OECD publishing

REVIEW OF THE OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY

OECD DIGITAL ECONOMY PAPERS
September 2023 **No. 359**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report reviews the continued relevance of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (the Recommendation). It provides an overview of the current legal and policy landscape, as well as of actions taken to implement the Recommendation.

This report was written by Kosuke Kizawa and Lisa Robinson, under the guidance of Clarisse Girot (all of the OECD Secretariat). It was prepared under the aegis of the OECD Committee for Digital Economy Policy, with input from delegates of the Working Party on Data Governance and Privacy. This paper was approved and declassified by written procedure by the Committee on Digital Economy Policy on 21 July 2023 and prepared for publication by the OECD Secretariat. The authors wish to thank Jeremy West for his support on earlier drafts of this paper and Andreia Furtado for editorial support.

Note to Delegations:

This document is also available on O.N.E. under the reference code:

DSTI/CDEP/2022/2/FINAL

Table of contents

Tables

Figures

Boxes

Executive summary

This Report reviews the continued relevance of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (OECD, 2007[1]) (the Recommendation), one of the key OECD legal instruments in the field of personal data protection and privacy. The Recommendation seeks to foster international co-operation among Privacy Enforcement Authorities (PEAs) in recognition that the cross-border enforcement of privacy laws is a central aspect in effectively protecting privacy.

Today, however, the technological and legal landscape has significantly changed since the Recommendation was first adopted in 2007. New privacy challenges triggered by unprecedented technological developments (for example in generative AI), increased cross border data flows, and new business models that rely on these data flows have generated growing needs in terms of international co-operation, including for cross-border enforcement. Privacy laws now commonly have extra-territorial applicability, adding a layer of complexity to co-operation processes between PEAs. Additionally, the ubiquity of data as a crucial element in not just privacy law enforcement but in the work of regulators in other areas (e.g. in competition, consumer, finance, health) has placed a spotlight on the need for not only cross-border, but also cross-sector co-operation. Taken together, these changes and the emergence of new regulatory practices make it necessary to reflect on the implementation, dissemination and continued relevance of the Recommendation. Accordingly in April 2021, the OECD's Working Party on Data Governance and Privacy (WPDGP) determined that a review of the Recommendation was timely.

The detailed findings in this Report shed light on this review process and its conclusions. They are based predominantly on a survey circulated to the WPDGP and to different networks of PEAs in late 2021, on the outcomes of an Expert Roundtable held in October 2022, desk research, work from other international fora, as well as discussions at the meetings of the WPDGP between 2021 and April 2023.

The report follows the structure of the Recommendation and considers in turn three sections: i) definition, objectives and scope; ii) domestic measures to enable co-operation; and iii) international co-operation. The main findings are as follows:

Definitions, objectives and scope:

While it is observed that the principles underlying this part of the Recommendation remain relevant, the Report finds that there is scope for improvement. For example, it was identified that certain terms which were not originally defined in the Recommendation could be clarified (e.g. cross-border and co-operation), and that cross-border co-operation is now necessary in many cases, not just in those dealing with serious violations of privacy laws. Indeed, given the interconnected nature of the broader digital economy today, cross-border co-operation has become a core imperative for PEAs. The constant increase in cross-border data flows increases the need for cross-border co-operation in proportion, and it is observed that this reality is not reflected in the current text of the Recommendation. The review also highlights a potential role for the OECD in helping to identify issues of common concern that may benefit from more coordinated enforcement actions.

Domestic measures to enable co-operation:

Adherents to the Recommendation have taken concrete action to incorporate measures in their domestic frameworks that enable cross-border co-operation in enforcing privacy laws. However, in practice, a number of challenges remain. For instance, discrepancies in confidentiality requirements can pose barriers to sharing information, or PEAs may lack the jurisdiction or competence to commence actions. Laws with extra-territorial applicability can compound challenges, leading to practical hurdles such as in serving complaints or enforcing compliance overseas. The issue of recognition and enforcement of decisions in other jurisdictions was highlighted as a particular challenge, and it was noted that there may be scope for the OECD to consider facilitating joint work on this issue.

Despite these challenges, a fairly large number of soft co-operation avenues are highlighted as good practice in overcoming them. Additionally, differences in legal frameworks are recognised as bringing opportunities such as encouraging the development of Memorandums of Understanding between PEAs, with a variety of direct and indirect benefits attached, including developing and strengthening relationships which are crucial to fostering international co-operation, including on enforcement.

International co-operation:

Adherents routinely engage with one another through various international fora and networks which aim to further cross-border enforcement co-operation, and the different groups that exist tend to fill different roles ranging from working level engagement, to the development of guidance and policies, to high-level discussions.

At the same time, co-operation with regulators from other sectors is seen as an imperative today, given the vital role of data in many business models and in turn its relevance to the work of other sectoral regulators in a large variety of domains (e.g. competition, consumer protection, finance, health, etc.). The Report finds that this need is not clearly articulated in the current language of the Recommendation, and there is scope for further work on fostering cross-sector co-operation.

Overall findings

The Report observes that the principles underlying the Recommendation remain solid and constitute an effective baseline for the cross-border enforcement activities of PEAs. However, it also identifies a number of gaps, challenges and opportunities for cross-border enforcement co-operation, due to the significant changes in the technological and legal landscape since the Recommendation was first adopted. These gaps, challenges and opportunities provide fertile ground for the OECD to elaborate guidance to support further implementation for the Recommendation, or even to revise it.

1. Background

On 12 June 2007, the OECD Council adopted the OECD Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy (OECD, 2007[1]) (the Recommendation), which was developed in recognition of the fact that the cross-border enforcement of privacy laws is a key dimension of effective privacy protection.[1] The Recommendation aims to foster international co-operation among the Privacy Enforcement Authorities (PEAs) of Member and non-Member countries having adhered to it (hereafter 'Adherents')[2] to better safeguard personal data and minimise disruptions to transborder data flows.

Divided into two main parts ("Domestic Measures to Enable Co-operation" and "International Co-operation"), the Recommendation reflects a commitment by Adherents to improve their domestic privacy law enforcement frameworks so as to better enable their PEAs to co-operate with foreign authorities, including through the provision of mutual assistance in the enforcement of privacy laws (OECD, 2007[1]).

The implementation, dissemination and continued relevance of the Recommendation was first assessed in 2011 when a Report on its implementation was approved by CDEP and submitted to the OECD Council.[3] The 2011 Report concluded that the Recommendation did not need to be revised (OECD, 2011[2]).

The present review of the continued relevance of the Recommendation was prompted by the findings of the 2021 Report on the implementation (OECD, 2021[3]) of the Recommendation concerning the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the OECD Privacy Guidelines) (OECD, 2013[4]).[4] Most notably, that 2021 Report found that advances in technology and increased cross-border flows of data, has resulted in an increased need for cross-border co-operation and a growing need for cross-regulatory and interagency co-operation.

Consequently, in April 2021 (OECD, 2021[5]), in the context of discussing follow-on work arising out of the 2021 Report on the implementation of the OECD Privacy Guidelines, the OECD's Working Party on Data Governance and Privacy (WPDGP) (a subsidiary body of the OECD Committee on Digital Economy Policy – CDEP) suggested that a review of the Recommendation be undertaken.

This document presents this review of continued relevance the Recommendation. It seeks to examine the ways in which it is currently being implemented, identify gaps, and outline possible next steps. The following section (section 2) describes the process and methodology for developing this Report. Thereafter, section 3 provides some context and background to the Recommendation itself. The main body of this Report is contained in section 4, which sets out the findings. Finally, section 5 provides conclusions.

2. Process and methodology

In July 2021, the Secretariat circulated a Work Plan for the Review of the Recommendation (OECD, 2021[6]) (the work plan), followed by a questionnaire in September 2021 (the 2021 questionnaire) centred around current trends and challenges that had been identified in the cross-border privacy law enforcement landscape,[5] namely:

- mutual assistance, information sharing and joint investigations;
- international arrangements and mechanisms;
- the intersection with other regulatory bodies (for example competition authorities);
- uncertainty around the compatibility of legal regimes; and
- powers and resources of PEAs.

The questionnaire was sent to WPDGP delegates, as well to members of the Global Privacy Enforcement Network (GPEN) and the European Data Protection Board (EDPB). Responses were received from twenty-eight jurisdictions.[6]

Following discussions of the preliminary results of the 2021 questionnaire (OECD, 2022[7])[7] and a first draft of this Report, an informal expert group was set up to help further guide this work. Additionally, the work was informed by an Expert Roundtable (OECD, 2022[8]), desk research and work from other international fora.

The structure of this Report follows the structure of the Recommendation, addressing in turn the implementation findings as they relate to the different parts of the Recommendation, namely:

- Definitions, objectives and scope (Parts I and II of the Recommendation);
- Domestic measures to enable co-operation (Part III of the Recommendation); and
- International co-operation (Part IV of the Recommendation).

It also considers the findings of the 2021 questionnaire regarding the overall continued relevance of the Recommendation, and provides conclusions and suggestions for future work.

Prior to considering the main findings, this next section provides some context to the Recommendation itself, including its structure and relationship with the OECD Privacy Guidelines.

3. Context

The Recommendation was developed in the context of implementing the OECD Privacy Guidelines and is a key aspect of the OECD's work on privacy. The 2011 Report on the implementation of the Recommendation helped shape the 2013 revision of the OECD Privacy Guidelines (OECD, 2013[4]). Similarly, this review was prompted by the findings of the 2021 Report on the implementation of the OECD Privacy Guidelines (OECD, 2021[3]). Accordingly, it is helpful to set out the relationship between the Recommendation and the OECD Privacy Guidelines.

Additionally, to aid in understanding the implementation findings (and this Report more generally) it is useful to briefly explain the structure of the Recommendation, as well as to consider what is meant by "cross-border co-operation in the enforcement of privacy laws".

3.1. Relationship with the OECD Privacy Guidelines

The importance of cross-border enforcement co-operation has been enshrined in the OECD Privacy Guidelines since their inception some four decades ago. The original Part Five of the of the Privacy Guidelines (adopted by the OECD Council on 23 September 1980), dealt with international co-operation, and provided that countries should (i) have simple and compatible procedures for the transborder flows of

personal data; (ii) establish procedures for facilitating the exchange of information and providing mutual assistance in investigations; and (iii) work towards developing principles to govern the applicable law regarding the transborder flows of personal data (OECD, 1980[9]).[8]

Subsequently, cross-border co-operation in the enforcement of privacy laws has remained a priority for the OECD in the implementation and dissemination of the OECD Privacy Guidelines. It was in the context of this work that the Recommendation was developed,[9] and accordingly it is firmly rooted in the OECD Privacy Guidelines. The two legal instruments remain interlinked and the findings of the 2011 Report on the implementation of the Recommendation informed the 2013 revision of the OECD Privacy Guidelines, which in a number of places sought to address key challenges that had been identified in that 2011 Report (OECD, 2013[10]).

For example, the 2011 report highlighted the need for further efforts to ensure that PEAs have sufficient powers to administer effective sanctions, as well as sufficient resources to accomplish their mission, and noted that legal limitations on the ability of PEAs to share information with foreign authorities remained an issue (OECD, 2011[2]). Accordingly, the Terms of Reference for the 2013 Privacy Guidelines Review called for a redoubling of efforts to develop a globally active network of PEAs (OECD, 2011[11]). And, in response, paragraph 20 of the OECD Privacy Guidelines (as revised in 2013) reiterates the commitments expressed by Adherents to the Recommendation to take appropriate measures to facilitate cross-border privacy law enforcement co-operation and to enhance information sharing between PEAs (OECD, 2013[4]).

3.2. The structure of the Recommendation

The Recommendation starts with a preamble (“Having Regards”; “Recognising”) which sets out other OECD legal instruments relevant to the Recommendation at the time of its adoption, as well as context.

It is then “Recommended” that Adherents co-operate across borders in the enforcement of laws protecting privacy, by taking appropriate steps to:

- improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities (expanded on in Annex Part III);
- develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation (expanded on in Annex Part IV);
- 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 (expanded on in Annex Part IV); and
- engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy (expanded on in Annex Part IV).

The main detail of the Recommendation is found within the Annex, which sets out Definitions (Part I), Objectives and Scope (Part II), Domestic Measures to Enable Co-operation (Part III) and International Co-Operation (Part IV). Where this Report refers to numbers or parts of the Recommendation, it is referring to the Annex.

3.3. What is meant by cross-border co-operation in the enforcement of privacy laws?

The Recommendation does not include definitions for the terms "cross-border co-operation" or "enforcement of privacy laws", but it is helpful to consider what these terms mean. A useful starting point is to look back at how they were understood at the time the Recommendation was drafted.

A 2006 report which underpinned the Recommendation provides some clarity. The report considered "enforcement" to include efforts by government authorities to:

> *"i) secure legal remedies for individuals that have been harmed; ii) carry out regulatory audits and inspections; and iii) secure compliance by formal legal action of an administrative, civil, or criminal nature." (OECD, 2006, p. 13[12])*

The same report noted that:

> *"cross-border" aspects of enforcement is a term used in a broad sense to include cases in which "the data subject is located in a different country from the data controller, the data itself has passed to a third country, or simply where important evidence is located in a third country." (OECD, 2006, p. 20[12])*

Building on the above understanding, the scope of the Recommendation is described as:

> *"focused on co-operation with respect to those violations of Laws Protecting Privacy that are most serious in nature. Important factors to consider include the nature of the violation, the magnitude of the harms or risks as well as the number of individuals affected." (II.4)*

Additionally, the Recommendation calls for:

- domestic measures that enable PEAs from different jurisdictions to co-operate effectively (at III.7), that provide for redress for individuals who have suffered harm no matter where they are located (at III.9), and for co-operation in cases of mutual concern regarding the use of evidence, judgments and enforceable orders between foreign PEAs (at III.10);
- improved co-operation between PEAs including regarding the sharing of relevant information with, and in providing assistance to, a foreign PEA when faced with a possible violation of a privacy law (at III.B.12.a & b);
- practical steps which can enhance mutual assistance, for example: providing sufficient information with any request for assistance (at IV.A.14.a); specifying the purpose for which information will be used (at IV.A.14.b); designating a national contact point (at IV.B.19); and sharing information on enforcement outcomes (at IV.B.20); and
- establishing an informal network of PEAs and other stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices, develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising activities (at IV.B.21).

From the above, it can be inferred that cross-border co-operation in the enforcement of privacy laws involves (or in 2007 was understood to involve):

- legal and policy frameworks that enable PEAs from different jurisdictions to co-operate effectively;
- legal and policy frameworks which provide redress for individuals, no matter their location;
- legal and policy frameworks which can ensure compliance of privacy laws through formal legal action of an administrative, civil, or criminal nature;

- practical actions which enhance information sharing regarding specific cases or specific concerns; and
- general co-operation to share information, best-practices, develop shared priorities, and to raise awareness.

4. Implementation and continued relevance

4.1. Definitions, objectives, and scope (Annex, Part I and II)

Part I of the Annex to the Recommendation provides definitions of the terms "Laws Protecting Privacy" and "Privacy Enforcement Authorities". Part II sets out its objectives and scope, specifying that the Recommendation seeks to foster international co-operation between PEAs as a means of addressing the challenges of protecting the personal information of individuals (wherever they may be located) (at II.2). It is explicitly stated that the Recommendation does not intend to interfere with governmental activities that relate to national sovereignty, national security, and public policy (at II.6).

