Last Updated and Presented at the 43rd Global Privacy Assembly, Mexico City, October 18 – 21, 2021

Originally Presented at the 37th International Conference of Data Protection and Privacy Commissioners, Amsterdam, October 26 – 29, 2015.

# AN ENFORCEMENT COOPERATION HANDBOOK

**PREPARED BY:**
**Office of the Privacy Commissioner of Canada and**
**The UK Information Commissioner's Office**

**WITH THE SUPPORT OF:**
**The Colombia Superintendencia de Industria y Comercio and**
**Jersey Office of The Information Commissioner**

GPA
Global Privacy Assembly

# Table of Contents


Introduction ..... 4

Cross-regulatory collaboration ..... 5

The benefits of enforcement cooperation ..... 7

Cooperation regarding emerging events and strategic trends ..... 8

Major events - COVID-19 ..... 8

Strategic trends - facial recognition technology ..... 9

Strategic trends – the digital economy is accelerating instances of regulatory overlap ..... 9

Laying the foundation for cooperation ..... 11

Developing Enforcement Cooperation Relationships ..... 11

Information-sharing arrangements ..... 13

Enforcement cooperation protocols and training ..... 17

Identifying and evaluating opportunities for cooperation ..... 18

Contacting potential partners ..... 18

Enforcement Cooperation Model ..... 21

A model of enforcement cooperation ..... 22

Choosing the appropriate form of enforcement cooperation ..... 23

Sharing non-confidential information and experience (Item 1) ..... 23

Coordinated compliance action (Item 2) ..... 24

Confidential Information or Personal Data Sharing and Assistance (Item 3) ..... 29

Collaborative investigations (Item 4) ..... 31

Conclusion ..... 47

APPENDIX A ..... 48

Global Cross Border Enforcement Cooperation Arrangement ..... 48

APPENDIX B ..... 61

MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES FEDERAL TRADE COMMISSION AND THE DUTCH DATA PROTECTION AUTHORITY ON MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR ..... 61

MEMORANDUM OF UNDERSTANDING BETWEEN THE PRIVACY COMMISSIONER OF CANADA AND THE INFORMATION COMMISSIONER OF THE UNITED KINGDOM ON MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR ..... 71

MEMORANDO DE ENTENDIMIENTO ENTRE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DEL REINO DE ESPAÑA..... 76

APPENDIX C ..... 84

Letter to operators of the Insecam website ..... 84

Data protection authorities urge Google to address Google Glass concerns ..... 86

APPENDIX D ..... 89

Enforcement Cooperation Reference Tool ..... 89

APPENDIX E ..... 91

Example template for authorities to use when developing their own mechanisms for consideration of international enforcement cooperation ..... 91

Example Template Joint or Coordinated Investigation Plan ..... 94

Milestones ..... 99

Glossary ..... 100

# Introduction

The 2014 International Conference of Data Protection and Privacy Commissioners'[1] Global Cross Border Enforcement Cooperation Arrangement (the Arrangement) represented a milestone global statement of intent to cooperate among privacy enforcement authorities[2], and provided a visionary framework for achieving this.

This handbook was originally created as a tool to assist authorities in taking their first steps to participate in the Arrangement and pursue new avenues of collaboration. Since those early days, global enforcement cooperation on privacy has steadily increased and provided many benefits, many of which will be illustrated in this document. Given the developments and advancements in this space, the International Enforcement Cooperation Working Group (IEWG) has worked to gather and share the lessons learned by various authorities to provide a guide to support and promote future cooperation and greater global engagement on problematic behaviour relevant to privacy and data protection.

Based on input received from various authorities, this new revision of the handbook focuses on the practical elements of cooperation and brings together, as points of reference, examples and case studies of enforcement cooperation activities that have taken place over the last few years.

This handbook is not intended to be instructional or prescriptive. It is up to each Authority to determine how it wishes to participate in, and leverage the benefits of, enforcement cooperation. Rather, it is intended to provide guidance that may assist authorities wishing to engage in enforcement cooperation, including:

- a non-exhaustive list of issues an Authority may face in preparing for, and engaging in, enforcement cooperation
- potential models, approaches and solutions that authorities can consider implementing to address such issues
- factors to consider in determining what, if any, proposed strategies may be appropriate in specific circumstances

[1] Now the Global Privacy Assembly

[2] The term 'privacy enforcement authorities' also encompasses data protection authorities for the purposes of this handbook. Similarly, the notion of privacy shall be understood to also encompass data protection.

Authorities should always remain flexible and innovative in applying the approaches outlined in this handbook. Each set of circumstances (for example, relevant authorities, legislation, issues, parties to a case, etc.) will require a unique approach, potentially a hybrid of the approaches detailed in this handbook, or even a completely different and novel approach not contemplated in this handbook.

The handbook is legislatively neutral, recognizing that the wide variety of laws and national policies in place today would be difficult to address in this document.

# Cross-regulatory collaboration

Data is at the centre of our digital economy and does not conform to regulatory or geographic boundaries. This is reflected in the growing focus on intersection issues taking shape in the form of new laws and regulations, policy initiatives, inquiries and increased enforcement action by authorities across regulatory spheres. While cooperation in the privacy space has become increasingly common and well-developed, cross-regulatory cooperation, particularly with competition authorities, is in its nascent stages.

In collaboration with the GPA's Digital Citizen and Consumer Working Group (DCCWG), the handbook has therefore been expanded to highlight and support cross-regulatory cooperation. Cooperation between privacy enforcement authorities and other regulators can provide new and valuable avenues to address problematic behaviour in a holistic manner. For instance, privacy issues can often intersect with competition and consumer protection issues in new and complex ways as highlighted in the DCCWG's 2019 and 2021 annual reports.

Cooperation in this area is particularly important and timely as we see the emergence and morphing of data-driven business models that leverage personal information and data in novel ways, integrating it at every level of the commercial process. A mapping table containing examples of intersection activities can be found in the DCCWG's 2021 annual report.

Recent efforts by the GPA, the Global Privacy Enforcement Network (GPEN) and the International Consumer Protection and Enforcement Network (ICPEN) have underscored this need through workshops focusing on cross-regulatory enforcement activities and the practical experiences of various authorities. The 2019 GPEN practitioner's workshop, co-hosted by and the Office Personal Data Protection, Macao, China and the Privacy Commissioner for Personal Data, Hong Kong, China explored joint activities, strategies to address cross-regulatory challenges, and examples of best practices.

These matters were further discussed that same year at the Digital Clearinghouse, a forum initiated by the European Data Protection Supervisor. Takeaways from these discussions can be found in the DCCWG's 2019 annual report in Appendices E and F, and include the following:

- There is an increasing overlap between cross-regulatory authorities, either with respect to jurisdiction, common legal or practical issues concerning data protection, or unfair trade practices, where multiple authorities will be engaged[3]
- There is substantial cross-regulatory collaboration on a policy level, which can be leveraged as a foundation for future enforcement cooperation

- In a number of cases, DPA's and other regulators have participated in public consultations together

- Understanding of the intersection between privacy and other regulatory spheres, and development of strategies for cross-regulatory enforcement collaboration, are still in their early stages, but expanding

- A notable recurring theme is increased cooperation between DPA's and authorities responsible for addressing cybercrime and cybersecurity, with a number of examples of cooperation with the police

- Relationship building and having designated points of contact between authorities is of critical importance

    - Trust and rapport between points of contact can sometimes make a substantial difference in creating conditions favourable to collaboration

Additionally, in February 2021, during an ICPEN/GPEN best practices workshop, privacy and consumer protection enforcement professionals from across the globe discussed a hypothetical case study involving issues of potential regulatory intersection, and the potential for cross-regulatory cooperation. Participants recognized the substantial intersection and complementarity between their 2 regulatory spheres, and the potential for mutually beneficial collaboration in this area.

More specifically, participants identified the need for privacy and consumer protection authorities to find opportunities to work together and develop the partnerships that could serve as the foundation for enforcement cooperation in future. More information on this session can be found in the upcoming 2021 GPEN annual report.

As data and personal information continue to take on greater importance in competitive assessments, and affect consumer rights, gaining a better understanding of how to approach, and improve, cross-regulatory cooperation will become an increasingly pressing issue. This handbook considers cross-regulatory collaboration through each facet of the cooperative process, and leverages the recent work of a variety of authorities and the DCCWG to present tools, methods, examples and case studies, thus equipping authorities considering cross-regulatory work.

[3] Examples include, but are not limited to: data breaches, e-commerce, tech mergers, telemarketing, spam and unfair trade practices related to personal data (particularly in the context of tech companies).

# The benefits of enforcement cooperation

Increasingly, organizations that process personal data have a multinational presence, both physically and within the realm of digital commerce. The fluidity and frequency of cross-border information flows has rendered international enforcement cooperation a necessary tool in promoting privacy rights both globally and domestically. In its truest sense, enforcement cooperation can be an efficiency-enhancing and capacity-expanding exercise. The independence of privacy enforcement authorities can also stand to benefit by bolstering cooperation with other regulators to assist in weathering budgetary challenges, and buffering the tides of political pressures at the national level. As enforcement cooperation has become more common, the benefits of cooperation continue to be borne out:

- authorities can achieve results more efficiently via one coordinated investigation or enforcement action, rather than through multiple, duplicative proceedings

- by working together, authorities can leverage their cumulative weight and comparative strengths to achieve a more impactful result, even across regulatory spheres, in their enforcement activities than they could individually

- through information sharing and investigative assistance, authorities may be able to pursue or facilitate enforcement action or investigations that involve activities outside their own individual borders

- during the process of cooperation, each Authority is able to learn from the others' knowledge and experience, thus augmenting individual and collective expertise

- authorities may be able to leverage different time zones to increase productivity, in some cases achieving almost around-the-clock coverage and allowing significantly more work to be accomplished in a short timeline

- since data does not conform to regulatory boundaries, working with cross-regulatory counterparts can advance the objectives of both regimes without sacrificing either

- the global privacy enforcement community is sending a message to organisations processing personal data, as well as to individuals worldwide, that we are coordinated, and committed to a global response to global privacy risks

# Cooperation regarding emerging events and strategic trends

Recent developments have illustrated the viability of collaboration for authorities in relation to major events and general trends of global importance. These significant collaborative activities have helped establish expectations of multilateral action, and lay the foundation for enforcement cooperation. The following events and trends are but a few that demonstrate the importance and effectiveness of a global response to emerging issues and trends:

## Major events - COVID-19

The COVID-19 pandemic introduced significant privacy and data protection challenges for authorities around the world as governments and commercial organizations were forced to rapidly adapt to the new global reality. Personal data became critical for health initiatives such as contact tracing, outbreak response and vaccination management, as well as for other changes associated with the pandemic, such as online schooling and a large-scale shift to remote work.[4]

The privacy issues related to COVID-19 were so acute that the GPA Executive Committee convened an extraordinary meeting in April 2020 to address them. In response to this challenge, the GPA formed the COVID-19 Taskforce 2020, with membership from authorities from around the world. This international task force analysed and reported on the issues related to COVID-19, produced a compendium of best practices and supported the GPA's Resolution on the Privacy and Data Protection Challenges arising from the COVID-19 Pandemic. This global approach allowed authorities to address COVID-19-related privacy issues in a united, holistic way, leveraged global talent and resources, allowed members to freely share expertise and supported the development of strong relationships between authorities.

Similarly, GPEN conducted 2 initiatives examining COVID-19 implications for privacy enforcement. The 2020 GPEN sweep focused on whether COVID-19 initiatives and solutions implemented by governments and private sector organizations around the world had adequately considered privacy, while a parallel GPEN initiative called resetting privacy, led by the U.K. Information Commissioners' Office (ICO) and supported by 27 authorities, examined the pandemic's impacts on privacy and consumer protection authorities' regulatory and enforcement activities.

[4] For an example of a joint initiative on the topic of remote work, please see the Case Study on page 24.

# Strategic trends - facial recognition technology

Facial recognition technologies (FRT) present a significant strategic privacy issue for authorities across the world. FRT uses biometric information, widely considered to be inherently sensitive, and its core purpose of identification introduces a number of privacy concerns. Use of FRT is becoming increasingly common, and is relied upon by a variety of organizations across the globe, ranging from national security and law enforcement to commercial organizations offering or using identification and authentication services.

In response to the rapidly increasing use of FRT, the GPA adopted a resolution on facial recognition technology, recognizing the usefulness and value of FRT, but also the globally significant risks and concerns surrounding it. To analyze and take action on the issue, the IEWG and the Working Group on Ethics and Data Protection in Artificial Intelligence (AIWG) jointly assembled the Facial Recognition Technology Working Group (FRTWG), an international group of authorities with interest in the issue. To help ensure that personal information and privacy are adequately protected, the working group's mandate includes:

- considering the risks of FRT
- providing recommendations to mitigate those risks
- developing and promoting a set of principles and expectations that technology developers and users around the world should abide by

Work on this matter is ongoing as of the time of this publication, and more details will be available on the GPA website when the FRTWG annual report is released. In addition to the FRTWG, the IEWG has conducted a number of collaborative sessions devoted to FRT, as well as specific FRT investigations. In these sessions, a variety of authorities have learned about and shared insights and information regarding FRT.

# Strategic trends – the digital economy is accelerating instances of regulatory overlap

The digital economy has thrust the privacy, competition and consumer protection regulatory spheres together in ways not previously explored or fully understood. These intersections present many regulatory complements as tensions. Arguably, all authorities, regardless of regime, find themselves at an inflection point on the way forward, as they develop strategies on how best to address regulatory intersections. Such challenges and dynamism have come into sharper focus in 2020/21 owing to the pandemic, which has driven increased consumer, business and societal reliance on all things digital.

Instances of regulatory overlap are likely to increase in both number and complexity as more jurisdictions move towards the creation of dedicated digital regulatory regimes, and the ability of DPAs to collaborate with their consumer protection and competition counterparts will be key to delivering the regulatory objectives of each sphere. The following case study represents an excellent example of this collaboration in action.

**Case study - European Commission's investigation - proposed acquisition of Fitbit by Google:** In August 2020, the European Commission (EC), Europe's competition authority, opened an in-depth investigation into Google's proposed acquisition of Fitbit. As stated in its press release, the EC "is concerned that the proposed transaction would further entrench Google's market position in the online advertising markets by increasing the already vast amount or data that Google could use for personalization of the ads it serves and displays." Recognizing the intersection with privacy regulation, in July 2020 the EC sought the assistance of the European Data Protection Board (EDPB).

In light of its long-standing commitment to promote the fair processing of personal data within open markets, as a member of the EDPB, the European Data Protection Supervisor (EDPS) took an active role in cooperating with the EC. This decision was based in part on the EDPS' long-held position that competition, consumer protection and data protection law are three inextricably linked policy areas in the context of the online platform economy. The EDPS considers that the relationship between these three areas should be a relationship of complementarity, convergence and coherent application, not a relationship where one area replaces or enters into friction with another.

One of the main challenges that the EDPS faced was the short timelines necessitated by the EC's procedural requirements and strict deadlines. As a result the EDPS prioritized key areas of focus, starting with analyzing areas where the possible negative impact of the merger for privacy and data protection might most likely manifest itself. The EDPS then focused on any possible friction with privacy and data protection triggered by pro-competitive measures. For example, situations where third parties might be able to receive access to personal data. Ultimately, EDPS' efforts have allowed them to derive an increased awareness of competition law specificities and of the procedures applicable to the assessment of mergers in the context of competition law.

In light of this experience, the EDPS considers that institutionalized and structured cooperation between competition and data protection authorities, relying on a clear legal basis for administrative cooperation and the exchange of any relevant information, would significantly improve collaboration on data protection and competition matters.

# Laying the foundation for cooperation

## Developing Enforcement Cooperation Relationships

While legislation and information-sharing arrangements provide for the ability to cooperate, in many instances up to the global level,[5] it is the inter-agency and inter-personal relationships which, when nurtured, will provide the comfort, trust, organizational knowledge[6] and open lines of communication necessary to make cooperation a reality. Authorities can develop and build such relationships by joining and participating actively in various privacy and enforcement cooperation networks, through monthly calls, volunteering for initiatives or working groups.

- For example, the IEWG holds regular closed enforcement cooperation sessions, in which authorities come together to discuss enforcement topics of global interest. Previous activities include online data scraping, FRT and credential stuffing. These have resulted in collaborative compliance activities, including:
    - a joint investigation by the U.K.-ICO and OAIC into Clearview AI's personal information handling practices[7]
    - a joint letter to, and engagement with, video teleconferencing companies
    - an initiative led by the Gibraltar Regulatory Authority, to develop guidance for businesses and individuals to mitigate the risk of credential stuffing[8]

[5] Recognition of common values all the way up to the global level is already necessary when considering how each authority can best serve individuals' interests and rights in this globalised and digital age. For example, the common inspiration for individual governments on the basis of widely accepted (if not quite global but as intentionally diverse as currently exists) texts such as Article 12 of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" or the OECD's 2007 Recommendation on Cross-border Cooperation.

[6] By leveraging specific authorities' strengths, legal capabilities, strategic priorities.

[7] The U.K.'s Information Commissioner's Office and the Office of the Australian Information Commissioner initiated and publicly announced a joint investigation into Clearview AI's practices in July 2020.

[8] This guidance is expected to be issued later in 2021.

- GPEN holds monthly conference calls and meetings to discuss enforcement issues, trends and experiences amongst participating members. There are generally 2 conference calls scheduled each month. In line with the international character of GPEN, one call is scheduled for the convenience of Pacific members and the other for Atlantic members. In the past, discussions have included privacy enforcement during and after COVID-19, smart cities initiatives, online exam proctoring and use of artificial intelligence in the public sector.

- Similarly, in the area of cross-regulatory cooperation, the DCCWG focuses on the intersection of privacy, consumer protection and competition. The DCCWG provides, as part of its mandate, a forum for authorities to discuss collaborative efforts. Its work has also focused on increasing awareness, in various fora, regarding the need for greater cross-regulatory collaboration.

- Authorities can also arrange face-to-face discussions and teleconferences to build rapport - starting with agency heads, and other senior personnel, but then growing relationships at the operational level (for example, via regular operational calls).

- Authorities can participate in secondments, work exchanges or joint training activities, which allow staff to bring back in-depth knowledge and build familiarity with potential partners. For instance, the Gibraltar Regulatory Authority and Mexico's INFOEM[9] conducted a week-long familiarization visit in which delegates were able to attend sessions to learn about policies and procedures and observe enforcement activities. As of publication, the FTC has an open International Fellows Program. This program provides an opportunity for authorities to send staff to work with the FTC for 3-6 months. International fellows participate in investigations, enforcement actions, and other projects with FTC attorneys, investigators, and economists and share insights and experience from their home Authority

- Authorities could also create collaborative groups at the national level. One example of such an engagement, involving cross-regulatory collaboration, is the U.K.'s Digital Regulation Cooperation Forum (DRCF), a group consisting of various national regulators[10], including the U.K.-ICO as well as authorities from competition, consumer protection, telecommunications and finance spheres, which seek to cooperate and coordinate their activities related to the digital economy.

[9] Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México.

[10] Consisting of the U.K.'s Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA).

# Information-sharing arrangements

Sharing confidential information and/or personal data is often crucial to enforcement cooperation (even if only for authorities to share that they are in fact, or are considering, investigating a matter). In many cases, parties will be able to share such information, in compliance with their respective legal limitations, pursuant to a non-binding memorandum of understanding (MOU) or an arrangement. Such a document will detail each party's expectations regarding the circumstances under which they may share information. It is important to note, however, that some authorities will not be able, either practically or legally, to share information pursuant to a non-binding arrangement, while others may not be in a position to sign binding agreements.

Understanding that many arrangements will be issue- or need-driven, signing an arrangement in advance can save time when the opportunity to cooperate arises, and will allow for regular discussions, which will in turn make it easier to identify opportunities for cooperation.

Authorities can also share information pursuant to bi-lateral arrangements between established partners. However, broad-based arrangements, like the GPA Arrangement or the Asia Pacific Economic Cooperation organization's (APEC) Cross-border Privacy Enforcement Arrangement (CPEA), provide flexibility for multilateral sharing. Broad-based arrangements may be particularly useful in addressing risks involving many jurisdictions, like global data breaches, while still allowing any participating Authority to decline cooperation and choose the partners with which they will share information.

