i.e. populating the Authorities Database using the information gathered through the **census questionnaire**, preferable. The Working Group noted, however, that the census answers are not necessarily automatically publishable. In light of that, the Working Group decided that, in recommending a design for the Authorities Database and making a choice between manual or automated population of the Database, the benchmark should be that automated population is not excluded, but only insofar as it simplifies the task. In order for the census information to be relevant and operable for inclusion in the Authorities Database, corresponding questions must be drafted in collaboration with the Working Group on Data Metrics, which is responsible for the Conference Census. In the communication of such questions to the ICDPPC members, it should be made clear which information will be publicised on the website and which information will not be. The Working Group agreed to include members of the Conference in the Authorities Database only. Observers of the Conference could be added at a later stage.

### **1.2.1 First scenario**

In this scenario, the conclusion of the Working Group on the Future of the Conference would be that a secure space can be implemented relatively swiftly and easily. That means that in that scenario, it would be favourable to embed the Authorities Database in that secure space, as it avoids double work and takes full advantage of the restricted environment by expanding the information included in the Authorities Database to also include more detailed general information and more specific enforcement contact details, which is potentially beneficial and hence desirable.

#### **Where the first scenario applies, then the Working Group would recommend the following design specifications for the Authorities Database:**

- The Authorities Database will be embedded in the secure space.
- The Authorities Database will include all information on members that is relevant to the identification, evaluation and contact of potential enforcement cooperation partners, including more detailed general information and more specific enforcement contact details of members.
- The information included in the Authorities Database will be 'tombstone information'; even though this means that the information in the Authorities Database might not remain fully up-to-date, this avoids any disadvantages that might occur should only links to member's websites be provided.
- The Authorities Database will be populated and updated using answers to the census questionnaire. To that end, relevant questions will be composed so as to ensure that the information received is readily operable for the Authorities Database.
- In principle and initially, the Authorities Database shall be populated manually, i.e. by using and manually inserting the questionnaire answers; automated population is not excluded only insofar as it simplifies population and maintenance of the Authorities Database,



considering that not all census answers are automatically publishable without manual intervention.

- There will be the potential for a member to request, manually to the Secretariat to the Executive Committee, that information about that member be changed as is necessary.
- The Authorities Database shall include members of the Conference only; observers to the Conference can be added at a later stage.

### **1.2.2 Second scenario**

In this scenario, the conclusion of the Working Group on the Future of the Conference would be that a cautious approach is required towards the implementation of a secure space, and that consequently the Authorities Database merits finalisation before more concrete steps are undertaken towards implementation of such secure space. Should, in a later stage, a secure space be created on the ICDPPC platform, the Authorities Database could be transferred there. Though the Working Group recognised that sharing more specific enforcement contact details of members is potentially beneficial and hence desirable, the Working Group also acknowledged that it is not desirable to include such information on a publicly accessible platform. Therefore, the Working Group recommends that the Authorities Database include only:

- General contact information that is already publicly available on the websites of each member of the Conference;
- Possible links to websites and social media of members;
- Applicable laws; and
- A short summary of each member's jurisdiction.

#### **Where the second scenario applies, then the Working Group would recommend the following design specifications for the Authorities Database:**

- In principle, the Authorities Database will be non-secure and publicly accessible; information that is not to be shared publicly could be added in a later stage depending on the outcomes of the Working Group on the Future of the Conference work.
- The Authorities Database will include general contact information that is already publicly available on the websites of each member of the Conference, possible links to websites and social media of members, applicable laws, and a short summary of each member's jurisdiction.
- The information included in the Authorities Database will be "tombstone" (i.e. headline) information; even though this means that the information in the Authorities Database might not remain fully up-to-date, this avoids any comprehensibility disadvantages that might occur should only links to member's websites be provided. A note or disclaimer shall be added to this end.
- The Authorities Database will be populated and updated using answers to the census questionnaire. To that end, relevant questions will be composed so as to ensure that the information received is readily operable for the Authorities Database.
- In principle and initially, the Authorities Database shall be populated manually, i.e. by using and manually inserting the questionnaire answers; automated population is not excluded only insofar as it simplifies population and maintenance of the Authorities Database, considering that not all census answers are automatically publishable without manual intervention.
- Depending on the presence of possibilities for members to make adjustments within the secure space, there will be the potential for a member to request, manually to the Secretariat to the Executive Committee, that information about that member be changed as is necessary.
- The Authorities Database shall include members of the Conference only; observers to the Conference can be added at a later stage.

## **Workstream 2: Legal Solutions for Enhancing Enforcement Cooperation**

This workstream builds on the work of the 2017 Group of Experts. The 2017 Group of Experts presented its final Report at the 39th Conference of the ICDPPC in Hong Kong. This report proposed a list of potential future enforcement cooperation projects. These initiatives were flagged as individual and practical short, medium and longer term projects; the aim of these projects being to give effect to the ICDPPC Executive Committee mandate to better coordinate the efforts towards global enforcement cooperation. Three possible approaches to devising model bilateral or multilateral cooperation tools were discerned, one of which was making relevant adjustments in order to further encourage increased participation in the existing ICDPPC Global Cross Border Enforcement Cooperation GCBECA (GCBECA).

The 2017 Group of Experts underlined the relevance of a set of Key Principles in streamlining cooperation between ICDPPC members. These Key Principles can be adapted to national, regional and local needs to reduce uncertainty and facilitate cooperation, and enable the Members to protect privacy more effectively. The Key Principles were also endorsed at the 39th Conference of the ICDPPC in Hong Kong and they also encourage members and observers to, as they deem appropriate, adapt the key principles and the Explanatory Memorandum to their national, regional and local needs. This could include presenting the key principles to their governments, with a view to assisting in the development of laws that will facilitate more effective privacy enforcement cooperation.

Workstream 2 has, similarly to Workstream 1, been subdivided into sub-workstreams. Workstream 2.1 focusses on the possible expansion of the GCBECA, where the emphasis of Workstream 2.2 lies on the possibility of producing a set of model contract clauses or a model bi-lateral or multi-lateral agreement to be used by authorities wishing to co-operate. Finally, Workstream 2.3 sets out the parameters for a feasibility study into developing a Mutual Legal Assistance Treaty (MLAT).

The ICDPPC members from Belgium and Mexico acted as rapporteurs for Workstream 2.1, the ICDPPC members from the United Kingdom, the Netherlands and Gibraltar for Workstream 2.2 and for Workstream 2.3, the members from Germany, Canada and the Netherlands functioned as rapporteur. Valuable input has also been provided by the other members of the Working Group.