The Recommendation's main focus is the activities of PEAs, although it acknowledges that other entities (e.g. law enforcement) play an important role and encourages co-operation with such entities (at II.3). In recognition that cross-border co-operation can be complex and resource intensive, the Recommendation focusses only on those violations that are the most serious in nature (at II.4). It is primarily aimed at facilitating co-operation in the enforcement of privacy laws that govern the private sector, although the Recommendation notes that Adherents may also wish to co-operate on matters involving the public sector (at II.6).

4.1.1. Findings from the 2021 questionnaire

The majority of Respondents (21 out of 28) felt that the terminology and definitions within the Recommendation remain relevant. However, one Respondent commented that the definition section was insufficient and, in addition to the two definitions currently listed, suggested that terms such as "cross-border" and "co-operation" could be defined. Another noted that the terminology and definitions section could be revised to indicate that PEAs should be independent.

Likewise, the majority (24 of 28) of Respondents considered that, *in general*, the objectives and scope of the Recommendation have kept pace with technological developments and advancements and remain relevant today. One Respondent noted that this is because the Recommendation is already drafted in broad terms.

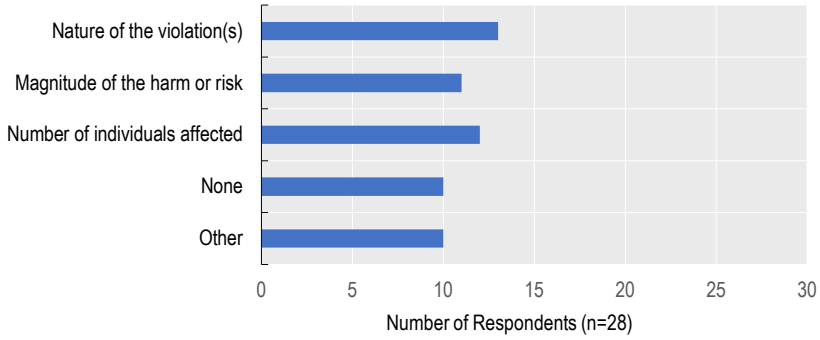
Nonetheless, it was noted that particular aspects of this part could be updated. For example, three Respondents considered that the Recommendation could explicitly recognise factors such as increasing cross-border data flows (in the scope and/or within the definitions), the fast pace of technological advancement and innovation on a global scale, and the resulting increase in the need for cross-border co-operation and enforcement.

As noted above, the scope of the Recommendation is intended to cover only those violations of privacy laws which are the most serious in nature. Factors to consider in determining the seriousness of the violation include, "… the nature of the violation, the magnitude of the harm or risks as well as the number of individuals affected". One Respondent felt that limiting the co-operation to only those violations which

are the most serious in nature is outdated, noting that the reality today is that there is an increasing prevalence of multi-national companies who deal exclusively in data, and given the interconnected nature of the digital economy, PEAs should be encouraged to co-operate on a routine basis (where practical). Another considered that broadening the Recommendation's scope beyond only the most serious violations, would help normalise cross-border co-operation as a necessity in today's digital environment.[10]

The 2021 questionnaire also asked Respondents about the extent to which they used these criteria (nature of the violation, magnitude of harm/risk, number of individuals affected) in deciding whether or not to accept a cross-border request for assistance. Whilst 10 out of 28 Respondents indicated they did not take any of these factors into account, for the most part Respondents took one, or a combination, of these factors into account (see Figure 1).

Figure 1. Factors for deciding whether to accept a request for assistance



Source: 2021 questionnaire (B8)

However, in expanding on their responses, Respondents indicated that whilst these three factors (magnitude, nature of harm/risk, number of individuals affected) may be considered relevant (and therefore taken into account when deciding whether or not to accept a request for assistance) they are not necessarily determinative factors, nor are they the only factors considered. Indeed, only a few PEAs (4 out of 28) indicated that they have declined a request for assistance from a PEA in another country.[11] This finding, however, should be considered together with the findings under 4.2.1.1 which discusses the challenges a PEA may face when seeking to act on such a request.

Respondents which are Member States of the European Union (EU) noted that within the EU/European Economic Area (EEA) the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) creates a general duty of co-operation between EU/EAA Member States, and as long as the requirements of the GDPR are met, there is an obligation to accept cross-border[12] requests for assistance from other EU/EEA Member States (European Union, 2016[13]). However, the GDPR itself provides an exception, stating that EU Member States may decline to comply with such a request if they lack competence, or if complying with the request would infringe the law (either of the EU, or of the EU Member State).[13]

It was also highlighted that PEAs take into account certain practical factors when assessing a request for assistance, and the reasons for (or limitations on) accepting requests may be unrelated to the three factors listed in the Recommendation. For example, one Respondent noted that whilst their PEA has a broad and general authority to accept a request for assistance, they may only disclose information if the request relates to an ongoing (or potential) investigation or proceeding regarding conduct that would be substantially similar to conduct that would contravene their own domestic legislation. Another noted that the conduct being a violation of (or conduct substantially similar to a violation of) laws administered by their regulatory authority was a requirement of accepting a request.

Some Respondents indicated that they take into account public interest factors, whether any legal obligations preclude them from providing assistance, and whether or not the requesting country is providing reciprocal assistance.

4.1.2. Insights from the Expert Roundtable

The challenges that PEAs face in identifying and prioritising issues for regulatory intervention was highlighted. For example, different PEAs may make different decisions regarding which cases to pursue due to different factors (e.g. legal criteria, cultural factors, public interest priorities). This then creates a challenge for broader cross-border enforcement co-operation as there may not be a shared understanding of the appetite for intervening in matters that cut across-borders.

In this regard, it was noted that there may be a role for the OECD to support PEAs in coordinated horizon scanning, assisting in identifying and prioritising issues of common interests across borders. It was suggested that work could be done to increase the visibility of relevant issues (or common concerns), and that the OECD may be well placed to help in identifying issues worthy of consideration. It was pointed out that engaging in this coordinated horizon scanning could help create a better shared understanding of cross-border privacy issues, allowing for PEAs to make more informed decisions about prioritising issues as well as whether or not to engage in cross-border enforcement co-operation. It was also noted that there may be scope for the OECD to develop metrics to help PEAs measure and articulate the impact of cross border co-operation. Through such metrics the added value of cross-border co-operation could be better demonstrated, providing a tangible evidence base to policy makers, and promoting broader and more diverse uptake amongst PEAs.

The positive impact of joint investigations, and cross-border co-operation was also highlighted, and it was noted that often the biggest impact of investigations is not just on the individual company concerned, but also on the ability to encourage broad compliance through a communication strategy. It has been seen that the impact of media messaging is significantly better from joint investigations than from solo ones. It was also highlighted that even where a decision is appealed the initial action can have a positive impact, such as the company in question withdrawing the services (considered to be in breach of the law) from the jurisdiction.

4.1.3. Definitions, objectives and scope - Brief conclusions

In general, Respondents indicated that the definitions, objectives and scope of the Recommendation remain relevant, and (as noted by one Respondent) the broad terms in which it was drafted has meant that it has kept pace with technological development and advancements.

Nonetheless, the findings of the 2021 questionnaire with regards to these parts of the Recommendation indicate a number of areas which could benefit from further clarification and/or amendment should it be decided to revise the Recommendation. These relate to:

- expanding definitions to include terms such as “cross-border” and “co-operation”;
- explicitly highlighting the reality today that increasing cross-border data flows, and the continual fast paced technological advancement and innovation, has resulted in a much-increased need for cross-border co-operation and enforcement; and
- assessing whether or not limiting the scope of the Recommendation to only those violations which are the most serious in nature remains appropriate. As noted by several Respondents, this does not reflect actual practice and seems outdated given the interconnected nature of the digital economy today.

Discussion at the Roundtable highlighted that there may be a role for the OECD to assist in coordinated horizon scanning to help identify issues of common concern and assist PEAs in making informed decisions regarding whether or not to engage in cross-border enforcement actions.

4.2. Domestic Measures to Enable Co-operation (Annex, Part III)

Part III of the Annex to the Recommendation sets out a number of domestic actions that Adherents should take to enable co-operation. This includes general measures, as follows:

- developing and maintaining effective domestic measures, which can enable PEAs to co-operate effectively with foreign (and other domestic) PEAs (at III.7);
- reviewing and adjusting their existing domestic frameworks (as needed, and when appropriate) (III.8);
- considering ways to improve remedies for, and (where appropriate) provide redress to, persons who suffer harm due to a violation of privacy laws (at III.9); and
- considering how, in cases of mutual concern, the Adherents' own PEA may use evidence, judgements, and enforceable orders obtained by a PEA in another jurisdiction as a means of improving their ability to address the same or related conduct in their own jurisdiction (at III.10)

Additionally, Part III sets out measures relating to the powers and authorities of PEAs (at III.A.11), as well as measures designed to improve the ability of PEAs to cooperate with their counterparts in other jurisdictions (at III.B.12).

4.2.1. Findings from the 2021 questionnaire

This section deals with the factors covered by Part III of the Annex to the Recommendation, namely: i) domestic measures (including the compatibility of legal frameworks, and the ability of PEAs to co-operate with their foreign counterparts); and ii) the powers and authorities of PEAs (including their resources, power to enforce laws, and available remedies/redress).

4.2.1.1.Domestic frameworks

Legislative compatibility

As transborder flows of data increase and grow in volume and importance worldwide, it has become even more essential for different legal authorities to be able to work together to ensure that privacy laws (and any safeguards for cross-border data flows contained within them) are respected, and where needed, can be effectively enforced. However, the growing number of legislative frameworks which have been enacted in response to this reality adds complexity to enforcement co-operation, particularly where a privacy violation, or the actions underlying that violation, span different jurisdictions.

The findings of the 2021 Report on the implementation of the OECD Privacy Guidelines highlighted that diversity in legal frameworks can present challenges for countries. Notably, as part of that assessment, incompatibility of legal regimes was the most common response when Adherents were asked to indicate the main challenges they face in cross-border co-operation, followed by restrictions in sharing information.[14] Nonetheless, in response to this survey finding, and in the course of the 2021 review of the Privacy Guidelines, OECD delegates noted that it remained unclear which legal regimes were being referred to and where such incompatibility actually lies (OECD, 2021[3]).

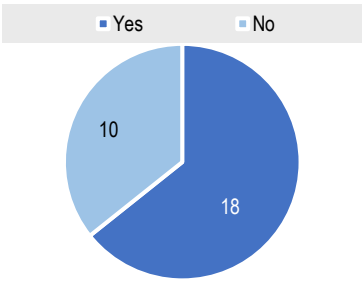
Accordingly, the 2021 questionnaire sought to expand upon the findings of the 2021 Report on the implementation of the Privacy Guidelines and to further understand the extent to which differences in legal

frameworks (including the capacity for countries to share information in accordance with their domestic laws) affects cross-border enforcement co-operation.

It is useful to understand the extent to which cross-border co-operation is actually needed. That is, how often are countries being called on by other countries to provide assistance, and how often are breaches of privacy laws cross-border in their nature. Unfortunately, in terms of how often countries are being called upon to provide assistance to a foreign PEA (or how often they are faced with possible violations of this nature), statistics on lodged complaints often do not provide a breakdown of whether or not complaints have a cross-border element, or such statistics are not made publicly available.[15]

Nonetheless, responses to the 2021 questionnaire indicate that Respondents are often faced with breaches of privacy laws that are cross-border in nature. Nearly two thirds of PEAs have experienced situations where violations of privacy laws span multiple jurisdictions (see Figure 2).

Figure 2. Over half of Respondents' PEA have faced situations where violations of privacy laws have spanned two or more jurisdictions



Source: 2021 questionnaire (F1)

One Respondent noted that today's economic reality means that it is quite common for multinational companies to be present in multiple jurisdictions, that these companies represent a large portion of highly complex cases, and that this presents a number of challenges. For example, where violations span two or more jurisdictions, that PEA's competency has to be established through identifying a "real and substantial" connection to the country in question, and should this test not be met, the PEA will not have the competency to investigate the complaint. Two Respondents noted that when the main location of the data controller being investigated (or complained about) is in a foreign country, they may need to rely on the foreign PEA to take action.

A number of other challenges and barriers were noted. For example, even when the PEA has the competence to bring actions and issue sanctions, they may face practical or legal hurdles in enforcing any meaningful compliance with orders. Some Respondents indicated that they can face challenges in serving complaints or in receiving information. One noted that the enforceability of corrective actions and sanctions when the foreign controller challenges their PEA's powers is yet to be tested, as they have had no cases of this nature to date.

Ability of PEAs to Co-operate

The Recommendation (at III.B.12) recommends that Adherents should take steps to improve the ability of their PEAs to co-operate with foreign PEAs, including by: (a) providing their PEAs with mechanisms to share relevant information with foreign authorities; and (b) enabling their PEAs to provide assistance to foreign authorities, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying organisations or persons involved or things.

Most Respondents to the 2021 questionnaire (23 out of 28) have measures in their domestic frameworks to enable co-operation. This includes measures relating to the capacity to share information with, and to provide investigative assistance to, foreign authorities. Often, however, such measures come with conditions or limitations, such as on the scope, the confidentiality of information, regarding reciprocity, or require agreement between the two authorities (i.e. on launching investigations, issuing binding decisions).

Adherents may be restricted in sharing information due to strict confidentiality requirements in their domestic laws, or PEAs may need to seek a formal agreement from their national government before co-operating and sharing information. One Respondent highlighted that their domestic legal framework explicitly prohibits the exchange of (identifiable) personal data which has been obtained by their PEA in the course of professional activities. This professional secrecy requirement creates difficulties in that it prevents information sharing with other PEAs (even when the other PEA permits the sharing of such information).

It was noted that even within the EU, where the GDPR has harmonised privacy laws, differences in the individual EU Member States' jurisprudence or doctrine may mean that courts or PEAs interpret what amounts to a violation of the GDPR differently, and this can impact the capacity of Member States to respond to violations in other jurisdictions.

However, one Respondent noted that the diversity between privacy laws has in itself created opportunities for co-operation, for example through encouraging the development of Memorandums of Understanding (MOU) and providing an opportunity to build a working relationship. Likewise, another Respondent, in commenting on the work plan, noted that differing legal regimes, competences, and powers can often present opportunities to leverage each PEAs separate strengths and more holistically address a concern. For instance, PEAs may choose to investigate a breach or issue in a coordinated manner and address different aspects separately depending on their laws and powers.

Other types of domestic measures to enable cross-border co-operation highlighted included those concerning complaint handling, undertaking research, [16] reimbursement of expenses for assistance provided, and staff exchanges between PEAs.

Insights from the Expert Roundtable

Speakers at the Roundtable considered complex and practical legal challenges to co-operation and highlighted that in today's interconnected world co-operation between PEAs is no longer merely nice to have, but has become an imperative that can provide more impactful, holistic and consistent outcomes.

The situation in the EU/EEA was highlighted, where the harmonised approach means that should one PEA take a decision that could have an impact across the EU/EEA this action must be done unanimously. [17] Despite this obligation, even within the EU/EEA understanding and applying co-operation procedures in the same consistent manner is a challenge. For instance, there can be divergences in how to apply the same provisions across different EU Member States. It was noted that developing a common culture and a consistent understanding of co-operation needs is imperative for addressing such challenges, and that this requires time invested in translation and developing a strong network of interlocutors (e.g. through meetings, joint investigations and task forces).

