

*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*



Office of the  
Privacy Commissioner  
of Canada

**ico.**  
Information Commissioner's Office

# TABLE OF CONTENTS

---

- TABLE OF CONTENTS..... 1
- INTRODUCTION..... 3
  - The Benefits of Enforcement Cooperation ..... 4
- LAYING THE FOUNDATION FOR COOPERATION ..... 5
  - Developing Enforcement Cooperation Relationships..... 5
  - Information-sharing Arrangements ..... 5
  - Enforcement Cooperation Protocols and Training ..... 7
- IDENTIFYING AND EVALUATING OPPORTUNITIES FOR COOPERATION..... 8
  - Contacting Potential Partners..... 8
- ENFORCEMENT COOPERATION MODELS..... 10
  - A Model of Enforcement Cooperation..... 11
- CHOOSING THE APPROPRIATE FORM OF ENFORCEMENT COOPERATION..... 12
  - No Cooperation or Sharing Non-confidential Information / Experience (Item 1) ..... 12
  - Joint Letter (Item 2) ..... 12
    - Drafting ..... 13
    - Follow-up ..... 13
  - Information Sharing or Assistance (Item 3) ..... 14
  - Collaborative Investigations (Item 4)..... 15
    - Forms of Collaborative Investigations ..... 15
    - Preliminary Matters ..... 16
      - Sharing Information ..... 16
      - Establishing a Common Understanding..... 16
      - Determining the Scope of Investigation ..... 16
      - Agreeing on Timeframes..... 17
      - Identifying Points of Contact ..... 17
  - Stratifying Engagement..... 17
  - Allocating Specific Investigative Activities ..... 18
    - Information Gathering and Communication with the Organization ..... 18
    - Analysis ..... 19
    - Public Communications..... 20
    - Enforcement Powers..... 21
- CONCLUSION..... 22

APPENDIX A.....	23
36 <sup>th</sup> International Data Protection Commissioners Conference Balaclava Fort, Mauritius October 13-16, 2014 Global Cross Border Enforcement Cooperation Arrangement .....	23
Table of Contents.....	23
Preamble.....	24
1. Definitions.....	25
2. Purpose .....	26
3. Aims.....	26
4. Nature of the Arrangement .....	26
5. Reciprocity Principle.....	27
6. Confidentiality Principle .....	28
7. Respecting Privacy and Data Protection Principles .....	29
8. Coordination Principles.....	29
9. Resolving Problems.....	30
10. Allocation of Costs .....	30
11. Return of Evidence.....	30
12. Eligibility Criteria .....	30
13. Role of the International Conference Executive Committee.....	31
14. Withdrawal from the Arrangement .....	31
15. Commencement.....	32
Schedule One .....	32
APPENDIX B.....	35
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 .....	35
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.....	45
APPENDIX C.....	50
Letter to operators of webcam website .....	50
Data protection authorities urge Google to address Google Glass concerns.....	52
Appendix D.....	55
Enforcement Cooperation Reference Tool.....	55
Glossary.....	57

## INTRODUCTION

---

The International Conference of Data Protection and Privacy Commissioners (“ICDPPC” or the “Conference”) Global Cross Border Enforcement Cooperation Arrangement (the “Arrangement”, included in **Appendix A**) represents a milestone ‘global statement of intent’ to cooperate among privacy enforcement<sup>1</sup> authorities, and provides a possible framework for achieving this.

Authorities that wish to participate in the Arrangement will undoubtedly have queries regarding the practical implementation of enforcement cooperation. Each authority will make its own internal decisions regarding the way in which it will participate in the Arrangement (or enforcement cooperation in general), but since this may represent a new area of exploration for many authorities, it makes sense for us to support and learn from each other at this early stage. In this handbook, the Office of the Privacy Commissioner of Canada and the UK Information Commissioner’s Office, as co-chairs of the former International Enforcement Cooperation Working Group that prepared the Arrangement, will endeavour to share the experience we have gained and/or observed through interaction with our international partners, in the area of enforcement cooperation.

This handbook is not intended to be instructional or prescriptive. Rather, is intended to provide guidance that may be of assistance to authorities wishing to engage in enforcement cooperation. More specifically, its intent is to provide:

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

Authorities should always remain flexible in applying the approaches outlined in this handbook. Each set of circumstances (e.g., 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.

---

<sup>1</sup> 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.