### **Workstream 2.1: Schedule 2 to the GCBECA**

#### **2.1.1 Work to date on the GCBECA**

Progress within Workstream 2.1 was last reported on by the Working Group to the 2018 ICDPPC Conference in Brussels. Over the last twelve months the Working Group has been considering ways of revising the GCBECA to ensure relevance to our European colleagues in particular, but also to ensure relevance to other legal frameworks developing around the world.

The GCBECA is not a tool for providing a legal basis for international transfer of personal data, but rather sets forth participants' commitment to cross-border privacy enforcement cooperation, based on their abilities and obligations in national law. In Workstream 2.1, the Working Group focused on potential amendments to the GCBECA including the potential to add additional clauses via a "Schedule Two". This would draw on the conclusions from the recent work of the Council of Europe (CoE) and insight from the developing work of a Working Group on International Transfers within the then Article 29 Working Party [now EDPB] which would be relevant to the GCBECA's development.

The updates proposed to the GCBECA form part of the full package of documents summarising the work done by the Working Group and are submitted to the 41<sup>st</sup> Conference in Tirana for consideration. The GCBECA as it is, with the revised Schedule One, remains available to all Conference members and the Working Group heartily welcomes and encourages other and new members to participate.

### **2.1.2 State of the debate on development of Schedule Two**

In February 2019, the Working Group met in The Hague to discuss a proposal from Prof. Dr. Gert Vermeulen of the former Belgian Privacy Commission for a new version of the GCBECA which could sit alongside the existing version but be legally binding on the Members who decide to participate in it. Therefore, there would be both non-legally binding and legally binding versions of the GCBECA on offer to ICDPPC members, according to their local needs. The Schedule Two to the GCBECA represents the legally binding version.

The Working Group would wish to pause here and extend its sincere gratitude to Prof. Vermeulen for leading the drafting work involved. Prof. Vermeulen also kindly prepared an accompanying draft explanatory text to sit alongside the GCBECA to explain to the wider Conference membership the extent to which the current draft is a starting point and that any necessary local law conditions, in respect of GDPR or otherwise, would need to be built in to the final text of any version that would ultimately be put into place for active use. Prof. Vermeulen then provided an updated version of the document which addresses comments from The Hague meeting in February 2019 and the comments of the FTC, Mexico, Hong Kong and Turkey. These two documents, in their most updated form are annexed to this Report.

At the February 2019 meeting in The Hague, the Working Group noted it is aware that not all Members consider that they have the power to enter into a legally binding arrangement. One key point of discussion was in respect of how the necessary requirement(s) drawn from Convention 108 and GDPR may require any agreement to be legally binding and how that could be squared with the legal restrictions in certain jurisdictions whose own national laws prevent Members from entering into any such legally binding agreement.

Regarding the relationship between GCBECA, Schedule One and Schedule Two, it was noted there may be gaps in Schedule One that could possibly be addressed by Schedule Two. It was suggested to further promote membership to the GCBECA in order to increase participation and to recommend participation in the GCBECA as a starting point for cooperation. Further comments from Working Group members were sought following the meeting.

Comments following the February 2019 meeting in The Hague suggested amendments introduced are around:

- Omission of explicit reference to EU or CoE in Article 1.1 and 1.5 requested by FTC; and
- Insertion of definitions of genetic and biometric data in the definitions.

Prof. Vermeulen provided his comments (post the February 2019 the Hague meeting) on the remarks on the draft amendments ahead of the February 2019 The Hague meeting from FTC, Turkey, Hong Kong and Mexico. These comments were around:

- The nature of Schedule Two and the considered impossibility for some authorities to enter into it; and
- Enforceability: non-compliance with the Schedule may prompt legal effects and liability under the laws of the signatory authorities (see Art 11).

Attention was also drawn to various points, including:

- a clear definition of “personal data” under Article 2(a) in Schedule Two to include “data from which it is practicable that the identity of the individual can be directly or indirectly ascertained” so to reflect the definition of personal data protection laws of some other jurisdictions; and
- a clear definition of “data processing” under Article 2(b) in Schedule Two to include “use of personal data”.

### 2.1.3 Recommendations for future steps

- The Working Group is of the view that Schedule Two would require some **additional revision** for it to work for each individual member. The Conference has taken a valuable first step with this work to address member’s needs, as previously revealed by Conference member surveys.
- Schedule Two should be considered to be an **optional piece**. It provides Members with a starting point and can be adapted by each individual Member on an ongoing basis, according to need, for each cooperation agreement that they wish to enter into. Any necessary local law conditions in respect of GDPR or otherwise would need to be built in to the final text of any version that would ultimately be put into place for active use by Members.
- A **mapping exercise** could also be beneficial to find out which Members would benefit from and be interested in what kind of arrangements and which provisions would cause Members difficulties. Once such information had been obtained it was suggested that the Conference as a whole would be better able to assess what the appetite amongst Members would be for such an agreement and how many of its Members would actively be in a position to use it.
- If the agreement of the Conference is obtained, an **opinion or advice could be sought** from the CoE and the EDPB as to the proposed Article 11.
- Once the Working Group completes its current mandate in October 2019, the Working Group would recommend for the ICDPPC to have a **permanent Working Group** on enforcement cooperation working matters, the purpose (at least partially, depending on the overall mandate granted by the Conference) to be to keep the GCBECA under review and make periodic recommendations to the Executive Committee for further action.

## Workstream 2.2: Model Clauses and Agreements

The objective of this Working Group’s Workstream 2.2 is to consider the possibility of producing a set of model contract clauses or a model bi-lateral or multi-lateral agreement to be used by authorities wishing to co-operate (or to promote to a government who would normally act to develop any such agreement on behalf of an authority) but requiring a separate, legally enforceable agreement to do so.

As already identified by previous work by the OECD and the ICDPPC, privacy enforcement cooperation could cover a range of activities from sharing good practice to transfer and exchange of personal data relating to specific investigations both civil and criminal. Differences in jurisdiction and national or regional laws could result in a variety of approaches and different types of cooperation could necessitate different requirements such as formal arrangements or binding legal agreements. Conversely, some members may not be permitted to enter into legally binding agreements for international enforcement co-operation.

In order to assess the range of clauses or other agreement that could be required or useful in this work area, the group determined that it would need to clarify the variety of laws, powers and restrictions on authorities, assess the different situations affecting authorities and on this basis, decide on the most useful and achievable work product from this area.