Sometimes continuing or general bi-lateral arrangements are not an available option, due to legislative or policy constraints. In such instances, authorities should consider the use of more limited case-specific memoranda or agreements. These types of agreements can be especially helpful for first-time collaboration or proof of concept exercises, and pave the way to broader arrangements – such an arrangement could serve as, for example, a starting point for cross-regulatory collaboration where one Authority is supporting the other's investigation.

Authorities may be subject to legislation that requires special treatment of personal data, including in relation to international personal-data transfers. If one or more authorities are subject to such requirements, they may wish to consider one of 2 options:

- agree that no personal data will be shared (recognizing that it is often unnecessary to share personal data for the purposes of enforcement collaboration)

- include provisions in their arrangement, or in addition to their arrangement, that clearly detail the parties' requirements or sharing limitations

**Note**: For an example of such provisions in a general agreement, see s. 7 and Schedule 1 of the GPA Arrangement. For an example from a bilateral MOU between data protection authorities, that deals with the issue of personal data, see s. IV of the MOU between the Office of the Privacy Commissioner of Canada and the U.K.'s Information Commissioner's Office

Some authorities may require individuals' consent before sharing their personal data. Where it is not possible to gain such consent, an Authority may choose to proceed via option (i), above.

Cooperation will be based in large part on trust between the parties sharing information. To that end:

i. the party providing information should expressly detail[11] its requirements with respect to the treatment[12] of shared information

ii. where legally possible, the party receiving information should treat such information as confidential[13] unless the Authority that has provided it has provided express consent to treat it otherwise

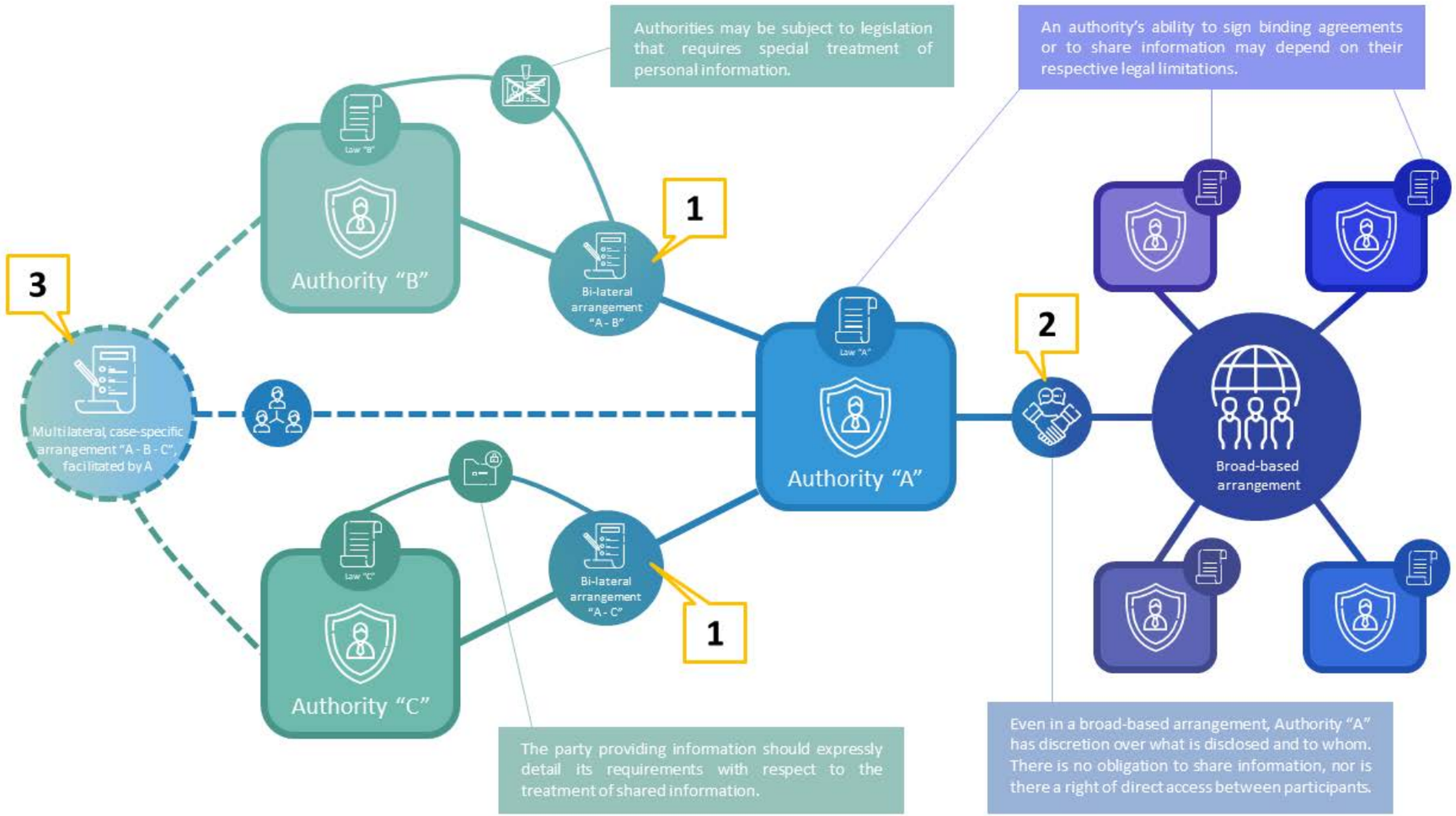
(Note: For an example of a documented process for responding to requests for disclosure of confidential information, see the s. 6.1(iv) of the GPA Arrangement.)

[11] See s. 6 of the GPA Arrangement in Appendix A for an example.

[12] See s. V of the Memorandum of Understanding between the United States Federal Trade Commission and the Dutch Data Protection Authority in Appendix B for an example.

[13] See s. V of the Memorandum of Understanding between the Office of the Privacy Commissioner of Canada and the U.K. Information Commissioner's Office in Appendix B for an example.

**Figure 1: Organizations can use a variety of information sharing mechanisms based on legislative requirements and operational needs (Infographic Symbol Legend Follows)**




In this illustration, Authority A has initiated an investigation into a multinational organization and wishes share information with partner authorities, with a view to supporting its own investigation and considering potential coordinated enforcement. It does so in 3 ways:
(1) Authority A reaches out to authorities B and C through pre-existing bilateral agreements, carefully assessing the sharing of personal information and setting out requirements for the use of shared information. The Authority ultimately determines that personal information sharing is not required as the authorities are more interested in evaluating the organization's technology and associated practices.
(2) Authority A reaches out, via the GPA Arrangement, to 2 participants in whose jurisdiction the organization under investigation operates, in order to obtain information that might be relevant to its investigation.
(3) Authority A notes that authorities B and C both have significant information and interest in the case, but no current avenue to share information. After discussion with both authorities, A facilitates the development of a multi-lateral, case specific arrangement to allow all 3 to work together. Authorities B and C may use this arrangement as a stepping-stone to further cooperation in the future.

**Figure 2: Infographic Symbol Legend**

| Icon | Concept Represented |
|---|---|
| | Data protection authority. |
| | Data protection authority's constitutive law. |
| | Arrangement between data protection authorities. |
| | International cooperation network between authorities. |
| | An authority's discretion over what is shared within a cooperation network. |
| | Restrictions over how personal information is shared between authorities. |
| | Information shared between authorities. |
| | Participation in the drafting of an arrangement between authorities. |
| | External organization (i.e. not a data protection authority). |
| | Notification to an external organization that the information they provided is being shared. |
| | Investigation being conducted by a data protection authority. |
| | Information relevant to an investigation. |
| | Established partnership between authorities. |
| | An authority's enforcement powers, applicable against organizations in their jurisdiction. |
| | Coordinating separate investigations. |
| | Assisting another authority's investigation. |
| | An authority's public communications (ex. press release, open letter, public statement). |

**Note:** When sharing confidential information obtained from an organization during investigative activities, authorities should consider whether it is appropriate to inform the organization that the information has been, or may be, shared. It may not be a legal requirement to inform the organization, but failing to do so could have consequences for business secrets (or commercial confidential information), or could create a chilling effect for future dealings with this organization or others, if the case attracts publicity.

> Before sharing information, an Authority should carefully analyze of its own legal requirements (for example, governing legislation or conventions) to ensure that it clearly understands the circumstances and limitations under which it may share confidential information **and** personal data.

For reference, sample MOUs can be found in **Appendix B** and in the Enforcement Cooperation Repository. As the repository is intended to be a living resource, we **strongly encourage** authorities to consider **adding new documents** to the repository when possible, to facilitate greater enforcement cooperation.

# Enforcement cooperation protocols and training

Authorities should consider developing internal protocols and training enforcement staff so that they are aware of the benefits and potential options for enforcement cooperation, and have an understanding of their respective legal and regulatory frameworks. Ideally, this will create an environment where enforcement cooperation comes naturally to enforcement staff as part of their everyday operations—as an additional tool in their compliance toolbox —and where the Authority is able to respond quickly to cooperation opportunities as they arise. Similarly, training sessions regarding other relevant regulatory spheres may help bridge the information gap, and lay the foundation for future cross-regulatory cooperation.

> Privacy issues often evolve quickly and require a prompt response. Authorities are urged to respond to requests for cooperation in a timely and expedited manner. This can be accomplished by developing, and training staff with respect to, an internal enforcement cooperation protocol to facilitate a prompt response when opportunities to cooperate arise.

# Identifying and evaluating opportunities for cooperation

Authorities will identify potential opportunities for cooperation via various means – media reports, public complaints, internal research, working groups and enforcement networks (including those for other regulatory spheres, where possible), etc. In evaluating whether an issue may be appropriate for enforcement cooperation, authorities may consider whether it represents:

- a potential risk across multiple jurisdictions or regulatory regimes
- a risk of significant harm and/or broad-based impact
- an emerging or strategic privacy issue

Authorities will need to develop internal decision-making processes to ensure that they have duly considered whether they can cooperate with another Authority, and that they are clear which law applies (generally through engagement with their respective legal departments). Lack of jurisdiction, either geographic or regulatory, will not necessarily preclude cooperation, depending on the applicable legal framework and the facts of the case, but should be a consideration. Authorities should consider casting a wide net when requesting information, as both expertise and key intelligence can be widely distributed among national, international and cross-regulatory counterparts.

> The GPEN Alert Tool provides a platform for participants to share information related to ongoing or potential investigations, which will in turn assist in identifying potential opportunities for cooperation.

# Contacting potential partners

It may be easiest to start with established partners where information-sharing arrangements are in place, or where there is a common legal framework. After developing a level of comfort with enforcement cooperation, an Authority may choose to expand its strategic partnerships.

The appropriate partner(s) in each specific case will depend on the facts, but may be best determined based on the potential for synergies via coordination - for example, where the potential partner may have:

- a mutual interest in the issue
- access to relevant evidence, such as consumer complaints, or the ability to obtain and share relevant documents and records

- clear jurisdiction over the matter (where others' jurisdiction might be questioned)
- geographic/time-zone proximity to the organization's operations (to assist with teleconference or in-person communication –for example, site visit)
- capacity to deal with the organization in its primary language
- ability to communicate between partners in a common language
- an existing relationship with the organization
- relevant technical/policy expertise – particularly when the conduct at issue can/should be addressed by authorities across multiple regulatory spheres
- enforcement powers which may assist in obtaining redress, including for individuals affected by the alleged contravention(s)
- resources to share the workload associated with a complex investigation

An Authority may contact another Authority through various means, including:

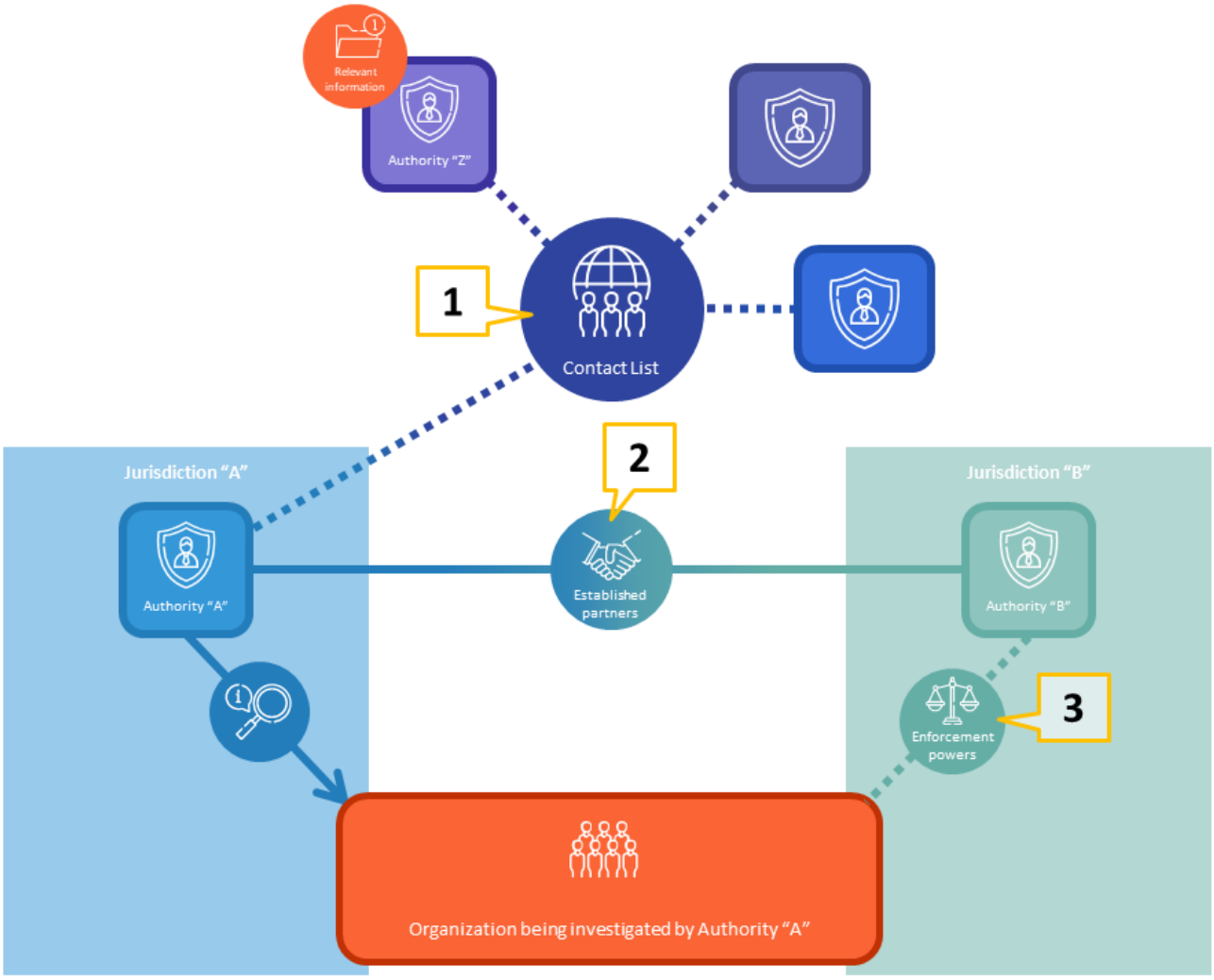
i. existing organizational contacts for established partners

ii. contact lists available via organizations, for example,
    - the GPA Arrangement
    - GPEN enforcement contacts list or the Alert Tool contact mechanism
    - other global, regional or linguistic-based networks, such as the:
        - Unsolicited Communications Enforcement Network
        - Iberoamerican Data Protection Network
        - European Data Protection Board
        - Association Francophone des Autorités de Protection des Données Personnelles

If an agency does not have the legal authority to share confidential information, it can start by sharing general details of the issue in question. If there is mutual interest in pursuing the matter further, the authorities could then take the steps necessary to share further information for example, by entering into an information-sharing arrangement.

Where possible, to avoid delays associated with translation, authorities should attempt to contact prospective partners in a language that is mutually understood.

**Figure 3: Distribution of relevant information and capabilities among organizations**




In this case, Authority **A** wants to identify and evaluate what assistance authorities may be able to provide in the context of the investigation. It does so in 3 ways:

(1) Authority **A** uses the GPEN Alert Tool to notify participating authorities of its investigation, and receives a response from Authority **Z**, which indicates that it has previously examined the organization. Authority **Z** shares information that assists Authority **A** in establishing the grounds to commence an investigation.

(2) Authority **A** then reaches out to Authority **B**, an established enforcement cooperation partner that also has jurisdiction over the organization under investigation. They agree to coordinate enforcement actions given potential synergies:

- Authority **A** can leverage its geographic proximity to the organization's headquarters to serve as the main point of contact for evidence gathering

(3) Authority **A** identifies that Authority **B** would be able to leverage enforcement powers that **A** lacks (the power to issue orders and monetary penalties) to help ensure compliance with their ultimate findings

# Enforcement Cooperation Model

The following matrix and associated flowchart will serve as the basis for discussion.

**Figure 4: Enforcement Cooperation Matrix**

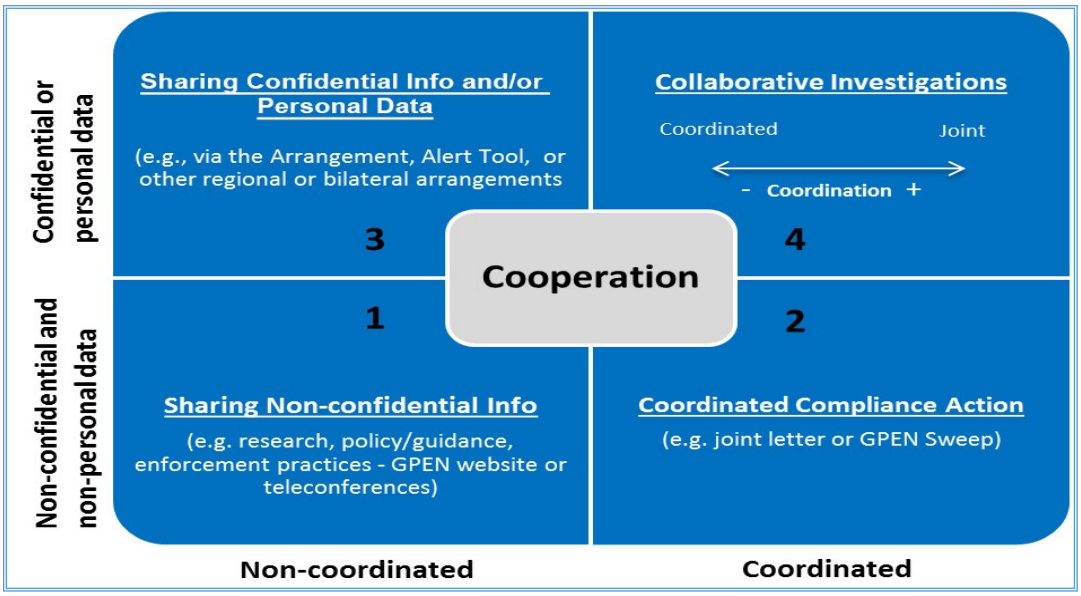
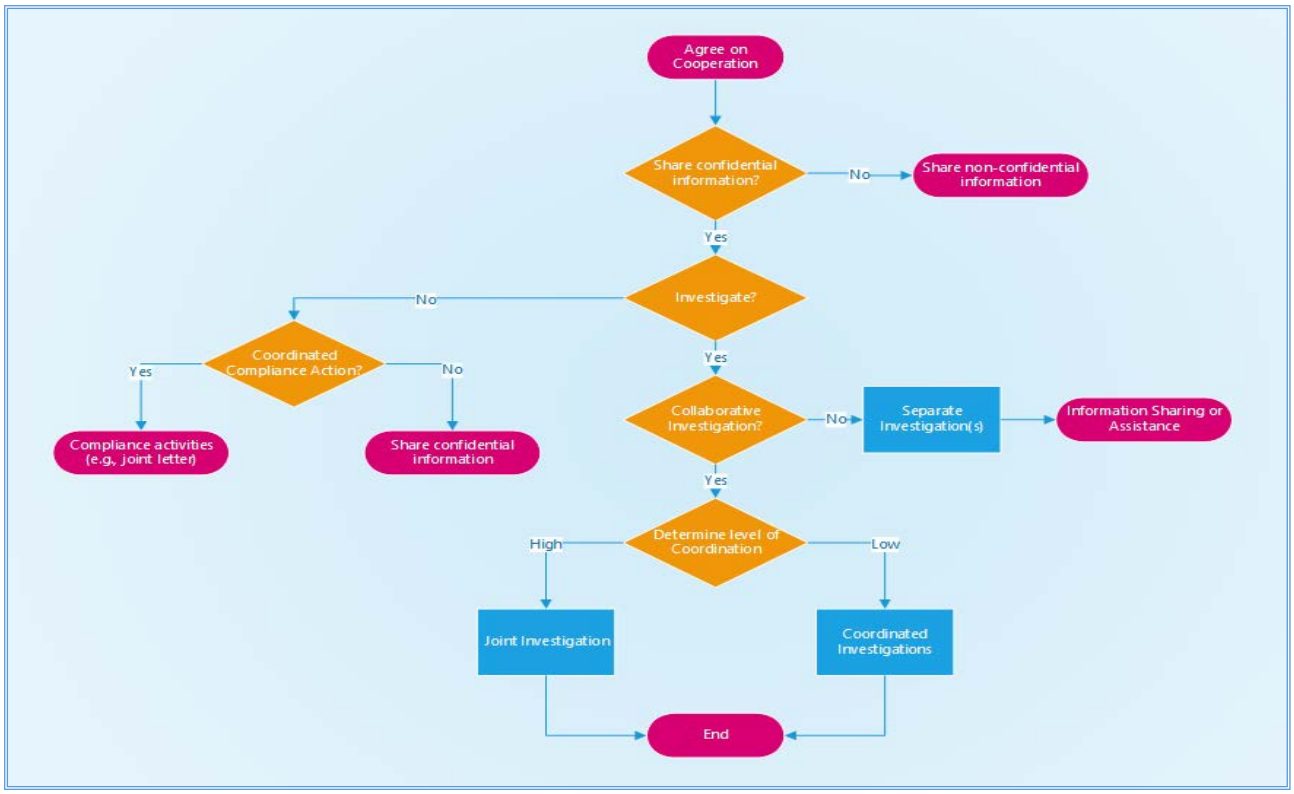