## The Benefits of Enforcement Cooperation

With the continuing move towards organizations which process personal data having a multinational presence both physically and within the realm of digital commerce (including outsourcing of key operational functions), 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. This is especially important to recognise, and indeed even to promote, as a lesson learned from the recent climate of governments' general cutbacks to the budgetary resources of authorities in our enforcement community during the global financial crisis. The independence of privacy enforcement authorities can also stand to benefit by focussing on bolstering cooperation with other independent entities in such a challenging climate, to assist in weathering the storm of cuts, and buffering the tides of political pressures at the national level. Not surprisingly, privacy enforcement cooperation is in a state of progressive evolution, with ground-breaking new global vehicles such as the ICDPPC Arrangement and the GPEN Alert tool slated to come into operation very shortly, but early experiences have already demonstrated the potential benefits of cooperation:

- i. authorities can achieve results more efficiently via one coordinated investigation or enforcement action, rather than by multiple, duplicative proceedings;
- ii. by working together, authorities can leverage their cumulative "weight" and comparative strengths to achieve a more extensive or cross-cutting result in their enforcement activities than they could individually;
- iii. 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;
- iv. during the process of cooperation, each authority is able to learn from the others' knowledge and experience, thus augmenting its own expertise; and
- v. 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.

# 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<sup>2</sup>, it is the inter-agency and inter-personal relationships which, when nurtured, will provide the comfort, trust, organizational knowledge (e.g., specific authorities' strengths, legal capabilities, strategic priorities) and open lines of communication necessary to make cooperation a reality. Authorities may choose to develop and build such relationships by:

- joining and participating actively in various privacy and enforcement cooperation networks (e.g., monthly calls, volunteering for initiatives or working groups);
- arranging face-to-face discussions and teleconferences to build rapport - perhaps starting with Agency Heads, and other senior personnel, but then growing relationships at operational level (e.g., via regular operational calls);
- participating in secondments, work exchanges or joint training activities, which allow participating staff to bring back in-depth knowledge, and resulting comfort, in relation to potential partners; and
- seeking out scalable opportunities to develop the comfort and capacity to cooperate.

## 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 or an arrangement. Such a document will detail each party's expectations regarding the circumstances pursuant to 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 support the identification of opportunities for cooperation.

---

<sup>2</sup> 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.

Authorities may choose to share information pursuant to bi-lateral arrangements between established partners. However, broad-based arrangements, like ICDPPC or APEC (Cross-border Privacy Enforcement Arrangement, “CPEA”), provide flexibility for multilateral sharing (which may be of particular utility in addressing risks involving many jurisdictions - e.g., a global data breach), while still leaving it up to each participating authority to choose the partners with which they will share.

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 two options:

- i. agree that no personal data will be shared; or
- ii. 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, see the Arrangement, s. 7 and Schedule 1)

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 its requirements with respect to the treatment of shared information; and
- ii. where legally possible, the party receiving information should treat such information as confidential unless the authority that has provided it has expressly consented otherwise.

**Note:** When sharing confidential information obtained from an organization during the course of investigative activities, authorities should consider whether or not 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 carry out a careful analysis of its own legal requirements (e.g., governing legislation or conventions) to ensure that it clearly understands the circumstances and limitations pursuant to which it may share confidential information and personal data.***

For reference, sample MOUs can be found at **Appendix B**.

## **Enforcement Cooperation Protocols and Training**

Authorities may consider developing internal protocols and providing training to 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.

***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. It may be appropriate to develop and train 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, etc. In evaluating whether an issue may be appropriate for any type of enforcement cooperation, authorities may consider whether it represents:

- a potential risk across multiple jurisdictions;
- a risk of significant harm and/or broad-based impact; and/or
- 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 won't necessarily preclude cooperation, depending on the applicable legal framework and the facts of the case, but should be considered.

***The GPEN Alert Tool, slated to become operational later this year, will provide 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 - e.g., where the potential partner may have (this is a non-exhaustive list):

- 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 - e.g., site visit);
- capacity to deal with the organization in its primary language;
- an existing relationship with the organization;
- relevant technical/policy expertise;

- enforcement powers which may assist in obtaining redress; and/or
- resources to share the workload associated with a complex investigation.