After considering the scoping document prepared by UK, it was agreed at the second teleconference of the Working Group in autumn 2018 that a questionnaire should be circulated to all ICDPPC member authorities to collect information to assist the Working Group in determining the best possible work product.

The questionnaire was originally circulated to members in late 2018, and the interim results were analysed by NL and jointly presented by NL and UK to the Working Group in a meeting hosted by the NL Co-chair Authority in The Hague. The Working Group discovered highly important potential benefits that gathering this information could have for members’ future enforcement work and shared its interim findings with the ICDPPC Executive Committee. The Executive Committee agreed with the high value of this work and encouraged the Working Group to relaunch the survey to request that as many additional ICDPPC members as possible respond to this survey. The relaunch took place in late spring with responses due by 10<sup>th</sup> May 2019. The analysis of the second set of questionnaire results was conducted by Gibraltar. The information set out below includes the combined responses from both circulations of the survey.

**2.2.1 Results of the questionnaire**

13 questions were asked and of these, one question related to Workstream 2.3 and one was a request for copies of any existing MOUs or agreements relied upon to facilitate enforcement cooperation.

In total, 40 ICDPPC members provided answers to the survey: Albania (AL), Australia - Federal (AU), Australian State of Victoria (ASV), Austria (AT), Bosnia Herzegovina (BA), British Columbia (OIPC, CAN), Bulgaria (BG), Burkina Faso (BF), Canada - Federal (CA), Catalunya (CT,ES), Croatia (HR), Cyprus (CY), EDPS (EDPS, EU), Estonia (EE), Federal Trade Commission (FTC, USA), France (FR), Germany – Federal (DE), Gibraltar (GI), Greece (GR), Guernsey (GG), Hong Kong (HK), Ireland (IE), Italy (IT), Jersey (JE), Lithuania (LT), Mali (ML), Mexico (MX), the Netherlands (NL), Newfoundland (NF, CAN), Peru (PE), Poland (PL), Quebec (Q, CAN), Rheinland Pfalz (RP, DE), Slovakia (SK), Slovenia (SI), Switzerland (CH), Thuringen (TH, DE), Turkey (TR), the United Kingdom (UK) and Uruguay (UY).

Geographically speaking, the respondents are divided as follows:

Europe (European Union)	26 (21)
North-America	5
South-America	3
Oceania	2
Middle East	1
Asia	1
Africa	2

The questions in the questionnaire and the answers given thereto have been attached to the report as an annex: see **Annex I**.

**2.2.2 Observations**

The Working Group observed that 40% of the respondents were unable to enter into binding agreements for enforcement co-operation. This suggests that for many, the development of model contract clauses and bi-lateral or multi-lateral binding agreements would not contribute to enabling greater, or easier cooperation. The Working Group believes that it would benefit from more extensive research into the barriers that members encounter to enforcement cooperation and the extent to

which these can be resolved by contact/agreements or whether it would be better to focus the work of the ICDPPC on alternative tools. For those members seeking more binding commitments, the research and conclusions drawn from Workstream 2.1 on the new Schedule Two to the Global Cross-Border Enforcement Cooperation GCBECA may be a more appropriate starting point.

It was noted that there are already a number of agreements that are in use to facilitate cooperation and it may be that greater availability of copies of those agreements to members would enable authorities to utilise these examples of existing clauses or example agreements.

Furthermore, it was apparent that there is a real diversity of opinion on the oversight mechanism required for legally binding agreements. The feasibility of the suggested mechanisms requires greater consideration by the ICDPPC, should the ICDPPC mandate this, before it would be in a position to put forward model clauses or agreements.

### **2.2.3 Recommendations**

When the Working Group met at The Hague in February 2019, it became clear that the work being undertaken in relation to Workstream 1 could be of considerable assistance in taking this Workstream 2.2 forward. In order to develop the most useful tools for cooperation it is essential to have a true understanding of what members can and cannot share, what the potential barriers are to different types of enforcement cooperation and what tools are already being used to overcome them.

The development of the ICDPPC website, in ways described in Workstream 1 earlier in this report, and the information that will populate the site should enable members to share their relevant legislation, relevant cooperation experiences, current tools and membership of other international organisations/networks such as GPEN. As such, it should be much more transparent across the ICDPPC membership as to what cooperation is lawful in different jurisdictions and what requirements must be met to enable particular types of cooperation.

The Working Group recommends that once the website is fully populated, a mapping exercise is undertaken to identify where the legal impediments lie in relation to enforcement cooperation, whether there are regional restrictions, which countries can rely upon which existing mechanisms and what further tools would benefit which members.

Consideration should be given to extend the scope of the census to gather the necessary data to undertake this mapping exercise.

## **Workstream 2.3: Mutual Legal Assistance Treaty**

### **2.3.1 Introduction**

The objective of this Working Group's Workstream 2.3 is to consider the feasibility of negotiating and drafting an international treaty on enforcement cooperation in the realm of privacy and data protection. This workstream is based on the 2017 Resolution on exploring future options for International Enforcement Cooperation and builds upon the work of the 2016-2017 Group of Experts.<sup>10</sup> After preliminary scoping, this Working Group decided to focus on the creation of a new stand-alone international treaty on international enforcement cooperation in the realm of privacy and data protection, created through either the traditional consensus approach (generally within the auspices of the United Nations), or a 'coalition of the willing' approach.<sup>11</sup>

---

<sup>10</sup> Resolution on exploring future options for International Enforcement Cooperation, Hong Kong: 2017; Final Report 2017.

<sup>11</sup> See in more detail the Final Report 2017.

In order to determine the feasibility of a possible international treaty on enforcement cooperation in the field of privacy and data protection, this Working Group issued a questionnaire, asking the Conference members about their stance towards any such treaty. The answers to these questions were discussed in the Working Group's Face-to-Face meeting in February 2019 and supplemented by practical experiences of negotiating international treaties in other fields of law. This gave the Working Group an impression of the possible benefits, but also the practical drawbacks of concluding international treaties in any field.

In this section of the report, the Working Group outlines the possible benefits of an international treaty (2.3.2), the process surrounding the creation of an international treaty based on members' practical experiences in the past, including a projected timeline for this exercise (2.3.3), the Conference members' general stance towards creating an international treaty at this moment (2.3.4), and recommendations on future steps (2.3.5).