When co-operating outside the EU/EEA it was stressed that PEAs have to consider if the country's legal system permits such co-operation, as well as the strict rules under the GDPR (e.g. the high threshold for data transfers, and a requirement for an equal level of protection). In order to help foster co-operation with third countries the EDPB has developed a Toolbox on essential data protection safeguards for enforcement co-operation between EEA data protection authorities and competent data protection authorities of third countries (EDPB, 2022[14]), setting out key principles and data protection safeguards.

It was noted by some that meaningful enforcement co-operation requires common rules on substance; common values, culture and trust; similar and compatible procedures; and a common prioritisation of the

same case. One speaker noted that while many laws are technically different, they are rooted in the same or similar underlying principles, rendering many challenges surmountable and providing great potential for leveraging co-operation to avoid the duplication of efforts.

It was highlighted by one speaker that whilst the sharing of personal information is often seen as a hurdle to cross-border co-operation, this can be overcome through agreements or separate legal arrangements, and that importantly often sharing of information that is personal in nature is not necessary. For example, much impactful co-operation that has occurred has been in respect of issues such as understanding technologies in the context of privacy principles and other regulatory spheres, which are issues that do not relate to the personal details of the affected data subjects.

Additionally, it was stressed that in joint investigations, communication and planning is important in overcoming practical hurdles (e.g. different approaches, timelines). One speaker, in discussing a successful joint investigation, noted that joint briefings helped overcome challenges and allowed for a greater understanding of the differences between information sharing powers and restrictions; as well as identifying a pathway for overcoming issues (i.e. through an MOU with clear terms of reference).

It was further noted by one speaker from a PEA that there may be scope for the Recommendation to be clearer and more explicit in its call for Adherents to recognise the importance of enforcement co-operation in their legal frameworks, and to go a step further and make it a core function of a PEAs role, rather than an optional extra. The speaker highlighted that this could help ensure appropriate resourcing and capacity for PEAs to fulfil enforcement co-operation as a statutory function, broaden the diversity of PEA engagement in co-operation, and amplify the impact of the privacy enforcement community as a whole.

Lastly, it was highlighted that cross-border co-operation comprises a spectrum of tools, which PEAs should all have at their disposal. Soft mechanisms are good for exchanging good practices and building trust and interpersonal connections, while strong legal tools are helpful to overcome the challenges in concrete cases.

4.2.1.2.Powers and Authorities of PEAs

Part III.A.11 of the Annex to the Recommendation recommends that Adherents take steps to ensure that they have the necessary power and authority to prevent (and to respond to in a timely manner) breaches of privacy laws. Accordingly, this section considers the responses to the 2021 questionnaire as they relate to the resources of PEAs, their investigative powers and authority, as well as what remedies and redress are available for persons who have suffered harm as a result of a violation of privacy laws.

Sufficient Resources

The Recommendation does not explicitly call upon Adherents to ensure that their PEAs are sufficiently resourced. However, the OECD Privacy Guidelines do call for the establishment and maintenance of PEAs, "with the governance, **resources** and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis" (emphasis added).[18] This section was added as part of the 2013 revision to the OECD Privacy Guidelines and reflects the finding in the 2011 Report on the implementation of the Recommendation that further efforts were needed to ensure that PEAs were sufficiently resourced (as well as having sufficient powers).

A lack of sufficient financial and human resources, as well as lack of independence in setting budgets and making recruitment decisions, may seriously impede a PEA's ability to ensure fulfilment of its mandate. PEAs require sufficient financial and personnel resources to do their job properly, and to ensure regulatory independence (OECD, 2021[3]).

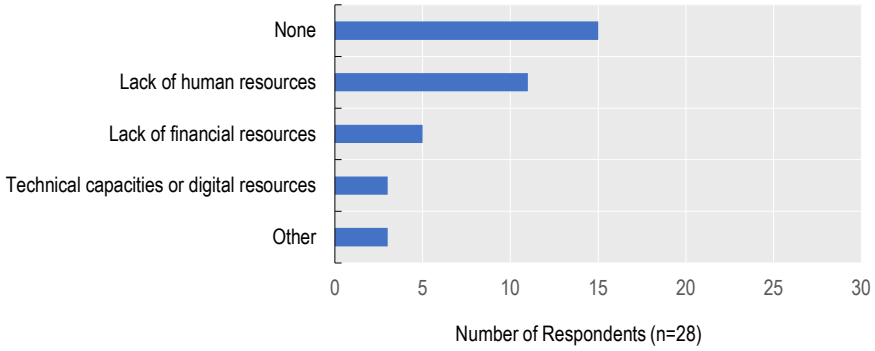
Recent research by the OECD has shed some light on the organisational and financial constraints faced by PEAs. For example, a 2019 survey by the OECD on data breach notification practices revealed that the

majority of PEAs, while involved to some degree in the budget-setting process, had little to no power to influence decisions regarding funding or the allocation of resources (OECD, 2021[15]). In addition, the 2021 Report on the implementation of the OECD Privacy Guidelines found that despite a general tendency of increases in PEAs' human resources, Respondents to the questionnaire on the OECD Privacy Guidelines most often cited insufficient staffing as a contributor to enforcement challenges (OECD, 2021[3]).

Regulatory challenges linked to new digital technologies and the increase in both the volume and frequency of data flows are also likely to create further resource restraints. As noted as part of the 2021 Report on the implementation of the OECD Privacy Guidelines, the changing technological environment has implications regarding the resources needed to ensure that PEAs have appropriately qualified technical staff with the necessary skills and knowledge to understand, work in, and respond to the rapidly changing digital environment (OECD, 2021[3]). This note reflects a shared opinion that the new privacy challenges posed to PEAs by the unprecedented development of new technologies, such as Generative AI, can only be properly met by pooling available expertise within the framework of international co-operation, including in the context of cross-border enforcement actions.

The results of the 2021 questionnaire, however, illustrate an improved situation – at least in a cross-border context. Half of the Respondents indicated that they did not face any resourcing constraints (financial, human or technical) in facilitating the cross-border enforcement of privacy laws (see Figure 3).

Figure 3. Resourcing constraints on PEA's capacity to facilitate cross-border co-operation



Source: 2021 questionnaire (Question G8)

Nonetheless, even though some PEAs indicate that efforts have been made to increase their human and financial resources, others note that they do face constraints in these areas. For example, even when requests for increases in funding or staffing are accepted, having this actioned can often be delayed by administrative processes. It was also pointed out that constraints can be caused by a lack of available tools and/or connections with the necessary interlocutors for cross-border co-operation.

Powers & Authority[19]

PEAs must not only have sufficient resources, but also the necessary powers to enforce the laws that they are implementing. The Recommendation (at Part III.A.11) calls on Adherents to take steps to ensure that PEAs have the necessary authority to prevent, and act in a timely manner against, privacy law violations that are committed *from their territory* or *cause effects in their territory*. In this regard, the Recommendation particularly refers to measures to: a) deter and sanction violations; b) permit effective investigations, including the ability to obtain access to relevant information; and c) permit corrective action against data controllers who engage in privacy law violations.

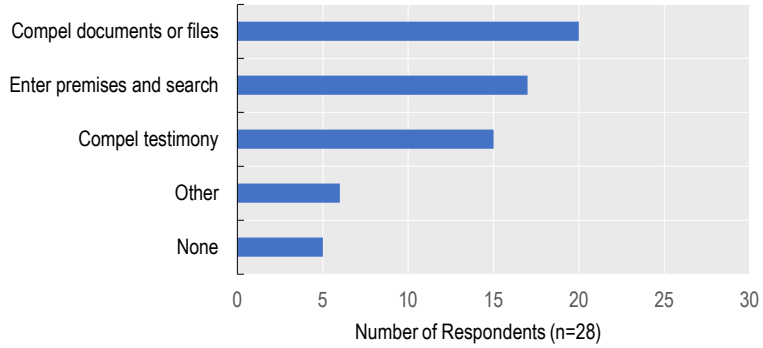
Overall, responses to the 2021 questionnaire have shown a promising picture in terms of PEAs' powers and authority. Most of the Respondents (24 out of 28) considered that, in general, their PEAs had the

necessary powers and authority to effectively engage in cross-border enforcement co-operation. Nonetheless, at least one EU Member State considered that their legal framework presented barriers to co-operation with countries outside of the EU/EEA. Another (non-EU) Respondent felt that whilst their legal framework gave their PEA the appropriate powers and authority, they nonetheless faced constraints due to territorial and jurisdictional issues.

The 2021 questionnaire further examined PEAs' powers of investigation, their capacity to use documentation from other jurisdictions, their power to commence actions regarding alleged violations, and to sanction proven ones.

With regards to investigative powers and authority,[20] the majority of Respondents' PEAs indicated that they are legally authorised to investigate alleged violations of privacy laws that have a cross-border element. This includes through compelling documents or files, entering and searching premises, and compelling testimony (see Figure 4).

Figure 4. Investigatory powers/authority against violations with a cross-border element



Source: 2021 questionnaire (Question G2)

However, some Respondents indicated that such powers may be subject to certain conditions. For example, one Respondent indicated that these powers are only available when the data controller is located in their jurisdiction, or that a search of premises can only occur should the premise be on their territory.

A number of Respondents pointed out that practical limitations are more likely to occur when the law that has been breached has extraterritorial application.[21] One noted that the above powers are only exercisable if extraterritoriality applies in relation to the violation. Another noted that they are exercisable only once a proceeding has been commenced. Another noted that whilst their PEA has these powers, there may nonetheless be practical barriers to exercising them, for example should the law of the foreign country prevent the extraterritorial exercise of such powers.

An example of cross-border enforcement in practice is depicted in Box 1.

Box 1. Example of enforcement in practice with a cross-border element

The investigations by the UK Information Commissioner's Office (ICO) into the use of data analytics in political campaigning (often referred to as the Facebook/Cambridge Analytica case) involved entities located outside of the UK.

Among such entities was AggregateIQ Data Services Ltd (AIQ), a political consultancy and technology company based in British Columbia (Canada). AIQ had in its possession and control, personal data of individuals in the UK as a result of its work on behalf of UK political organisations.

The UK ICO investigated AIQ in relation to its compliance with applicable legal data protection requirements. The UK ICO had the power to do so because the GDPR and the UK Data Protection Act 2018 (DPA 2018; regarding actions before implementation of the GDPR) both have extra-territorial scope by virtue of article 3 of the GDPR and section 207 of the DPA 2018.

Despite this power, the UK ICO has stated in its report that the investigation into the activities of AIQ presented a number of jurisdictional challenges. For example, during the course of the investigations, AIQ insisted that it was not subject to the jurisdiction of the UK ICO. The UK ICO had to advise the Canadian Parliament that AIQ had not been co-operating with the investigations, which resulted in agreement by AIQ for full co-operation.

The UK ICO issued an enforcement notice to AIQ in July 2018 (reissued in October 2018), ordering the company to cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes.

The UK ICO made referrals to the federal Office of the Privacy Commissioner of Canada (OPC), who was carrying out a joint investigation with the Office of the Information and Privacy Commissioner of British Columbia (OIPC), to confirm the UK ICO's findings. The on-going joint investigation by Canada OPC and British Columbia OIPC informed the ICO that no UK personal data was located other than that identified within the scope of the UK ICO's enforcement notice issued to AIQ.

Source: (ICO, 2018[16])

The Recommendation (at Annex Part III.10) states that Adherents should consider how their PEAs could (in cases of mutual concern) use evidence obtained by, or judgments/orders made by, a foreign PEA. In response to the 2021 questionnaire, over half of the Respondents (17 out of 28) indicated that their domestic framework gave their PEAs the capacity to do this.

However, a number of these responses related to the use of evidence and judgements/orders in investigations only, with some Respondents indicating the order would need to be explicitly recognised by their domestic court for it to be enforced. One EU/EEA Respondent noted that they would consider the enforceability of judgments on a case-by-case basis, and that not all judgments from another jurisdiction would be considered binding, although those from a senior authority in the EU/EEA would be. Two Respondents noted that they have no authority to enforce a foreign court order. However, each can use evidence provided by a foreign authority, with one of these Respondents noting that the judgment itself could be used as evidence and to aid the PEA in their legal analysis of the matter under investigation.

Insights from the Expert Roundtable

At the Roundtable, it was stressed that the lack of capacity to have decisions recognised and enforced in other jurisdictions is a real challenge. Uncertainty around whether or not a decision will be able to be enforced can have a significant impact on a PEAs decision to commence an investigation.

One speaker noted that there is room for joint work to be done to explore and leverage experience in other legal and regulatory spheres (regulatory or commercial), such as in enforcing obligations or debts, locating and attaching assets in other jurisdictions, and having judgments (including default judgments) recognised via foreign courts. Box 2 below provides some examples in this regard.

Box 2. Examples of recognition of orders from, and enforcement of orders in, other jurisdictions

Challenges regarding the recognition and enforcement of orders in other jurisdictions are not unique to privacy and data protection. In other legal and regulatory areas, different solutions exist, from guiding principles (examples one and two) to binding obligations in international conventions (examples three and four).

Example 1: OECD 2021 Implementation Toolkit on Legislative Actions for Consumer Protection Enforcement Co-operation

The OECD 2021 Implementation Toolkit on Legislative Actions for Consumer Protection Enforcement Co-operation (the Toolkit) (OECD, 2021[17]), aims to support the implementation of different principles regarding cross-border enforcement co-operation contained in relevant OECD Recommendations.[22]

The Toolkit's Guiding Principle 4 ("Enforcement powers to protect domestic consumers from foreign businesses") recognises that consumer protection authorities should have the power to pursue the same core remedy(s) against foreign businesses (in another jurisdiction) as they would be able to seek in their own jurisdiction. Underlying this principle is the rationale that, "there should be some mechanism that permits an appropriate enforcement remedy made in one jurisdiction to be recognised and enforced in the other jurisdiction, e.g. through the administrative or judicial processes of the foreign jurisdiction, subject to appropriate safeguards" (OECD, 2021, p. 37[17]).

Example 2: Enforcement co-operation between competition authorities

Recognising, among others, the issues regarding enforcement/remedial actions with extraterritorial reach, the 2014 OECD Recommendation of the Council Concerning International Co-operation on Competition Investigations and Proceedings (OECD, 2014[18]) puts forward a framework of consultation and comity as well as notification between Adherents when one Adherent's enforcement action can be expected to affect interests of other Adherents (at III, IV and V of the Recommendation).

Comity occurs when the authorities of one jurisdiction respects the laws and judicial decisions of another jurisdiction, as a matter not of obligation but of mutual respect. In the context of the above Recommendation it helps facilitate appropriate enforcement actions with respect to anti-competitive activities occurring in one territory and adversely affecting important interests of another territory. This enables effective allocation of enforcement resources by allowing the better-placed party to deal with the problem (e.g. avoiding difficulties of obtaining evidence in a foreign jurisdiction) and minimises conflicts between Adherents that may be caused by enforcement actions against activities occurring in another jurisdiction (OECD, 2021[19]; OECD, 2021[20]). The OECD Competition Division provides inventories of relevant provisions of bi-lateral or multi-lateral arrangements between governments or competition agencies relating to competition enforcement co-operation (including notifications, comity and consultation), which helps jurisdictions in the negotiation or interpretation of co-operation agreements (OECD, 2022[21]; OECD, 2022[22]).