An authority may contact another authority via:

- i. existing organizational contacts for established partners; or
- ii. contact lists available via, for example,
  - an ICDPPC Arrangement contact list;
  - GPEN (i.e., the 'APEC / OECD / Council of Europe Enforcement Contacts' list or the Alert Tool contact mechanism); or
  - other global, regional or linguistic-based networks (e.g., London Action Plan, European Commission, Article 29 Working Party, 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 – e.g., enter into an information-sharing arrangement.

# ENFORCEMENT COOPERATION MODELS

The following matrix and associated flowchart will serve as the basis for our discussion of enforcement cooperation.

Figure 1: Enforcement Cooperation Matrix

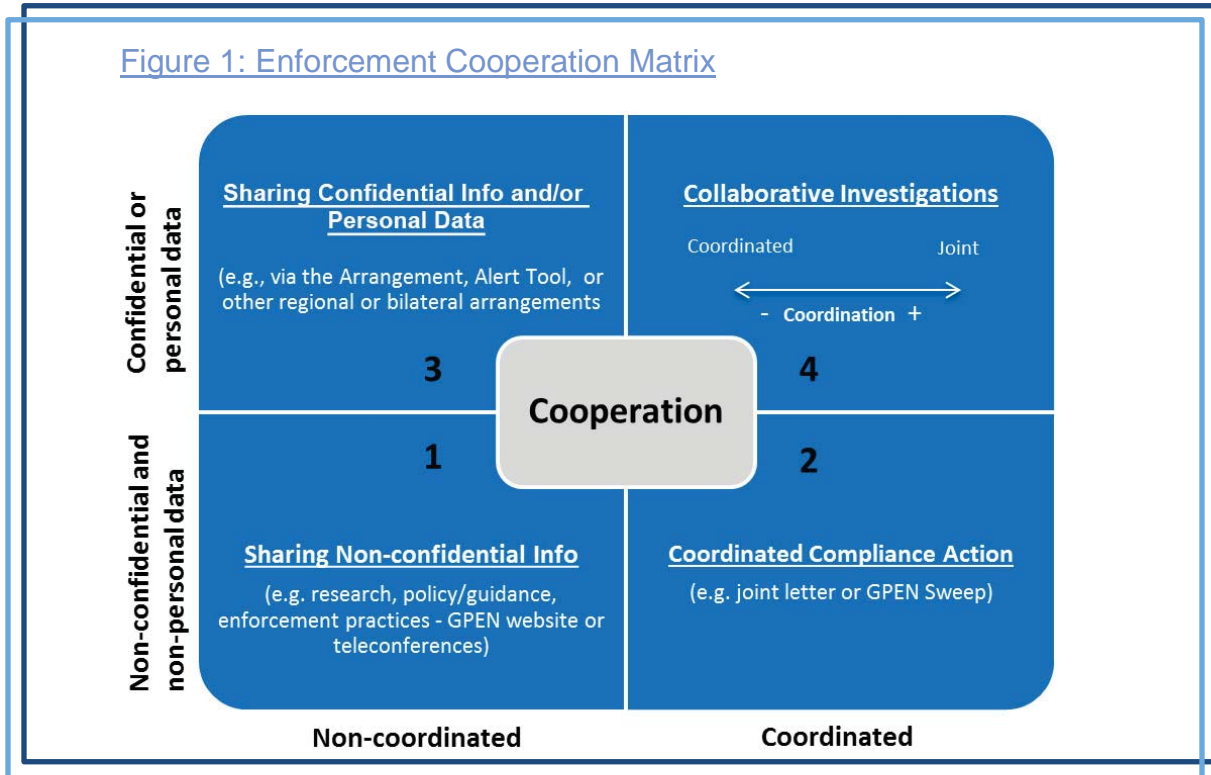
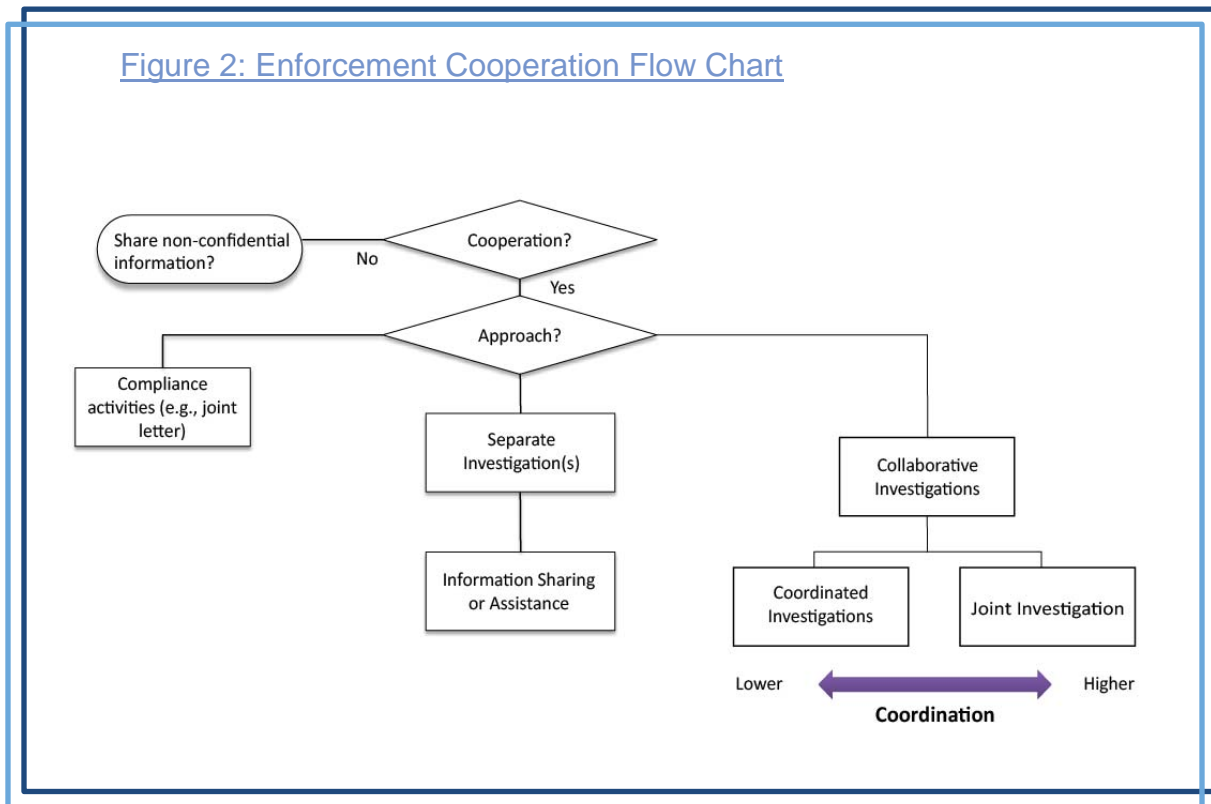