**Figure 5: Enforcement Cooperation Flowchart**



# A model of enforcement cooperation

Enforcement cooperation can take several forms, whether amongst DPAs or across regulatory regimes:

1. **Sharing non-confidential information and experience**: for example, sharing general policy/research/practice on enforcement matters, via various networks, web-based platforms and meetings (generally outside the scope of this handbook)

2. **Coordinated compliance action**: which will not generally involve sharing confidential information (for example, thematic initiatives like the GPEN sweeps, and joint correspondence with specific organizations outside a formal investigation)

3. **Confidential information or personal data sharing and assistance**: one or more separate and unilateral uncoordinated investigation(s) supported by information sharing or other assistance, for example, on the basis of MOUs like the GPA Arrangement or another multilateral or bilateral arrangement

   **Note:** This can include providing assistance to an Authority from another regulatory regime[14] with its investigation – for example:
   - where a consumer protection or competition authority initiates an investigation but a privacy authority does not have a comparable investigation, there exists the possibility for the privacy authority, which enjoys an advantage with respect to knowledge of how certain privacy functions operate, to assist its cross-regulatory counterpart in considering those factors in its analysis through the sharing of case-specific information
   - where Authority A enlists the assistance of Authority B to gather evidence from a relevant third party within Authority B's jurisdiction

4. **Collaborative investigations**: (with sharing of confidential information) can include varied levels of coordination along a continuum from:

   - **Separate but coordinated investigations**: involving coordination of certain aspects of the investigative process, such as information gathering or public communication

   - **Joint investigations**: involving coordination of most or all aspects throughout the investigative process

[14] For an example of such assistance, please see the Case Study on page 26

In this handbook, we will focus primarily on forms of enforcement cooperation (from above) designed to address issues involving specific organizations, as would be dealt with via: (2) joint compliance activities; (3) sharing confidential information; and (4) collaborative investigations.

Again, these modes of cooperation are neither mutually exclusive nor exhaustive. For example:

- authorities could start by simply sharing confidential information or issuing a joint compliance letter and subsequently decide to engage in a collaborative investigation

- two authorities engaged in a joint investigation could share confidential information with another Authority that is independently investigating the same matter[15]

# Choosing the appropriate form of enforcement cooperation

## Sharing non-confidential information and experience (Item 1)

While resources, legislative limitations or strategic considerations may create barriers to cooperation in certain circumstances, it is important to recognize that enforcement cooperation can be as simple and informal as sharing best practices, innovative enforcement strategies or other non-confidential information.

With this in mind, authorities are encouraged to be as reciprocal as possible in their cooperation partnerships, which will in turn strengthen the trust between partners and foster further cooperation. To this end, authorities can start small by choosing to share non-confidential information or experience in support of each other's activities as they work towards better outcomes for individuals in their respective jurisdictions, and the development of strong partnerships in the future.

As previously highlighted, authorities can also share experience through mechanisms such as secondments and interchanges, staff exchanges and activities such as the GPEN enforcement practitioner's workshop, and the February 2021 joint virtual workshop organized by ICPEN and GPEN explore the intersection of consumer protection, privacy and cross-regulatory enforcement cooperation in practice.

[15] For an example of such a collaboration, please see the Ashley Madison Case Study beginning on page 30.

# Coordinated compliance action (Item 2)

Outside of coordination and collaboration on investigations, authorities can also consider more informal compliance actions. These coordinated activities can yield valuable intelligence and often offer greater flexibility than formal investigations. In many cases, these forms of collaboration have proven to be highly effective in promoting compliance with privacy laws.

## Sweeps

Authorities can participate in privacy sweeps alongside enforcement partners. Each year, GPEN member authorities conduct a sweep on a different issue or area of interest[16]. In these sweeps, authorities from around the world generally assess the practices of hundreds of organizations across multiple countries. These sweeps are informal in nature, and focus on gathering intelligence, with the aim of identifying trends and concerns in various privacy-related topics, and encouraging specific compliance by swept organizations.[17]

## Joint letters

Authorities may choose, as an alternative to engaging in a formal investigation, to issue a joint letter to one or more organizations. Issuance of a joint letter will not generally require the sharing of confidential information or personal data.

Such a practice may be particularly appropriate when time is of the essence or where authorities believe they can achieve results expediently, without dedicating the more costly resources associated with a formal investigation.

Authorities would generally follow certain steps in developing and issuing a joint letter.

### Drafting

One or 2 authorities may take the lead by proposing the letter to a group of authorities,[18] offering to hold the pen and suggesting, for example:

- the issues the letter will address and its ultimate objective
- to which organization(s) it should be sent

---

[16] Previous topics include: Privacy Accountability (2018), The Internet of Things (2016) and Mobile Apps (2014).

[17] Authorities involved in Sweeps may opt to follow up with swept organizations in their jurisdiction by sending compliance letters that identify the concerns observed and encouraging improvements to achieve compliance with applicable laws.

[18] E.g. via the IEWG "closed enforcement sessions," GPEN Alert Tool or multilateral direct relationships.

- whether or not the letter will be made public

The letter may or may not reference a contravention of specific legislative provisions, which can vary across jurisdictions. It may alternatively raise concerns with respect to general privacy principles (for example, the OECD Privacy Guidelines) or ask factual questions to assist the signatories in better understanding the new practice or technology. Signatories should also agree on whether or not they expect a response from the organization, so that the letter can be drafted accordingly. It is often advantageous to actively engage with the organization and set timelines. These efforts can be successful in achieving positive privacy enhancements in a resource-efficient way, as will be demonstrated in the case study on page 26.

The drafting process can span from a few days to a few months, depending on the number of signatories and the amount of input from each Authority. If authorities are flexible with respect to wording, it will generally allow the drafters to finalize the letter quickly, with as many signatories as practicable, for greatest impact.

**Note:** As a practical matter, to assist with the challenge of coordinating multiple signatures, the drafters may request a PDF version of each Authority's logo and/or signature to be affixed to the letter before sending on behalf of all signatories.

## Follow-up

Before drafting and sending the letter, signatories may discuss potential follow-up strategies:

- if the letter is simply intended to raise privacy awareness, either for the company or the public, the signatories may take no follow-up action or, subject to legal limitations, simply make public the organization's response

- if the letter is in relation to a potential egregious privacy issue, which the letter has been unsuccessful in resolving, one or more of the authorities may investigate the matter (possibly in a collaborative manner)

Ultimately, it will be at each Authority's discretion which action(s) they choose to take beyond issuing the joint letter, although signatories should keep each other informed of their intended follow-up activities.

## Examples

Below are 4 examples illustrating when a joint letter may be appropriate, though other pertinent situations may arise:

- When there are potentially serious privacy issues or risks affecting multiple jurisdictions, it may be possible to achieve compliance via a letter encouraging the organization(s) to comply with the signatories' expectations
- Such an approach can be implemented very expediently, with limited resources, and may be effective even in situations where jurisdiction has not been clearly established

- As of the publication of this handbook, the most recent example of this is the jointly issued Open Letter to Video Teleconferencing Companies (VTCs) signed by 6 authorities
    - This letter set out privacy concerns and best practices for VTCs in the context of COVID-19 (discussed further in a case study, below). Another example, found in **Appendix C,** is a joint compliance letter sent by 7 authorities to Insecam, a webcam streaming website.

- When an organization is preparing to launch, or has recently launched, a new privacy practice or technology which raises significant privacy concerns, a joint letter can:
    - give the organization an opportunity to explain how it is complying with privacy laws or amend its privacy practices to address potential contraventions
    - if published, raise public awareness regarding potential privacy issues and demonstrate solidarity amongst authorities in respect of the issue
- As of the publication of this handbook, a recent example is the jointly issued open letter on the global privacy expectations of the Libra network, signed by 7 authorities from around the world
    - This letter set out privacy concerns and questions for the members of the Libra Association[19] regarding their planned information handling practices. Another example, found in **Appendix C,** is a joint letter sent on behalf of 38 authorities to Google, seeking further information on Google Glass

[19] The Libra Association, now known as the Diem Association, is a group of private sector entities, led by Facebook, that are in the process of creating a new privately backed cryptocurrency and digital payment network. As of publication, the network remains in the planning and regulatory approval phase.

**Case Study—Open Letter to video teleconferencing companies:** In early 2020, the GPA's IECWG held a series of safe space (or closed enforcement) discussions on various privacy risks related to COVID-19. One such discussion focused on the privacy concerns and risks associated with a sharp global increase in the use of video teleconferencing (VTC) products due to the pandemic. In the course of this session, 6 participating DPAs took coordinated action.

On July 21, 2020, the 6 DPAs jointly issued an open letter to VTC companies in response to new and expanded privacy risks related to the technology and its implementation. The letter set out concerns and best practices related to: (i) security; (ii) privacy-by-design and default; (iii) the importance of VTC platforms knowing their audience; (iv) transparency and fairness; and (v) end-user control. While the open letter was directed to all VTCs, it was specifically sent to Microsoft, Cisco, Zoom, Google and Houseparty. As of the publication of this handbook, all of the recipients, save Houseparty, replied to the letter to demonstrate the steps that they had taken to comply with data protection and data requirements, including policies, tools, practices and security measures. Joint signatories further engaged with each of these companies, in a series of virtual meetings on various VTC platforms, to clarify certain areas of residual concern and better understand their platforms and privacy practices.

This collaborative effort yielded a number of benefits by:

- identifying and approaching a global privacy concern in a holistic manner
- preventing duplication of effort and saving resources through an informal compliance approach agreed upon by all participating authorities
- leveraging the expertise of 6 authorities from around the world in the drafting, communications and engagement process
- carrying out a scalable enforcement action allowing DPAs of various sizes to participate and benefit from coordinated action
- taking advantage of various time-zones, relative strengths and professional relationships to divide work related to engagement with VTCs in different locations

This global compliance initiative will soon be finalized, with the publication of a final statement on findings, lessons learned and expectations to encourage broad-based compliance and best practices across the industry. In December 2020, the joint signatories encouraged Houseparty to engage with them, including via a press release. To date, Houseparty has not contacted the group of joint signatories. However, Houseparty has engaged directly with the U.K. ICO as part of enquiries separate to those of the joint signatories. In September of 2021, Houseparty announced that it would cease offering its VTC service.

## General Coordination

Authorities are not limited to Joint Letters and Sweeps, and can engage in a variety of forms of coordination and cooperative activity outside of investigations, including coordinating on the acceptance and handling of complaints or intelligence activities. This can be particularly useful when considering cross-regulatory collaboration, where formal investigative collaboration options are not yet fully developed.

**Case study - Australian Consumer Data Right:** The Australian Consumer Data Right (CDR) is an Australian government initiative aimed at giving consumers greater control over their data. It enables a consumer to direct a data holder to provide their CDR data to an accredited data recipient, in a CDR compliant format. While the Australian Federal Treasury Department and the Data Standards Body are involved in the CDR system, it is the Office of the Australian Information Commissioner (OAIC) and the Australian Competition and Consumer Commission (ACCC) who regulate it.

In light of their shared CDR enforcement mandate, they took many of the core cooperation steps outlined in this Handbook (that is, entering into an MOU, developing robust Information Sharing Agreements). The ongoing nature of their shared regulatory responsibility also allowed them to develop and publicly issue a joint Compliance and Enforcement Policy. Available online and drafted for consumers and CDR participants, this Policy sets out the approach that the OAIC and ACCC will take to encourage compliance with CDR Rules and legislation, and how they will respond to breaches of the regulatory framework.

Given the co-regulation of the CDR regime, and the intention to roll it out economy-wide on a sector-by-sector basis, a number of bodies may assist consumers with complaints and enquiries. To provide simplicity and convenience for consumers, and to ensure they are not bounced between regulators or other bodies, a ‘no wrong door’ approach has been applied to contacts and complaints- consumers are directed to a single contact point on the CDR website, whereby the OAIC and ACCC triage enquiries, reports or complaints to ensure they are forwarded to the relevant regulator/body.

### Policy and Research Coordination

While outside of the scope of this Handbook, it is important to mention the value of policy and research collaboration among global DPAs and other Regulatory Authorities. Through mechanisms such as various GPA working groups, including the policy strategy working group[20], and other bilateral/multilateral research initiatives and publications, authorities can combine their expertise and gain global insights that are particularly valuable in an age of constantly evolving innovative data practises.

In particular, authorities can gain significant benefits through collaboration on the research of technical trends in privacy and the digital economy, by working with partner authorities that have greater technical capacity, expertise and resources, such as dedicated technical labs, analysts and forensic software. These activities help support a global, holistic approach to enforcement, support general compliance, and are of great importance in establishing and developing relationships with potential partner authorities.

# Confidential Information or Personal Data Sharing and Assistance (Item 3)

In certain circumstances, an Authority may choose to share information, or provide assistance, (pursuant to legislative authority and/or an arrangement) in support of an ongoing or prospective investigation by another Authority. Below are just a few examples where such an approach may be appropriate:

i. **Authority A** obtains, pursuant to its own investigation evidence gathered in an investigation, information which relates to the practices of an organization within the jurisdiction of **Authority B**. **A** either does not have jurisdiction over the organization in question, or believes that **B** would be better positioned to investigate, due to geography, language, legislative powers or its relationship with the organization. **A** may approach **B** to determine if it would like to receive the information and/or if it would be in a position to investigate

ii. **Authority A** and **Authority B** are each investigating the same or related matters, but do not wish to coordinate their investigations, due to differences in their legislation and desired timelines for completion. The authorities may agree to share evidence obtained during the course of their respective investigations, their outcome or their follow-up, to support consistency

iii. **Authority A** is engaged in an investigation and believes that **Authority B** may have, or be able to obtain, information that would be of assistance to its investigation. **A** may approach **B** to determine if it is able to provide such assistance.[21]

[20] Recent reports by the PSWG include the topics of: Global frameworks and standards, Digital Economy and the relationship between privacy/data protection and other rights and freedoms

[21] Either pursuant to legislative authority and/or an arrangement like the CPEA or GPA Arrangement.

**Case study - Bundeskartellamt's (BKartA) Facebook/WhatsApp Investigation:** In 2019, the BKartA, Germany's competition authority, found that Facebook/WhatsApp's terms of service and the manner and extent to which it collects and uses data amounts to an abuse of dominance and prohibited Facebook/WhatsApp from combining user data from different sources.* As the conduct at issue involved a violation of the European GDPR, the BKartA sought and received the assistance of Data Protection Authorities in Germany, namely the Hamburg Data Protection Commissioner (HDPC) and the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit – BfDI) – collectively the DPAs. In deciding to assist the BKartA, the DPAs recognized their overlapping goals of protecting consumer rights – including protecting consumers' personal data. The DPAs also adopted the view that an exchange of legal views between authorities is always helpful, as it serves to ensure the consistent interpretation and implementation of the GDPR and that data protection and competition law should go hand in hand.

In order to make the most of this collaboration, all agencies concerned in this matter recognized the benefits of a close collaborative strategy built around this and other relevant issues. Among other things, this resulted in a successful exchange of views between authorities – effectively allowing the BKartA to obtain a second opinion and to secure support of the DPAs for its decision. At the same time, the DPAs were able to gain insights into BKartA's investigation, and laid the foundation for a continued partnership with the BKartA in the future.

*As of September 2021 a final decision by the responsible legal court (Oberlandesgericht Düsseldorf) is still pending, as the court has tabled some guiding questions to the European Court of Justice of the European Union. Facebook/WhatsApp had challenged the BKartA´s 2019 decision in a juridical manner.

In any of these instances, each Authority must satisfy itself that it has the legal authority under its own applicable legislation to share and/or assist, and should make clear, in writing, the conditions pursuant to which it is providing any information or assistance. An Authority that has the legal authority to share information may choose to do so even where the recipient cannot reciprocate.

An Authority receiving information should ensure that it clearly understands the purposes for which such information may be used, pursuant to the information sharing arrangement and its own applicable laws. For example, an Authority should ensure it understand whether it would be able to: (i) refer to such information in its written findings, within the terms of the information sharing arrangement; or (ii)

use the information it receives as evidence in domestic legal proceedings considering the type of proceeding in question (that is, administrative or civil vs. criminal) and any applicable evidentiary requirements within its own legal framework (for example, procedural fairness).

Partners should also possess a common understanding with respect to requirements for safeguarding the data to be shared. The agreed measures should reflect the nature of the information in question and the harm that may result from its unauthorized disclosure, accidental loss or destruction. Such measures could include: (i) transmission via an existing platform (for example, GPEN Alert) or via encrypted / password protected email; (ii) limited, need-based staff access; and/or (iii) storage in encrypted format or in locked cabinets.

> An authority which has received information should treat it as confidential and, where legally possible, obtain express written consent from the authority that provided it, before disclosing in any way.