### 2.3.2 Benefits of an international treaty

The conclusion of a multilateral mutual legal assistance treaty potentially holds quite substantial benefits for enforcement cooperation, and ultimately for the ICDPPC membership as a whole, as it may contribute to broadening both the geographic and functional scope of privacy enforcement cooperation, thereby speaking to important aspects of the ICDPPC's Vision and Mission.

More specifically, a multilateral mutual legal assistance treaty negotiated at an international level is potentially beneficial in various ways including, but not limited to:

- **Broad participation**

As noted by the Group of Experts in their Final Report in 2017, similar multilateral international instruments involve broad global participation, some counting over 100 participants. As the ICDPPC counts, at the time of writing, 122 members, the potential enforcement cooperation benefits under a single mutual legal assistance treaty are significant.

- **Wide scope of mutual assistance possibilities**

The Group of Experts, in their review of similar instruments, found a broad range of specific mutual assistance possibilities that are currently unavailable to the majority of the members, or at least for the majority of members on a global cooperation scale, including but not limited to:

- The possibility to **exchange of information** spontaneously or upon request, for unilateral or parallel investigations;
- The possibility to compel the provision of digital, physical and oral **evidence**;
- Possibilities to request/perform **search and seizure**;
- The possibility to share videoconference **testimonies** or investigative statements;
- The possibility to cooperate in **joint investigative teams**;
- The recovery of amounts owing and conserving **assets**;
- The possibility to request/perform **service of documents**; and
- Any **other** type of assistance that is not contrary to the domestic law of the requested State Party

- **Possibility to share personal data**

Besides the possibility to share personal data, a binding international and multilateral mutual legal assistance treaty would allow and provide the conditions for the sharing of **confidential information** between State Parties.

- **The possibility to arrange matters not foreseen in national law**, but still compatible with it. One advantage of international treaties is the circumstance that they potentially may include newer or additional measures than those provided to data protection and privacy supervisory



authorities by their respective national or regional legislation with the effect that the array of means available to those authorities could be amended, as long as these means are in line with principles laid down in applicable regional or national laws.

### 2.3.3 Practical experiences + timeline

Though the potential benefits are manifest, the process of negotiation and conclusion of an international treaty can be quite demanding. Drawing from members' shared practical experiences in the past regarding the conclusion of international treaties, the following aspects must be taken into account before venturing on such a path.

Firstly, the negotiation and conclusion of an international treaty requires the consideration of the following points<sup>12</sup>:

- It must be carefully detailed whether there is an issue that requires a multilateral international solution (whether there is a **weighty and legitimate issue**);
- The issue at stake must be identified, and **defined** precisely and specifically;
- It must be assessed whether an international treaty *can* provide a solution to the issue at hand (whether an international treaty is **suitable**); and
- It must be assessed whether the issue at hand requires an international treaty as a solution and whether there are no other, less burdensome methods available for achieving the same purpose. This means that it must be concluded that existing solutions (existing bi- and multilateral treaties or other instruments such as MOUs or arrangements as the GCBECA) are not sufficiently adequate and that there is a gap in the existing legal instruments (whether an international treaty is **necessary**).

Only when and after these four points have been addressed and the outcome is positive, is it advisable to engage in the process that eventually culminates in the negotiation and drafting of an international treaty.

Secondly, after it has been established that a sufficiently weighty interest warrants and demands the conclusion of an international treaty, a coordinated and planned approach must be determined and agreed on. For international treaties, there are roughly two options as was already remarked above. Both options carry advantages as well as drawbacks.

As to the route of bringing the envisioned treaty under the auspices of the United Nations, the drawbacks are mainly the rather inflexible conditions that must be met in order to successfully bring the creation of the international treaty to its conclusion. This is dependent on bringing the topic under the right body and whether it fits in the then current agenda of the (sub)-committees of the UN. The involvement of the UN Committees will undoubtedly also influence the content of the envisioned treaty. Similar difficulties must be expected when bringing the envisioned treaty under the auspices of other international organisations, such as for example the Council of Europe.

The second option is negotiating the envisioned treaty as a stand-alone treaty. This involves a large assessment of the political and geographical playing field as well as precisely gauging the (amount of) political will and momentum, as the successful conclusion of the envisioned treaty is largely dependent on political support. This is because the parties involved are, as will be elaborated on below, not the individual member authorities of the ICDPPC, but their respective national or regional governments. It is especially this political aspect of negotiating an international treaty that demands a lot of effort and attention. If absent, political will and momentum must be created in each member's

---

<sup>12</sup> I.e. principles of subsidiarity (see, for example, <https://eur-lex.europa.eu/summary/glossary/subsidiarity.html>) and proportionality (see, for example <https://eur-lex.europa.eu/summary/glossary/proportionality.html>).



state by repeatedly reaffirming its importance and getting it on the political agenda through every possible channel. Besides effort, this takes time, resources and capacity.

A general and returning theme in all drawbacks mentioned above, and one that returns in both 'routes', is the handing over and loss of control throughout the entire negotiation process, including its instigation, and the content of the envisioned treaty, from the individual ICDPPC member authorities to national and regional governments that are not necessarily legally obliged to take into account the wishes of member authorities.

In sum, negotiation of an international treaty is a long-term effort that, even in best-case scenarios where the content of the treaty is uncontroversial and largely undisputed, could take up to eight or ten years. It requires the existence of an issue that can only be satisfactorily addressed through an international treaty, a carefully coordinated comprehensive and planned-out approach, and the stamina, both financial and time/capacity-wise, to create the political momentum necessary to commence the negotiation.

#### **2.3.4 Feasibility viewed by ICDPPC members**

In November and December 2018, the Working Group issued a questionnaire to the members of the Conference in order to determine the necessity for further tools for international enforcement cooperation. The questionnaire mainly focussed on legally binding agreements between authorities, but also included references relevant to the creation of an international treaty between governments.<sup>13</sup>

First and foremost, it is important to mention here that a significant number of respondents indicated that it is not possible for them to enter into legally binding arrangements *between authorities* – as is discussed at length in Workstream 2.2 above. For these members, the ability to do so is reserved for their responsible national Ministries or other relevant governmental bodies. This means that even in case of an arrangement *between authorities*, national government may have to be involved.