Figure 2: Enforcement Cooperation Flow Chart



## A Model of Enforcement Cooperation

Enforcement cooperation can take several forms:

1. **Sharing Non-confidential Information and Experience**: e.g., 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 may or may not involve sharing confidential information (e.g., thematic initiatives like the GPEN or Article 29 Working Party Sweeps, and joint correspondence with specific organizations outside a formal investigation);
3. **Confidential Information and Personal Data Sharing, and Assistance**: one or more separate and unilateral uncoordinated investigation(s) supported by information sharing or other assistance – e.g., on the basis of MOUs like the ICDPPC Arrangement or another multilateral or bilateral arrangement;
4. **Collaborative Investigations**: (with sharing of confidential information) Can include varied levels of coordination along a continuum from:
  - a. **Separate but Coordinated Investigations**: involving coordination of certain aspects of the investigative process (e.g., information gathering or public communication); to
  - b. **Joint Investigations**: involving coordination of most or all aspects throughout the investigative process.

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

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

- authorities could commence by simply sharing confidential information or issuing a joint compliance letter, but then subsequently decide to engage in a collaborative investigation; or
- two authorities engaged in a joint investigation could share confidential information with another authority that is independently investigating the same matter.

# CHOOSING THE APPROPRIATE FORM OF ENFORCEMENT COOPERATION

---

## No Cooperation or Sharing Non-confidential Information / Experience (Item 1)

While authorities are encouraged to be reciprocal in their cooperation partnerships (the ICDPPC Arrangement's concept is based on such reciprocity, which will in turn strengthen the trust between partners and foster further cooperation), an authority will not generally, subject to domestic legal requirements, be required to cooperate on any particular issue, even if it has entered into an information-sharing arrangement. Cooperation will not always be the appropriate option (e.g., the authority is legally precluded from cooperating or may be unable to cooperate due to resource constraints). Specifically, the ICDPPC Arrangement recognizes circumstances whereby participating authorities may choose not to cooperate - refer to section 5 of the Arrangement, paragraphs (i) – (viii) (**Appendix A**). Authorities may still choose to share non-confidential information or experience in support of each other's enforcement activities.