Example 3: Hague Conference on Private International Law (HCCH) 1996 Child Protection Convention

The Convention of 19 October 1996 on Jurisdiction, Applicable Law, Recognition, Enforcement and Co-operation in Respect of Parental Responsibility and Measures for the Protection of Children (HCCH, 1996[23]) provides a binding framework for the recognition and enforcement of orders among contracting parties to the Convention. Article 23 of the Convention provides that (subject to certain exceptions and safeguards) "the measures taken by the authorities in one State shall be recognised by operation of law in all other Contracting States". In practice, this is facilitated by Contracting States enacting enabling

provisions in their domestic law, as well as by the Hague Network of Judges. This network allows for communication between judges prior to a decision being made on the laws and procedures in the jurisdiction where it is intended that the order be recognised and enforced (HCCH, 2014[24]).

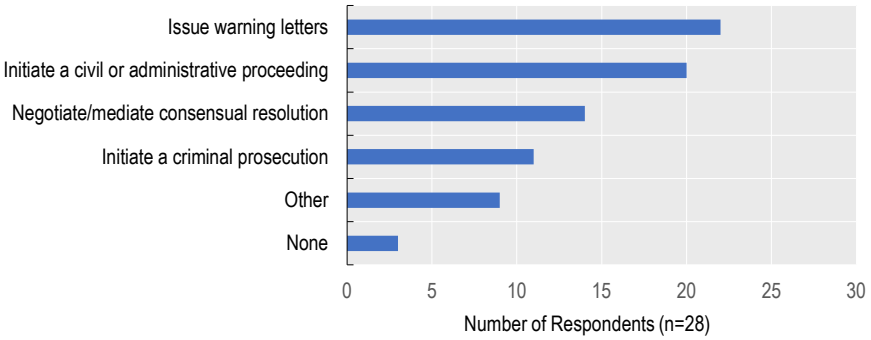
Example 4: UN Convention on the Recognition and Enforcement of Foreign Arbitral Awards

The United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (also known as the "New York Convention"), is a key instrument in international arbitration. International arbitration allows for the non-judicial resolution of a dispute by an agreed arbitrator. In general, once parties have agreed to arbitration they are bound by the decision of the arbitrator and have no recourse to courts save for seeking the enforcement of the arbitral decision.

The New York Convention requires each contracting State to recognise foreign arbitral awards as binding and enforce them in its jurisdiction, in the same way as it would do for domestic awards (Art. 3) (UNCITRAL, 2015[25]). In effect, it allows foreign arbitral awards to be recognised and enforced in any other contracting State. The New York Convention is widely accepted with 172 State parties as of 2023.

The 2021 questionnaire further asked about capacity to formally respond to alleged violations of privacy laws with a cross-border element. Most Respondents indicated that their PEAs have this power, although the severity of the action varies – ranging from issuing warning letters, to the commencement of criminal proceedings (see Figure 5).

Figure 5. Powers/authority for corrective action against violations with a cross-border element



Source : 2021 questionnaire (Question G4)

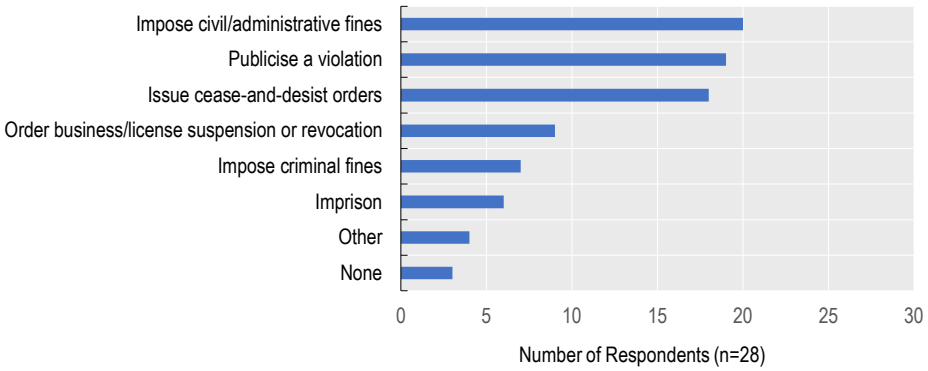
Issuing warning letters was the most common response reported, with at least one Respondent indicating that their PEA may engage with an organisation to highlight their concerns in an attempt to resolve issues prior to commencing an investigation. Negotiation or formal alternative dispute resolution processes may be used to reach an agreement, which can then (in one Respondent) later be approved as a formal settlement before a court or tribunal, or in another be turned into a formal compliance agreement directly with the organisation. One PEA indicated that it may, upon the completion of an investigation, issue a report with findings setting out the contraventions and making recommendations to correct them.

Respondents are more likely to commence civil or administrative proceedings, rather than criminal actions, with a number of Respondents indicating that for the most part they refer cases to public prosecution authorities to commence criminal proceedings, although some Respondents do have quasi-criminal powers for some cases. One Respondent's newly adopted law extends their PEAs power beyond what previously only permitted giving guidance, advice and making recommendations, to enable the making of

orders and public announcements regarding privacy law violations, and specifically for cross-border violations.

Lastly, with regards to powers and authority, the 2021 questionnaire sought to understand the capacity of PEAs to impose sanctions[23] in response to proven violations of privacy law which have a cross-border element. Most Respondents have some form of power to impose a sanction, although the severity of sanctions vary, with it being much more likely that a civil or administrative fine be issued than any form of criminal penalty (see Figure 6).

Figure 6. Powers/authority for imposing sanctions against violations with a cross-border element



Source : 2021 questionnaire (Question G5)

Typically, sanctions involve imposing a civil or administrative fine, publicising a violation, or issuing cease-and-desist orders. For the latter, one Respondent noted that they did not have the power to issue such orders themselves and would need to refer the matter to a Court.[24] Another noted that whilst they have the power to issue cease and desist orders, the enforceability of such orders in a cross-border context is unclear as they have not yet been faced with a situation where they would need to seek a cross-border order of this kind.

A number of Respondent indicated that they routinely publicise the results of investigations, with some noting that they do not consider this a sanction, but rather a necessary transparency practice, and an essential element of a democratic society.

Civil and administrative fines are more common than criminal penalties, with some Respondents indicating that they only have the power to issue administrative fines, or that fines are available only for certain sectoral violations (e.g. children's privacy).

With regards to other sanctions, two Respondents noted that they could not suspend a business' licence *per se* but could suspend the use of personal data (including pending the finalisation of an investigation). One Respondent noted that they have powers to provide direction to data controllers and processors on the necessary measures needed to ensure compliance with the law.

Remedies & Redress

The Recommendation acknowledges that not only is it important that PEAs have the power to investigate and sanction organisations who violate privacy laws, but also that Adherents should consider ways in which the remedies and redress available for the victims of these violations (wherever they may be located) could be improved.[25]

The majority of Respondents to the 2021 questionnaire (24 out of 28) indicated that their legal framework includes administrative or judicial remedies and/or redress for individuals who have suffered harm as result

of a privacy law violation with a cross-border element. For many Respondents, the right for individuals to file a complaint and seek such a remedy lies in data protection legislation and applies regardless of whether or not there is a cross-border element to the violation. The most common remedy cited is compensatory damages.

However, whilst some PEAs have the power to seek compensation (or other remedy) on behalf of the victim of the violation, in a number of cases the person who has suffered harm must commence their own civil action.[26]

One Respondent noted that ensuring parity of remedies/redress across jurisdictions is a challenge, as the differences between PEAs' levels of power or ability to issue orders / sanctions could result in different enforcement outcomes afforded to individuals.[27]

4.2.2. Domestic measures to enable co-operation – Brief conclusions

Whilst the responses to the 2021 questionnaire indicate that Respondents have taken a number of actions to enable cross-border co-operation in enforcing privacy laws, a number of practical challenges remain to fully effect this core function of the PEAs role.

Differences between legal frameworks continue to pose practical barriers to taking action. For example, discrepancies in confidentiality requirements can pose barriers to sharing information or there may be a lack of jurisdiction or competence to commence actions. A number of challenges are posed by laws that have extraterritorial application and liability, and enforcement co-operation is seen as essential to support the practical application of such laws. Even where there is competence to commence an action, Adherents may face hurdles when attempting to serve complaints, or enforce compliance, in another jurisdiction.

Discussions at the roundtable painted a positive picture in that often the sharing of personal information is unnecessary, and that many hurdles can be overcome through soft co-operation. Nonetheless the issue of recognition and enforcement of foreign decisions was highlighted as a particular challenge, and it was noted that there may scope for the OECD to consider facilitating joint work on this.

Additionally, a lack of statistics relating to the number of violations (or alleged violations) of privacy laws that have a cross-border element poses challenges in identifying the scale of the issue, and the consequent need for action. At present, the Recommendation does not explicitly recommend that Adherents keep statistics in this regard, and this may be an issue worth addressing in any revision of the Recommendation, or in any implementation guidance.

At the same time, at least two Respondents noted that differences in legal frameworks can bring opportunities (i.e. in encouraging the development of MOUs or allowing for the different countries to tackle the different aspects of the investigation most in line with their legal framework). The benefits that this can bring, and how they can be further embraced, is also worth further exploring.

4.3. International co-operation (Annex, Part IV)

Part IV of the Annex to the Recommendation sets out a number of actions designed to facilitate international co-operation. Divided into three main parts, this includes:

- actions relating to the provision of mutual assistance (at Part IV.A.14 -18)
- engaging in collective initiatives to support mutual assistance (at Part IV.B.19 – 21); and
- co-operation with other authorities and stakeholders (at Part IV.C.22).

4.3.1. Findings from the 2021 questionnaire

4.3.1.1.Providing mutual assistance

The importance of mutual assistance in international co-operation has long been recognised by the OECD Privacy Guidelines. Part Five of the original 1980 Privacy Guidelines, "International Co-operation", focused on co-operation between Adherents in the context of transborder flows of personal data and provided *inter alia* that Adherents should establish procedures to facilitate exchange of information and mutual assistance in investigations.

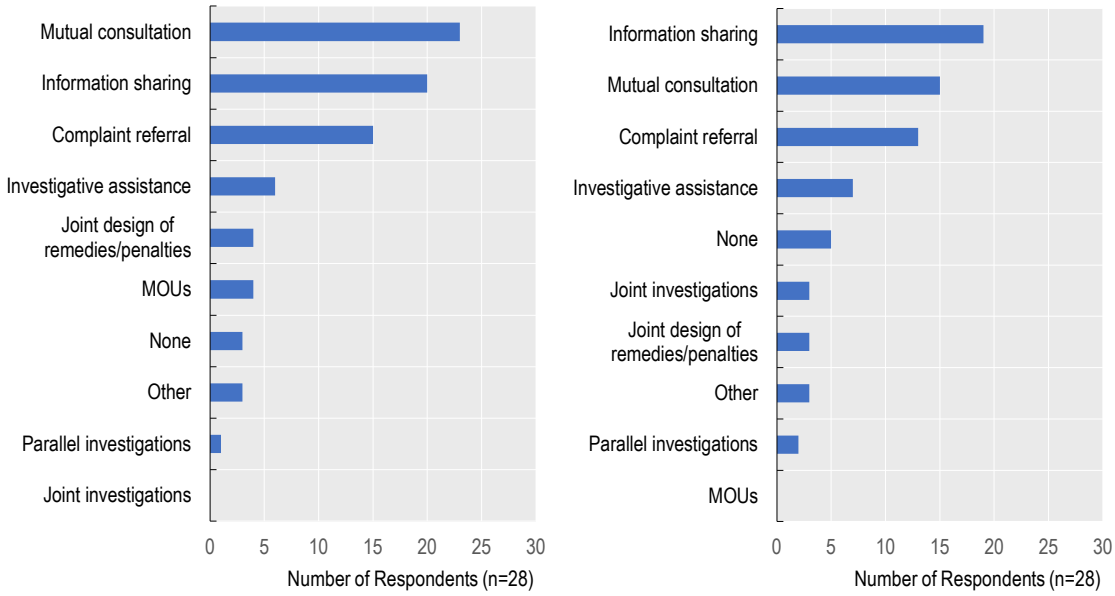
A main objective of the Recommendation is to provide further context and clarity around how to achieve this, setting out provisions regarding providing mutual assistance, and related good practice measures (such as the designation of a national contact point and the sharing of information on enforcement outcomes) (OECD, 2011[2]). Likewise, when revised in 2013, the OECD Privacy Guidelines highlighted the importance of international co-operation (at Part Six).

The 2021 questionnaire sought to further understand the different mechanisms through which PEAs co-operate and to consider the effectiveness of the various mechanisms. Specifically, the 2021 questionnaire set out eight different forms of mutual assistance as follows:[28]

- *Mutual consultation*: Informal exchanges of information with foreign PEA(s) regarding lessons learned and technical advice as a means to supplement enforcement activities.
- *Information sharing*: Sharing relevant information (including confidential information) with foreign PEA(s) relating to alleged violations of privacy laws.
- *Complaint referral*: Passing on a complaint to a foreign PEA (in which case, no further action may be taken by the original PEA).
- *Provision of investigative assistance*: Providing assistance to foreign PEA(s) relating to alleged violations of privacy laws. In particular, this may relate to: obtaining information from persons; obtaining documents or records; or locating or identifying organisations, things or persons involved.
- *Parallel investigation*: Situations where PEAs in two or more jurisdictions conduct an investigation on the same or related issues, independently but in close collaboration with one another (including through the sharing of information).
- *Joint investigation*: Situations where PEAs in two or more jurisdictions conduct a combined investigation, often involving the streamlining of resources.
- *Joint design of remedies / penalties*: Coordinated enforcement outcomes (e.g. sanctions, redress, and joint statements).
- *Memorandums of Understanding (MOU)*: Bi-lateral or multi-lateral agreements between PEAs which aim to facilitate co-operation, and clarify the scope and means of such co-operation. MOUs are generally non-binding agreements.

All Respondents use each of these methods, although with varying frequency. Respondents were asked which of the above they employed most often, as well as which methods were considered to be most effective. Mutual consultation, information sharing, and complaint referral were the most commonly selected options, both in terms of most employed methods and those considered to be the most effective (see Figure 7).

Figure 7. Forms of mutual assistance employed most often (left) and considered most effective (right)



Note: Respondents were asked to choose up to four answers.
Source : 2021 questionnaire (Question B2 and B3)

These responses imply a preference for engaging in less formal methods of mutual assistance or ones that might require a one-off action, rather than entering into a prolonged collaboration with another country. It was also indicated that mutual consultation, as well as information sharing, often occur through participation in formal or informal networks (this kind of collaboration is discussed further under Section 4.3.1.2).

With regards to complaint referral, some Respondents indicated that it is common for them to make regular referrals to a particular jurisdiction or within a particular region. Others noted that this is a common response employed when it appears that they lack competence and another jurisdiction is likely to be best placed to investigate the complaint.

MOUs are another method of collaboration often engaged in to facilitate co-operation between two or more PEAs (or with other regulatory bodies). MOUs often seek to clarify the scope and means of co-operation in a manner that is non-binding and compatible with each countries' legal framework. In response to the 2021 questionnaire, Respondents indicated that in addition to setting out parameters for investigative assistance and information sharing, MOUs have been used to establish education and training programs and joint research projects (see Table 1 for a list of existing MOUs reported by countries).

Although a less frequently used tool, provision of investigative assistance, joint/parallel investigation and joint design of remedies/penalties are another form of mutual assistance that Respondents employ and consider effective. One Respondent noted that parallel investigations allow for significant coordination between jurisdictions, and that joint investigations can be highly effective in that they bring pressure from multiple jurisdictions on the basis of shared facts.

One notable example is the joint investigation by Australia and Canada in relation to a data breach that threatened exposure of the accounts of approximately 36 million users. Box 3 provides a summary of this case.