As international treaties are negotiated *between governments*, a logical follow-up question is whether the Conference members' governments would be open to entering into exploratory talks or negotiations on the creation of an international enforcement cooperation treaty. Given the inevitable involvement of national governments in the negotiation of any treaty, a first practical step is to gauge the governments' priorities at this point. Unfortunately, the majority of the members indicated that they do not have sufficient information to give a conclusive answer to this question. In addition, a number of members indicated that they have a strong indication that their governments would be – at least at this point – unwilling to enter into exploratory talks or negotiations. A small minority of members indicated that it suspected willingness on the side of their governments, and merely two members answered this question in the affirmative. Finally, the questionnaire has not been able to take into account the possible problems that could arise with regard to the position of EU Member States in the negotiation of an international data protection treaty, which is considered as an area of EU institutions', rather than national competence. That means that national governments of EU Member States may not always be in a position to enter into negotiations.

All in all, the Working Group concluded that there are insufficient grounds at this point to conclude that ICDPPC members are ready to approach their governments, and in turn that governments are sufficiently ready to explore the possibility of an international enforcement cooperation treaty. It might be a task for the future to initiate efforts to eventually build up sufficient momentum for

---

<sup>13</sup> See in more detail Chapter 2.2 above.

national governments so that they deem it appropriate and necessary to commence negotiations for an international agreement or treaty on cooperation of data protection and privacy authorities.

### **2.3.5 Recommendations on future steps**

Based on the elements outlined above, the Working Group concludes that there is insufficient support at this time to take first concrete steps towards the creation of an international enforcement cooperation treaty. Even though the potential advantages of such a treaty are clear, it appears that the overwhelming majority of members consulted so far find that the practicalities involved in its creation seem to strongly outweigh any benefits at this point. In particular, the Working Group has noticed a lack of willingness or ability to provide a long-term commitment from Conference members towards creating content that would help their respective governments to negotiate any such treaty – especially since the precise requirements have not yet fully crystallized.

For these reasons, the Working Group recommends:

- to pause the work on Workstream 2.3 in favour of pursuing the work as outlined in Workstream 2.2 above;
- to host any future work on this workstream in the to-be created Permanent Working Group on International Enforcement Cooperation, or other Working Group as may be mandated by the Conference; and
- to propose to re-open discussions on this topic after the members' own capacity to enter into cooperation arrangements has been fully explored, provided that this has the new Working Group's full commitment.

## Conclusions

The Working Group was created on the basis of the 2017 Resolution on exploring future options for International Enforcement Cooperation. In 2018, the Working Group presented its progress at the 40<sup>th</sup> Conference in Brussels. As mandated, this final report presents the work of the Working Group to the 41<sup>st</sup> Conference in Tirana and proposes recommendations for future work. Following the mandate 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*”, the Working Group divided the scope of the mandate into two separate workstreams; one to propose **practical solutions** for better cooperation and knowledge-sharing on the topic, and one to work on **legal solutions** to frame international enforcement cooperation.

Workstream 1 on practical solutions was subdivided into two sub-streams, the first of which (Workstream 1.1) focussed on the design and implementation of a permanent and easily accessible **repository** that links to enforcement cooperation-related resources on the ICDPPC website. The Working Group found that the repository is to take the form of a database that provides links to, on the one hand, non-confidential, publicly available information contributed by members, and on the other hand links to relevant materials, resources and tools that are available through the Conference and other networks, including an advanced search option. The input shall be published monthly with an option to subscribe to an RSS-feed, and is to be gathered from members of the Conference, where appropriate including a translated title and short summary in English. The Working Group proposes the presentation of a Resolution to the 41<sup>st</sup> Conference in which commitment is pronounced towards 1) promoting the repository, 2) keeping the repository a living instrument, and 3) creating and supporting a small dedicated team or task force that will be tasked with the maintenance of the repository and the monitoring of contributions.

The second sub-stream (Workstream 1.2) focussed on the creation and population of a **database** about member **authorities**, their contact details, their legal powers to cooperate, evidence-gathering requirements and definitions of personal data and confidential information, possibly in tandem with the development of an online secure space. Taking into account *inter alia* the work done by the Future of the Conference Working Group on the costs and benefits (among which, importantly, the possibility to share confidential information) of such a secure space, the possibility of collaboration with GPEN to use the existing GPEN secure website, and the existing need for sharing confidential or non-public information, the Working Group favoured an approach in which steps are taken towards a public, non-secure Authorities Database first. That said, should the Future of the Conference Working Group recommend that a secure space for Conference members can be implemented swiftly and easily, the advantages of having more detailed information on all member authorities may merit the transfer of an Authorities Database in the public space into the restricted part of the website.

Workstream 2 focussed on potential future enforcement cooperation projects and was also subdivided, this time into three sub-streams. The first sub-stream (Workstream 2.1) concerns the possible expansion of the existing GCBECA via the addition of a possible ‘Schedule 2’. A suggestion for such a Schedule was discussed in the February 2019 Face-to-Face meeting in the Hague, which would be a parallel but legally binding version of the existing GCBECA. After review, the Working Group recommends that the Schedule requires additional revision and that it should be regarded as an optional piece that can be adapted according to individual members’ needs. To further the work on the Schedule, future steps could include a mapping exercise to find out which provisions cause difficulties and what kind of arrangements would best suits members’ needs, but also the possible creation of a permanent Working Group on Enforcement Cooperation to keep the GCBECA under review and a sought opinion on the proposed Article 11 of Schedule 2 from the CoE and EDPB.

The second sub-stream (Workstream 2.2) considered the possibility of producing a set of model contract clauses or model bilateral or multilateral agreements to be used by authorities that wish to cooperate. To that end, the Working Group circulated a questionnaire that, given the range of activities that could fall under privacy enforcement cooperation, sought to clarify the variety of national requirements that are provided for such cooperation activities and to assist in finding the best possible work product. As one of the main results from the questionnaire it was found that many of the respondents are unable to enter into binding agreements for enforcement cooperation and that hence, model clauses or bilateral or multilateral agreements would not necessarily contribute to facilitating easier cooperation. For those seeking a legally binding solution, other instruments are already available such as the proposed Schedule 2 to the GCBECA. The Working Group suggests that the development of the ICDPPC website according to the suggestions made under Workstream 1 could aid in enabling members to determine what sorts of cooperation could be sought with other members and the requirements for such cooperation. Additionally, after completion of the website, a mapping exercise could be undertaken to identify the legal impediments related to enforcement cooperation. A possible vessel to consider for this exercise is the annual census, which could be extended accordingly.