## Joint Letter (Item 2)

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

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

- There is a clear or apparent egregious contravention affecting multiple jurisdictions, and authorities believe it may be possible to achieve compliance via a letter encouraging the organization(s) to comply with the signatories' expectations (legal requirements or best practices). 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. See **Appendix C** for: (i) a joint compliance letter sent by seven authorities to Insecam, a webcam streaming website; and (ii) a joint letter sent on behalf of 38 authorities to Google, seeking further information on Google Glass.
- An organization is preparing to launch, or has recently launched, a new privacy practice or technology which raises significant privacy concerns. Authorities may use a joint letter as a vehicle to: (i) give the organization an opportunity to explain how it is complying with privacy laws or amend its privacy practices to address potential contraventions; and/or (ii) if published, raise public awareness regarding potential privacy issues and demonstrate solidarity amongst privacy authorities in respect of the issue.

## Drafting

One or two authorities may take the lead by proposing the letter to a group of authorities (e.g., those within one or more specific networks), 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; and
- 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 (e.g., the OECD Fair Information Principles or the Madrid Standards) and/or ask factual questions to assist the signatories in better understanding the new practice or technology. Signatories should also agree as to whether or not they expect a response from the organization, so that the letter can be drafted accordingly.

The drafting process can span from a few days to a few months to complete, depending on the number of signatories and the amount of input from each authority. If authorities can be flexible with respect to letter wording, it will generally assist 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

Prior to drafting and sending the letter, signatories may discuss potential follow-up strategies, which could include:

- i. 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; or
- ii. if the letter is in relation to a potential egregious privacy issue, which the letter is unsuccessful in resolving, one or more of the authorities may choose to 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 issuance of the joint letter, although it is suggested that signatories keep each other informed with respect to their intended follow-up activities.

### **Information Sharing or 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 investigative process (e.g., via a complaint to its Office or via evidence collected 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 (due to geography, language, legislative powers, relationship with the organization, etc.) to investigate. “**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 (e.g., for legislative or strategic reasons). 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 (either pursuant to legislative authority or an arrangement – e.g., the CPEA) to provide such assistance.

In any of these instances, each authority must satisfy itself that it has the legal authority to share and/or assist, and should make clear the conditions pursuant to which it is providing any information or assistance. Such conditions may include, for example, specific requirements with respect to data safeguards (e.g., encryption, password protection, locked cabinets) for confidential information or the treatment of personal data.

Similarly, an authority receiving information should ensure that it clearly understands the purposes for which the information it receives may be used and the safeguards it has to respect. For example, can it refer to such information in its written findings, or use the information as evidence in legal proceedings.

***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 organization(s) in question to achieve greater impact more efficiently.

### **Forms of Collaborative Investigations**

Collaborative Investigations will generally involve the sharing of confidential information, but will also involve the coordination of certain enforcement-related activities. Such collaboration can, itself, extend along a continuum, and can involve a combination of the approaches outlined below (particularly when more than two authorities are involved):

- i. **Separate but Coordinated Investigations:** In other circumstances, two 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 (e.g., technical analysis or publication of complementary findings). Such circumstances could include:
  - an authority’s legislation prevents it from coordinating (e.g., requires that it send separate notifications, requests for information and/or findings);
  - authorities are at different stages of the investigative process; and/or
  - authorities have material legislative or policy differences (such that the authorities wish to investigate materially different issues).
  
- 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 organization in question. 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 two or more authorities;
  - the matter represents an apparent multi-jurisdictional 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; and/or
  - each authority would choose to 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.***



## **Preliminary Matters**

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

### ***Sharing Information***

Are the authorities in question 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, the parties may choose to sign on to an existing arrangement (like the ICDPPC Arrangement) or enter into a new ad hoc bi-lateral or multi-lateral arrangement.

**Note: If there are more than two coordinating authorities, and even if all authorities in question are party to an information-sharing arrangement, the parties should agree on the extent to which information can be shared amongst the authorities (e.g., Authorities A, B and C are coordinating activities. “A” shares confidential information with “B”. Does “A” consent to “B” onward sharing that information with “C”?).** As noted earlier, if the information being shared contains personal data, parties may agree or arrange that it be subject to specific treatment requirements or restrictions.