Box 3. Ashley Madison – Joint Investigation Australia & Canada

In 2015, a data breach occurred of Ashley Madison, an adult dating website operated by Avid Life Media Inc. (ALM), now Ruby Life Inc. Headquartered in Canada, Ruby Life's websites have a global reach, with users in over 50 countries, including Australia and the US.

Given the scale of the data breach (approximately 36 million user accounts), the sensitivity of the information involved, the impact on affected individuals, and the international nature of the business, Australia's Office of the Information Commissioner (OAIC) and Canada's Office of the Privacy Commissioner (OPC) jointly investigated Ruby Life's privacy practices. They also collaborated with the US Federal Trade Commission (FTC) who conducted a parallel investigation. This collaboration was undertaken in the interests of avoiding duplication, and in ensuring that it was conducted expeditiously.

This joint OPC-OAIC investigation considered potential violations under both the Australian Privacy Act 1988 and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). To facilitate this co-operation, OPC and OAIC shared information under their relevant statutes and the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (CPEA).

The resulting joint investigation report identified a number of contraventions of both pieces of legislation, as well as findings specific to one law or the other. This demonstrated the effectiveness of fully joint investigations and reports, even where scope and legal requirements are not identical. It resulted in both a compliance agreement with the OPC under the provisions of the PIPEDA and an Enforceable Undertaking with OAIC under the Australian Privacy Act.

In this instance, the effectiveness of the collaboration was further supported by the coordination and mutual sharing of information with the FTC's parallel investigation into Ashley Madison. This contributed to well-aligned conclusions on the issues examined by all three authorities, in addition to related consumer protection issues addressed by the FTC, who reached their own settlement with the company. To facilitate this co-operation, the FTC relied on key provisions of the U.S. SAFE WEB Act that allows the FTC to share information with foreign counterparts to combat deceptive and unfair practices that cross national borders.

Source: (OAIC, 2016[26]; OPC, 2016[27]; FTC, 2016[28])

In Part IV.A.14, the Recommendation, also sets out practical information that Adherents should routinely share when making a request for assistance from a foreign PEA, such as ensuring that sufficient information is provided, or specifying the purpose of the request. In this regard, the 2021 questionnaire asked if procedural guidance was in place regarding the information to include when making a request for assistance. Only 13 out of 28 Respondents reported that they had such guidance. Where guidance was in place, often Respondents noted that it was in the context of another co-operation agreement (for example, the EDPB's procedural guidance, as part of an MOU, or as part of the EU's Internal Market Information System).

4.3.1.2.Engaging in collective initiatives to support mutual assistance

The Recommendation sets out that Adherents should engage in collective initiatives to support mutual assistance, including by: designating a national contact point (at IV.B.19); sharing information on enforcement outcomes to improve collective understanding of how privacy law enforcement is conducted (at IV.B.20); and fostering the establishment of an informal network of PEAs (and other stakeholders) (at IV.B.21). The Global Privacy Enforcement Network (GPEN) was established in response to this call and is described in more detail in Box 4.

Box 4. The Global Privacy Enforcement Network (GPEN)

On 10 March 2010, representatives from several PEAs came together at a meeting hosted by the OECD and officially launched the Global Privacy Enforcement Network (GPEN). The *Action Plan*[29] which serves as the basis of the network stresses that "it is important that government authorities charged with enforcing domestic privacy laws strengthen their understanding of different privacy enforcement regimes as well as their capacities for cross-border co-operation." (GPEN, 2013[29])

GPEN is an informal network, open to public authorities that are responsible for enforcing laws or regulations (the enforcement of which has the effect of protecting personal data), and that have powers to conduct investigations or pursue enforcement proceedings. The network had expanded significantly from the original 11 member authorities to 71 authorities of 52 jurisdictions from different geographic regions of the world by 2021.

As specified in its *Action Plan*, GPEN focuses on the practical aspects of privacy enforcement co-operation. In line with the Recommendation, its mission is to promote co-operation by exchanging information about relevant issues, trends and experiences; encouraging training opportunities; sharing enforcement know-how, expertise and good practice;[30] promoting dialogue with organisations who have a role in privacy enforcement; creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral co-operation; and undertaking or supporting specific activities. Participants are required to designate a point of contact within their authority to facilitate GPEN-related communications and enforcement co-operation dialogue.[31]

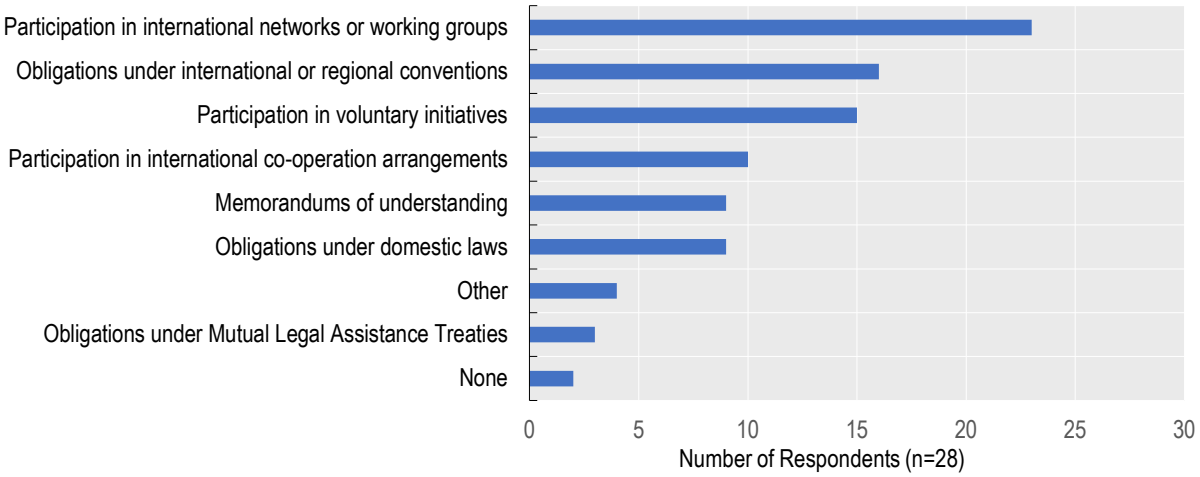
In order to provide further practical support to cross-border co-operation, the OECD established a website, www.privacyenforcement.net, which is now hosted by Canada OPC and used/maintained by GPEN in order to support privacy enforcement co-operation between its members.

GPEN's activities include regular conference calls and meetings to discuss enforcement issues, trends, and experiences; annual workshops for sharing effective investigative techniques and enforcement strategies; facilitation of coordination of investigations involving multiple authorities; a joint compliance activity known as the "GPEN Sweep" conducted each year to review organisations' privacy practices (relating to a particular topic); coordination with other enforcement networks with complementary mandates; and other *ad hoc* activities.

Source: (GPEN, n.d.[30])

In addition to GPEN, Respondents routinely participate in various international fora and initiatives to advance co-operation in the cross-border enforcement of privacy laws. These range from participation in networks, to voluntary initiatives, to obligations under mutual legal assistance treaties. Figure 8 sets out the different international arrangements and mechanisms that countries employ.

Figure 8. International arrangements or mechanisms employed



Note: Respondents were asked to choose all that apply.
Source: 2021 questionnaire (D1)

A number of examples of the different arrangements and mechanisms engaged in were provided in response to the 2021 questionnaire. Of note, a number of Respondents pointed to the initiatives of the Global Privacy Assembly (GPA),[32] which recognises enforcement co-operation as one of its three key pillars in its Policy Strategy, and has a number of initiatives designed to further enforcement co-operation. Notably, as a result of this strategy, the GPA's International Enforcement Cooperation Working Group (IEWG) was permanently established with a mandate to foster co-operation in practice on live and pressing issues, which it facilitates via regular closed enforcement sessions.[33]

The GPA's Global Cross Border Enforcement Cooperation Arrangement seeks to foster compliance with data protection laws, encourages co-operation between PEAs, and coordinates the PEA enforcement activities.[34] It sets out commitments (on behalf of the participants[35]) regarding international cross-border privacy enforcement co-operation, particularly on reciprocity, confidentiality, data protection, and coordination (GPA, 2017[31]).

Additionally, the GPA's "Enforcement Cooperation Handbook", provides practical guidance to PEAs (GPA, 2021[32]), and its "Enforcement Cooperation Repository" is a platform through which PEAs can share (publicly available) information, which may be useful for enforcement co-operation (GPA[33]). The IEWG's "Transnational Case Map" provides a visual representation of how actions taken in one country can affect another, and seeks to identify all cases that IEWG members have had with transnational implications between 2020 and 2022 (GPA, 2022[34]) (GPA, n.d.[35]).

At the regional level, Respondents from the EU/EEA pointed to the work of the EDPB, which was established to ensure regulatory co-operation and the consistent application of data protection rules throughout the EU/EEA.[36] Additionally, it was noted that the GDPR creates a general duty of co-operation between supervisory authorities of the EU/EEA Member States.[37] Of note, the GDPR introduced the so-called "one-stop-shop mechanism", which ensures co-operation between data protection authorities of the EU/EEA countries in the case of cross-border processing.[38] Also within Europe, the Council of Europe's Convention 108 Committee monitors the implementation of Convention 108+.[39] This Convention[40] requires co-operation between the supervisory authorities[41] of different parties including through mutual assistance, information sharing and co-ordinated investigations.

Another regional example is APEC's Cross-border Privacy Enforcement Arrangement (CPEA), which seeks to establish conditions to allow effective information sharing, referrals and co-ordination (similar to

GPA's Global Cross Border Enforcement Cooperation Arrangement). Australia and Canada have indicated that the joint investigation of the Ashley Madison Case cited above in Box 3, was made possible through the CPEA (OECD, 2020[36]).

One notable example of a (regional) practical mechanism is the EU's Internal Market Information System (IMI).[42] The IMI is a secure, multilingual online tool that facilitates the exchange of information between public authorities involved in the implementation of EU law (European Commission[37]). In the context of privacy enforcement, EU/EEA supervisory authorities (i.e. PEAs) use the IMI to find national contact points of other supervisory authorities and exchange information. Cases with a cross-border component are registered in a central database (called IMI Case register), which facilitates the sharing of enforcement outcomes [43] and/or information on follow-up of cases. The IMI includes procedural guidance and explanations on which information should be included when making a request through the IMI.

Overall, Respondents indicated that they participate in a wide range of different international arrangements and mechanisms. These are set out in Table 1.[44]

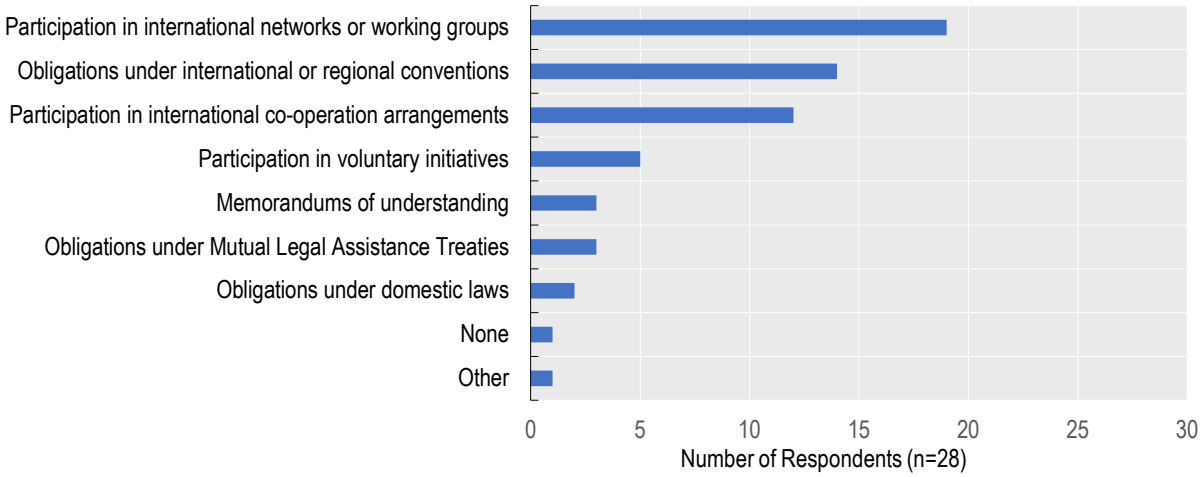
Table 1. Examples of international arrangements or mechanisms

International networks or working groups	Global Privacy Enforcement Network (GPEN) Global Privacy Assembly (GPA) - International Enforcement Cooperation Working Group (IEWG), Digital Citizens and Consumers Working Group (DCCWG) Working groups of Convention 108 of the Council of Europe European Data Protection Board (EDPB) APEC Cross-border Privacy Enforcement Arrangement (CPEA) Asia Pacific Privacy Authorities (APPA) Forum Ibero-American Data Protection Network (RIPD) Unsolicited Communications Enforcement Network (UCENet) Joint Cyber Security Working Group (US/Philippines)
International co-operation arrangements	GPA's Global Cross Border Enforcement Cooperation Arrangement (CBECA) APEC Cross-border Privacy Enforcement Arrangement (CPEA)
Obligations under international or regional conventions, or mutual legal assistance treaties (MLATs)	Convention 108 GDPR Art.60 co-operation procedure USMCA Agreement (US/Mexico/Canada) US/Canada Cooperation Agreement
Memorandum of understanding (MOU's)	MOU's between the PEAs of US/UK, US/Ireland, US/the Netherlands, Jersey/Guernsey, Jersey/Dubai, Philippines/UK, Philippines/Singapore, and various MOUs between Canada and other jurisdictions (e.g. Canada/UK, Canada/Uruguay, Canada/Germany, Canada/Dubai)
Voluntary initiatives	Initiatives under GPEN, GPA, APEC CPEA, APPA, RIPD Sweeps Joint letters
Other	Administrative arrangements Conferences such as G7 roundtables

Source: 2021 questionnaire (D1, D2)

With regards to the effectiveness of international arrangements or mechanisms, most Respondents considered participation in international networks or working groups to be the most effective tool for cross-border enforcement co-operation, followed by obligations under international or regional conventions, and participation in international co-operation arrangements (see Figure 9).

Figure 9. International arrangements or mechanisms considered most effective



Note: Respondents were asked to choose up to three answers.
Source: 2021 questionnaire (D2)

In particular, some Respondents emphasised that international networks are particularly effective for fostering communication, building trust, co-ordinating cases, sharing information, and discussing legal and technical issues. The success of GPEN was highlighted, as was the work of the GPA's IEWG.

Others noted that the approaches of international co-operation arrangements and/or obligations under international/regional conventions can be effective, in terms of enabling specific timing and clearer commitments for enforcement. Other forms of co-operation considered effective include joint letters and coordinated theme-based studies (e.g. GPEN Sweeps), as they can bring combined international interest and pressure into play, resulting in voluntary compliance actions by organisations.

Insights from the Expert Roundtable

Speakers at the Roundtable discussed the different fora and networks that exist and provided further context regarding their varied strengths and complementarities. These fora and networks can be divided into those that are at working level and dedicated to providing support and facilitating connections between front line staff (i.e. GPEN, and some working groups at GPA and G7 level); those that operate on a high level and issue policy recommendations and advice (i.e. GPA, G7); and those that are more general networks not dedicated to enforcement co-operation, but that nonetheless provide an opportunity to build relationships on this issue (i.e. ASEAN, APEC).