# Collaborative investigations (Item 4)

A collaborative investigation, whether joint or separate but coordinated, can provide an opportunity for participating authorities to:

- avoid duplication of effort
- leverage each other's relative strengths and obtain increased cooperation from the subjects of the investigation
- achieve more impactful outcomes with greater efficiency
- amplify the impact by bringing greater national/international attention or establishing a combined cross-regulatory position

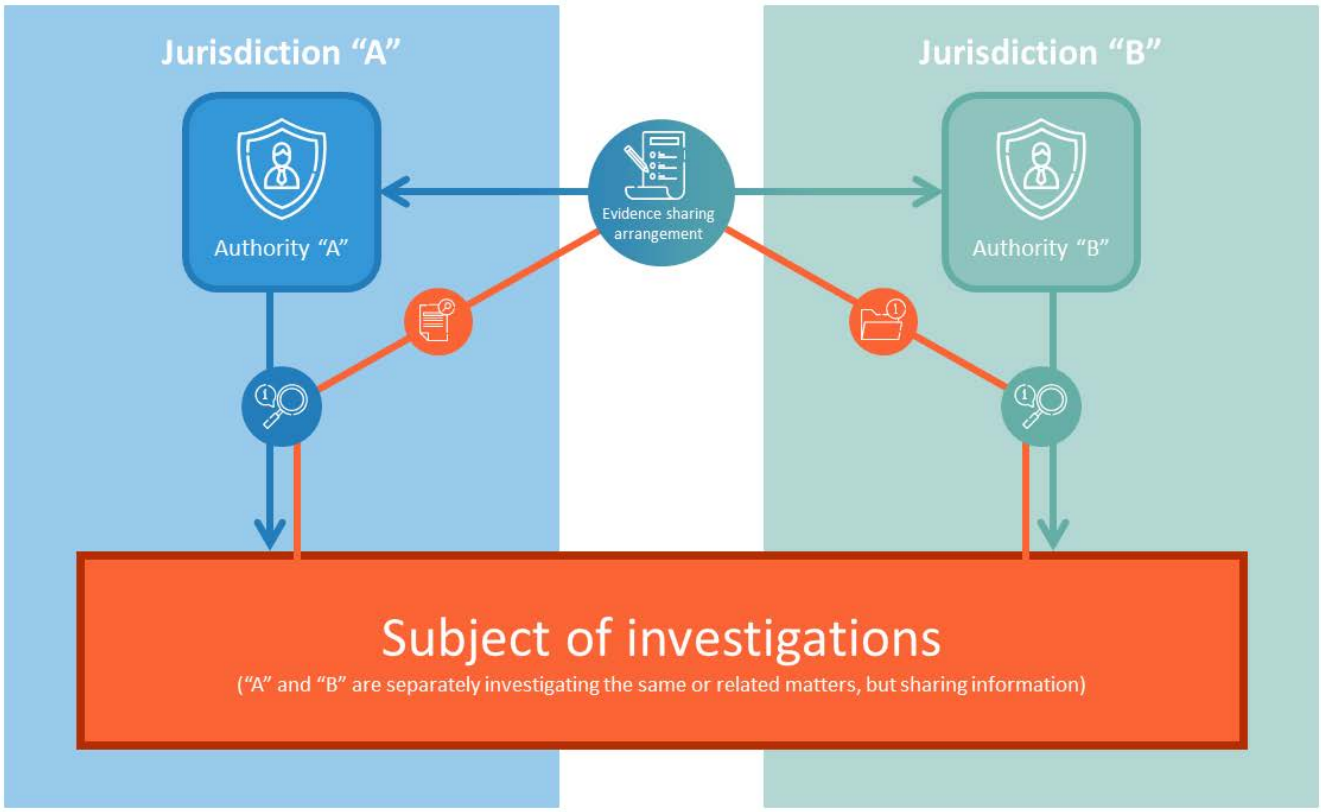
## Forms of collaborative investigations

Collaborative Investigations will generally involve sharing confidential information, but not necessarily personal information. It will also involve the coordination of certain enforcement-related activities. Such collaboration can extend along a continuum, and can involve a combination of the approaches outlined below (particularly when more than 2 authorities are involved):

i. **Separate but coordinated investigations**: In other circumstances, 2 or more authorities may determine that it would be most effective and efficient to pursue separate but concurrent investigations, whereby certain limited aspects of the investigative process are coordinated (for example, technical analysis or publication of complementary findings). Such circumstances could include:

- an Authority's legislation prevents it from jointly investigating (for example, requires that it send separate notifications, requests for information and/or findings)
- authorities are at different stages of the investigative process
- authorities have material legislative or policy differences (such that the authorities wish to investigate materially different issues)

**Figure 6: Separate but Coordinated Investigations**




In this situation, Authority A has initiated an investigation into the organization of concern approximately 3 months after Authority B began an investigation**.** The organization is a multinational company that operates in both jurisdictions. Authority A noted a post by Authority **B** in the GPEN discussion forum asking if other authorities were looking into the matter, and reached out pursuant to APEC's CPEA framework to discuss further. Based on this discussion, the authorities determined that they had overlapping interests in the organization. Authority B had chosen to focus its investigation on consent and retention issues, while Authority A was primarily interested in issues surrounding consent, accuracy and necessity/proportionality. Given the differing stages of investigation and focus of the authorities, it was determined that coordination of their separate investigations through information sharing was the best way forward.

ii. **Joint Investigations**: Two or more authorities may agree to coordinate most aspects of an investigation (including information gathering and analysis, report drafting and communications) in respect of an agreed upon set of issues. The process may appear as one investigation to the subject of the investigation. Circumstances whereby a joint investigation might be appropriate could include:

- the matter represents a high risk of harm or affects a large number of constituents of 2 or more authorities
- the matter represents an apparent multi-jurisdictional, geographic and/or regulatory, contravention
- each Authority asserts jurisdiction over the organization and matter
- relevant legislation and related policy positions with respect to the issues in question are relatively aligned
- each Authority would otherwise investigate the matter independently

Given the relative legislative uniformity across authorities in the consideration of security safeguards, global breaches may often represent an excellent opportunity for all forms of collaboration.

**Case study -** Ashley Madison**:** In 2015, a data breach occurred with respect to Ashley Madison, an alternative adult dating website operated by Avid Life Media Inc. (ALM), which now operates as Ruby Life Inc. Headquartered in Canada, Ruby Life's websites had a global reach, with users in over 50 countries, including Australia and the U.S. based on discussions facilitated by the GPEN, it was determined that there was international interest in investigating this matter.

Given the scale of the data breach (approximately 36 million Ashley Madison user accounts), the sensitivity of the information involved, the impact on affected individuals, and the international nature of the business, Australia's Office of the Information Commissioner and Canada's Office of the Privacy Commissioner jointly investigated ALM's privacy practices. Both authorities cooperated, and shared information, with the U.S. Federal Trade Commission, which conducted a parallel investigation. This case will be discussed in detail as we proceed through the relevant steps of cooperation, below.

**Case study -** Clearview AI**:** In January 2020, Clearview AI, Inc. (Clearview), a company specializing in facial recognition technology, came to global public attention. Clearview obtained information for its database by collecting publicly accessible images from a number of sources across the internet, including social media profiles. It then offered a service whereby this database could be searched using biometric information to identify individuals.

Given the apparently indiscriminate collection and use of personal information of Canadians, the Office of the Privacy Commissioner of Canada and its provincial counterparts, the Office of the Privacy Commissioner of Alberta, the Office of the Information and Privacy Commissioner for British Columbia, and the Commission d'accès à l'information du Quebec discussed the matter during a specially convened meeting between authority heads.

The authorities determined that a joint investigation would be the best use of resources, given the fact that each authority intended to investigate independently. This case will also be discussed in detail as we proceed through the relevant steps of cooperation.

# Preliminary matters

Before commencing a collaborative investigation, it is generally important for the authorities in question to address certain preliminary matters.[22]

## Sharing information

Are the authorities party to an information-sharing arrangement, or do they have the ability to share confidential information and/or personal data pursuant to legislation? If not, they may choose to sign on to an existing arrangement (like the GPA Arrangement) or enter into a new ad hoc bilateral or multilateral arrangement.

**Note:** If there are more than 2 coordinating authorities, and even if all of the authorities are party to an information-sharing arrangement, they should agree on the extent to which information can be shared amongst the authorities (for example, Authorities **A** and **B** are coordinating activities. **A** only has a privacy mandate, while **B** is responsible for privacy, competition and consumer protection. When **A** shares confidential information with **B**, should **B** share that information internally with its otherwise uninvolved competition and consumer protection units?). As noted earlier, if the information being shared contains personal data, authorities may agree or arrange that such data be subject to specific treatment requirements or restrictions.

**Ashley Madison example:** In order to share information and cooperate regarding this case, the authorities relied on a number of existing agreements and legislative authorities. To allow for cooperation via a joint investigation, the OPC and OAIC shared information under their relevant statutes and the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (CPEA). As mentioned previously in this handbook, the CPEA creates a framework for participating APEC members to cooperate in the enforcement of privacy laws. Meanwhile, to support cooperation with the OPC and OAIC, the FTC relied on key provisions of the U.S. SAFE WEB Act, which allowed it to share information with foreign counterparts to combat deceptive and unfair practices that cross national borders.

**Clearview AI example:** The guiding legislation of all four authorities allow for collaborative enforcement activities. The OPC, OIPC-AB and OIPC-BC have a collective Memorandum of Understanding (MOU) on federal/provincial collaboration regarding private sector privacy laws. This written arrangement sets out the terms pursuant to which the Offices can efficiently share information and collaborate on issues of mutual interest. After confirming a shared interest in investigating Clearview, the authorities also signed a case-specific MOU with the CAI, to share information and conduct a joint investigation.

[22] Authorities may find the template provided in Appendix E useful for documenting these.

## Strategic approach and terms of the collaboration

Authorities may also consider creating an overarching strategic approach document[23] to clearly set out their mutual understanding regarding important matters such as, but not limited to: the issues to be investigated; respective roles and responsibilities of each participant; timeframe for completion and key milestones; and points of contact. Given the evolving nature of developments in any investigation (many potentially unforeseen), this living document could be referenced, and updated as necessary, throughout the investigation to maintain a common understanding.

## Establishing a common understanding

Authorities should invest time in discussing the potential for coordination very carefully, to ensure mutual understanding with respect to each other's capabilities (for example, expertise or enforcement powers/penalties) and expectations. Establishing a common understanding before commencing a joint or coordinated investigation will allow authorities to: (i) ensure that a collaborative investigation is in fact the optimal strategy; and (ii) agree on a collaboration strategy that will ensure the most efficient and effective outcome. Simplifying an objective to a collaborative initiative will often allow the greatest flexibility in charting the path towards achieving that objective.

In particular, authorities that are considering collaboration on an investigation should ensure they understand the similarities and material differences in their respective legislation. This becomes more important when collaborating with authorities from different regulatory regimes. For example, authorities will likely need to pay additional attention to ensuring that they are speaking the same language, given the potential for common terms to carry different meanings across regimes. Differences will not necessarily preclude collaboration but, identifying those differences will assist in addressing many of the matters outlined below. For example, an Authority may wish to consider whether evidence gathered and shared with it by another Authority, perhaps for purposes of a different form of investigation (for example, administrative or civil vs. criminal), would be admissible for its own purposes.

## Determining the scope of investigation

For a joint investigation, authorities would generally agree on a set of common issues. Ideally, those issues could be framed in terms of each Authority's jurisdiction.

Authorities may also agree that an Authority will investigate one or more additional issue(s) outside the common scope.

---

[23] An example of a tool which may be of assistance in this process is this Joint or Coordinated Investigation Plan template in Appendix E. This template was developed by the Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia, based on the Handbook.

## Agreeing on timeframes

Recognizing that authorities will generally coordinate with respect to matters that are of strategic importance to their respective organizations, for such coordination to be successful, there should be a consensus with respect to timeframes for completion. Authorities should consider setting target milestones - for example: (i) notification to the organization; (ii) completion of analysis; and (iii) issuance and publication of findings. These milestones can be captured, and re-visited, as necessary, in a 'strategic approach' document.

Some authorities are legally required to conclude certain stages of their investigation, or to publish findings, within prescribed timeframes. Where this is the case, all the authorities involved should be made aware of such requirements, so that they can be factored into the determination of any milestones.

## Identifying Points of Contact

Efficient coordination will require close communication between authorities. Each Authority may therefore choose to establish:

- one or more operational level contacts for purposes of regular communication (for example, an investigator or technical analyst)
- back-up contacts so that the investigation does not stall during inevitable absences over the course of the investigation
- a senior management/executive contact for strategic discussions and to re-ignite momentum, as necessary

Given time zone differences and busy schedules, it can be challenging to arrange ad hoc teleconferences, and email correspondence can cause delays (particularly when the time difference between authorities is significant). It may therefore be useful to establish regularly scheduled teleconferences, to allow authorities to keep each other abreast of their progress and material developments on the file.

Each Authority should, where possible, assign points of contact who can communicate in a language understood by the other authorities. Communication via translation is an alternative option but can cause protracted delays.

**Ashley Madison example:** The authorities put in writing, through an exchange of emails, the legal basis for cooperation and sharing of information and discussed the scope of issues they would expect to investigate early on. In the initial phases, the authorities established a formal schedule of regular meetings to touch base frequently on steps, timelines, roles and responsibilities. Over time, once connections between members of the investigation teams were well established, the Authorities moved to a more ad hoc approach – driven by a shared understanding of the target final products and planned timing.

**Clearview AI example:** The authorities produced a Joint Investigation work plan, using a template that the Offices developed based on the Enforcement Cooperation Handbook. They leveraged the document to plan the investigation and ensure a common understanding with respect to key aspects of the collaboration, including to: define the scope of investigation; agree on the role of each Office; set a timeline for completion; and identify contacts for investigative team members and their backups. The work plan was a living document which served as a touchstone throughout the investigation.

## Stratifying engagement

There may be efficiencies to be gained in stratifying the level of engagement for the authorities involved in a collaborative engagement. For example, collaborating authorities may agree that participants in the investigation will play one of 3 roles:

i. **Lead Authority**: The authorities may agree that one Authority will serve as the lead. That lead Authority may: (i) conduct its own investigation, in lieu of multiple investigations by various authorities; or (ii) where there are separate but coordinated investigations, serve as a liaison between the authorities to coordinate various aspects of the investigative process (for example, information gathering and sharing, or public communications).

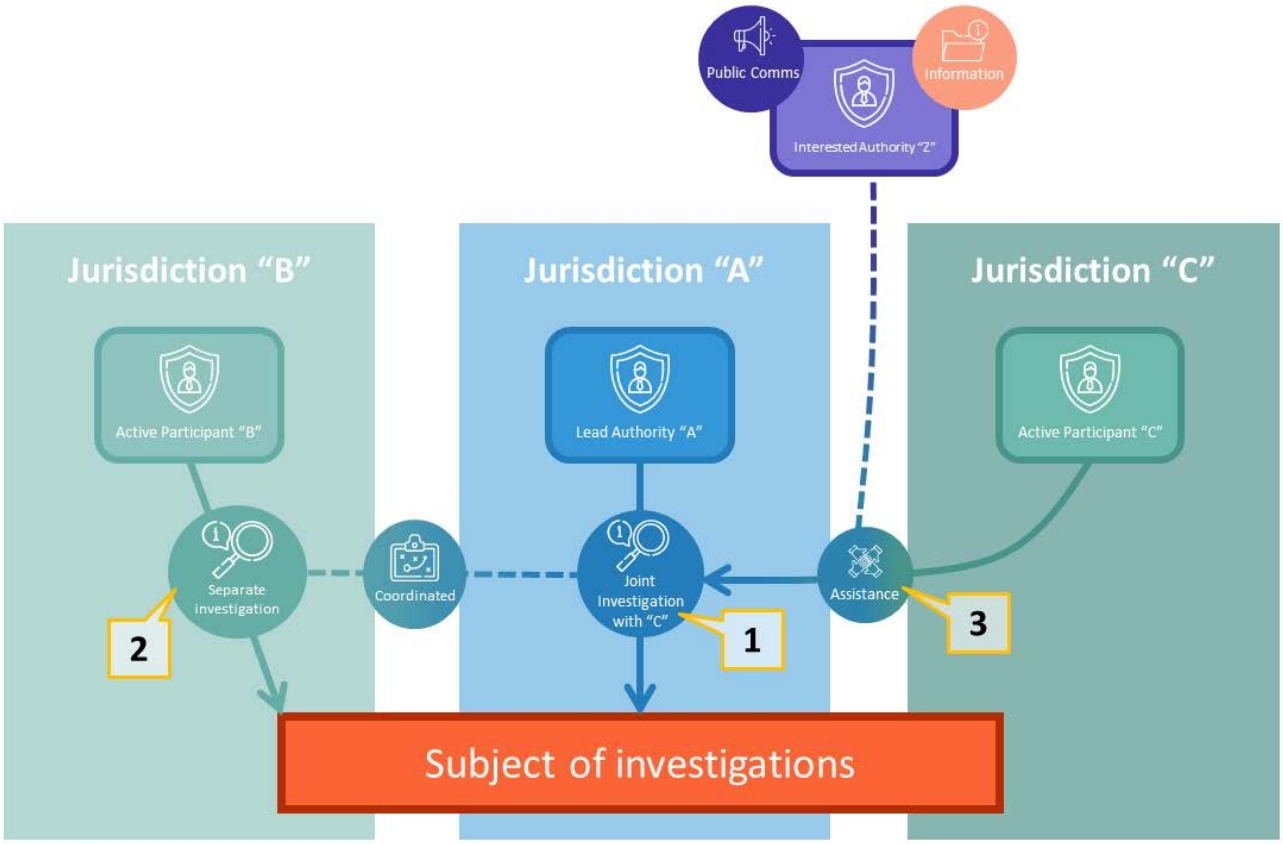
   Relevant criteria for determining which Authority, if any, should be the lead, could include:

   - the location of the organization and relevant jurisdiction
   - a large number of individuals affected in a particular jurisdiction
   - the matter is a strategic priority for one Authority
   - one Authority possesses the relevant technical resources to enable an investigation

ii. **Active participants**: Certain authorities may wish to either: (i) conduct their own joint or separate but coordinated investigations; or (ii) assist a lead Authority with certain aspects of its investigative process. Collaborating authorities would generally agree, up front, and reconsider throughout the investigative process, the allocation of investigative activities between the lead and/or active participants.

iii. **Interested authorities**: An Authority may choose not to investigate, and rely on other authorities' actions to ensure that the matter is addressed without dedication of its own resources to what could be a duplicative process. In such an approach, an interested Authority could still lend support to the investigating authorities via public communications or information sharing, thus signalling its own interest in the matter and encouraging compliance with the ultimate findings, within its jurisdiction.

**Figure 7: Stratified Engagement Scenario**




In this situation, Authority **A** is working with 3 other authorities to pursue an investigation into an organization.

(1) Authority **A** has initiated a joint investigation with **C** in which the 2 have agreed that **A** will be the lead authority. As the lead, **A** is the single point of contact with the organization and main technology analyst. Both are active participants, coordinating on each step of the investigation, with the intention of writing a single final report, and taking joint action if needed.

(2) Authority **B** is investigating the same organization of concern, but has opted to conduct its own separate investigation due to legislative requirements. While **B** is also an active participant, and is sharing information with **A** and **C**, it is focusing on different questions and sending its own correspondence, with the intention of issuing its own separate report.

(3) Authority **Z** is interested in the case but has determined that given the work being done by the other 3 authorities, it would not be an efficient use of its resources to join as an active participant. Instead, **Z** is sharing what background information it has, and issued an open letter indicating its concern and interest in the matter.

## Allocating specific investigative activities

To reap the benefits of a collaborative investigation, authorities should attempt to, where possible, allocate tasks within the investigation to leverage their comparative strengths and available resources towards achieving the most effective and efficient outcome.

### Information gathering and communication with the subject of the investigation

i. **Contact with the subject of the investigation**: For a joint investigation, authorities may choose to designate one Authority to be the main point of contact for regular/administrative communication/correspondence with the subject of the investigation to: (i) limit the duplication or potential confusion associated with multiple points of contact; (ii) address language or time zone differences; and/or (iii) simply to share responsibilities, and associated workload amongst coordinating authorities. Each Authority would generally communicate with its own complainant(s), as necessary.

ii. **Correspondence**: Authorities may agree that any material correspondence (for example, notification of investigation, initial/detailed requests for information, etc.) will be drafted by one Authority that will then incorporate comments from the other authorities prior to sending.

    Authorities should determine whether correspondence will be sent by one Authority on behalf of all coordinating authorities, or be sent under signature of each Authority. If multiple signatures are to be affixed to one document, to facilitate the process, each Authority could: (i) agree on the method by which documentation will be approved (for example, via email); and (ii) provide PDFs of the appropriate signature and authority logo, as well as signature block text.

iii. **Information gathering**: Even where questions are to be relayed to the subject of the investigation by the main point of contact on behalf of the group, authorities would generally confer on the development of those questions to ensure that they address the informational requirements of each Authority, based on their unique legislative frameworks.

    Where information gathering will take place via teleconference or meeting, authorities may consider participating jointly in the engagement, in lieu of multiple unilateral discussions. Live interactions often take discussions in an unforeseen direction, and each Authority's presence will allow it to: (i) ensure a clear understanding of the material orally/visually presented; (ii) ask any additional questions that may arise; and (iii) avoid the creation of differing/conflicting evidentiary narratives should the subject of the investigation give each Authority different responses to the same questions.

    Even where multiple authorities participate in the meeting, authorities may agree, in advance, on a preliminary list of questions to be asked during the engagement, and/or on who will lead the discussion (generally the main point of contact). This approach may assist in avoiding duplication, and ensure that each Authority's questions can be addressed in the time available.

Authorities should consider leveraging their respective powers with respect to evidence gathering when establishing authorities' roles in this regard – for example, certain authorities may have the power to:

- interview witnesses under oath
- compel sworn affidavits or the production of documents and records
- enter/search premises and seize evidence
- carry out online investigations (for example, search of electronic devices or storage)
- take action if the subject of an investigation is engaged in obstruction

In gathering evidence, it is important to consider any evidentiary requirements of the individual partners to ensure that each Authority that may seek to exercise its enforcement powers would be able to make use of the shared information. For example, some authorities may require certain details as to how information was gathered, or require particular methods not to be used (for example, to comply with procedural fairness requirements).