### ***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 (e.g., 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. Differences will not necessarily preclude collaboration but 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 (e.g., 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.

### ***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 may also consider setting target milestones. For example: (i) notification to the organization; (ii) completion of analysis; and (iii) issuance and publication of findings.

### ***Identifying Points of Contact***

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

- a. one or more operational level contacts (e.g., an investigator or technical analyst) for purposes of regular communication;
- b. back-up contacts so that the investigation doesn't stall during inevitable absences over the course of the investigation; and
- c. 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.

### **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 three 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 (e.g., 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 organisation and relevant jurisdiction;
- a large number of individuals affected in a particular jurisdiction;
- the matter is a strategic priority for one authority; and/or
- 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” investigation; 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**: Other authorities 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. Pursuant to 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.

### **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 Organization***

- i. **Contact with the Organization**: 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 organization 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 (e.g., 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 (e.g., 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 an organization 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; and (ii) ask any additional questions that may arise.

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 may also wish to consider leveraging their respective powers with respect to evidence gathering when establishing authorities' roles in this regard – e.g., certain authorities may have the power to:

- interview witnesses under oath;
- compel sworn affidavits or the production of documents;
- enter/search premises and seize evidence; and/or
- carry out online investigations (e.g., search of electronic devices or storage).

**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.

### ***Analysis***

Where determination of the issues in question requires analysis against materially similar legislative provisions (e.g., 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 (e.g., 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 to be completed (including the technical questions to be answered), as well as any specific evidentiary requirements (e.g., 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 (albeit that it should be unlikely for coordinating authorities to come to completely

different conclusions, given that they would have discussed the issue in terms of their respective legislative frameworks in advance of commencing the collaborative investigation). For a joint investigation, coordinating authorities will generally have two options:

- a. Joint Report: Where determinations will be based on analysis 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 may also offer 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;
- b. 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 may leverage the strength of a unified message by issuing the separate reports concurrently, under a joint cover letter summarizing their findings and/or expectations of the organization going forward.

**Note: Opportunity for information sharing:** If authorities choose not to coordinate their analysis or report writing, they may 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.

### ***Public Communications***

Public communications offer authorities the opportunity to amplify the results of 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 (e.g., **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 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 (i.e., 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.***

### ***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;
- carry out administrative or injunctive measures;
- pursue compliance via court proceeding; and/or
- publicly name an organization.

Authorities should ensure they are aware of their partners' enforcement powers (or limitations thereof) 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 educate 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.

## CONCLUSION

---

There is a continuing move towards organizations having a global presence, and technology allowing ever increasing volumes of personal data to be processed. Coordination 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, at the most senior and operational levels – they are the foundation for cooperation.
- ii. Build internal capacity to be able to identify and respond to enforcement cooperation opportunities – e.g., via development of protocols, enforcement cooperation training or secondments/exchanges.
- iii. Information-sharing arrangements are generally necessary to 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.
- 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

---

**36<sup>th</sup> International Data Protection Commissioners Conference**  
**Balacava Fort, Mauritius**  
**October 13-16, 2014**

**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 1



## **Preamble**

*Recalling* that the resolution of the Warsaw Conference mandated an extension to the work of the International Enforcement Coordination Working Group to develop a common approach to cross-border 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<sup>1</sup>, 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 organizations relating to these transborder flows can quickly and adversely affect the privacy and the protection of the personal data of vast numbers of individuals across the world and that therefore increased transborder data flows should be accompanied by increased cross-border information sharing and enforcement cooperation between privacy enforcement authorities with such information sharing and enforcement cooperation being essential elements to ensure privacy and data protection compliance, serving an important public interest.

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

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

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

- improve their domestic frameworks for privacy law enforcement to better enable cross-border cooperation, in a way consistent with national laws;
- provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards; and
- engage relevant stakeholders in discussions and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

*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 organizations 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.

*Recognizing* 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, coordinated 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 maximize 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’)**<sup>2</sup> 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 organizations processing personal data across borders. It encourages and facilitates all PEAs' cooperation with each other by sharing information, particularly confidential enforcement-related information about potential or on-going 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 enforce against in its domestic legislation.
- iii. There are resource constraints.
- iv. The matter is inconsistent with other priorities or legal obligations.
- v. There is an absence of mutual interest in the matter in question.
- vi. The matter is outside the scope of this Arrangement.
- vii. Another body is a more appropriate body to handle the matter.

viii. 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.