The final sub-stream (Workstream 2.3) considered the feasibility of negotiating and drafting an international treaty on enforcement cooperation in the realm of privacy and data protection (a mutual legal assistance treaty). Though the benefits are potentially substantial, including possibilities to exchange confidential information, personal data and/or evidence and possibilities to request the performance of other cooperation activities, the negotiation of an international treaty is a long-term effort that requires a careful coordinated comprehensive approach and stamina in both financial and time/capacity terms to create the necessary political momentum. Besides that, the questionnaire that was circulated in the context of this workstream has provided strong indications that there is, at least at present, insufficient ground to conclude that ICDPPC members are ready to approach their governments and explore the negotiation of an international treaty. The Working Group hence recommends that the work under this sub-stream is paused in favour of the sub-stream 2.2 and that any future steps in this field, including the full exploration of members' capacity to enter into binding cooperation agreements, are taken under the proposed Permanent Working Group on International Enforcement Cooperation or other Working Groups as mandated by the Conference.

## Way forward

Considering the above, the Working Group recommends the following steps for a way forward:

- To pause the Working Group after the completion of its mandate in October 2019;
- To propose to the Conference the creation of a permanent Working Group on International Enforcement Cooperation;
- To issue a call to the Conference for members and (new) co-chairs for the suggested Permanent Working Group;
- To further promote the existing Global Cross-Border Enforcement Cooperation Arrangement (GCBECA) to new members of the Conference;
- To present for discussion and eventual adoption to the 41<sup>st</sup> Conference in Tirana, Albania a resolution that expresses commitment to supporting, maintaining and promoting the repository on the Conference website, that recommends a way forward for an Authorities Database, and that invites the Conference members to take note of the work done by the Working Group in the context of Workstream 2 and to use the output at national level for further work as each member deems appropriate to their needs.

## **Annex 1: Global Cross Border Enforcement Cooperation Arrangement (GCBECA) – Optional Schedule 2**

The following document is a suggestion for an amended version of the GCBECA, drawing on the conclusions from the recent work of the Council of Europe (CoE) and insight from the developing work of a Working Group on International Transfers within the then Article 29 Working Party [now EDPB]. It would be a parallel but legally binding version of the existing GCBECA.

After review, the Working Group recommends that the Schedule requires additional revision and that it should be regarded as an *optional* piece that can be adapted according to individual members' needs. Additionally, future steps could include a mapping exercise to find out which provisions cause difficulties and what kind of arrangements would best suits members' needs.

The updates proposed to the GCBECA form part of the full package of documents summarising the work done by the Working Group and are submitted to the 41st Conference in Tirana for consideration. The GCBECA as it is, with the revised Schedule One, remains available to all Conference members and the Working Group heartily welcomes and encourages other and new members to participate.

Please see separate PDF document: *Annex Workstream 21 Schedule 2 to the GCBECA and Explanatory Text*.

## Annex 2: Questionnaire relating to Workstream 2.2

Questionnaire

### Question 1

**What enforcement cooperation activities are you currently able to carry out and which of these could involve the sharing of personal data?**

The first question was answered by all respondents.

All EU Member States differentiate between intra-EU cooperation and international cooperation. For all 21 EU-respondents, the following holds true:

The GDPR, Chapter VII in particular, contains provisions pertaining to cooperation highlighting enforcement cooperation in cross-border cases, allowing EU Member States to exchange information (including information containing personal data) if necessary in all other cases.

The GDPR furthermore stimulates EU Member States to develop international cooperation mechanisms, provide international mutual assistance (including complaint referral, investigative assistance and information exchange), engage in activities furthering international cooperation and exchange personal data protection legislation and practice (Article 50 GDPR).

In the table below, only the possibilities for international cooperation (outside the EU) is included for the EU Member States, as the envisaged cooperation tools should not be limited to specific geographical areas. These possibilities are marked with 'EU' and counted as 22 respondents. Where EU Member States have listed specific other options, they are included separately.

Membership of an international organisation promoting cooperation	All	40
Training and workshops (including exchange of personnel)	EU, AL, BA, CA, EDPS	25
Sharing general information (including exchange of best practices)	EU, AL, AU, EDPS, HK, ML, MX, CH, OVIC, FTC, UY, BF	33
Memoranda of Understanding <sup>14</sup>	IT, NL, UK, PE	4
Coordinated compliance sweep	EU, CA, EDPS	23
Mutual assistance (in specific cases)	EU, AL, EDPS, HK, MX, FTC, GG, UY, Q	30
Joint investigations	AU, FTC	2

6/40 indicated that even though they may be competent to engage in such enforcement cooperation activities, they have not yet used any tools to do so (CT, HR, EE, GI, GG, TH), 2 indicated they have no specific competences, other than membership to the ICDPPC (NF, TR) and 1/40 respondent referenced 'various tools' without further specifying which tools could be used (Jersey). Q indicated that although it cooperates with the Federal government of Canada and other provinces, at present there are no international enforcement operations outside Canada.

<sup>14</sup> Questions 6, 7 and 13 below give a more precise overview of the number of agreements concluded among the respondents.

1/40 respondents referenced that legislation only provides for the sharing/disclosing of personal information necessary to conduct an investigation, audit or inquiry (British Columbia)

## **Question 2**

### **Do these enforcement cooperation activities include personal data?**

The second question was answered by 39/40 respondents with 2/39 indicating that this question was not applicable to them, as they do not engage in enforcement cooperation activities (NF, TR).

2/37 referenced the "One Stop Shop" mechanism and highlighted that the exchange of personal data is through the Internal Market Information System (IMI) (AT, IE).

33/37 indicated that – to some extent – personal data may be shared when carrying out the enforcement cooperation activities, subject to legal limitations.<sup>15</sup> Switzerland furthermore indicated not to have shared personal data outside the Schengen area before, and the United Kingdom specified which types of enforcement cooperation activities could necessitate the sharing of personal data.

3/37 respondents indicated that their enforcement cooperation activities do not necessitate sharing personal data, or only to a very limited extent (e.g. names of participants in workshops) (AU, DE<sup>16</sup>, BA).

1/37 respondent indicated not to be able to share personal data in international enforcement cooperation.

## **Question 3**

### **What is the basis upon which these activities can be carried out, i.e. does there need to be a specific agreement in place for each type of activity?**

38/40 respondents answered this question (EE indicated that it was 'not able to answer'). 2 indicated that this question was not applicable to them (NF, MX) and 1 answer was unclear and therefore not included in the analysis below.