GPEN was described as having a heavy emphasis on inclusiveness, with any agency with responsibility for enforcing privacy able to participate (GPEN, 2013[29]). The fact that cooperating with GPEN is not binding, nor is it exclusive of cooperating with other networks facilitate this inclusiveness. GPEN's working level focus was highlighted as a key factor underlying its success. Participants do not need to issue public opinions, positions papers, or recommendations on privacy policy. This allows the group to operate on a very practical level, allows for speed and agility in that there is no need to make challenging decisions, and means that its work does not overlap with the work of other networks and organisations.

It was noted that GPEN is very open to new agencies joining and this is facilitated through the simple joining process.[45] The online nature of the network eases the burden of participation, and the well-developed resources (e.g. sweep kits) allow newer and smaller authorities to engage in (and learn from) activities that they may not otherwise have the resources to develop on their own. GPEN's staff level

engagement was emphasised, in particular its focus on allowing exchange on day-to-day work. In this way, it was noted, GPEN fills a niche role and is complementary to other networks.

The GPA's IEWG has around 35 members from all the regions of the globe. This provides the group with diversity in terms of language and legal culture as well as regarding the size and experience of the PEAs represented. The IEWG welcomes observers from any organisation that works in the field of data protection (e.g. the OECD). To encourage new members joining (or those with limited resources), the IEWG allows participants to choose the level of resources they wish to commit as well as the extent they wish to participate (e.g. listening to meetings or actively contributing). An objective in the IEWG's Action Plan is to ease the burden on smaller PEAs of participating in multiple networks through better coordination with other networks of regulators as well as to find ways to support and amplify the work of these other groups.

The IEWG takes a practical stance and seeks to produce tangible outputs (e.g. the Enforcement Cooperation Handbook, Enforcement Cooperation Repository and Transnational Case Map mentioned above). One tool for producing these outputs includes "safe space meetings" (also known as "closed enforcement sessions") where participants can discuss a strategically important topic or case, providing an opportunity for discussion in a free and open manner and encouraging other PEAs to consider how they might address a similar or the same issue.

Unlike GPEN, the IEWG may facilitate the publication of documents (such as guidance and awareness raising materials) as well as public statements. For example, publishing open letters in response to concerns that certain data controllers are not being mindful of their obligations under privacy and data protection law. On this, it was noted that despite member's varied jurisdictions and differing legal frameworks it remains possible to find common ground to address key data protection issues.

The G7's Enforcement Cooperation Working Group,[46] is a working level subgroup of the G7's Roundtable of data protection and privacy authorities.[47] This subgroup engages in discussions at the expert level and has considered challenges related to facilitating enforcement co-operation across-borders, such as information sharing best practices, operationalising MOUs, domestic deterrent measures and enhancing co-operation with consumer and competition networks.

In the Asia-Pacific region, it was noted that there is a broad spectrum of countries at different levels of data protection maturity, and while a few groupings of regulators exist there are no specific fora focussed on enforcement co-operation. For example, the Asia Pacific Privacy Authorities forum (APPA) does not hold meetings specifically on enforcement co-operation. It however will discuss enforcement issues (e.g. information sharing, case studies) on an *ad hoc* basis at its regular meetings. The Association of Southeast Asian Nations (ASEAN) has started a data protection and privacy forum, but again this is not focussed on enforcement issues and rather provides a platform for policy makers and regulators from ASEAN Member States to discuss privacy and data protection issues.

In light of the lack of a dedicated fora in the region, it was noted that authorities in the region are likely to rely on bi-lateral enforcement co-operation. This was described in three tiers. The first level is information sharing, particularly the sharing of information which is no longer confidential (e.g. detailed grounds for a decision). The second tier occurs when an agreement is in place making it possible to share (potentially confidential) information regarding incomplete investigations, allowing investigations in two jurisdictions to continue apace. The last tier involves mutual assistance, whereby one authority may record evidence on behalf of another. The speaker noted that in practice, they had only observed the first tier of co-operation occurring in the region.

The Roundtable also heard a North and Latin American perspective. Like the Asia-Pacific region no specific groups exist focussed solely on enforcement co-operation, however it is a feature of different agreements and networks in the region. For example, the United States, Mexico, Canada trade agreement (USMCA) recognises obligations related to co-operation mechanisms on a regional level (e.g. sharing information and experiences, promoting and developing mechanisms for cross-border co-operation, and actively

participating in regional and multilateral fora). The Ibero-American Data Protection Network was highlighted as an example of a coordinated regional mechanism. This network recognises co-operation between Member States as a basic principle, for example through information sharing, education and training, and the exchange of experiences (e.g. on regulatory proposals or the actual exercise of statutory powers). One tool to foster this co-operation is the network's database of relevant decisions in the field of data protection and privacy (RIPD, n.d.[38]).[48]

A number of challenges and barriers to improving co-operation in this region were identified. For example, language and resource gaps as well as complications regarding the extra-territorial application of laws. To address language barriers, it was noted that there has been an interest in increasing regional and linguistic diversity in groups such as the IEWG, and for this purpose the importance of inclusive actions (e.g. translating guidelines and products) was stressed.

4.3.1.3.Co-operating with other authorities and stakeholders (Section IV.C)

The Recommendation recognises that, "other entities, such as criminal law enforcement authorities, privacy officers in public and private organisations and private sector oversight groups, also play an important role in the effective protection of privacy across borders" and encourages appropriate co-operation with other relevant bodies and regulatory authorities (at II.3).

However, since 2007, the number of different bodies and agencies involved in assuring the effective enforcement of privacy laws both in domestic and cross-border contexts has expanded significantly. Indeed, the finding in the 2021 Report on the implementation of the OECD Privacy Guidelines that there is a need for stronger co-operation between different regulatory agencies helped prompt this review of the implementation of the Recommendation (OECD, 2021[3]).

This issue has also been recognised and discussed in various international fora. For example, the Digital Citizens and Consumers Working Group of the GPA has been exploring intersections between privacy and other regulatory spheres (such as competition and consumer protection bodies). The group has engaged in various activities, including a series of studies on cross-regulatory intersection (GPA, 2020[39]). Additionally, PEAs from the G7 member countries highlighted, at their roundtable in 2021, the need for greater collaboration between data protection and privacy authorities and competition regulators (G7, 2021[40]).

The Recommendation does not directly address cross-regulatory co-operation (other than co-operation with criminal law enforcement authorities), and the 2021 questionnaire explored the extent to which the intersection with other regulatory bodies impacts the cross-border enforcement of privacy laws. It also considered how co-operation between different disciplines can be enhanced to better protect privacy, as well as what opportunities this kind of collaboration can present.

Just over half of the Respondents (15 out of 28) indicated that they have experienced cross-regulatory interactions in a cross-border context. However, only three indicated that they interact with criminal law enforcement bodies,[49] and for the most part Respondents noted that their interactions are generally with regulators responsible for consumer protection, competition/antitrust, cybersecurity, telecommunication, financial regulation, public health and transportation/infrastructure. It should be noted that the recognition of a growing need for cross-regulatory co-operation is not unique to the privacy enforcement sphere. For example, OECD work on communication regulation has highlighted that regulatory co-operation is a key element of regulatory quality, and that capacity to engage in such co-operation will be increasingly important for communication regulators, both at the domestic, cross-sectoral and international level (OECD, 2022[41]).

Co-operation with other regulators is often necessary when a case involves broad policy areas, when data protection obligations are provided by sectoral laws and enforced by sectoral regulators, when developing legislative or administrative measures in relatively new policy areas (e.g. data portability), and/or where

PEAs are consulted for regulatory opinions which may concern privacy and data protection. A number of different practical examples are outlined in Box 5.

Box 5. Examples of cross-regulatory intersection

Australia

The Office of Australian Information Commissioner (OAIC) has been working with the Australian Competition and Consumer Commission (ACCC) on a range of projects. One example is the development of the "Consumer Data Right" (a data portability reform) in a variety of sectors (OAIC, 2020[42]) (OECD, 2021[19]). Another example is the OAIC's engagement in the ACCC's Digital Platforms Inquiry, which examined the impact of digital platforms on competition in the media and advertising services markets. In support of the ACCC's recommendations for reform of Australia's privacy framework made in the Digital Platforms Inquiry Final Report, the OAIC provided comments to the Report from the viewpoint of a PEA acting internationally, to ensure the interoperability of Australia's data protection laws globally and optimal regulatory outcomes in the public interest. The OAIC highlighted a need for broader review of privacy law, given recent domestic privacy reforms (e.g. Consumer Data Right) and international developments such as the GDPR and the California Consumer Privacy Act. (OAIC, 2019[43])

Furthermore, in 2022, the ACCC, Australian Media and Communications Authority (ACMA), eSafety Commissioner and OAIC established the Digital Platform Regulators Forum (DP-Reg). The DP-Reg provides a forum for the different bodies to share information about, and collaborate on, cross-cutting issues and activities relating to the regulation of digital platforms, including consideration of how competition, consumer protection, privacy, online safety and data issues intersect. (ACMA, 2022[44])

France

The French data protection authority (CNIL) and the Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF) (the French authority responsible for consumer protection) have collaborated on the processing of personal data by social networks, deceptive marketing practices related to compliance with the GDPR and the use of personal data in electronic commerce. (CNIL, 2019[45])

Luxembourg

Luxembourg's data protection authority (CNPD) has collaborated with foreign consumer protection authorities competent for matters under the ePrivacy Directive (Directive 2002/58/EC) through the Consumer Protection Cooperation Network, a network of the EU's consumer protection authorities.

United Kingdom

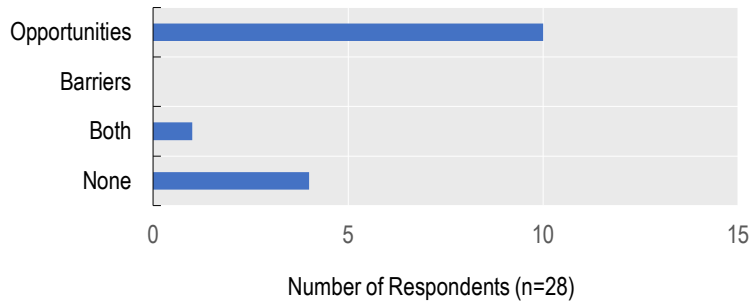
Given the unique challenges posed by regulation of online platforms, in July 2020 the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO) and the Office of Communications (Ofcom) established the Digital Regulation Cooperation Forum (DRCF) to ensure a greater level of co-operation. The Financial Conduct Authority (FCA) joined the DRCF as a full member in April 2021.

The ICO regularly engages with these regulators on a number of matters in relation to data protection and areas of mutual interest. For example, the FCA-ICO and CMA-ICO Memoranda of Understanding sets out a range of ways to co-operate, notably through regular communications and consultations, which may include sharing information about investigations, relevant action and relevant information regarding data breaches, fraud and criminal activity (ICO and FCA, 2019[46]) (ICO and CMA, 2021[47]).

A recent joint statement between the CMA and the ICO set out their shared views on the interactions and next steps, highlighting the synergies and potential tensions between different policy areas (CMA and ICO, 2021[48]).

The 2021 questionnaire revealed that among those PEAs who have experienced cross-regulatory interactions, many see opportunities in cross-regulatory co-operation (see Figure 10).

Figure 10. Opportunities and barriers of cross-regulatory interactions



Source: 2021 questionnaire (E1b)

Specifically, Respondents noted that cross-regulatory co-operation creates opportunities to exchange information on the different processes of the different agencies, to understand the scope of different mandates, to share expertise, and to broaden understanding of enforcement issues by bringing in different investigative perspectives, resulting in coordinated and aligned enforcement outcomes.

Insights from the Expert Roundtable

Speakers at the Expert Roundtable emphasised the multi-dimensional policy challenges that the digital world presents, and in particular the centrality of privacy and data protection in many (if not all) of these challenges. For example, digital platforms play an essential role in controlling data and can be accused of using market dominance to both limit competition and erode privacy; or, certain practices may create both consumer protection and privacy challenges. A proliferation of privacy related challenges is rendering cross regulatory co-operation essential for PEAs, and there is an emerging need for multiple disciplines to work together, rather than just bi-lateral collaboration (e.g. consumer, competition *and* privacy). It was highlighted that cross-regulatory co-operation between privacy and other policy areas could provide new and valuable avenues for holistically addressing problematic behaviours.

Speakers noted the importance of emphasising complementarities, and that often the different regulators are considering the same issues, albeit through a different lens (i.e. both privacy and competition regulators share an emphasis on promoting consumer choice and trust in markets). From a regulator's perspective, one speaker stressed that all regulators are established with the common goal of promoting the public interest. Regulators do this through i) addressing harms (both risks and actual harm); and ii) promoting behaviours that create good outcomes. Whilst different regulators may approach the same issues through different perspectives, they all have in common the fact that that they are facing difficult public policy questions that fall outside of their traditional remits. This is particularly the case when considering the issues that digital markets pose, given that those markets (and the firms within them) are fuelled by personal data.

At the same time, there is potential for tension between the different disciplines. For example, competition policy may prioritise data access and flows to promote online competition (regardless of whether the data is personal or not), while privacy lawmakers are more likely to be concerned with ensuring trust in data

flows to preserve user privacy. Companies themselves when faced with alleged violations of competition law may seek to rely on obligations to protect end-user privacy as a defence.

Not only is co-operation important to address the complex issues that are emerging, but it is also increasingly expected by both the public and the lawmakers representing them. For example, the UK's Information Commissioners Office, "ICO25 Strategic Plan" recognises the strategic importance of cross-regulatory co-operation and identifies practical actions for achieving this (e.g. MOUs that set out information sharing powers, and legal basis for collaboration) (ICO, n.d.[49]). Other tools include joint statements and setting out shared policy positions.

Fostering cross-regulatory co-operation requires fostering relationships, and one speaker stressed that "co-operation starts with an email" highlighting that, while legislation and information sharing arrangements may provide the ability for different authorities to cooperate, it is the interagency and interpersonal relationships, which (when nurtured) can provide the trust, organisational knowledge, and open lines of communications necessary to make co-operation a reality. Suggested methods for fostering such relationships included developing internal protocols and providing staff training that can develop awareness of the benefits of, and potential options for, enforcement co-operation, as well as deepening the understanding of counterpart legal and regulatory frameworks. The OECD was noted as having a clear role in facilitating dialogue and fostering informal relationships.

Lastly, the Expert Roundtable heard an example of a legal action that concurrently dealt with competition and privacy law issues. This case is expanded on in Box 6 below.

Box 6. Enforcement action of the Germany's Federal Cartel Office against Meta Platforms

In 2019, the Bundeskartellamt (Federal Cartel Office, Germany), imposed restrictions on Facebook (now Meta Platforms) regarding the processing of user data, and more specifically on combining user data from different sources. This finding involved consideration of provisions under the GDPR, and the Court of Justice of the European Union (CJEU) was asked to decide whether national competition authorities can assess the compliance of data processing with the GDPR as a standard for examining exploitative abuse under competition law.

Background

Facebook uses different data sources from its different social networks and messaging services, as well as from third party websites. The Bundeskartellamt found that Facebook has a dominant position in the market for social networks and abuses this dominant position by combining data from these different sources. In response, the Bundeskartellamt imposed far reaching restrictions on Facebook's processing of user data, prohibiting Facebook from assigning user data from WhatsApp, Instagram and third-party websites to the Facebook user account without voluntary consent.