## **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 minimize, 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 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.
- 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 recognized 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 recognized 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. The list should be easily available to all Participants.

### **13. Role of the International Conference Executive Committee**

The Committee will:

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

### **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 endeavor 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 minimize, to the fullest extent possible any such application.
  - b. notify the Participant that supplied the information forthwith and seek to obtain that Participant's consent for the disclosure of the information in question.
  - c. 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.

---

<sup>1</sup> For the avoidance of doubt and for the purposes of this document, the term 'privacy enforcement authorities' also includes data protection authorities.

<sup>2</sup> 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 Cooperation 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 28<sup>th</sup> 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  
Chairwoman

United States Federal Trade  
Commission

---

Jacob Kohnstamm  
Chairman

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 cooperation 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

*Original signed by*

Jennifer Stoddart  
Privacy Commissioner of Canada

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

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

## APPENDIX C

---

### Letter to operators of webcam 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<sup>1</sup>, 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<sup>2</sup>. 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

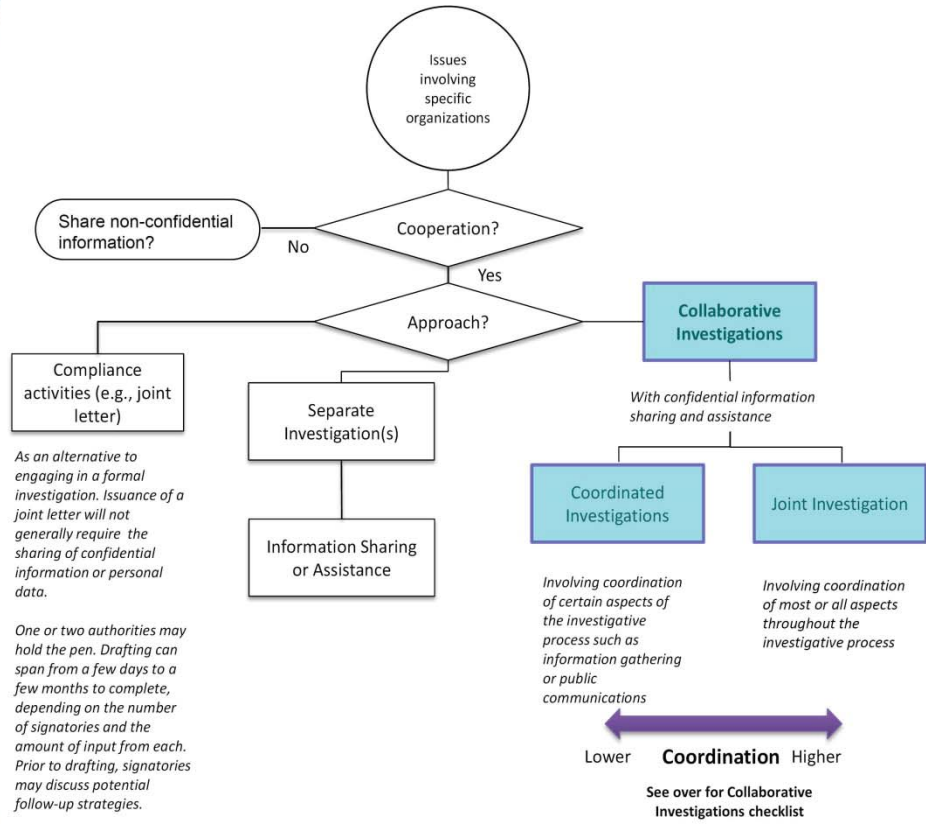


**Collaborative Investigations Checklist**

Laying the Foundation	Preliminary Matters	Allocating Investigative Activities
<input type="checkbox"/> <b>Develop Relationships</b>	<input type="checkbox"/> <b>The right approach</b>	<input type="checkbox"/> <b>Contact with the Organization</b>
<ul style="list-style-type: none"> <li>• Leverage Networks</li> <li>• Face-to-face meetings</li> <li>• Secondments and exchanges</li> <li>• Start small and build from there</li> </ul>	<ul style="list-style-type: none"> <li>• Separate but coordinated investigations?</li> <li>• Joint investigation?</li> </ul>	<ul style="list-style-type: none"> <li>• What authority(ies) will be the primary point of contact with/for the organization?</li> </ul>
<input type="checkbox"/> <b>Train Staff</b>	<input type="checkbox"/> <b>Level of engagement</b>	<input type="checkbox"/> <b>Correspondence</b>
<p>Develop process and train staff such that enforcement cooperation becomes part of the normal course of business</p>	<ul style="list-style-type: none"> <li>• Lead authority(ies)?</li> <li>• Active participants?</li> <li>• Interested authorities?</li> </ul>	<ul style="list-style-type: none"> <li>• What authority(ies) will draft material correspondence (e.g., notification of investigation)?</li> <li>• Consider incorporating comments from other authorities prior to sending?</li> <li>• Will it be sent by one authority on behalf of all others, or under signature of each authority?</li> </ul>
<input type="checkbox"/> <b>Info Sharing Arrangements</b>	<input type="checkbox"/> <b>Sharing information</b>	<input type="checkbox"/> <b>Information Gathering</b>