**Note:** Even if authorities choose to pursue separate concurrent investigations, they may choose to confer with each other in developing their respective information requests so that each Authority is able to obtain information that may be of use to the other.

Alternatively, where an Authority is aware that an organization has already provided responses to another Authority, it may consider requesting a copy of those responses directly from the organization. This can prevent complications associated with sharing such information pursuant to an information sharing arrangement (for example, transmitting large documents, restrictions of the use of information provided by another Authority).

## Analysis

Where determination of the issues in question requires analysis against materially similar legislative provisions (for example, based on the OECD Fair Information Principles, or the Madrid Standards or the Council of Europe Convention 108) or technical standards in the assessment of adequate safeguards (for example, Payment Card Industry Data Security Standard), it may be possible for authorities to share the responsibility for certain aspects of that analysis.

i. **Technical analysis**: Multi-jurisdictional data breaches, or other investigations related to technology, may offer an opportunity for one Authority to conduct technical analyses on behalf of a group. Technical analyses will often require the dedication of significant specialized equipment, software and/or expertise that not all authorities will possess.

   If authorities wish to agree that one Authority will conduct specific technical analyses, they may choose to confer in advance to agree on the scope of the analyses (including the technical questions to be answered), as well as any specific evidentiary requirements (for example, documentation of the analytical process or results).

Again, where one Authority will conduct analyses on behalf of multiple authorities, it should ensure that it understands its partner authorities' legislative frameworks.

ii. **Report drafting (policy/legal analysis)**: Coordinating authorities will always retain the ability to conduct their own analysis, and ultimately, to come to different conclusions. Generally, it is unlikely for coordinating authorities to come to dramatically different conclusions, given that they would have discussed the issue in terms of their respective legislative frameworks. Additionally, regular communication throughout the course of the investigation will help ensure that authorities coordinate as new decisions are made based on evidence. For a joint investigation, coordinating authorities will generally have 2 options:

- **Joint report:** Where determinations will be based on analyses pursuant to materially similar legislation, and where the authorities are able to come to a general consensus with respect to their respective findings, the authorities may choose to issue a joint report. While it may be challenging to agree on wording, the report can be drafted to identify differences between the authorities' legislation and resulting analyses. A joint report also offers an opportunity to communicate and leverage a unified position with a view to obtaining greater cooperation from the organization and a more privacy robust outcome

- **Separate but coordinated reports:** Where an Authority must issue its own independent report, or where analyses may not be consistent across jurisdictions (even where the ultimate findings may be quite similar), coordinating authorities may choose to draft separate reports. Where their findings are similar, the authorities should consider leveraging the strength of a unified message by issuing the separate reports concurrently, perhaps under a joint cover letter summarizing their findings and/or expectations of the organization going forward

  **Note: Opportunity for information sharing:** If authorities do not to coordinate their analysis or report writing, they can still benefit from sharing the details of their respective analyses, to increase efficiency and validate findings. Such a strategy may allow authorities to: (i) come to more consistent conclusions based on a consistent understanding of the facts and with the benefit of each other's perspective; and/or (ii) be better prepared to explain any differences in findings across jurisdictions.

**Ashley Madison example:** In the context of the joint investigation conducted between the OPC and OAIC, the authorities mutually agreed that the OPC would be the single point of contact with Ashley Madison due to the company being based in Canada. All formal communications were discussed and approved in advance by both authorities. The OPC and OAIC jointly drafted and issued the final report of findings in close consultation, with the OAIC leading the process.

Simultaneously, the OPC/OAIC and FTC shared correspondence and responses from Ashley Madison, but did not have joint communications, given the demarcation between investigations. This was useful, as cross-referencing the responses from Ashley Madison to the 2 investigative processes provided valuable insights. All 3 authorities also conducted a joint site visit, which provided significant benefits by allowing investigators from the 3 authorities to coordinate and share expertise. The 3 authorities also shared high-level information regarding findings and planned next steps.

**Clearview AI example**: One of the first steps taken in planning the joint investigation was to establish which Office would take the lead/coordinating role, given the number of authorities. The authorities jointly agreed that the OPC was best positioned to fill this role, given capacity and the fact that Clearview provided its services across every province. The OPC closely coordinated with the other 3 authorities to obtain input, agreement and approval on each step of the investigation. The final report of findings was jointly drafted and issued.

## Public Communications

Public communications offer authorities the opportunity to amplify the results and lessons learned from their coordinated activities, and to build trust between partners by ensuring that the other partners are fully informed and prepared to respond to the resulting public reaction and enquiries.

Each Authority's legislative framework (or strategic approach) will dictate the extent to which it can publicize its involvement in an ongoing investigation or its findings in a completed investigation. It is important that all coordinating authorities: (i) understand, in advance of commencing an investigation, any limitations on publication; and (ii) respect each Authority's requirements when issuing its own public statements (for example, **Authority A** cannot publicize that it is investigating a matter but **Authority B** can. **B** wishes to publicize that it is investigating the matter. It may need to do so without referencing **A**'s involvement.)

Subject to the above limitations, authorities may choose to issue public communications using one of the following approaches:

i. **Joint communications:** Authorities may issue joint public communications. It may take time and effort to agree on exact wording, or to produce translations, but joint communications indicate unity and solidarity across jurisdictions, and can therefore be more impactful.

ii. **Coordinated communications:** If a coordinating Authority decides to issue separate and independent public communications, there will generally be value in sharing that messaging with its partners in advance of release. This will allow: (i) other authorities to issue coordinated, and therefore more impactful, concurrent messaging; (ii) to ensure that the messaging does not reveal information contrary to another partner's wishes; and/or (iii) allow authorities to be better prepared to explain any material differences between their respective messages.

Even if one authority's contribution to another authority's stand-alone investigation is limited (that is, information sharing, consultations on approach, etc.), a simple public statement that "an investigation benefitted from the assistance of Authority X can still send a positive message on international collaboration.

**Ashley Madison example:** In the context of the joint investigation conducted between the OPC and OAIC, the authorities pursued a coordinated communications strategy. The authorities issued separate and independent public communications, but discussed messaging and strategy in the context of the joint investigation.

Independent communications from the FTC also assisted in drawing attention and amplifying the results of the investigations.

The conclusion of the joint investigation received significant public attention in all 3 jurisdictions, and internationally. Based on media analysis, approximately 128 million people were reached via published news stories about the investigation. This informed a global audience of people and data-driven organizations about the importance of privacy protection in the digital age and the value of cross-border cooperation and enforcement, as well as providing a strong and global deterrence effect.

**Clearview AI example:** The authorities in the Clearview investigation used a mixture of joint and coordinated public communications to raise public awareness. In particular, the authorities jointly issued the initiation of the investigation and the news release of the results. The authorities agreed upon the content of these releases in advance, and issued them simultaneously. All 4 authorities also proceeded with a joint press conference, where the Commissioners and President of the CAI made statements and answered questions from the press. This communication strategy contributed to global coverage of the investigation and report of findings by national and international media, and amplified the impact of the case. Media analysis determined that an international audience of approximately 33 million was reached via published news stories about the

## Enforcement powers

Authorities' enforcement powers vary widely across jurisdictions, and can include the power to:

- issue fines or administrative monetary penalties
- issue orders
- enter into enforceable agreements, which can sometimes offer flexibility to achieve more holistic remedies
- carry out administrative or injunctive measures
- pursue compliance via court proceeding
- publicly name an organization

Authorities should ensure they are aware of their partners' enforcement powers (or limitations thereon) prior to entering into a collaborative investigation. Each power can be effective in achieving compliance, particularly as each Authority becomes adept at leveraging the unique set of enforcement tools in its toolkit. Enforcement powers may be complementary, offering an opportunity to exert increased pressure on an organization to comply. As such, respective enforcement powers may be an important factor to consider in choosing coordination partners.

For example, coordinating partners may choose a multi-phased approach to best leverage their respective powers. One Authority may start by publicly naming the organization with a view to encouraging expeditious voluntary compliance, and to educating stakeholders. In the event that this approach is unsuccessful, as an escalation measure, a second Authority could follow-up with legal proceedings to enforce compliance.

**Ashley Madison example:** As a result of the investigation, Ruby Corp made legally binding commitments to all 3 authorities, as well as several U.S. states, to improve its information security practises, and be more transparent with users about its information handling practices. Under an enforceable undertaking with Australia and a compliance agreement with Canada, Ruby Corporation was also required to reduce retention periods for customer data and enhance the accuracy of information it collected, while as a result of a settlement with the FTC and several U.S. states, the company was also required to pay approximately 1.6 million USD.

# Conclusion

There is a continuing move towards organizations having a global presence, and technology allowing ever-increasing volumes of personal data to be processed. Cooperation offers an opportunity for the global privacy enforcement community to address a global problem with a global solution. When considering enforcement cooperation, keep in mind the following key take-aways:

i. Develop and nurture inter-authority relationships, both formal and informal, at the most senior and operational levels – they are the foundation for cooperation. As the number of cross-regulatory matters increases, efforts should also be made to develop/maintain new relationships with authorities outside of the privacy sphere.

ii. Build internal capacity to be able to identify and respond to enforcement cooperation opportunities – for example, via development of protocols, enforcement cooperation training or secondments/exchanges.

iii. Information-sharing arrangements are generally necessary for enforcement cooperation – be proactive and put such arrangements in place to be responsive as enforcement cooperation opportunities arise.

iv. The appropriate form of cooperation will depend on the circumstances. Authorities can achieve positive results by simply sharing information or issuing a joint letter.

v. Enforcement cooperation, in all its forms, offers the opportunity to achieve greater compliance outcomes, more efficiently, in an era of increasing cross-border flows. Consider authorities' complementary strengths in choosing cooperation partners. At the same time, DPAs should consider whether their privacy expertise may be of assistance to authorities in other regulatory regimes (and vice versa) when exploring cross-regulatory opportunities.

vi. To avoid duplication of effort and fully maximize the benefits of a joint or coordinated investigation, develop consensus on a strategic plan that leverages each partner's strengths (whether that be location, available capacity, special expertise or powers).

vii. Trust is key to successful cooperation. To the greatest extent possible, partners should endeavour to: keep each other fully informed with respect to coordinated activities, adhere to their respective commitments, and be flexible with a view to achieving consensus.

# APPENDIX A

## Global Cross Border Enforcement Cooperation Arrangement

## Table of Contents

Preamble

1. Definitions

2. Purpose

3. Aims

4. Nature of the Arrangement

5. Reciprocity

6. Confidentiality

7. Respecting privacy and data protection principles

8. Coordination principles

9. Resolving problems

10. Allocation of costs

11. Return of evidence

12. Eligibility

13. Role of the Executive Committee

14. Withdrawal

15. Commencement

Schedule One

# Preamble

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

*Acknowledging* that a global phenomenon needs a global response and that it is in the interests of privacy enforcement authorities,[24] individuals, governments and businesses that effective strategies and tools be developed to avoid duplication, use scarce resources more efficiently, and enhance effectiveness in relation to enforcement in circumstances where the privacy and data protection effects transcend jurisdictional boundaries.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 1. Definitions

The following definitions will apply in this Arrangement:

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

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

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

'**Privacy Enforcement Authority**' (hereafter 'PEA')[25] means any public body that has as one of its responsibilities the enforcement of a privacy and/or data protection law, and that has powers to conduct investigations or take enforcement action.

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

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

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

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

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

## 2. Purpose

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

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

particularly confidential enforcement-related information about potential or ongoing investigations, and where appropriate, the Arrangement also coordinates PEAs' enforcement activities to ensure that their scarce resources can be used as efficiently and effectively as possible.

## 3. Aims

This Arrangement aims to achieve its objective by:

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

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

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

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

## 4. Nature of the Arrangement

This Arrangement sets forth the Participants' commitment with regard to international cross-border privacy enforcement cooperation, particularly on reciprocity, confidentiality, data protection, and coordination.

This Arrangement is NOT intended to:

i. replace existing national and regional conditions or mechanisms for sharing information, or to interfere with similar arrangements by other networks:

ii. create legally binding obligations, or affect existing obligations under other arrangements or international or domestic law;

iii. prevent a Participant from cooperating with other Participants or non-participating PEAs, pursuant to other (binding or non-legally binding) laws, agreements, treaties, or arrangements.

iv. create obligations or expectations of cooperation that would exceed a Participant's scope of authority and jurisdiction; or

v. compel Participants to cooperate on enforcement activities including providing non-confidential or confidential information which may or may not contain personal data.

## 5. Reciprocity Principle

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

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

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

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

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

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

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

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

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

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

## 6. Confidentiality Principle

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

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

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

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

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

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

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

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

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

## 7. Respecting Privacy and Data Protection Principles

Depending on Participants or the enforcement activity in question, it may be necessary to exchange personal data. However, in accordance with recognised privacy and data protection principles, the exchange of such personal data should be limited to what is necessary for effective privacy and data protection enforcement. All Participants to this Arrangement who either disclose or receive personal data will use their best efforts to respect the data protection safeguards of each other. However, it is recognised that these best efforts alone will not always be sufficient to enable the exchange of personal data.

In that case, if the Participant disclosing the personal data requires specific data protection safeguards, they should either:

- request the other Participants to provide assurance that they will comply with the requirements outlined in Schedule One; or,

- make other arrangements between those who disclose and receive personal data to ensure that each Participant's privacy and data protection requirements are fully observed. Participants should notify the Committee if they are committing to the requirements set out in Schedule One or notify the Committee of other arrangements as referenced above. In principle, this notification should be done when submitting a notice of intent to participate in accordance with section 13, or, in any case before receiving personal data from another Participant under this Arrangement. A list of Participants, including their initial and updated notifications regarding Schedule One and/or other arrangements as described above, will be made available to all Participants.

## 8. Coordination Principles

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

(i) Identifying Possible Coordinated Activities

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

(ii) Assessing Possible Participation

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

(iii) Participating in Coordinated Actions

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

(iv) Facilitating Coordination

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

(v) Leading Coordinated Action

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

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

## 9. Resolving Problems

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

## 10. Allocation of Costs

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

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

## 11. Return of Evidence

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

## 12. Eligibility Criteria

Any PEA may submit a notice of intent to the Committee indicating that they intend to participate in this Arrangement:

(i) As a Member, if they are an accredited member of the International Conference of Data Protection and Privacy Commissioners (the Conference) and, as such, fulfil the membership requirements of Paragraph 5.1 of the Rules and Procedures of the Conference, including the requirement of appropriate autonomy and independence; or

(ii) As a Partner if, although not an accredited member of the Conference, they are:
   a. from a Member State signatory to the Convention for the Protection of Individuals with Regard to Automatic Processing (Convention 108); or
   b. a member of the Global Privacy Enforcement Network (GPEN); or
   c. a Participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA); or
   d. a member of the Article 29 Working Party.

The Committee will keep an updated list of all PEAs that have committed to participate in the Arrangement and of all Participants that have committed to respect Schedule One or that have submitted a notice in accordance with section 5. The list should be easily available to all Participants

## 13. Role of the International Conference Executive Committee

The Committee will:

a. Receive notices of intent to participate in or withdraw participation in this
b. Arrangement;
c. Receive notices of commitment to Schedule One or such other arrangements as referenced in clause seven above and notices submitted in accordance with section 5;
d. Review such notices in order to verify that a PEA is eligible to sign this Arrangement;
e. Review the operation of the Arrangement three years after its commencement and submit its findings to the International Conference;
f. Publicise this Arrangement;
g. Recommend to the International Conference, upon due consideration of evidence, that a Participant to this Arrangement should have their participation suspended. Or, in the most serious cases of breach of the requirements set out in this Arrangement and thus breaching the trust that this Arrangement establishes between Participants, recommend to the International Conference that the Participant should be excluded from the Arrangement.

## 14. Withdrawal from the Arrangement

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

A Participant shall, as soon as reasonably practicable after notifying the Committee of its intention to withdraw participation in this Arrangement, take all reasonable steps to make its withdrawal from participation known to

other Participants. This should include posting such information on the Participant's website whilst still participating in the Arrangement and for a reasonable period after ceasing to participate.

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

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

## 15. Commencement

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

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

## Schedule One

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In particular, those personal information which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be

considered sensitive data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.

---

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

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

# APPENDIX B

## MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES FEDERAL TRADE COMMISSION AND THE DUTCH DATA PROTECTION AUTHORITY ON MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR

The United States Federal Trade Commission ("FTC") and the Dutch Data Protection Authority (“College bescherming persoonsgegevens” or “CBP”), (collectively, "the Participants"),

RECOGNIZING the nature of the modern global economy, the increase in the flow of personal information across borders, the increasing complexity and pervasiveness of information technologies, and the resulting need for increased cross-border enforcement cooperation;

RECOGNIZING that the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, the Global Privacy Enforcement Network’s Action Plan, resolutions of the International Conference of Data Protection and Privacy Commissioners, and the APEC Privacy Framework call for the development of cross-border information-sharing mechanisms and enforcement cooperation arrangements; and that such information sharing and enforcement cooperation are essential elements to ensure privacy and data protection compliance, serving an important public interest;

RECOGNIZING that the U.S. Federal Trade Commission Act, 15 U.S.C. § 41 et seq., as amended by the U.S. SAFE WEB Act, authorizes the FTC to share information with law enforcement authorities from other countries under appropriate circumstances;

RECOGNIZING that subsection 1 and 2 of Section 2:5 of the Dutch General Administrative Law Act (de Algemene wet bestuursrecht) provide that a Dutch public body may disclose confidential information to (a) person(s) or organization who is involved in the execution of the task of this Dutch public body if this is

necessary to fulfill the supervisory task of the Dutch public body and the confidentiality of the information is maintained;

RECOGNIZING that the CBP is the designated authority in the Netherlands for the purposes of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (which was opened for signature on 28th January 1981) and is the supervisory authority in the Netherlands for the purposes of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

RECOGNIZING that the Participants each have functions and duties with respect to the protection of personal information in their respective countries;

RECOGNIZING that the Participants have worked together in connection with several international initiatives related to privacy;

REGOGNIZING that the Participants have cooperated in the context of several international networks, including the Global Privacy Enforcement Network, and the International Conference of Data Protection and Privacy Commissioners; and

RECOGNIZING that the Participants would not be able to provide assistance to the other if such assistance is prohibited by their respective national laws, such as privacy, data security, or confidentiality laws; or enforcement policies.

HAVE REACHED THE FOLLOWING UNDERSTANDING:

## I. **Definitions**

For the purposes of this Memorandum,

A. "Applicable Privacy Law" means the laws identified in Annex 1, which may be revised by mutual consent of the Participants, including any regulations implemented pursuant to those laws, the enforcement of which has the effect of protecting personal information.

B. "Covered Privacy Violation" means practices that would violate the Applicable Privacy Laws of one Participant's country and that are the same or substantially similar to practices prohibited by any provision of the Applicable Privacy Laws of the other Participant's country.

C. “Person” means any natural person or legal entity, including corporations, unincorporated associations, or partnerships, established, existing under or authorized by the laws of the United States, its States, or its Territories, or the laws of the Netherlands.

D. "Request" means a request for assistance under this Memorandum.

E. "Requested Participant" means the Participant from which assistance is sought under this Memorandum, or which has provided such assistance.

F. “Requesting Participant” means the Participant seeking assistance under this Memorandum, or which has received such assistance.

## II. **Objectives and Scope**

A. This Memorandum of Understanding sets forth the Participants’ intent with regard to mutual assistance and the exchange of information for the purpose of investigating, enforcing and/or securing compliance with Covered Privacy Violations. The Participants do not intend the provisions of this Memorandum of Understanding to create legally binding obligations under international or domestic laws.

B. The Participants understand that it is in their common interest to:

1. cooperate with respect to the enforcement of the Applicable Privacy Laws, including sharing complaints and other relevant information and providing investigative assistance;

2. facilitate research and education related to the protection of personal information;

3. facilitate mutual exchange of knowledge and expertise through training programs and staff exchanges;

4. promote a better understanding by each Participant of economic and legal conditions and theories relevant to the enforcement of the Applicable Privacy Laws; and

5. inform each other of developments in their respective countries that relate to this Memorandum.