In reaching this decision, the Bundeskartellamt took GDPR principles into account, and dedicated a third of its decision to data protection issues. As a result, the authority heard critique that it had acted as a data protection authority. However, it was argued that it is the Bundeskartellamt's core task to assess dominance, and in this case the dominance was data driven. As such, the Bundeskartellamt had to assess how such data is gathered and processed; and to make that legal assessment, it was necessary to take all relevant legal parameters into account. The Bundeskartellamt determined it was most appropriate to apply the existing legal parameter (i.e. GDPR principles). To do this, the Bundeskartellamt worked in close co-operation with the German and Irish data protection authorities.

Meta Platforms appealed the decision of the Bundeskartellamt to the Higher Regional Court of Düsseldorf, which subsequently requested a preliminary ruling.

Decision of the Court of Justice of the European Union (CJEU)

In July 2023, the CJEU delivered a ruling in the case. It stated that a competition authority may, in the context of examining whether or not an organisation abused their dominant position, also consider whether the organisation's conduct complies with rules other than those relating to competition law – including those prescribed by the GDPR. In such circumstances, a competition authority may only assess compliance with the GDPR for the purpose of establishing whether there has been an abuse of a dominant position. A competition authority cannot replace the supervisory authorities established under the GDPR.

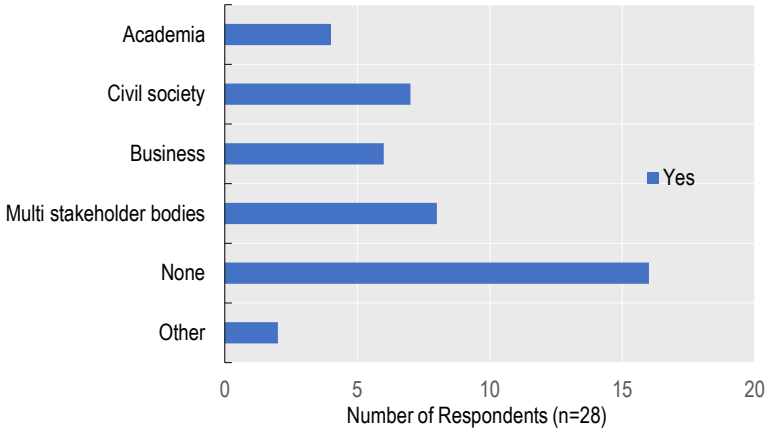
The CJEU stated that in making such an assessment, and in order to ensure consistent application of the GDPR, competition authorities should consult and co-operate with the relevant privacy authorities. Should a competition authority decide that it is necessary to assess whether or not an organisation's conduct is consistent with the GDPR, it must ascertain whether or not that conduct (or similar conduct) has already been the subject of a decision by either the privacy authority or the Court. If so, the competition authority cannot depart from the previous decision, although it may make its own assessment from the point of view of the application of competition law.

Source: (Court of Justice of the European Union, 2023[50])

The Recommendation also encourages engagement with "civil society and business on their respective roles in facilitating cross-border enforcement of Laws Protecting Privacy, and in particular in helping raise awareness among individuals on how to submit complaints and obtain remedies, with special attention to the cross-border context" (at IV.C.22.c).

With respect to this provision, responses to the 2021 questionnaire indicate that Respondents rarely co-operate with different stakeholders specifically for the purpose of furthering cross-border enforcement co-operation (see Figure 11).

Figure 11. Engagement with stakeholders in facilitating cross-border enforcement co-operation



Source: 2021 questionnaire (C1)

When they do engage, however, various forms of co-operation exist. This includes through engagement with existing institutional frameworks (e.g. business advisory services within PEAs); with various international working groups (e.g. GPA); through conferences; through outreach and educational

programmes; through the provision of information directed at certain stakeholders;[50] and through funding independent privacy research and public education initiatives.

One Respondent in its feedback[51] considered that this part of the Recommendation may need some further examination. It was noted that while it may be necessary for PEAs to collaborate with non-regulatory (or non-law enforcement) partners to fulfil their mandate in general, the need to do this for ensuring cross-border co-operation in enforcing privacy laws is less clear and this emphasis in the Recommendation may need to be re-examined.

4.3.2. International co-operation – Brief conclusions

The responses to the 2021 questionnaire indicate that Respondents have taken a large number of actions to ensure that they can co-operate with one another in the cross-border enforcement of privacy laws. Respondents routinely participate in various international fora and networks that aim to further this goal. Respondents appear keen to harness the possibilities of joint or parallel investigations, and those provided by co-operating with other regulatory bodies, and they see opportunities not only in formal and legal aspects of cross-border enforcement co-operation, but also in less formal types of co-operation.

Whilst these are positive aspects of the review, they may still warrant further action. For example it may be beneficial for the Recommendation to recognise broader aspects of enforcement co-operation. This could help encourage less experienced, or fewer resourced PEAs, be more engaged in actual enforcement co-operation initiatives by lowering the barrier of entry for such collaborative actions. In practice, insights from the Roundtable indicate that certain fora are taking steps to ensure broad and diverse participation in their networks (i.e. low barrier to entry, option to passively engage in groups), although a need for further action in regard to accommodating language differences was noted. Gaps in dedicated enforcement co-operation networks at the regional level was also highlighted. Given that both the questionnaire and the workshop highlighted the crucial role these networks play, further consideration of ways in which to ensure their sustainability may be warranted.

Cross-border enforcement co-operation through international arrangements and mechanisms has extended well beyond what the Recommendation envisages. International networks provide a variety of useful tools and platforms. Insights from the Roundtable demonstrate that different networks seek to complement each other by fulfilling different roles. For example, while both the GPEN and the GPA's IEWG take a practical stance and seek to engage working level members GPEN focusses on exchanges regarding the day-to-day work of front-line staff, whereas the IEWG uses its engagement with members to develop concrete tools and outputs. Nonetheless, some countries in response to the work plan noted that it may be useful to consider how these networks could best coordinate, and it may be prudent for any future work to further consider this.

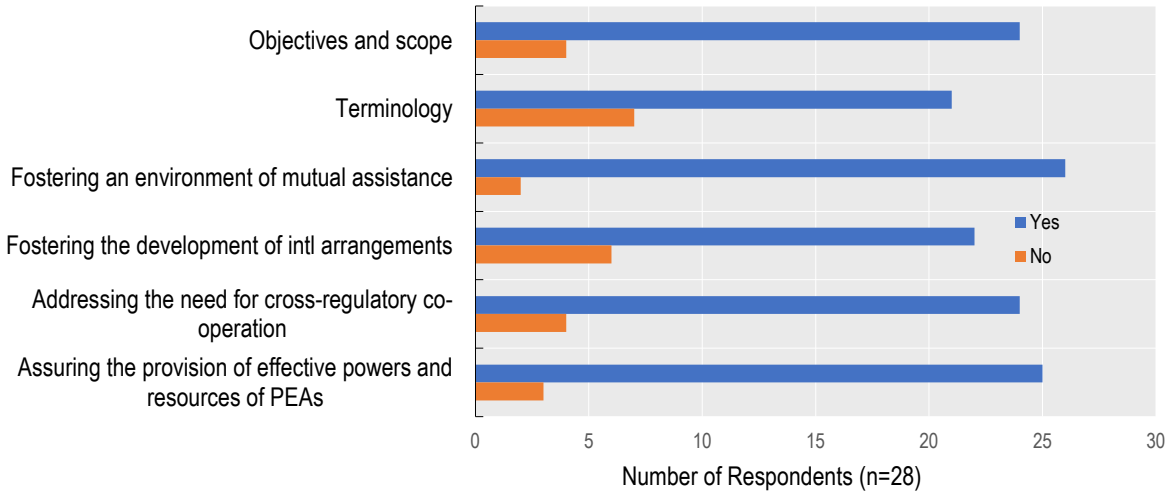
Further, it would be useful to consider how to better improve engagement with stakeholders. This Report highlights that Respondents rarely engage with other stakeholders (as was envisaged in Part IV.C of the Recommendation) and there is scope to investigate whether or not this kind of co-operation should be improved.

Lastly, the reality of cross-regulatory co-operation today is not currently reflected within the Recommendation. It is evident both from the responses to the 2021 questionnaire and the discussions at the Roundtable that there is an emerging need for multiple disciplines to work together, and that fostering co-operation between regulators from different sectors is becoming essential for PEAs –not just in seeking to enforce privacy laws, but also in the development and administration of data protection laws generally.

4.4. Overall relevance of the Recommendation

The 2021 questionnaire asked whether or not the Recommendation remained relevant and instrumental in enhancing cross-border co-operation, as well as whether or not it had kept pace with advancements since 2007 (across a number of different areas). As can be seen from Figure 12, the majority of Respondents consider that the Recommendation remains relevant in each of the different areas asked about.

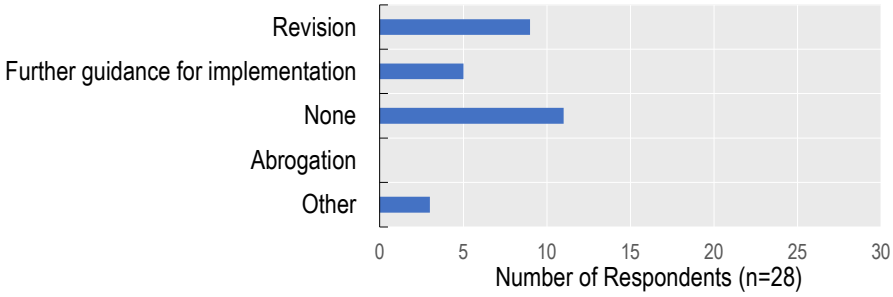
Figure 12. The majority of Respondents consider the Recommendation remains relevant



Source: 2021 questionnaire (H1)

Nonetheless, 14 out of 28 Respondents considered that the Recommendation would benefit from either further implementation guidance (5 Respondents), or revision (9 Respondents) (see Figure 13).

Figure 13. Necessary actions for the Recommendation



Source: 2021 questionnaire (H2)

In explaining their above responses, one Respondent noted that further guidance would be useful in terms of providing context to how co-operation can work across different regulatory areas, whether trade deals could be used to reinforce and support co-operation, as well as to what extent co-operation mechanisms are needed to support laws with extraterritorial scope. Another noted that further guidance could include the development of practical implementation tools and templates. One Respondent commented that the Recommendation should include stronger language and/or more concrete recommendations regarding fostering the development of international arrangements. Another noted that this is essential as the lack of

such mechanisms may pose a barrier to effective cross-border co-operation, and their enhancement may mean that the potential interplay with other regulatory areas could be better addressed.

Some Respondents who suggested a revision pointed to the fact that the Recommendation pre-dates significant privacy law reform (i.e. the GDPR) and that it may be worth revisiting the Recommendation to ensure that it appropriately complements the current legislative landscape. Another noted that it should be brought up to date with today's enforcement reality. One Respondent (who chose 'other' to the above question), noted that the Recommendation should be updated to reflect the increase in cross-border data flows and to explicitly recognise the value of co-operation as a matter of public interest and in promoting trust in such data flows.

5. Conclusions

Cross border co-operation in the enforcement of privacy laws is considered even more of an imperative today, than it was when the Recommendation was first adopted in 2007. The enforcement practices of PEAs show that, due to continually advancing technologies and the centrality of data to the business models of companies operating in multiple jurisdictions, cross-border co-operation should be normalised as a necessity in today's digital economy, not only when there has been a serious violations of privacy laws.

This Report has observed that while the 2007 Recommendation remains relevant at the level of principle, and Adherents to it have taken significant steps towards its implementation, a number of gaps challenges and opportunities exist that warrant further consideration.

At the domestic level, while legal frameworks are in place to enable co-operation, this does not always translate to co-operation in practice. Challenges persist in regard to the sharing of information, and countries may lack the jurisdiction or competence to commence actions. The issue of recognising and enforcing orders in foreign jurisdictions was pointed to as a clear challenge which can deter PEAs from commencing investigations, and it was highlighted that there may be scope for the OECD to facilitate joint work in this regard. Additionally, a lack of record keeping regarding the number of cross-border cases renders the scale of the issue unclear.

Internationally, it is clear that there is strong engagement in networks which foster international co-operation, and that soft co-operation (both through formal networks and informally) is a vital tool that can help overcome practical barriers to enforcement in cross-border cases. Nonetheless, there is scope to better understand the factors underlying a country's decision to take enforcement action (e.g. human and financial resources, ability to enforce compliance), and that the OECD could assist in developing relevant metrics, coordinated horizon scanning and in identifying issues of common concern.

There is an emerging need for multiple disciplines to work together to address the multi-dimensional policy challenges presented by digital transformation, and privacy and data protection is central to many of these challenges. As a result cross-regulatory co-operation, is essential for PEAs and this need should be better reflected in the Recommendation.

Given the findings in this report, the OECD proposes to undertake further work to either revise the Recommendation (including developing implementation guidance for any revised version) or by developing further implementation guidance for the Recommendation in its current form.

References

ACMA (2022), *Digital Platform Regulators Forum (DP-Reg)*, https://www.acma.gov.au/dp-reg-joint-public-statement. [44]

CMA and ICO (2021), "Competition and data protection in digital markets: a joint statement between the CMA and the ICO", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf. [48]

CNIL (2019), *La CNIL et la DGCCRF font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et de leurs données personnelles*, https://www.cnil.fr/fr/la-cnil-et-la-dgccrf-font-evoluer-leur-protocole-de-cooperation-pour-renforcer-la-protection-des. [45]

Court of Justice of the European Union (2023), *Judgment of the Court (Grand Chamber) of 4 July 2023 (request for a preliminary ruling from the Oberlandesgericht Düsseldorf – Germany) – Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd, Facebook*, https://curia.europa.eu/juris/document/document.jsf;jsessionid=334C2578FB69BFEF9F27281C002FD3D6?text=&docid=276478&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1856324. [50]

EDPB (2022), *Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries*, https://edpb.europa.eu/our-work-tools/our-documents/toolbox-essential-data-protection-safeguards-enforcement-cooperation_ga. [14]

EDPB (2021), "Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities", https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_en. [51]

EDPB (n.d.), *GDPR Cooperation and Enforcement*, https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement_en. [53]

European Commission (n.d.), *Internal Market Information System*, https://ec.europa.eu/internal_market/imi-net/index_en.htm. [37]

European Union (ed.) (2016), *European Union (n.d.), Regulation (EU) 2018/1807 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Direct*, https://eur-lex.europa.eu/eli/reg/2016/679/oj. [13]

FTC (2022), *International Reports by Federal Trade Commission: Cross Border*, https://public.tableau.com/app/profile/federal.trade.commission/viz/InternationalReports/Cross-Border. [52]

FTC (2016), *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information*, https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting. [28]

G7 (2021), "Roundtable of G7 Data Protection and Privacy Authorities 07-08 September 2021 - communiqué -", https://ico.org.uk/media/about-the-ico/documents/4018242/g7-attachment-202109.pdf. [40]

Gobierno de Mexico (2016), *Corpus Iuris Nacional e Internacional*, http://pot.diputados.gob.mx/Unidad-de-Transparencia/Datos-Personales-Archivo-y-Gestion-Documental/Corpus-Iuris-Nacional-e-Internacional. [54]

GPA (2022), *International Enforcement Working Group - Report July 2022*, https://globalprivacyassembly.org/wp-content/uploads/2022/11/International-Enforcement-Cooperation-Working-Group.pdf. [34]

GPA (2021), "An Enforcement Cooperation Handbook", https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf. [32]

GPA (2020), "Digital Citizen and Consumer Working Group Report – adopted October 2020", https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2g-Day-3-3_2h-Version-1_0-Digital-Citizen-and-Consumer-Working-Group-Report-Final.pdf. [39]