<p>Signing an arrangement, to address sharing of confidential info and/or personal data, in advance can save time when the opportunity to cooperate arises, and will allow for regular discussions, which will in turn support identification of opportunities.</p>	<ul style="list-style-type: none"> <li>• Are the authorities party to a sharing arrangement, are they able to share under legislation, or is a new Arrangement required?</li> <li>• Are special arrangements necessary to address the sharing of personal data?</li> </ul>	<ul style="list-style-type: none"> <li>• Which authorities will             <ul style="list-style-type: none"> <li>• Confer on the questions?</li> <li>• Participate in teleconferences or meetings?</li> <li>• Prepare questions to be asked in meetings?</li> </ul> </li> <li>• Using what powers (e.g., compel sworn affidavits, power to enter premises)?</li> </ul>
<input type="checkbox"/> <b>Identify and Evaluate Opportunities for Cooperation</b>	<input type="checkbox"/> <b>Establish a common understanding</b>	<input type="checkbox"/> <b>Analysis</b>
<p>Consider whether the issue represents:</p>	<p>Take time to develop a mutual understanding of:</p>	<ul style="list-style-type: none"> <li>• What are the applicable legislative provisions or technical standards?</li> </ul>
<ul style="list-style-type: none"> <li>• A potential contravention across jurisdictions</li> <li>• A risk of significant harm and/or broad-based impact</li> <li>• An emerging or strategic privacy issue</li> </ul>	<ul style="list-style-type: none"> <li>• Each partner's capabilities (e.g., expertise or enforcement powers/penalties)</li> <li>• Similarities / differences in respective legislation</li> </ul>	<ul style="list-style-type: none"> <li>• Which authority(ies) will conduct             <ul style="list-style-type: none"> <li>• Technical analysis?</li> <li>• Report drafting (policy/legal analysis)?</li> </ul> </li> </ul>
<input type="checkbox"/> <b>Contact Potential Partners</b>	<input type="checkbox"/> <b>Determine the scope of investigation</b>	<input type="checkbox"/> <b>Public Communications</b>
<p>Use available lists to contact partners which may have:</p>	<ul style="list-style-type: none"> <li>• Frame common issues in terms of applicable legislation</li> </ul>	<ul style="list-style-type: none"> <li>• Joint or coordinated?</li> <li>• Timing?</li> <li>• Public Naming?</li> </ul>
<ul style="list-style-type: none"> <li>• A mutual interest in the issue</li> <li>• Clear jurisdiction over the matter</li> <li>• Geographic/time zone proximity</li> <li>• Certain capacity (e.g., language)</li> <li>• Relationship with the organization</li> <li>• Relevant technical/policy expertise</li> <li>• Relevant enforcement powers</li> <li>• Resources to share the workload</li> </ul>	<input type="checkbox"/> <b>Agree on timeframes</b>	<input type="checkbox"/> <b>Enforcement Powers</b>
	<ul style="list-style-type: none"> <li>• Identify milestones and target completion dates, including when public communications will be issued</li> </ul>	<ul style="list-style-type: none"> <li>• Which authority will use which powers in which order (e.g., issuing orders or financial penalties; publicly naming)?</li> </ul>
	<input type="checkbox"/> <b>Identify points of contact</b>	
	<ul style="list-style-type: none"> <li>• Operational; back-ups and senior management/ executive level</li> </ul>	



# Enforcement Cooperation Flow Chart



## 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. **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.
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. **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’.
5. **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.
6. **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.
7. **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.