C. In furtherance of these common interests, and subject to Section IV, the Participants intend to use best efforts to:

1. share information, including complaints and other personally identifiable information, that a Participant believes would be relevant to investigations or enforcement proceedings regarding Covered Privacy Violations of the Applicable Privacy Laws of the other Participant's country;

2. provide investigative assistance in appropriate cases, including obtaining evidence under the Participants' respective legal authorities on behalf of the other Participant;

3. exchange and provide other relevant information in relation to matters within the scope of this Memorandum, such as information relevant to consumer and business education; government and self-regulatory enforcement solutions; amendments to relevant legislation; technological expertise, tools or techniques; privacy and data security research; and staffing and resource issues;

4. explore the feasibility of staff exchanges and joint training programs;

5. coordinate enforcement against cross-border Covered Privacy Violations that are priority issues for both Participants;

6. participate in periodic teleconferences to discuss ongoing and future opportunities for cooperation; and

7. provide other appropriate assistance that would aid in the enforcement against Covered Privacy Violations.

## III. **Procedures Relating to Mutual Assistance**

A. Each Participant is to designate a primary contact for the purposes of requests for assistance and other communications under this Memorandum.

B. If a Participant requests assistance for matters involved in the enforcement of Applicable Privacy Laws, then Participants understand that:

1. requests for assistance are to include sufficient information to enable the Requested Participant to determine whether a request relates to a Covered Privacy Violation and to take action in appropriate circumstances. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request;

2. requests for assistance are to specify the purpose for which the information requested will be used;

3. consistent with Section V.A., a request for assistance certifies that, subject to any relevant applicable legal restrictions in its own jurisdiction on its ability to do so, the Requesting Participant is to maintain confidentiality in respect of:
- each request for assistance,
- the existence of any investigation related to the request,
- all materials related to each request, and
- all information and material provided in response to each request, unless otherwise decided; and,

4. prior to requesting assistance, Participants should perform a preliminary inquiry to ensure that the request is consistent with the scope of this Memorandum.

C. Participants should use their best efforts to resolve any disagreements related to cooperation that may arise under this Memorandum through the contacts designated under Section III.A, and, failing resolution between the designated contacts in a reasonably timely manner, by discussion between appropriate senior officials designated by the Participants.

## IV. **Limitations on Assistance**

A. The Requested Participant may exercise its discretion to decline the request for assistance, or limit or condition its cooperation, including where it is outside the scope of this Memorandum, or more generally, where it would be inconsistent with domestic laws, or important interests or priorities.

B. The Participants recognize that it is not feasible for a Participant to offer assistance to the other Participant for every Covered Privacy Violation.

Accordingly, the Participants intend to use best efforts, as outlined in Section II, to seek and provide cooperation focusing on those Covered Privacy Violations most serious in nature, such as those that cause or are likely to cause damage or distress to a significant number of persons, and those otherwise causing substantial damage or distress, especially if this concerns both countries.

C. If the Requested Participant is unable to offer full assistance or declines assistance, it should explain the reasons why.

D. Participants intend, in so far as they are able and are allowed by their domestic laws, to share confidential information pursuant to this Memorandum only to the extent that it is necessary to fulfill the purposes set forth in Section II.

## V. **Confidentiality, Privacy, and Limitations on Use**

A. Subject to any restrictions imposed by their respective national laws, to the fullest extent possible, each Participant certifies the confidentiality of information to be shared under this Memorandum. The certification of confidentiality applies not only to the shared information, but also to the existence of an investigation to which the information relates. The Participants are to treat the shared information, the existence of the investigation to which the information relates, and any requests made pursuant to this Memorandum as confidential, and so far as they are able, not further disclose or use this information for purposes other than those for which it was originally shared, without the prior written consent of the Requested Participant.

B. Notwithstanding Section V.A., it is understood that:

1. A Participant may disclose information provided pursuant to this Memorandum in response to a formal request from a Participant country's legislative body or an order issued from a court with proper jurisdiction in an action commenced by the Participant or its government.

2. Material obtained in connection with the investigation or enforcement of criminal laws may be used for the purpose of investigation, prosecution, or prevention of violations of either Participant's country's criminal laws.

C. Each Participant is to use best efforts to safeguard the security of any information received under this Memorandum and respect any safeguards decided by the Participants. In the event of any access to, or disclosure of, the information not authorized by a Participant, the Participants are to take all reasonable steps to prevent a recurrence of the event and are to notify the other Participant of the occurrence.

D. Where a Participant receives an application by a third party for disclosure of confidential information or materials received from a Requested Participant, the Requesting Participant should notify the Requested Participant forthwith and seek to obtain that Participant's consent to the release of the information or – if the Requested Participant does not agree with the disclosure – oppose, to the fullest extent possible consistent with their countries' laws, any request for disclosure. Where the Participant that receives an application for disclosure from a third party is unable to obtain consent for its disclosure from the Requested Participant, if the Receiving Participant is nevertheless obliged under its laws to release the information, it should notify the Requested Participant as soon as possible of its decision to disclose the information, as well as the general procedure concerning the disclosure of information.

E. The Participants recognize that material exchanged in connection with investigations and enforcement often contains personally identifiable information. If the Requesting Participant wishes to obtain confidential information that includes personally identifiable information, then the Participants understand that they are to take additional appropriate measures to safely transmit and safeguard the materials containing personally identifiable information. Protective measures include, but are not limited to, the following examples and their reasonable equivalents, which can be used separately or combined as appropriate to particular circumstances:

1. transmitting the material in an encrypted format;

2. transmitting the material directly by a courier with package tracking capabilities;

3. transmitting the materials by facsimile rather than non-encrypted email;

4. maintaining the materials in secure, limited access locations (e.g., password-protected files for electronic information and locked storage for hard-copy information); and

5. if used in a proceeding that may lead to public disclosure, redacting personally identifiable information or filing under seal.

## VI. **Changes in Applicable Privacy Laws**

In the event of significant modification to the Applicable Privacy Laws of a Participant's country falling within the scope of this Memorandum, the Participants intend to consult promptly, and, if possible, prior to the entry into force of such enactments, to determine whether to modify this Memorandum.

## VII. **Retention of Information**

A. If Participants wish to retain materials obtained from the other Participant under this Memorandum, the Participants understand they are not to retain such materials for longer than is reasonably required to fulfill the purpose for which they were shared or for longer than is required by the Requesting Participant's country's laws.

B. The Participants recognize that in order to fulfill the purpose for which the materials were shared, the Participants typically need to retain the shared materials until the conclusion of the pertinent investigation or related proceedings for which the materials were requested, including until a judgment has become irrevocable.

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

## VIII. **Costs**

Unless otherwise decided by the Participants, the Requested Participant is expected to pay all costs of executing the request for information. When such costs are substantial, the Requested Participant may ask the Requesting Participant to pay those costs as a condition of proceeding with the Request. In such an event, the Participants should consult on the issue at the request of either Participant.

## IX. **Duration of Cooperation**

A. The Participants intend cooperation in accordance with this Memorandum to become available as of the date it is signed by both Participants.

B. Assistance in accordance with this Memorandum is understood to be available concerning Covered Privacy Violations occurring before as well as after this arrangement is signed.

C. A Participant should endeavor to provide 30 days advance written notice to the other Participant that it plans to withdraw from the understanding set out in this Memorandum. However, prior to providing such notice, each Participant should use best efforts to consult with the other Participant.

D. Upon cessation of cooperation through this Memorandum, the Participants, in accordance with Section V, are to maintain the confidentiality of any information communicated to them by the other Participant in accordance with this Memorandum, and return or destroy, in accordance with the provisions of Section VII, information obtained from the other Participant in accordance with this Memorandum.

## X. **Legal Effect**

Nothing in this Memorandum is intended to:

A. Create binding obligations, or affect existing obligations, under international or domestic law.

B. Prevent a Participant from seeking assistance from or providing assistance to the other Participant pursuant to other agreements, arrangements, or practices.

C. Affect any right of a Participant to seek information on a lawful basis from a Person located in the territory of the other Participant's country, or preclude any such Person from voluntarily providing legally obtained information to a Participant.

D. Create a commitment that conflicts with either Participant’s national laws, court orders, or any applicable international legal instruments.

E. Create expectations of cooperation that would exceed a Participant's powers.

Signed at Washington, D.C.
On March 6, 2015, in duplicate.

| | |
|---|---|
| _____ | _____ |
| Edith Ramirez<br>Chairwoman | Jacob Kohnstamm<br>Chairman |
| United States Federal Trade Commission | Dutch Data Protection Authority |

# MEMORANDUM OF UNDERSTANDING

# BETWEEN

# THE PRIVACY COMMISSIONER OF CANADA AND THE INFORMATION COMMISSIONER OF THE UNITED KINGDOM

# ON

# MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR

The Privacy Commissioner of Canada ("PCC") and the Information Commissioner of the United Kingdom ("IC") ("the Participants"):

RECOGNISING the nature of the modern global economy, the increase in circulation and exchange of personal information across borders, the increasing complexity and pervasiveness of information technologies, and the resulting need for increased cross-border enforcement cooperation;

RECOGNISING that both the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy and the APEC Privacy Framework call on member countries and economies to develop cross-border information sharing mechanisms and bilateral or multilateral enforcement cooperation arrangements;

RECOGNISING that s. 23.1 of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 authorizes the PCC to share information with authorities from other countries that have responsibilities relating to the protection of personal information in the private sector;

RECOGNISING that the IC is the designated authority in the United Kingdom for the purposes of Article 13 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which was opened for signature on 28th January 1981 and is the supervisory authority in the United Kingdom for the purposes of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

RECOGNISING that the Participants each have functions and duties with respect to the protection of personal information in the private sector in their respective countries; and

RECOGNISING that nothing in this Memorandum requires the Participants to provide assistance in the enforcement of laws protecting personal information in the private sector if such assistance is prohibited by their respective national laws or enforcement policies.

HAVE REACHED THE FOLLOWING UNDERSTANDING:

I. **I. Definitions**

For the purposes of this Memorandum,

A. "Applicable Privacy Laws" means the laws and regulations of the Participant's country the enforcement of which have the effect of protecting personal information. In the case of the PCC, "Applicable Privacy Law" means Part 1 of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*") and, in the case of the IC, it means the Data Protection Act 1998; as well as any amendments to the Participants' Applicable Privacy Laws, and such other laws or regulations as the Participants may from time to time jointly decide in writing to be an Applicable Privacy Law for purposes of this Memorandum.
B. "Person" means any natural person or legal entity, including any corporation, unincorporated association, or partnership.
C. "Request" means a request for assistance under this Memorandum.
D. "Requested Participant" means the Participant from which assistance is sought under this Memorandum, or which has provided such assistance.
E. "Requesting Participant" means the Participant seeking or receiving assistance under this Memorandum.
F. "Covered Privacy Contravention" means conduct that would be in contravention of the Applicable Privacy Laws of one Participant's country and that is the same or substantially similar to conduct that would be in contravention of the Applicable Privacy Laws of the other Participant's country.

## II. Objectives and scope

A. The Participants understand that it is in their common interest to:
    1. cooperate with respect to the enforcement of the Applicable Privacy Laws, including the sharing of relevant information and the handling of complaints in which the Participants are mutually interested;
    2. facilitate research and education related to the protection of personal information;
    3. promote a better understanding by each Participant of economic and legal conditions and theories relevant to the enforcement of the Applicable Privacy Laws; and
    4. keep each other informed of developments in their respective countries having a bearing on this Memorandum.
B. In furtherance of these common interests, and subject to Section IV, the Participants will use best efforts to:
    1. share information that a Participant believes would be relevant to ongoing or potential investigations or proceedings in respect of Covered Privacy Contraventions of the Applicable Privacy Laws of the other Participant's country;
    2. exchange and provide relevant information in relation to matters within the scope of the Memorandum, such as information relevant to consumer and business education; government and self-regulatory enforcement solutions; amendments to relevant legislation; and staffing and resource issues; and
    3. arrange for short-term, and possibly long-term, staff exchanges to facilitate and develop enforcement cooperation between the Participants.
C. In furtherance of these common interests, and subject to Section IV, the Participants recognize the following item as a priority issue for potential cooperation:
    1. potential parallel or joint investigations or enforcement actions by the Participants.

## III. Procedures Relating to Mutual Assistance

A. Each Participant will designate a primary contact for the purposes of requests for assistance and other communications under this Memorandum.

B. In requesting assistance in procedural, investigative and other matters involved in the enforcement of Applicable Privacy Laws across borders, Participants will ensure that:
    1. requests for assistance include sufficient information to enable the Requested Participant to determine whether a request relates to a Covered Privacy Contravention and to take action in appropriate circumstances. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request;
    2. requests for assistance specify the purpose for which the information requested will be used; and
    3. prior to requesting assistance, Participants perform a preliminary inquiry to ensure that the request is consistent with the scope of this Memorandum and does not impose an excessive burden on the Requested Participant.

C. Participants intend to communicate and cooperate with each other, as appropriate, about matters that may assist ongoing investigations.

D. The Participants will notify each other without delay, if they become aware that information shared under this Memorandum is not accurate, complete, and up-to-date.

E. Subject to Section IV, Participants may, as appropriate and subject to their Applicable Privacy Laws, refer complaints to each other, or provide each other notice of possible Covered Privacy Contraventions of the Applicable Privacy Laws of the other Participant's country.

F. Participants will use their best efforts to resolve any disagreements related to co-operation that may arise under this Memorandum through the contacts designated under Section III. A, and, failing resolution in a reasonably timely manner, by discussion between the heads of the Participants.

## IV. **Limitations on Assistance and Use**

A. The Requested Participant may exercise its discretion to decline a request for assistance, or limit or condition its cooperation, in particular where it is outside the scope of this Memorandum, or more generally where it would be inconsistent with domestic laws, or important interests or priorities. The Requesting Participant may request the reasons for which the Requested Participant declined or limited assistance.

B. Participants will only share personal information pursuant to this Memorandum to the extent that it is necessary for fulfilling the purposes of this Memorandum, and will, wherever possible, use best efforts to obtain the consent of the individual(s) concerned before doing so.

C. For greater certainty, the PCC will not share confidential information unless
    a. it is for the purpose set out in Section II.B.1; or
    b. it is necessary for making a request for assistance from the other Participant regarding information that may be useful to an ongoing or potential investigation or audit under Part 1 of *PIPEDA*.

D. Participants will not use any information obtained from the Requested Participant for purposes other than those for which the information was originally shared.

## V. **Confidentiality**

A. Information shared under this Memorandum is to be treated as confidential and will not be further disclosed without the consent of the other Participant.

B. Each participant will use best efforts to safeguard the security of any information received under this Memorandum and respect any safeguards agreed to by the Participants. In the event of any unauthorized access or disclosure of the information, the Participants will take all reasonable steps to prevent a recurrence of the event and will promptly notify the other Participant of the occurrence.

C. The Participants will oppose, to the fullest extent possible consistent with their countries' laws, any application by a third party for disclosure of confidential information or materials received from Requested Participants, unless the Requested Participant consents to its release. The Participants who receives such an application will notify forthwith the Participant that provided it with the confidential information.

## VI. Changes in Applicable Privacy Laws

In the event of modification to the Applicable Privacy Laws of a Participant's country that are within the scope of this Memorandum, the Participants will use best efforts to consult promptly, and, if possible, prior to the entry into force of such enactments, to determine whether to amend this Memorandum.

## VII. Retention of Information

Information received under this Memorandum will not be retained for longer than is required to fulfill the purpose for which it was shared or than is required by the Requesting Participant's country's laws. The Participants will use best efforts to return any information that is no longer required if the Requested Participant makes a written request that such information be returned at the time it is shared. If no request for return of the information is made, the Requesting Participant will dispose of the information using methods prescribed by the Requested Participant or if no such methods have been prescribed, by other secure methods, as soon as practicable after the information is no longer required.

## VIII. Costs

Unless otherwise decided by the Participants, the Requested Participant will pay all costs of executing the Request. When the cost of providing or obtaining information under this Memorandum is substantial, the Requested Participant may ask the Requesting Participant to pay those costs as a condition of proceeding with the Request. In such an event, the Participants will consult on the issue at the request of either Participant.

## IX. Duration of Cooperation

A. This Memorandum takes effect on the date it is signed.
B. Assistance in accordance with this Memorandum will be available concerning Covered Privacy Contraventions occurring before as well as after this Memorandum is signed.
C. This Memorandum may be terminated on 30 days written notice by either Participant. However, prior to providing such notice, each Participant will use best efforts to consult with the other Participant.
D. This Memorandum can be modified, or supplemented, as agreed by the Participants in writing.
E. On termination of this Memorandum, the Participants will, in accordance with Section V, maintain the confidentiality of any information communicated to them by the other Participant in accordance with this Memorandum, and return or destroy, in accordance with the provisions of Section VII, information obtained from the other Participant in accordance with this Memorandum.

## X. Legal Effect

Nothing in this Memorandum is intended to:

A. create binding obligations, or affect existing obligations under international law, or create obligations under the laws of the Participants' countries;
B. prevent a Participant from seeking assistance from or providing assistance to the other Participant pursuant to other agreements, treaties, arrangements, or practices;
C. affect any right of a Participant to seek information on a lawful basis from a Person located in the territory of the other Participant's country, nor is it intended to preclude any such Person from voluntarily providing legally obtained information to a Participant; or
D. create obligations or expectations of cooperation that would exceed a Participant's jurisdiction.

Signed in duplicate at Montreal, Quebec, Canada on May 14, 2012, in the English and French languages, each version being equally authentic.

*Original signed by*

Christopher Graham
Information Commissioner of the United Kingdom

Date: 2012-05-14
At: Montreal, Quebec, Canada

*Original signed by*

Jennifer Stoddart
Privacy Commissioner of Canada

Date: 2012-05-14
At: Montreal, Quebec, Canada

**MEMORANDO DE ENTENDIMIENTO ENTRE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DEL REINO DE ESPAÑA**

**REUNIDOS**

De una parte, Mar España Martí, Directora de la Agencia Española de Protección de Datos, cargo para el que fue nombrada por Real Decreto 715/2015 de 24 de julio, en nombre y representación de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (en adelante, la "AEPD"), y

De otra parte, Andrés Barreto González, Superintendente de Industria y Comercio, cargo para el que fue nombrado mediante el decreto 1806 del 20 de septiembre de 2018[1], en nombre y representación de la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA (en adelante, la "SIC").

**Reconociendo** la necesidad garantizar el debido tratamiento de los datos personales y los riesgos en la circulación e intercambio de información personal transfronteriza, la creciente complejidad de las tecnologías de la información y la consiguiente necesidad de incrementar la cooperación internacional;

**Reconociendo** la importancia de la protección de los datos personales para promover un desarrollo nacional sólido y la confianza en los flujos internacionales de información;

**Deseando** fomentar una cooperación más estrecha entre ambas partes en el campo de la protección de datos a fin de promover la creación, protección y aplicación de la normativa de protección de datos;

**DECLARAN**

I. Que la AEPD es una autoridad administrativa independiente, con personalidad jurídica propia y plena capacidad pública y privada, que ostenta las competencias atribuidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos o RGPD), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Corresponde a la AEPD ejercer las funciones establecidas en el artículo 57 del RGPD, entre las que se encuentran controlar la aplicación del propio Reglamento y hacerlo aplicar; promover la sensibilización del público y su comprensión de los riesgos; normas, garantías y derechos en relación con el tratamiento de los mismos; promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben, así como cualquier otra función relacionada con la protección de los datos personales.

II.- Que, de conformidad con lo dispuesto en el artículo 71 de la Ley 1151 de 2007 y el Decreto 4886 de 2011, la SIC es un organismo de carácter técnico con personería jurídica, que goza de

[1] Cfr. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201806%20DEL%2020%20DE%20SEPTIEMBRE%20DE%202018.pdf

autonomía administrativa, financiera, presupuestal y cuenta con patrimonio propio, denominada entidad estatal para efectos contractuales de acuerdo con lo señalado ene I literal b) del numeral 1 del artículo 2 de la Ley 80 de 1993.

III.- Que la SIC funge como Autoridad Nacional en materia de Protección de Datos Personales, y en sus acciones vela por garantizar que, en la recolección, el uso, la circulación y el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y en la Ley y además exige el respeto del "habeas data" previsto en el artículo 15 de la Constitución Política Nacional.

De la misma manera, el artículo 3 del Decreto 4886 de 2011 establece que, dentro de las funciones del Despacho del Superintendente de Industria y Comercio, está la de asesorar al Gobierno Nacional y participar en la formulación de las políticas relacionadas con la promoción a la protección de datos personales. A su vez, de acuerdo con el artículo 16 del Decreto 4886 de 2011, dentro de las funciones del Despacho del Superintendente Delegado para la Protección de Datos Personales, está la de velar por el cumplimiento de las normas y leyes vigentes en materia de protección de datos personales, y proponer nuevas disposiciones.

