



**GPA**

Global Privacy Assembly

# International Enforcement Working Group

Report – July 2022

Chair Authorities:

Superintendence of Industry and Commerce of Colombia (**SIC**)

Office of the Privacy Commissioner of Canada (**OPC**)

Norwegian Data Protection Authority (**Datatilsynet**)

Office of the Privacy Commissioner for Personal Data, Hong Kong, China (**PCPD**)



## Table of Contents

Executive Summary.....	1
Introduction.....	4
Working group activities.....	8
Forward looking plan 2022-23.....	12
Conclusion.....	13
Annexes.....	14



## Executive Summary

The International Enforcement Cooperation Working Group (IEWG) is pleased to present this report to the Global Privacy Assembly (GPA) on its activity, progress, and successes between July 2021 and June 2022.

Heading towards its third year in operation as a permanent Working Group of the GPA, the IEWG is co-chaired by the Office of the Privacy Commissioner of Canada, the Superintendence of Industry and Commerce of Colombia, the Norwegian Authority for data protection and the Office of the Privacy Commissioner, Hong Kong, China. It has increased its membership considerably since the GPA's virtual conference in 2021, with a total of 36 members and observers.

The IEWG's work continues to be integral to the GPA, particularly in advancing its objectives to promote and support enforcement cooperation in Pillar 2 of the Policy Strategy in the GPA Strategic Plan. To that end, the IEWG co-chairs are pleased to report that due to the interest of diversifying the contributions and members of the group, since the year 2021 the co-chairs are representatives from Europe, North America, Asia and Latin America. The new co-chairs are keen to continue to focus on practical activities which has been reflected in the publication of guidelines and manuals to materialize the cooperation; and in tools that highlight the importance of enforcement cooperation in different regions of the world.

The combination of tangible products has been the group's strength, such as the publication of the updated Enforcement Cooperation Handbook, the Closed Enforcement Sessions, Ad-hoc sub-working groups that focuses on hot topics of mutual interest such as Data Scrapping, Credential Stuffing, AdTech and FRT.

Moving forward, and in line with the strategic priorities of the GPA over the next year, the IEWG aims to maintain the momentum of its work, while also broadening its scope with a particular focus on capacity building activities; more inclusiveness of regional and linguistic authorities by facilitating the use of French and Spanish ; and exploring collaboration and coordination opportunities, with other GPA's working groups and other networks such as: Global Privacy Enforcement Network (GPEN), Asia Pacific Privacy Authorities (APPA), IberoAmerican Data Protection Network (RIPD) and the Organization for Economic Cooperation and Development (OECD).



## Introduction

### Background

Building on the work of previous, temporary, enforcement cooperation working groups, the International Enforcement Cooperation Working Group (IEWG) was established as a permanent working group of the Global Privacy Assembly (GPA) following the 41<sup>st</sup> Conference in Tirana in 2019. The overarching mandate of the IEWG is derived from Pillar 2 of the Policy Strategy in the [GPA's 2019-2021 Strategic Plan](#). This called for the IEWG to refresh its objective as:

“...an active group considering live issues and concerns related to enforcement, with a focus on sharing experience, tactics and approaches to tackling specific aspects, including common experience in investigating multinational companies.”

In its first year of operation as a permanent working group (2019-2020), the IEWG made good progress in working towards delivery of its mandate, as set out in its [annual report to the virtual GPA in 2020](#). Key achievements during this period include the introduction of ‘safe space’ sessions to support and encourage live enforcement cooperation, and the development of the ‘regional champions’ model to promote the work of the IEWG and increase the diversity of membership and participation in the group.

In its second year (2020-2021), the IEWG committed to build on these achievements by making substantive progress on other aspects of its work plan, including updating and refreshing practical tools to support enforcement cooperation such as the publication of the updated Enforcement Cooperation Handbook, and identifying and establishing contact with key networks of data protection and privacy enforcement authorities.

In its third year (2021-2022) the IEWG focused firstly on ensuring a smooth transition to the new co-chairs and secretariat and then on maintaining the momentum of the working group by organizing new closed enforcement sessions and advancing sub-working groups’ activities on Data Scrapping, Credential Stuffing and FRT. Finally, the working group included an ng innovative work, reflected by the launch of the Transnational Case Map which presents user-friendly maps on cases conducted around the world on enforcement cooperation.

### Membership

Between 2019-2021, the work of the IEWG was led by three co-chair authorities:

- Canada - Office of the Privacy Commissioner of Canada (OPC)
- United Kingdom - Information Commissioner’s Office (ICO - also provides IEWG Secretariat)
- United States of America - Federal Trade Commission (FTC)



The mandate of the new co-chairs and secretariat started during the last quarter of 2021 and will last until the third quarter of 2023. Therefore, the Superintendence of Industry and Commerce of Colombia (SIC) will be in charge of the Secretariat and the following authorities will serve as co-chairs:

- Canada - Office of the Privacy Commissioner of Canada (OPC)
- Colombia – Superintendence of Industry and Commerce (SIC)
- Hong Kong, China - Office of the Privacy Commissioner for Personal Data (PCPD)
- Norway - Norwegian Data Protection Authority (Datatilsynet).