The vast majority of respondents, 27 in total, explained that national or regional law provides the legal basis for enforcement cooperation, and that – in principle – no specific agreement is needed (AL, AU, AT, ASV, BA, BG, CT, HR, EDPS, FR, DE, GR, GI, GG, HK, IT, LT, NL, PE, RP, OIPC, SK, CH, UK, SI, TH, BF). BF noted that in the case of a subsidiary or branch of a foreign company and where there is a transfer of management information, which includes personal data or data relating to the private life of individuals, it would be appropriate to conclude an agreement

However, 13 respondents specifically mentioned that an agreement would be necessary to meet the legal requirements for the transfer of personal data, in case this takes place in the context of international enforcement cooperation (AT, CYP, EDPS, FR, FTC, HK, IE, IT ML, PL, NL, SI, UY). Even though this was not mentioned specifically by all EU Member States, this is true under the GDPR as well.<sup>17</sup>

---

<sup>15</sup> See question 5 below.

<sup>16</sup> Germany included that enforcement cooperation activities can be conducted with sharing non-personal information (only) as well.

<sup>17</sup> Excluding EE, which is part of the EU, but is not included in the analysis as it was unable to answer.

3/38 respondents indicated the need for a specific agreement when entering into international enforcement cooperation (CA, TR<sup>18</sup>, Q)

1 respondent (UK) highlighted that enforcement cooperation may be supported by high-level international agreements.

**Question 4**  
**If a specific agreement is required, does this need to be legally binding?**

Under half of the respondents answered this question. Of the 15 non-respondents, 8 provided no answer (AT, CT, EDPS, LT, RP, SK, CH, TR), 5 indicated that this question was not applicable to them ( OIPC, GR, Jersey, NF, TH) and 1 mentioned that it was unable to answer this question (EE).

Additionally, 3 answers were unclear and are not included in this analysis.

For the remaining members (22), the interpretation of the question varied quite a bit, indicating that the question may have been unclear in the light of the foregoing.

- 5/22 reiterated that a specific agreement is generally not required (AU, IE, UK, FTC, PE)
- 11/22 indicated that if an agreement were necessary, a legally binding instrument could be used to increase certain safeguards, but not necessary in all instances (ASV, BG, HR, FR, CYP, GI, HK, IT, NL, PL, UY)
- 5/22 indicated that a legally binding agreement would be necessary (DE, ML, MX, SL, BF).
- 1/22 indicated that – regardless of preference – it would not be able to enter into a legally binding agreement (CA)
- 1 indicated that the individually negotiated agreements were not legally binding (Q)

**Question 5**  
**Are there specific rules for the transfer of personal data to other jurisdictions?**

This question was answered by all members. 3/40 answers were unclear or unspecified, and are therefore not included in the analysis below.

For the EU Member States that answered this question the general rules on transfer of personal data are the same. Transfers of personal data to non-EU countries must be subject to appropriate safeguards (Article 46 GDPR). Such appropriate safeguards could be constructed through a legally binding and enforceable instrument between public authorities or bodies (Article 46(2)(a) GDPR), or provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights (Article 46(3)(b) GDPR). This is only necessary in absence of an adequacy decision from the European Commission. Where applicable, these options are marked with 'EU' and counted as 21 respondents.<sup>19</sup>

Authority in receiving state must ensure an 'adequate level of data protection'.	AL, AU, ASV, BG, EU, HK, CH, OIPC, GG, ML, PE	31
Authorised by an international agreement (legally binding or with enforceable data protection rights)	AU, BA, MX, FTC (EU)	4 (21)

<sup>18</sup> Note that TR indicated under Q1 not to have any tools at its disposal.  
<sup>19</sup> Would be 22, but LT did not respond to this question. The number 21 is maintained, even though BG,HR and CYP indicated that there are no specific rules for international transfers. This may have meant additional to the GDPR.



Pursuant to a written arrangement including sufficient safeguards	CA, CH, FTC, ML, PE, UY, Q	6
With the data subject's consent	AU, BA, MX, CH, PE	5
On another lawful basis for processing of personal data	BA, MX	2

1/37 respondent indicated it did not transfer personal data as a general rule (GR).

1/37 respondents highlighted the role of Convention 108, which indicates in Article 12 that "a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation trans-border flows of personal data going to the territory of another Party." (MX)

### Question 6

#### **Do you already have agreements or clauses in place that are used to enable enforcement cooperation?**

This question was answered by 39/40 members (except SK). 2 answers were unspecified, and are therefore not included in the analysis below (GG, Jersey).

17/37 members indicated they do not have agreements in place to enable cooperation (AT, BG, CT, CYP, HR, EDPS, EE, GR, LT, MX, NF PE, PL, RP, CH, TH, TR). PL indicated that the Polish supervisory authority had not yet entered into any such agreement and TR specified that it can interact with international organisations, but not with authorities from other jurisdictions.

Bi-lateral agreements for specific cases (MOU/NDA)	NL <sup>20</sup> , SL, FTC, ML <sup>21</sup> , BF, Q	5
General bi-lateral agreements (MOUs)	AL, AT, AU, BA, CA, IE, IT, DE, NL, OIPC, UK, UY	12
Global Cross Border Enforcement Cooperation GCBECA	AU, CA, DE, FR, GI, HK, OIPC. UK	8
Asia-Pacific Economic Cooperation Cross Border Privacy Enforcement GCBECA	AU, ASV, HK	3
Global Privacy Enforcement Network MOU	AU, OIPC, UK	3
UCENet MOU	CA	1
Data Security and Minimum Safeguards Certification for the GPEN Alert Tool	UK	1

### Question 7

#### **If so, are these agreements or clauses specific to the activity or more general?**

This question was answered by 30/40 respondents, although 7 of these answers were stating that the question was either not applicable to them, or they were unable to answer. Note that this question is dependent on the answer given under question 6. 1/30 answers was unspecified, and is therefore not included in the analysis below (Jersey). 1/30 answers referred to a previous answer, where they stated they had yet to define an approach, and is also not included below (Guernsey).

<sup>20</sup> As NL indicated to have concluded such an agreement with AU, AU could be included here as well.

<sup>21</sup> ML indicated to have signed a Cooperation Protocol with the IT Commission of Burkina Faso (CIL) which deals with mutual information and consultation in addition to cooperation on the handling of complaints and investigations.