IV.- Que la Superintendencia de Industria y Comercio aprobó o acordó la suscripción del presente Memorando.

V.- Que la AEPD y la SIC forman parte, en condición de Miembros, de la Red Iberoamericana de Protección de Datos (en adelante, RIPD), foro creado como respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los Países Iberoamericanos, a través del diálogo y la colaboración en materia de protección de datos de carácter personal.

VI. Que uno de los logros más destacados en el ámbito de la cooperación promovida en el marco de la RIPD ha sido la aprobación de los "Estándares en materia de Protección de Datos para los Estados Iberoamericanos" (en adelante, "los Estándares"), fruto de un importante esfuerzo por dotar a la Comunidad Iberoamericana de un marco común que sirva de referencia a la hora de aprobar las respectivas normativas de protección de datos, o para adaptar las vigentes.

VII. Que, entre los objetivos prioritarios de los Estándares, está el de "Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia". En particular, su numeral 45 establece que: "Los Estados Iberoamericanos podrán adoptar mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales aplicables en la materia, los cuales podrán comprender, de manera enunciativa más no limitativa: a) El establecimiento de mecanismos que permitan reforzar la asistencia y cooperación internacional en la aplicación de las respectivas legislaciones nacionales en la materia; b) La asistencia entre las autoridades de control a través de la notificación y remisión de reclamaciones, la asistencia en investigaciones y el intercambio de Información, y c) La adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en

materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países".

VIII. Que ambas instituciones, conscientes de la importancia de proteger de manera adecuada el derecho fundamental a la protección de los datos personales, quieren dejar constancia de su interés en desarrollar una estrecha colaboración que sirva de marco general para la realización de actividades conjuntas de cooperación, formación, desarrollo de programas y proyectos específicos en las áreas que ambas partes determinen de mutuo acuerdo.

IX. Que, en consideración a la voluntad de los firmantes de colaborar en las acciones descritas a continuación, la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS y la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO de Colombia, acuerdan suscribir el presente MEMORANDO DE ENTENDIMIENTO (en adelante, el Memorando), que se regirá por las siguientes

## CLÁUSULAS

**PRIMERA.- OBJETO.**

El presente Memorando tiene por objeto establecer las bases de la colaboración institucional entre sus firmantes, con la finalidad de promover la difusión del derecho a la protección de datos de carácter personal; velar por la cooperación conjunta en materia de protección de datos personales y brindar un marco para el intercambio de conocimientos técnicos y mejores prácticas, que permitan fortalecer las capacidades técnicas de ambas partes relacionadas con la aplicación de la ley en materia de protección de datos personales.

**SEGUNDA. ALCANCE DE LA COOPERACIÓN.**

Para el cumplimiento de los objetivos del presente Memorando, los firmantes asumen los siguientes compromisos generales:

a. Impulsar mecanismos específicos de cooperación técnica que permitan, de manera enunciativa más no limitativa, intercambiar conocimientos y experiencias, e identificar las mejores prácticas en materia de protección de datos personales;

b. Fomentar y contribuir a la realización de investigaciones, estudios, análisis e informes en materia de protección de datos personales;

c. Colaborar en la elaboración y difusión de guías, herramientas y otros materiales orientados a facilitar el cumplimiento de la legislación de protección de datos por parte de los sujetos obligados;

d. Favorecer los mecanismos de asistencia jurídica y cooperación técnica para la aplicación efectiva de sus legislaciones nacionales y, en especial, en el marco de las potestades de investigación conferidas por sus respectivas legislaciones nacionales;

e. Impulsar el desarrollo de iniciativas conjuntas, prioritariamente en el marco de programas y proyectos internacionales, que contribuyan a reforzar las respectivas competencias en sectores y ámbitos con un importante impacto social, ambiental e institucional, en especial en materia de igualdad de género, menores e innovación y emprendimiento, y

f. En general, impulsar cualquier actuación que consideren necesario para el más adecuado cumplimiento de sus respectivas competencias, dentro de los límites de sus legislaciones nacionales y, en su caso, del derecho internacional que pudiera resultar aplicable en la materia.

**TERCERA. COMPROMISO CON LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD).**

1. Los firmantes reafirman su compromiso con la Red Iberoamericana de Protección de Datos, destacando el papel relevante que dicha Red desempeña actualmente en la Región y coincidiendo en la necesidad de impulsar, en el estado actual de la misma, nuevos espacios e instrumentos de cooperación entre sus miembros, específicamente, a partir de la aprobación de los Estándares que se constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes, así como al desarrollo de mecanismos de cooperación internacional entre las autoridades de control.

2. En este sentido, la SIC, que desempeña en la actualidad la Presidencia de la RIPD, y la AEPD, en su condición de Secretaría Permanente de la RIPD, advierten sobre la necesidad imperiosa de impulsar mecanismos y acciones de colaboración concretas para que los Estándares impacten en las iniciativas y proyectos en la materia de la región y, en su caso, de otras regiones y organismos internacionales, con la finalidad de lograr su trascendencia más allá de su aprobación.

3. En especial, de conformidad con el Plan Estratégico de la RIPD 2021-2025, aprobado en la sesión cerrada (online) del XVIII Encuentro Iberoamericano de Protección de Datos, celebrada el 4 de diciembre de 2020, las instituciones firmantes trabajarán, en el marco de la RIPD, en favor de la creación de un nuevo espacio que promueva la cooperación efectiva entre las Autoridades Iberoamericanas de Protección de Datos, y en particular en el impulso de las siguientes acciones:

- Potenciar el papel del Grupo Permanente de Autoridades Nacionales de Protección de Datos (GPAN) creado en el marco del XVII Encuentro Iberoamericano de Protección de Datos como foro específico para que las Autoridades Iberoamericanas puedan establecer criterios o directrices comunes en ámbitos de especial impacto para la privacidad, especialmente los relacionados con el desarrollo de las nuevas tecnologías de tratamiento masivo de los datos personales (Big Data, Internet de las Cosas, Inteligencia Artificial ....). En tal sentido, se contemplará el establecimiento de un mecanismo para que esos criterios o directrices queden plasmados, por ejemplo, mediante la adopción de resoluciones específicas o la implementación de grupos de trabajo que puedan llevar a cabo el seguimiento de los temas.

- Identificar casos reales que afecten a ciudadanos de varios países de la red con miras a que todas las autoridades de la red o la mayoría de ellas actúen de oficio y desde sus países frente a dichas situaciones y dentro del marco de sus competencias legales.

- Difundir entre los países integrantes de la Red las resoluciones sobre casos relacionados al tratamiento ilícito de datos personales por parte de empresas transnacionales con la finalidad de promover experiencias que sirvan como antecedentes en la materia.

- Impulsar fórmulas e instrumentos de cooperación efectiva (enforcement) entre las Autoridades, especialmente de asistencia jurídica mutua en el ámbito de la investigación y evaluación tecnológica, así como en otros ámbitos (intercambio de información de guías y herramientas, planificación estratégica, etc.).

- Promover el desarrollo de unidades o divisiones de innovación para que las Autoridades puedan estar atentas a las últimas novedades y tendencias en el ámbito tecnológico.

- Fomentar el intercambio de buenas prácticas y la adopción de iniciativas concretas, incluso a título experimental, de experiencias de cooperación efectiva entre las Autoridades Iberoamericanas de Control.

- Apoyar la generación de estudios e investigaciones, y, en general, de cuantas iniciativas tengan por objeto un mejor conocimiento del estado de situación de la protección de datos en Iberoamérica.

- Desarrollar programas de capacitación y formación online del personal directivo y empleados de las Autoridades, tanto para reforzar la cultura de la protección de datos en estas organizaciones públicas, como para promover una formación especializada en la materia, necesaria en ámbitos tecnológicos cada vez más complejos y exigentes.

- Fomentar programas de estancias temporales entre empleados y directivos de las Autoridades Iberoamericanas de Protección de Datos, para mejorar el conocimiento y el intercambio de experiencias entre las distintas culturas administrativas que integran la RIPD.

**CUARTA. MEMORANDOS ESPECÍFICOS DE COLABORACIÓN.**

1. El desarrollo de las actividades conjuntas se realizará mediante la celebración y ejecución de Memorandos Específicos de Colaboración que se integrarán como anexos al presente instrumento, donde se deberá precisar lo siguiente:

a) Objetivos y actividades a realizar o ejecutar;
b) Compromisos asumidos por cada una de las partes;
c) En su caso, presupuesto disponible y fuentes de financiamiento;
d) Personal designado, instalaciones y equipo a utilizar;
e) Calendario de trabajo y mecanismos de evaluación, y

f) En general, todo aquello que resulte necesario para determinar con exactitud los fines y alcances aprobados por los firmantes en cada uno de los memorandos.

2. Cada uno de los Memorandos específicos serán sometidos previamente a su aprobación a informe jurídico de los respectivos firmantes, a efectos de determinar si contienen compromisos específicos de hacer o de financiar.

**QUINTA.- FINANCIAMIENTO.**

1. El presente Memorando no conlleva gasto alguno. Las aportaciones financieras para la realización de las actividades de cooperación a implementarse en el marco del mismo, serán acordadas por los firmantes en cada uno de los Memorandos Específicos de Colaboración.

2. La firma de cualquier Memorando Específico de Colaboración estará supeditada a su viabilidad y a la disponibilidad presupuestaria de cada uno de los firmantes.

3. Los firmantes promoverán la búsqueda de fuentes de financiación complementaria para los fines del presente Memorando.

**SEXTA.- AUTONOMÍA.**

Las acciones encaminadas a lograr el cumplimiento del presente Memorando se harán bajo el absoluto respeto y sin perjuicio de la autonomía o naturaleza propia de cada uno de los firmantes, así como de las determinaciones que corresponda a cada uno de ellos.

**SÉPTIMA.- PROPIEDAD INTELECTUAL.**

1. Los firmantes preservarán la titularidad de los derechos de aquellas obras que sean producto de su trabajo respectivo, de conformidad con lo que establecen las leyes en materia de propiedad intelectual de las respectivas legislaciones.

2. En el caso de aquellas obras, materiales y trabajos que sean producto de un trabajo conjunto, los firmantes convienen compartir la titularidad de los derechos, de conformidad con lo que establezcan sus respectivas leyes en materia de propiedad intelectual.

3. En el supuesto de que alguno de los firmantes desee utilizar en una publicación propia información o resultados de una investigación proporcionada por el otro firmante, deberá solicitar previamente autorización escrita a ésta, y ajustarse a las disposiciones legales que correspondan en la materia.

4. Una parte no podrá utilizar la marca, logotipo o emblema de la otra en publicaciones ni programas sin el previo consentimiento por escrito de ésta.

**OCTAVA. MECANISMO DE SEGUIMIENTO.**

1. Para el adecuado desarrollo de las actividades que se generarán con motivo de la ejecución del presente Memorando, cada uno de los firmantes designarán como contacto a un representante, quien podrá ser sustituido en cualquier momento, previa notificación al otro firmante.

2. Los representantes designados como puntos de contacto tendrán las siguientes funciones:

a) Promover la celebración de Memorandos específicos;
b) Determinar y apoyar las acciones a ejecutar con el fin de dar cumplimiento al objeto del presente Memorando y de los Memorandos Específicos de Colaboración;
c) Coordinar la realización de actividades señaladas en el presente Memorando;
d) Dar seguimiento a las actividades que se desprendan del presente Memorando e informar periódicamente a los firmantes sobre los resultados obtenidos;
e) Las demás que acuerden los firmantes.

3. Los criterios para la coordinación, seguimiento y ejecución del objeto de este Memorando que se consideren necesario instrumentar, serán determinados por los representantes que al efecto se designen.

4. La representación estará conformada por las siguientes personas:

| POR LA "SIC" | POR LA "AEPD" |
|---|---|
| Nelson Remolina Angarita. Superintendente-Delegado para la Protección de Datos Personales.<br>Domicilio: Carrera 13 No. 27-00, Bogotá D.C., Colombia<br>Teléfono: +571 5870000 | Jesús Rubí Navarrete. Coordinador de la Unidad de Apoyo y Relaciones Institucionales.<br>Domicilio: Calle Jorge Juán, 6. 28001. Madrid.<br>Teléfono: +34913996921 |

**NOVENA. RELACIÓN LABORAL.**

Los firmantes convienen que el personal asignado por cada uno para la realización de las actividades previstas en el presente Memorando, continuará bajo la dirección y dependencia de la Institución a la que pertenezca, por lo que no se crearán relaciones de carácter laboral con la otra, a la que no se considerará patrón sustituto o solidario.

**DÉCIMA. ENTRADA Y SALIDA DE PERSONAL.**

Los firmantes se apoyarán en sus autoridades correspondientes, a efecto de que se otorguen todas las facilidades necesarias para la entrada, estancia y salida de los participantes que en forma oficial intervengan en las actividades de cooperación que se deriven del presente Memorando. Estos participantes se someterán a las disposiciones migratorias, fiscales, aduaneras, sanitarias y de seguridad nacional vigentes en el país receptor y no podrán dedicarse a ninguna actividad ajena a sus funciones sin la previa autorización de las autoridades competentes en esta materia. Los participantes dejarán el país receptor, de conformidad con las leyes y disposiciones del mismo.

**UNDÉCIMA. TRANSPARENCIA DE LA INFORMACIÓN.**

Los firmantes llevarán a cabo las acciones necesarias para poner a disposición de la ciudadanía la información relacionada con el trabajo realizado con motivo de la ejecución del presente Memorando, así como la relativa al ejercicio de recursos públicos, siempre que dicha actuación no vulnere el deber de sigilo y secreto profesional exigible, así como la legislación nacional aplicable a cada uno de los firmantes en materia de protección de datos personales.

**DUODÉCIMA. SOLUCION DE CONTROVERSIAS.**

1. Cualquier diferencia derivada de la interpretación o aplicación del presente Memorando, será resuelto por los firmantes de común acuerdo.

2. El presente Memorando no es jurídicamente vinculante ni está sometido al Derecho internacional.

**DECIMOTERCERA. DISPOSICIONES FINALES.**

1. El presente Memorando será de aplicación a partir de la fecha de su firma y continuará siéndolo por un período de cuatro años contado a partir de esa fecha, pudiendo renovarse, por igual periodo, mediante el acuerdo expreso y escrito de los firmantes.

2. El presente Memorando podrá ser modificado por mutuo consentimiento de los firmantes, formalizado por medio de comunicaciones escritas, en las que se especifique la fecha de inicio de aplicación de dichas modificaciones.

3. Cualquiera de los firmantes podrá dar por terminado el presente Memorando, siempre que lo notifique por escrito a la otra parte, con un mínimo de tres (3) meses de anticipación a la fecha de terminación. La terminación anticipada del presente Memorando no afectará la conclusión de los proyectos iniciados en el marco del mismo.

Firmado el día ___ del año dos mil veintiuno, en dos ejemplares originales en idioma español, siendo ambos textos igualmente auténticos.

| POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA | POR LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DEL REINO DE ESPAÑA |
|---|---|
| | ESPAÑA MARTI MAR - DNI 05259618R<br>Firmado digitalmente por ESPAÑA MARTI MAR - DNI 05259618R<br>Fecha: 2021.03.25 10:14:30 +01'00' |
| Fdo: D. Andrés Barreto González<br>Superintendente de Industria y Comercio<br>14 Abril 2021. | Fdo: Dª. Mar España Martí<br>Directora |

# APPENDIX C

## Letter to operators of the Insecam website

**November 21, 2014**

Dear Sir or Madam:

We are writing to you jointly as privacy enforcement authorities to highlight an important privacy concern that has come to our attention.

We have strong concerns about your website and its aggregation of live video footage from internet connected cameras operating with the manufacturer's default username and password. Such cameras can be found in household, public and commercial spaces, including places of employment around the world.

Your website states that it carries out this practice with the intention of demonstrating the importance of security settings for surveillance cameras. We recognize in principle the importance of bringing to light potential security issues; however this should be done in a way that is not harmful to individuals.

Given the sensitive nature of the personal information collected via such cameras, especially those placed within the home, and the fact that your website is actively disclosing that personal information without the knowledge of the individuals on camera, this poses a serious threat to individuals' privacy around the world. This threat is further heightened by the inclusion of precise geographical location information.

Furthermore, as you are undoubtedly aware, this issue has received significant international media attention. This increased public attention will result in an even greater privacy risk to individuals from these cameras with remote access capabilities.

As such, we are calling on you to take immediate action to take down this website. We furthermore request that you refrain from re-establishing the website under its current domain name or any other domain name in the future if it continues to show any kind of camera footage featuring individuals where those individuals are not aware of the disclosure taking place. Failure to comply with this request for removal by November 26th, 2014 (00:00 GMT), will result in the consideration of additional enforcement action.

Sincerely,

*Original signed by*

Timothy Pilgrim,
Privacy Commissioner of Australia

*Original signed by*

Daniel Therrien,
Privacy Commissioner of Canada

*Original signed by*

Chan Hoi Fan
Coordinator, Office for Personal Data Protection of Macao – China

*Original signed by*

David Smith,
Deputy Commissioner, Information Commissioner's Office – United Kingdom

*Original signed by*

Me Jean Chartier,
President, Commission d'accès à l'information du Québec

*Original signed by*

Jill Clayton,
Information and Privacy Commissioner of Alberta

*Original signed by*

Elizabeth Denham,
Information and Privacy Commissioner for British Columbia

# Data protection authorities urge Google to address Google Glass concerns

**Ottawa, June 18, 2013**

Mr. Larry Page
Chief Executive Officer
Google Inc.
1600 Amphitheatre Parkway
Mountain View, California
USA 94043

Dear Mr. Page:

We are writing to you as data protection authorities to raise questions from a privacy perspective about the development of Google Glass, a type of wearable computing in the form of glasses[1], which is currently in beta testing and not yet available to the general public.

As you have undoubtedly noticed, Google Glass has been the subject of many articles that have raised concerns about the obvious, and perhaps less obvious, privacy implications of a device that can be worn by an individual and used to film and record audio of other people. Fears of ubiquitous surveillance of individuals by other individuals, whether through such recordings or through other applications currently being developed, have been raised. Questions about Google's collection of such data and what it means in terms of Google's revamped privacy policy have also started to appear.

As you may recall, data protection authorities have long emphasized the need for organizations to build privacy into the development of products and services before they are launched. Many of us have also encouraged organizations to consult in a meaningful way with our respective offices.

To date, what information we have about Google Glass, how it operates, how it could be used, and how Google might make use of the data collected via Glass largely comes from media reports, which contain a great deal of speculation, as well as Google's own publicizing of the device.

For example, our understanding is that during the beta testing of the product, Google has put in place extensive guidelines for software developers to follow in building applications for Glass[2]. These limits appear to be largely related to advertising within Glass. If this is indeed the case, we think this is a positive first step in identifying privacy issues, but it is only a first step and the only one we are aware of.

We understand that other companies are developing similar products, but you are a leader in this area, the first to test your product "in the wild" so to speak, and the first to confront the ethical issues that such a product entails. To date, however, most of the data protection authorities listed below have not been approached by your company to discuss any of these issues in detail.

For our part, we would strongly urge Google to engage in a real dialogue with data protection authorities about Glass.

The questions we would like to raise include:

- How does Google Glass comply with data protection laws?
- What are the privacy safeguards Google and application developers are putting in place?
- What information does Google collect via Glass and what information is shared with third parties, including application developers?
- How does Google intend to use this information?
- While we understand that Google has decided not to include facial recognition in Glass, how does Google intend to address the specific issues around facial recognition in the future?
- Is Google doing anything about the broader social and ethical issues raised by such a product, for example, the surreptitious collection of information about other individuals?
- Has Google undertaken any privacy risk assessment the outcomes of which it would be willing to share?
- Would Google be willing to demonstrate the device to our offices and allow any interested data protection authorities to test it?

We are aware that these questions relate to issues that fall squarely within our purview as data protection commissioners, as well as to other broader, ethical issues that arise from wearable computing. Nevertheless, we feel it is important for us to raise all of these concerns. We would be very interested in hearing about the privacy implications of this new product and the steps you are taking to ensure that, as you move forward with Google Glass, individuals' privacy rights are respected around the world. We look forward to responses to these questions and to a meeting to discuss the privacy issues raised by Google Glass.