GPA (2017), "Global Cross Border Enforcement Cooperation Arrangement", http://globalprivacyassembly.org/wp-content/uploads/2018/12/version-17-gcbeca-2017-icdppc.docx. [31]

GPA (n.d.), "Enforcement Cooperation Repository", http://globalprivacyassembly.org/enforcement-cooperation-repository/. [33]

GPA (n.d.), *Transnational Case Map*, https://app.powerbi.com/view?r=eyJrIjoiZDI5Y2YyNmItNGQ4MS00NjRiLWE3MmYtM2RmYzgyYjhlMDU4IiwidCI6Ijk0NzhlZWMyLThkZjctNDk0OC04MGQzLTc0MGExNmUxZGNjYSJ9&pageName=ReportSection. [35]

GPEN (2013), *Action Plan for the Global Privacy Enforcement Network (GPEN)*, https://www.privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen. [29]

GPEN (n.d.), *Global Privacy Enforcement Network*, https://www.privacyenforcement.net/content/home-public. [30]

HCCH (2014), *Practical Handbook on the Operation of the 1996 Hague Child Protection Convention*, https://assets.hcch.net/docs/eca03d40-29c6-4cc4-ae52-edad337b6b86.pdf. [24]

HCCH (1996), *Convention on Jurisdiction, Applicable Law, Recognition, Enforcement and Co-operation in Respect of Parental Responsibilty and Measures for the Protection of Children*, https://assets.hcch.net/docs/f16ebd3d-f398-4891-bf47-110866e171d4.pdf. [23]

ICO (2018), "Investigation into the use of data analytics in political campaigns", https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf. [16]

ICO (n.d.), *ICO25 strategic plan*, https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/. [49]

ICO and CMA (2021), "Memorandum of Understanding between the Information Commissioner and the Competition and Markets Authority", https://ico.org.uk/media/about-the-ico/mou/2619798/ico-cma-mou-20210430.pdf. [47]

ICO and FCA (2019), "Memorandum of Understanding between the Information Commissioner and the Financial Conduct Authority", https://ico.org.uk/media/about-the-ico/documents/2614342/financial-conduct-authority-ico-mou.pdf. [46]

OAIC (2020), *ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right*, https://www.oaic.gov.au/consumer-data-right/compliance-and-enforcement-policy. [42]

OAIC (2019), "Digital Platforms Inquiry final report — submission to the Australian Government", https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-final-report-submission-to-the-australian-government. [43]

OAIC (2016), *Ashley Madison joint investigaiton*, https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/ashley-madison-joint-investigation. [26]

OECD (2022), "Communication regulators of the future", *OECD Digital Economy Papers*, No. 333, OECD Publishing, Paris, https://doi.org/10.1787/f02209e6-en. [41]

OECD (2022), *Draft Summary Record: Virtual Meetings of 5th Session of the Working Party on Data (internal document)*, https://one.oecd.org/document/DSTI/CDEP/DGP/M(2021)2/en/pdf. [7]

OECD (2022), *Expert Roundtable on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (internal document)*, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)6/en/pdf. [8]

OECD (2022), *OECD inventory of international co-operation agreements between competition agencies (MoUs)*, https://www.oecd.org/daf/competition/inventory-competition-agency-mous.htm. [22]

OECD (2022), *OECD inventory of international co-operation agreements on competition*, https://www.oecd.org/daf/competition/inventory-competition-agreements.htm. [21]

OECD (2021), *Draft Summary Record: Virtual Meetings of 4th Session of the Working Party on Data Governance and Privacy (DGP) (internal document)*, https://one.oecd.org/document/DSTI/CDEP/DGP/M(2021)1/en/pdf. [5]

OECD (2021), "Implementation toolkit on legislative actions for consumer protection enforcement co-operation", *OECD Digital Economy Papers*, No. 310, OECD Publishing, Paris, https://dx.doi.org/10.1787/eddcdc57-en. [17]

OECD (2021), "Promoting comparability in personal data breach notification reporting", *OECD Digital Economy Papers*, Vol. 322, https://doi.org/10.1787/88f79eb0-en. [15]

OECD (2021), *Provisions on negative comity*, https://www.oecd.org/daf/competition/competition- [19]

inventory-provisions-negative-comity.pdf.

OECD (2021), *Provisions on positive comity*, https://www.oecd.org/daf/competition/competition-inventory-provisions-positive-comity.pdf. [20]

OECD (2021), "Report on the Implementation of the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", https://one.oecd.org/document/C(2021)42/en/pdf. [3]

OECD (2021), *Work Plan for the Review of the Recommendation (internal document)*, https://one.oecd.org/document/DSTI/CDEP/DGP(2021)8/en/pdf. [6]

OECD (2020), "Review of the implementation of the Privacy Guidelines: summary of the expert consultation on "Privacy and Personal Data Protection: Addressing Emerging Enforcement Challenges" (internal document)", https://one.oecd.org/document/DSTI/CDEP/DGP/M(2020)2/en/pdf. [36]

OECD (2016), *Recommendation of the Council on Consumer Protection in E-commerce*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422. [59]

OECD (2016), *Standard setting: Review of OECD legal instruments (internal document)*, https://one.oecd.org/document/DSTI/CDEP(2016)8/en/pdf. [55]

OECD (2014), *Recommendation of the Council Concerning International Cooperation on Competition Investigations and Proceedings*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0408. [18]

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [4]

OECD (2013), *The OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [10]

OECD (2011), *Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, http://dx.doi.org/10.1787/5kgdpm9wg9xs-en. [2]

OECD (2011), *Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, OECD Publishing, Paris, http://dx.doi.org/10.1787/5kg2b7l7pljk-en. [11]

OECD (2007), *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, https://www.oecd.org/sti/ieconomy/38770483.pdf. [1]

OECD (2006), *Report on the Cross Border Enforcement of Privacy Laws*, https://www.oecd.org/sti/ieconomy/37558845.pdf. [12]

OECD (2003), *Privacy Online: OECD Guidance on Policy and Practice*, https://doi.org/10.1787/9789264101630-en. [57]

OECD (2003), *Recommendation of the Council concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0317. [58]

OECD (1998), *Ministerial Declaration on the Protection of Privacy on Global Networks*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0301. [56]

OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 Version)*, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part5. [9]

OPC (2016), *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*, https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/. [27]

RIPD (n.d.), *Guías elaboradas por los países de la RIPD*, https://www.redipd.org/en/node/310. [38]

UNCITRAL (2015), *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/new-york-convention-e.pdf. [25]

Endnotes

[1] The Recommendation was developed on the proposal on the proposal of the Committee for Information, Computer and Communications Policy (now the Committee on Digital Economy Policy, CDEP).

[2] To date the Recommendation has no non-Member Adherents.

[3] The 2011 Report on implementation of the Recommendation arose out of a scheduled process in line with an instruction in the Recommendation. Namely, the Recommendation instructed the Committee for Information, Computer and Communications Policy (now the CDEP) to "exchange information on progress and experiences in implementing the principles, with a view to reporting back to Council within three years and thereafter as appropriate" (OECD, 2007[1]).

[4] Beginning in late 2018, in line with its 2016 Standard-setting Action Plan (OECD, 2016[55]), the CDEP conducted a comprehensive review of the implementation of the Privacy Guidelines. This review was informed by consultations with an ad-hoc group of over 60 privacy experts, the responses of 31 countries (28 Adherents to the Privacy Guidelines and 3 non-Adherents) to a questionnaire about their privacy practices, dedicated expert roundtables, and analytical work. A final Report concluding this work and recommending steps to improve the implementation of the OECD Privacy Guidelines was noted and declassified by the Council on 6 April 2021 (OECD, 2021[3]).

[5] Most of which emerged from the 2021 review of the implementation of the OECD Privacy Guidelines (OECD, 2021[3]).

[6] Adherents (Belgium, Canada, Chile, Colombia, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Japan, Korea, Lithuania, Luxembourg, Mexico, Norway, the Slovak Republic, Slovenia, Sweden, the Republic of Türkiye, the United Kingdom and the United States) and four non-Adherents (Brazil, Gibraltar, Bailiwick of Jersey and the Philippines), collectively referred to in this report as "Respondents".

[7] In February 2022, the Secretariat also presented the preliminary findings at a meeting of the GPEN.

[8] International co-operation is now covered in Part Six of the Privacy Guidelines.

[9] In 1998, the need for effective privacy enforcement was highlighted by Ministers in their Ottawa Declaration on the Protection of Privacy on Global Networks (OECD, 1998[56]), and again emphasised in 2003 in an OECD report calling for member countries to establish procedures to improve bilateral and multilateral mechanisms for cross-border co-operation by privacy authorities (OECD, 2003[57]). In 2006, the OECD released a Report on the Cross-border Enforcement of Privacy Laws (OECD, 2006[12]), and a year later, the OECD Council adopted the Recommendation.

[10] It is noted that this feedback was provided as part of comments on a draft version of this Report, rather than as a response to the 2021 questionnaire.

[11] It should be noted, however, that this includes (i) PEAs who have never received requests, or (ii) countries who indicated that they had refused assistance as they lacked competency as a matter of law.

[12] In this context the GDPR is referring to cross-border processing within the EU/EEA, and not to requests which come from outside the EU/EEA. Art 4 (23) of the GDPR defines 'cross-border processing' as either "(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."

[13] Art. 61(4), GDPR.

[14] The next most common challenge was insufficient resources, followed by lack of legal authority. These factors are addressed under 4.2.1.2 "Powers and authorities of PEAs".

[15] Only 13 out of 28 Respondents to the 2021 questionnaire indicated that they keep such records, with only six noting that their records are publicly available. One example, of publicly available statistics however, are those published by the European Data Protection Board (EDPB, 2021[51]), which includes the number of cross-border enforcement cases in the EU/EEA, generated by the IMI Case register (see under 4.3.1.2). The US FTC likewise keeps and publishes statistics on cross-border fraud reports (FTC, 2022[52]).

[16] Noting that these two examples related to co-operation between authorities within a Federated State, rather than between two foreign authorities.

[17] To resolve any disputes in this regard, the European Data Protection Board (EDPB) was established. It also develops guidance on common procedures, and guidelines on applying GDPR provisions in concrete cases (see Section 4.3.1.2).

[18] OECD Privacy Guidelines, at 19(c).

[19] While a number of the powers and authorities discussed in this section (and the responses received from Respondents) may also be relevant to purely domestic scenarios, the 2021 questionnaire responses discussed relate to questions which explicitly sought information on cross-border powers and scenarios.

[20] See, Part III.A.11(b) of the Annex to the Recommendation.

[21] Of note, the 2021 roundtable participated by the PEAs of the G7 member countries discussed the need to "[i]dentify opportunities for greater enforcement co-operation among G7 data protection and privacy authorities, starting by developing a shared understanding of the legal frameworks and enforcement practices across jurisdictions, including on the scope for their extraterritorial application" (G7, 2021[40]).

[22] The 2003 OECD Recommendation Concerning Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders (OECD, 2003[58]) and the 2016 OECD Recommendation on Consumer Protection in E-commerce (OECD, 2016[59]), and also the 2007 Recommendation on Consumer Dispute Resolution and Redress.

[23] See, Part III.A.11(a) of the Annex to the Recommendation

[24] Noting that this is a Federated State, and the answer refers to the Federal PEA. This country noted that PEAs in certain states / provinces have the power to issue such orders without court intervention.

[25] See, Part III.9 of the Annex to the Recommendation.

[26] For example through bringing a negligence claim, or a statutory claim arising out of the privacy legislation. On the latter, for example, in the EU, art. 82 of the GDPR provides a specific right to individuals to seek compensation for a contravention of the GDPR.

[27] In this regard, the 2021 G7 roundtable attended by the PEAs of G7 member countries (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States) discussed the need for legislators "to ensure that regulatory remedies keep pace with technological change and maintain sufficient parity across jurisdictions" (G7, 2021[40]).

[28] The definitions provided, are identical to those provided in the 2021 questionnaire.

[29] At the time of drafting this report, the GPEN is in the process of updating this Action Plan.

[30] This reflects a provision in Part IV.B.20 of the Recommendation. The 2021 questionnaire found that most Respondents (25 out of 28) have put in place measures to share enforcement outcomes.

[31] This reflects a provision in Part IV.B.19 of the Recommendation. The 2021 questionnaire found that most Respondents (23 out of 28) have in place national contact points for co-operation and mutual assistance.

[32] The GPA is a global forum for data protection and privacy enforcement authorities, made up of more than 130 accredited members. The GPA has several working groups, including the International Enforcement Cooperation Working Group (IEWG).

[33] This group is participated in by over 30 authorities from 6 continents.

[34] The Arrangement is not intended to: replace other mechanisms for sharing information or to interfere with similar arrangements by other networks; create legally binding obligations or prevent any authority from cooperating with other non-participating authorities; or compel any authority to engage in any on enforcement activities or provide any confidential information.

[35] The Arrangement is participated by 16 authorities.

[36] The EDPB is an independent EU body, tasked with ensuring the consistent application of EU legislation in the field of data protection, including by issuing guidelines, recommendations, and best practice, as well as providing the European Commission with opinions (GDPR Art. 70(1)).

[37] The Chapter VII GDPR provides for the co-operation framework within the EU/EEA. For general co-operation with third countries, Art. 50 GDPR applies. One EU/EEA country reported to the 2021 questionnaire that Art.50 had not been yet implemented by its PEA.

[38] Under the one-stop-shop mechanism, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority

for the cross-border processing carried out by that controller or processor, in accordance with the co-operation process under the GDPR (GDPR Art. 56(1)). Exceptionally, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State (GDPR Art. 56(2)).

[39] Convention 108+ represents the modernisation of Convention 108 (the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). Convention 108+ is yet to come into force, and will do so either once all signatories to Convention 108 have ratified, or on 11 October 2023 if there are 38 parties to the Convention on that date. For further information see: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

[40] At Article 17.

[41] See Article 15 for a definition of "Supervisory Authority".

[42] Currently, IMI supports 67 administrative co-operation procedures in 17 different policy areas. (European Commission[37]).

[43] The EDPB also publishes a register with all the final decisions taken by EU/EEA data protection authorities under the co-operation mechanism called the "One-Stop-Shop" and aims to offer harmonised enforcement on cross-border cases (EDPB[53]).

[44] It is noted that this list reflects responses to the 2021 questionnaire, however may not be an extensive list of all MOUs Adherents have in place regarding cross-border enforcement co-operation of privacy laws.

[45] To join it is only necessary to nominate a contact point and to endorse the Action Plan.

[46] Hosted by the Personal Information Protection Commission (PPC), Japan in 2022, and co-hosted by the PPC and the United States Federal Trade Commission in 2023.

[47] A high-level group established under the UK G7 Presidency in 2021. This group first met in the UK in September 2021, held a second meeting in Germany in September 2022 and a third meeting in Japan in June 2023.

[48] This resource, Corpus Iuris is available at: http://pot.diputados.gob.mx/Unidad-de-Transparencia/Datos-Personales-Archivo-y-Gestion-Documental/Corpus-Iuris-Nacional-e-Internacional (Gobierno de Mexico, 2016[54])

[49] Which is already explicitly referenced in the Recommendation at Part II.3, and Part IV.C.22.a.

[50] The examples provided in response to the 2021 questionnaire included: guidance on how cross-border cases are handled; guidance for foreigners to file complaints; provision of information on foreign privacy laws and regulations; and templates for reporting cross-border data breaches.

[51] It is noted that this feedback was provided as part of comments on a draft version of this Report, rather than as a response to the 2021 questionnaire.