Specific to the activity	AL, SL	2
General	ASV, AT, AU, BA, FTC, FR, GI, HK, IE, IT, TR <sup>22</sup> , UK, UY, BK	14
Both (depending on the agreement)	BC, CA, DE, ML, NL.	5

### Question 8

**Do you have the ability in you national (or regional/local) law to enter binding arrangements? (or is this ability reserved for your national ministry/relevant government department?)**

This question was answered by all respondents. 3 respondents stated that they were able to enter binding agreements but needed final approval from government/parliament and are also not included (FTC, GG, UY)

Yes (but limited to other privacy authorities)	ASV, BG, IE, Jersey, OIPC, PE, RP, TH, BF, GI (AL, BA, HK <sup>23</sup> , MX, SL)	10 (5)
Unclear (but possibly yes, if limited to other privacy authorities)	AT, DE, EE, PL (NL, UK)	4 (2)
No	AU, CA, CT, CY, HR, EDPS, FR, GR, IT, LT, ML, NF, SK, CH, TR, Q	16

This overview suggests that 40% of the members (16/40) are not able to enter into a binding arrangement – against 15/40 members who can. For 6 members, this is still uncertain.

### Question 9

**Are there any specific elements that must be included in any agreement or arrangements for enforcement cooperation, for example, protection for individuals' rights, purpose limitation, redress and remedies, retention, oversight?**

This question was answered by 38/40 members. Out of these, 4 specifically mentioned that this question was not applicable to them (e.g. because they cannot enter into arrangements) or that they could answer it. One of the answers was unspecified, and is therefore not included in the analysis below (Jersey).

For the respondents from EU Member States, there was consensus that such agreements or arrangements should comply with the GDPR, and therefore should – at least – include enforceable data subjects' rights (17). Data subject rights were furthermore mentioned by AT and AL specifically, and implied in the answers from, GG (which refers to the needs for safeguards for the protection of personal data and the "significant interests of data subjects"), DE, HK and CH (mentioning adequate protection and basic data protection principles), whilst UY referred to respecting "data protection public order"). Further, the FTC stated that agreements were limited to those that provide assistance, share information or engage in further cooperation and protect material from disclosure.

Other specific elements mentioned were:

Legal basis (AL, CH)

<sup>22</sup> Though TR indicated under question 6 not to have any agreements in place.

<sup>23</sup> HK specifies that this is except reciprocal juridical assistance.

Security measures (AL, HK, BF)  
 Confidentiality provisions (AL, CA, HK)  
 Purpose limitation (CA, AL, CH, BF)  
 Practical aspects (scope, form, content, etc.) (MX)  
 Legislation limiting or prohibition the publishing information about an ongoing investigation (CY)  
 Retention – (BF)  
 Redress – (BF)

Other respondents stated they did not have any specific elements that must be included in agreements or arrangements. They were:

ASV

OIPC (agreements refer to these matters but they are not formally required)

PE

Q (but they usually include a confidentiality clause)

### Question 10

**Are there any circumstances in which you would be required by virtue of legislative or professional obligations to make information you had received available to any other body?**

38/40 members responded although 2 said they could not answer the question (EE, and Jersey who indicated it would be a case by case decision). 4/38 confirmed there were circumstances in which they would have to disclose the information but gave no further detail (ASV, LT, SK,TR). 6/38 indicated they were not obliged to disclose the information (OIPC, CY, GG (but it does have discretion), MX, NF, Q).

DE indicated that it would have to disclose in the event of extremely serious crimes or international terrorism but noted that EU legislation and judicial decisions are very strict in this regard and BF indicated it would have to disclose for national security and defence but neither specified to whom the disclosure would be made.

Some of the respondents from EU Member States commented that under GDPR a supervisory authority is bound to share “relevant information” to implement and apply the regulation and the one stop shop mechanism might require sharing. The remaining responses are set out below;

Freedom of information or other access to information legislation	AU, CA, EDPS, FTC, NL, PE, PL, RP, SI, TH, UK	11/38
Disclosure to courts in certain circumstances	AL, AT, BG, CT, GR, PL, SI, GI	8/38
Disclosure to prosecutors	AL, AT, HR, FR, GR, ML	6/38
Disclosures to police or law enforcement authorities	AL, AT, HR, IT, PL, SF, UK, GI	8/38
Disclosures to anti-fraud office	EDPS	1/38
Disclosures for official auditing	EDPS	1/38
Disclosures to legislature	FTC, HK	2/38
Disclosures to EDPS/Commission	GI (although this would apply to others)	1/38
Disclosure pursuant to a court order or international legal instrument	IE, FTC, UK, UY	4/38

## Question 11

### **What oversight mechanism would you propose for the monitoring of compliance with any legally binding agreement?**

This question was answered by 38/40 respondents. For one of these respondents (AU), this is due to the fact that it cannot enter into legally binding arrangements. Additionally, 9/20 of the answers were unclear, unspecified, or "N/A" and therefore not included in the analysis below (AL, ASV, CY, GR, NF, RP, FTC, GG, Q).

In order to make use of the specific suggestions made by the responding members, the answers are only grouped together if they seemed exactly the same. That being said, the remaining respondents suggested the following solutions:

#### Internal oversight mechanism preferred

Generally, agreements themselves call for review and renewal and parties may terminate if not satisfied (OIPC)

Monitoring by signatory authorities (BG, CT, GI, IT, CH24, TH)

Monitoring by an ad-hoc committee, formed by the ICDPPC (IT, Jersey, NL, UK)

Taskforce to handle complaints about non-compliance, formed by the ICDPPC (HK)

Internal DPO (EDPS)

Panel of experts, unclear whether internally or externally (MX, SL)

Rely on the 4-eyes-principles of the Data Protection Act (that a transfer or "mutual assistance") request must be aligned with the head of the authority, and that internal procedures within the authority ensure that if a complaint is filed, proceedings are not performed by the same department in which the infringement is alleged (AIDPA)

Peer review and self-reports (UY)

Periodic compliance reports (PE)

Internal supervisory entity (ML)

Regular review and/or joint panel, that can handle complaints and discuss any issues arising among participants (unclear whether internally or externally) (DE)

#### External oversight mechanism

Consult policy experts, academics, data protection and regulatory specialists and international cross border law enforcement groups (IE)

Externally independent authority or body (HR, LT, SK)

Redress mechanism for data subjects before a judicial body (EDPS)

Supervising the supervisors through ad-hoc mechanisms (EDPS)

International organisation for dispute resolution and conflict management (NL, TR)

Legal means (PL)

## Question 12

### **Would your government be open to entering into exploratory talks or negotiations on the creation of an interim enforcement co-operation treaty with other governments?**

This question is analysed in this report to the Conference, featured in section 2.2.1 in relation to Workstream 2.3.

---

<sup>24</sup> CH specified that this could be done by including a checklist in the agreement/arrangement.