Sincerely,

*Original signed by*

Jennifer Stoddart
Privacy Commissioner of Canada

*Original signed by*

Jacob Kohnstamm
Chairman of the Article 29 Working Party, on behalf of the members of the Article 29 Working Party

*Original signed by*

Timothy Pilgrim
Privacy Commissioner of Australia

*Original signed by*

Marie Shroff
Privacy Commissioner, New Zealand

*Original signed by*

Alfonso Oñate Laborde
Secretary for Data Protection, Federal Institute for Access to Information and Data Protection, Mexico

*Original signed by*

Rivki Dvash
Head of the Israeli Law, Information and Technology Authority

*Original signed by*

Hanspeter Thür
Swiss Federal Data Protection and Information Commissioner

*Original signed by*

Jill Clayton
Information and Privacy Commissioner of Alberta

*Original signed by*

Jean Chartier
President, Commission d'accès à l'information du Québec

*Original signed by*

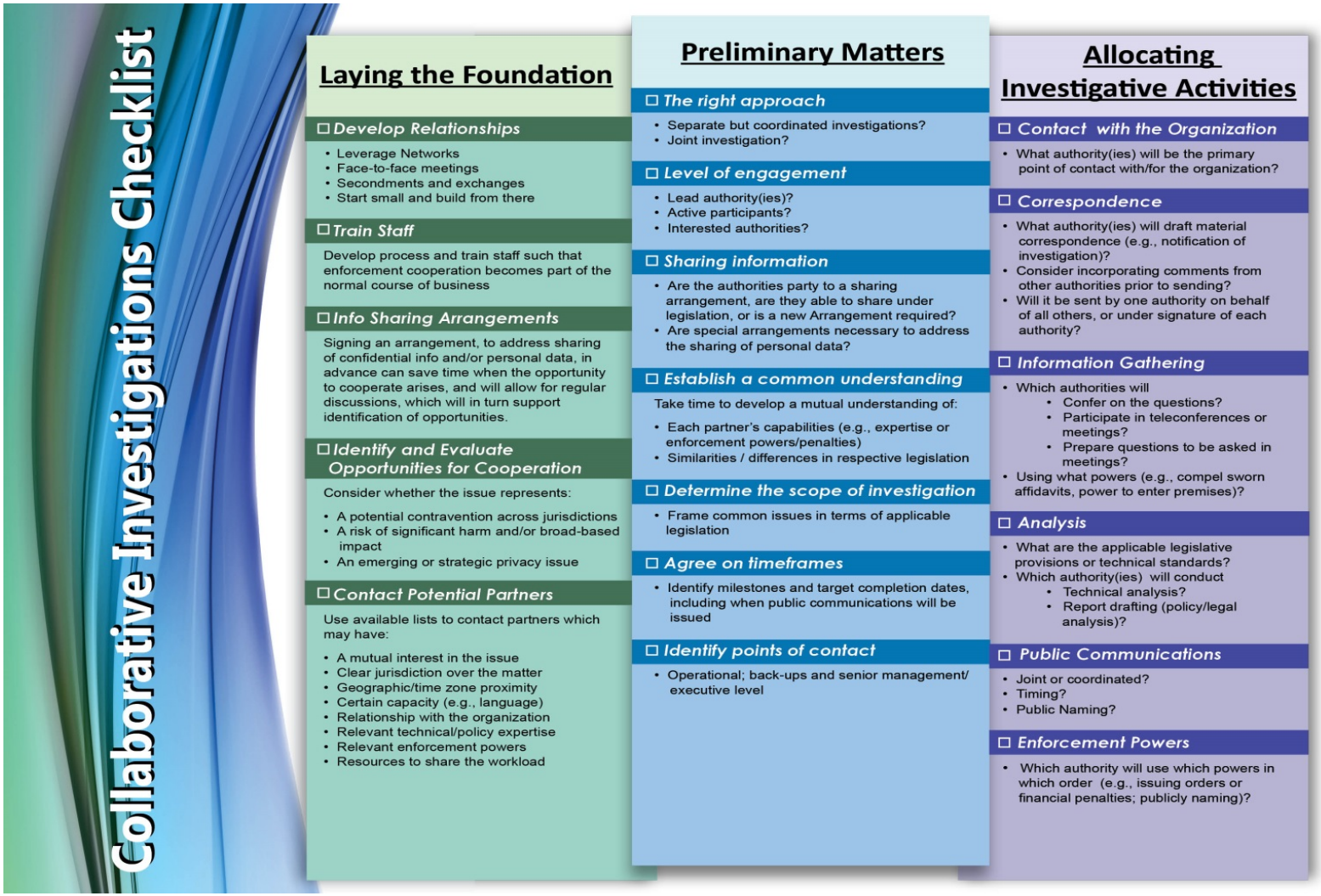
Elizabeth Denham
Information and Privacy Commissioner of British Columbia

[1] Google Glass includes an embedded camera, microphone and GPS, with access to the Internet. The Android Operating System powers Google Glass, and third-party applications are currently being built for Glass. To access Glass, a user needs a Google account.

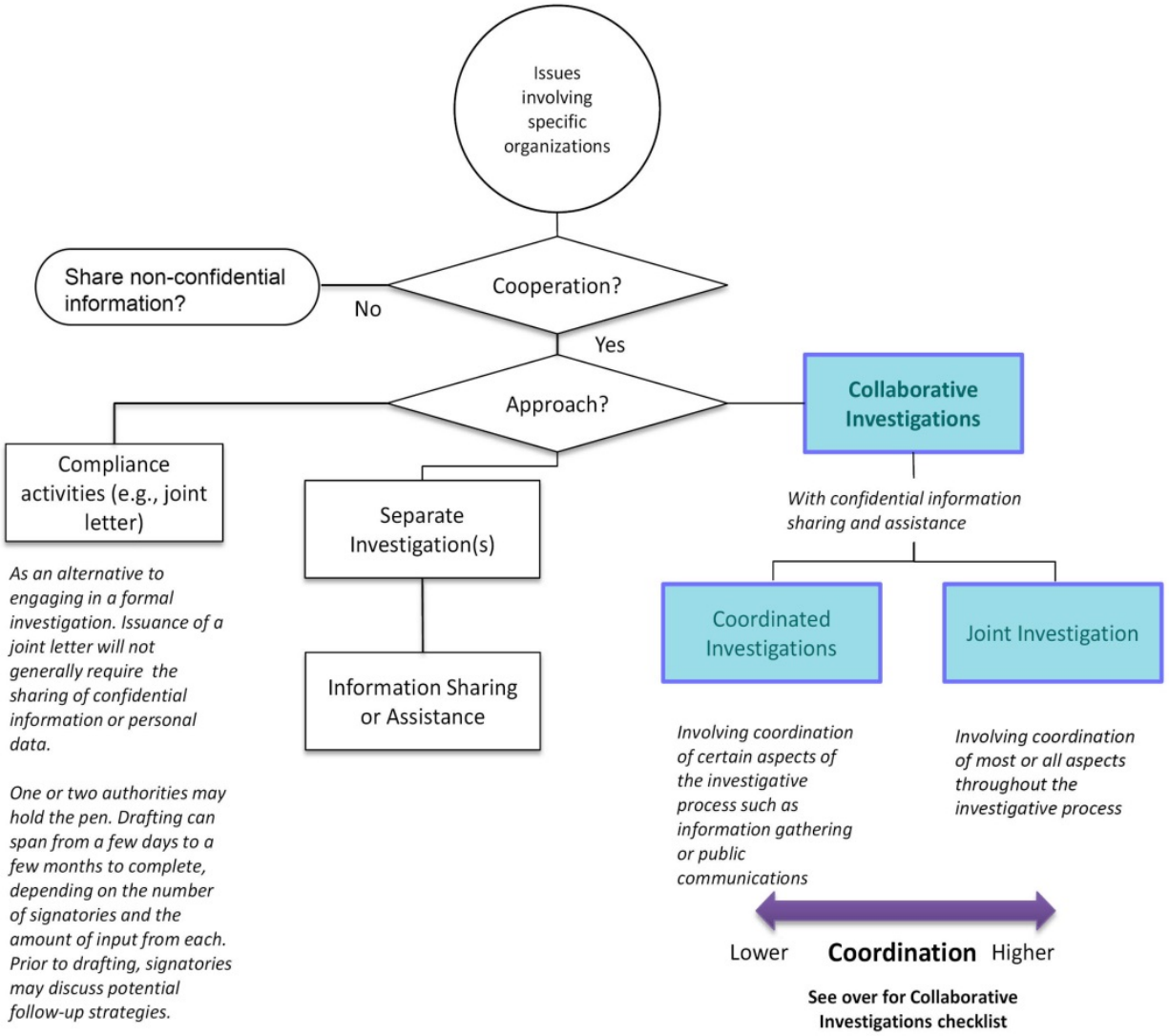
[2] https://developers.google.com/glass/overview

# APPENDIX D

## Enforcement Cooperation Reference Tool



# Enforcement Cooperation Flow Chart



# APPENDIX E

## Example template for authorities to use when developing their own mechanisms for consideration of international enforcement cooperation

**Enforcement cooperation checklist**

**Exploratory phase**

1. Organisation: (name and address if any)

2. **Issue:**

| |
|---|
| • Brief description of issue<br>• How the issue was identified (i.e. complaint, media, other DPA)<br>• International aspects |

3. **Do you have jurisdiction:** Yes No To be decided

4. **Potential enforcement partners:**

| Authority | Potential basis for cooperation |
|---|---|
| Name and jurisdiction | • Organization located in authority's jurisdiction<br>• Authority has expressed interest |

5. **Can my authority share confidential information in this case:** Yes No

| | |
|---|---|
| Ability to share information | • Legal basis, limitations<br><br>(if not, high level discussions only) |

6. **First contact with authority**

| | |
|---|---|
| Authorised by (prior to) | • e.g. Manager |
| Contact | Name / Title / Contact: |

| **Structure** | **Information sought** |
|---|---|
| Interested/investigating? | Yes or no |

| | |
|---|---|
| Rationale for interest in the issue | • complaints received<br>• investigating or required to investigate<br>• serious issue affecting constituents |
| Interested in cooperation or information sharing? | Yes or no |
| Sharing knowledge (subject to legal ability to share) | • Summary of authority's understanding, evidence already collected and material differences from own understanding |
| Exploring potential benefits of cooperation or information sharing | • Jurisdiction / relationship with organisation<br>• proximity/language<br>• ability or power to access relevant evidence<br>• specific expertise (policy/technical) |

**7. Investigating officer recommendations**:

- (i) No action by own authority;
- (ii) Own authority or other authority to investigate alone with info sharing;
- (iii) Own authority or other authority to coordinate investigation (including aspects of investigation which might be coordinated – see 11(b) below);
- Rationale: other authority interested; benefits/opportunities for own authority

**Investigative phase**

**8. Approval of cooperative approach**: (Senior manager)

**9. Understand and agree on terms of information sharing**:

| | |
|---|---|
| Who will share? | • Own authority, other authority or both |
| Type of information to be shared | • E.g. investigation updates, evidence |
| Frequency | • E.g. as received, monthly |
| Limitations / requirements | • Legal basis, safeguards, personal data handling, limitations on publication |

**10. Collaborative investigation**

**a. Preliminary Matters**

| | |
|---|---|
| Will own authority lead or co-investigate? | • Both wish/need to investigate<br>• Potential to pool resources for greater efficiency and/or impact |
| Understand partner's legislation | • Similarities and material differences<br>• Enforcement / evidence gathering powers |

| | |
|---|---|
| | • Limits on public communication |
| Determine Investigation scope | • Issues to be investigated (including differences between authorities) |
| Agreed timeframe/milestones | • Notification of organization<br>• Regular catch-up communication<br>• Completion/publication of investigation |
| <u>Contacts</u> | Investigative Contact |
| | Own authority: (Name, title, contact details)<br>Other authority: (Name, title, contact details) |
| | Deputy Investigative Contact |
| | Own authority: (Name, title, contact details)<br>Other authority: (Name, title, contact details) |
| | Executive Contact |
| | Own authority: (Name, title, contact details)<br>Other authority: (Name, title, contact details) |
| | Other (e.g. Technology) |
| | Own authority: (Name, title, contact details)<br>Other authority: (Name, title, contact details) |

**b. Coordination of investigative/enforcement activities**

| | |
|---|---|
| Point of contact with organization | • One contact from each authority |
| Correspondence with organization | • Joint or<br>• separate (still generally coordinated) |
| Information gathering from organization | • Who will gather what information, using what powers? (generally coordinated) |
| Analysis of evidence | • E.g. Technical, legal |
| Public communications | • Joint, or coordinated (messaging and/or timing) |
| Achieving compliance / enforcement | • Who will use what powers (naming, penalties, compelling compliance)? |

**11. Approval of final approach**: <u>(e.g. Senior Manager, Head of Enforcement)</u>

(approval generally required for any material change to the above)

# Example Template Joint or Coordinated Investigation Plan

## Tombstone Data

| | |
|---|---|
| *File #*<br>- *Authority A*<br>- *Authority B*<br>- *Authority C* | |
| *Respondent's name* | |
| *Respondent's address* | |
| *Date(s) of the commencement of the investigation* | |
| *Original date of the plan* | |
| *Revision history* | |

Form of Cooperation

| |
|---|
| *Separate but coordinated investigations, or a joint investigation.* |

Information Sharing

*MOU(s) pursuant to which information will be shared, and any additional requirements or limitations that the authorities would like to highlight.*

Issues to be Investigated

*Identify the scope of investigation(s), including those that will be investigated jointly and those that may be investigated separately. Issues should ideally be framed in terms of the respective Acts, referencing specific provisions of those Acts to ensure an understanding of what each authority will be examining.*

Timelines/Milestones

*Consensus on investigation timeframes and detailed milestones (e.g., sending notification, receipt of representations, site visit, draft report, final report – subject to adjustments due to operational needs or unforeseen circumstances). The attached Milestone template may be used as guidance.*

Points of Contact

*Each authority should designate a main point of contact for purposes of regular communication and a back-up contact in case of absences. A senior management contact may be designated for strategic discussions.*

Roles and Responsibilities

*Identify Lead Authority (or co-leads), Active Participants, and Interested Authorities.*

Information Gathering and Communication with the Organization

*Determine the following:*

- *Which authority will serve as the main point of contact with the parties?*
- *Will correspondence be sent under joint letterhead or under the lead authority's letterhead?*
- *Will discussions with the parties be with the lead authority or held jointly?*
- *How will questions for the parties be agreed upon – e.g., drafted by the lead authority for review and approval by the other authorities?*

- *How and by whom will information be gathered (e.g., by written submissions, interviews, independent research) and reviewed?*

Site Visits/Interviews

*Is a site visit expected? If so, identify the purpose and general details for the site visit. Which authorities will participate in the planning and which will attend the site visit. Whether interviews will be conducted under oath.*

Analysis

*Indicate which authority(ies) will be responsible for Technical Analysis and Report drafting (policy / legal analysis).*

Public Communications

*(potentially to be determined during the course of the investigation)*
*Determine a public communication plan, considering joint or coordinated communications, to amplify impact of lessons learned, and whether the respondent is to be named.*

Enforcement

*(potentially to be determined during the course of the investigation)*
*In the event it is necessary to enforce compliance with respective laws, which authorities will take what enforcement action.*

# Milestones

| Task | Designated Authority Responsible | Projected Start Date | Targeted End Date | Completion Date | Status & Notes |
|---|---|---|---|---|---|
| **Initiating the Investigation** | | | | | |
| Conduct preliminary research | | | | | |
| Identify evidence required | | | | | |
| Send out notifications and information requests | | | | | |
| Receive and analyze parties' responses to preliminary questions | | | | | |
| Follow-up with additional questions to respondent | | | | | |
| **Site Visit (if necessary)** | | | | | |
| Create a site visit plan | | | | | |
| Obtain internal approvals | | | | | |
| Notify respondent of site visit | | | | | |
| Conduct site visit | | | | | |
| Receive documentation requested during site visit | | | | | |
| **Analysis** | | | | | |
| Conduct technical analysis | | | | | |
| Conduct policy and legal analysis | | | | | |
| Draft and reach consensus on report of findings | | | | | |
| Obtain internal approvals | | | | | |
| Share findings and recommendations with Respondent, and obtain commitments | | | | | |
| Issue report of findings | | | | | |
| **Public Communication** | | | | | |
| Create a public communication plan | | | | | |
| **Enforcement** | | | | | |
| To be determined if necessary | | | | | |

# Glossary

This glossary is provided to explain the drafters' intended meaning for certain terms used in the handbook. It recognizes that authorities may assign different, equally valid, definitions to such terms in accordance with their applicable legal frameworks. The explanations are, therefore, not provided with a view to obtaining, or even suggesting, global acceptance thereof. This glossary should only be used for the purposes of interpreting and understanding this handbook. Individual authorities are best placed to make assessments of how this aligns with local terminology.

1. **arrangement (or memorandum of understanding, or MOU):** a non-legally binding document signed by two or more privacy enforcement authorities, which details the understanding between the signatories, of the circumstances and conditions pursuant to which those authorities may cooperate on enforcement activities, and in particular, share confidential information and/or personal data. Nothing in such a document requires signatories to provide assistance in enforcement if such assistance is prohibited by national/other applicable law or enforcement policies. For the purposes of this handbook, we do not distinguish between an 'arrangement' and an 'MOU'.

2. **competition authority:** An authority with responsibility for promoting, regulating and enforcing compliance with a jurisdiction's competition (or antitrust) laws. Generally works to ensure and maintain fair and efficient competition in the marketplace, by assessing the competitive impacts of proposed mergers and possible abuses of dominance among other anti-competitive conduct. Such authorities will frequently have a dual consumer protection mandate.

3. **confidential information**: Information that a "sharing authority" provides to a "receiving authority" (together, the "cooperating authorities") with the understanding that, subject to any further arrangements between the cooperating authorities, the receiving authority will ensure the information is only accessible to individuals within its authority that need to access that information for the purposes for which it was shared (e.g., in relation to a specified investigation). Confidential information will often be information relating to specific ongoing or potential enforcement action, which may or may not include personal data. It may also include other types of non-public strategic or policy information.

4. **consumer protection authority:** An authority with responsibility for promoting and enforcing compliance with consumer protection elements of a jurisdiction's laws. The term can capture a wide variety of regulatory activities related to consumer interests, ranging from unfair, deceptive and fraudulent business practices to consumer safety. Such authorities will frequently have a dual competition mandate. For the purposes of this handbook, the term includes any such authority.

5. **cooperation:** Two or more authorities working together towards the furtherance of privacy enforcement. It could involve: (i) the sharing of non-confidential policy or practice information; (ii) sharing of confidential information and/or personal data; or (iii) the coordination of activities for the purposes of enforcement or non-enforcement compliance activities.

a. **coordination:** A form of cooperation whereby two or more authorities link (or coordinate) their activities in relation to specific enforcement action(s) (i.e. a collaborative investigation or a non-enforcement compliance initiative like a joint letter or Sweep).

    i. **collaborative investigation:** A form of coordination whereby two or more authorities coordinate activities in relation to related enforcement actions in their respective jurisdictions (e.g., information gathering, technical analysis, publicly communicating outcomes). It will generally involve the sharing of confidential information and/or personal data. The level of collaboration (i.e., the number of activities which the authorities choose to coordinate) can be limited or extensive.

6. **enforcement action vs. compliance action:**

    a. **enforcement action:** action(s) taken by a privacy enforcement authority to either: (i) require an organization's (or individual's) compliance with privacy laws; or (ii) penalize same for non-compliance.

    b. **compliance action:** action(s) taken by a privacy enforcement authority outside of its enforcement powers to encourage voluntary compliance by organizations or individuals with privacy law or best practices.

7. **Jurisdiction:** Either: (i) the scope (e.g., legal or geographic limits) of a privacy enforcement authority's responsibilities; or (ii) the geographic region within which an authority has responsibility to enforce privacy laws.

8. **personal data (or personal information):** Information about an individual, that is, in many jurisdictions, subject to specific requirements under privacy or data protection laws (e.g., as addressed in s. 7 and Schedule 1 of the Arrangement). Personal data will in most instances also be confidential information. For the sole purposes of this handbook, we do not distinguish between 'personal data' and 'personal information'.

9. **privacy enforcement authority (or "PEA" or "authority"):** An authority with responsibility for promoting and enforcing compliance with a jurisdiction's privacy and/or data protection laws. For the purposes of this handbook, the term includes Data Protection Authorities.