The IEWG co-chairs are pleased to report that the group's membership went from 29 authorities in 2021 to 36 in 2022. In addition to the co-chairs, the IEWG now comprises **OECD** as an observer and the following authorities (new members highlighted in bold):

- Abu Dhabi - Office of the Data Protection Commissioner, Abu Dhabi Global Market
- Albania - Information and Data Protection Commissioner
- **Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)- Observer**
- Argentina - Access to Public Information Agency Argentina
- Australia - Office of the Australian Information Commissioner (OAIC)
- Belgium - Belgian Data Protection Authority
- Burkina Faso - National Commission for Informatics and Liberties
- Côte d'Ivoire - Telecommunications / ICT Regulatory Authority of Côte d'Ivoire
- Dubai - Data Protection Commissioner, Dubai International Financial Centre
- European Union - European Data Protection Supervisor (EDPS)
- **France – Commission Nationale de l'informatique et des libertés (CNIL)**
- Georgia - State Inspector's Service
- Germany - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
- Gibraltar - Gibraltar Regulatory Authority (GRA)
- Iceland - Icelandic Data Protection Authority
- **Israel – Privacy Protection Authority**
- **Japan – Personal Information Protection Commission (PPC)**
- Jersey - Jersey Office of the Information Commissioner (JOIC)
- **Korea – Personal Information Protection Commission (PIPC)**
- Mexico - National Institute for Transparency, Access to Information and Personal Data Protection
- Monaco - Commission for the Control of Personal Data
- Netherlands - Dutch Data Protection Authority
- New Zealand - Office of the Privacy Commissioner
- **Ontario, Canada – Information and Privacy Commissioner of Ontario (IPC)**
- **Organization for Economic Cooperation and Development (OECD) - Observer**
- Philippines - National Privacy Commission (NPC)
- Senegal – Personal Data Protection Commission



- Switzerland - Swiss Federal Data Protection and Information Commissioner (FDPIIC)
- Turkey – Turkish Personal Data Protection Authority
- United Kingdom – Information Commissioner’s Office (ICO)
- United States of America – Federal Trade Commission (FTC)
- **USA – Chief Privacy and Civil Liberties Officer (CPCLO) - Observer**

## Work plan

Taking account of the global pandemic, and focusing on the areas of the IEWG’s work that would add most value to its members and the wider GPA, the co-chairs prioritised the following items from the IEWG’s work plan for progression in 2021-23:

- **Priority 1 – Foundations:** Lay the foundations for the IEWG and GPA to facilitate practical enforcement cooperation, focusing on organisations and issues with significant global impact on people’s data protection and privacy rights.
  - Objective 1 - Use of and evaluation of the closed enforcement session’s framework.
  - Objective 2 – Develop an evergreen “transnational case map” that highlights cooperation enforcement activities worldwide.
- **Priority 2 – Tools:** Build on the work of the previous IEWG to further develop practical tools for enforcement cooperation.
  - Objective 1 – Promote and teach our members how to use the *Enforcement Cooperation Handbook*.
  - Objective 2 – Maintain and promote the enforcement cooperation repository.
- **Priority 3 - Awareness and communication:** Ensure that the IEWG has a good awareness of the global Privacy Enforcement Authority (PEA) network landscape and maintains or establishes mutual lines of communication and observation to coordinate and leverage activities.
  - Objective 1 – Promote and strengthen the communication channels between PEA of each region.
  - Objective 2 – Develop existing and new mutual observation agreements.
  - Objective 3 – Improve our communication outreach for more of our members to participate in the activities put in place.
  - Objective 4 – Translate to the best of our abilities and capacities the products, conferences and different activities the group may have to French and Spanish.

*Facial Recognition Technology (FRT):* Continue the work with the Ethics and Data Protection in AI Working Group (AIWG) to deliver the commitments in the [Resolution](#)



[on FRT](#) (adopted at the virtual GPA in 2020) to develop and promote a set of principles for the use of personal data in FRT.

1. Objective 1 – Develop principles, for adoption in a GPA resolution, based on research and stakeholder engagement.
2. Objective 2 – Promote principles and review industry application.

In addition, the co-chairs have the intention to continue working with two items of the IEWG work that followed the closed enforcement sessions held in 2020-21:

- *Credential Stuffing*: IEWG sub-group whose objective is to develop a guidance to the organizations and the general public on how to address and mitigate risks arising from credential stuffing attacks.
- *Data scraping*: Establishment of a temporary IEWG sub-group whose objective is to explore and consider joint actions to clarify and set expectations of the privacy regulatory community around companies' obligations to protect against the scraping of publicly accessible personal data.
- *Adtech*: mandate a sub working group to demystify the Adtech ecosystem and explore potential joined actions in this area.

### **Liaison with the Strategic Direction Sub-Committee**

In 2021-22, the IEWG continued to regularly update the Strategic Direction Sub-Committee (SDSC) on the progress of its work, in written quarterly reports. In May 2022, the IEWG participated in the eighth meeting of the SDSC to provide:

Further detail on activities undertaken to advance the GPA's 2022-23 Strategic Plan (including the organization of the closed enforcement sessions, updates to the Transnational Case Map, engagement with other working groups and ad-hoc sub-working groups on Credential Stuffing, Data Scrapping, and AdTech). The co-chairs seized this opportunity to debrief the SDSC on the IEWG's promotion action during interventions of chairs in international conferences and media interviews); and

The IEWG co-chairs were pleased to receive positive feedback from members of the SDSC, focusing on the yearly development of the Transnational Case Map and the intention to nominate the initiative to the 2022 GPA Awards.



## Working Group Activities

### Closed Enforcement Sessions

During 2021-2022, the following sessions were held:

- *Credential stuffing*

#### Current Status

As part of the group's research and efforts on the topic, a survey was conducted to establish how the credential stuffing topic is dealt with by data protection and privacy authorities. The group also engaged and collaborated with key external stakeholders, including cyber security experts, the private sector and cyber security agencies, to seek their input and comments on the guidance on this topic that the IEWG developed.

The SWG has completed credential stuffing guidelines for organizations and credential stuffing awareness raising material for the public including a short video.

The material produced will support authorities in cases that relate to credential stuffing attacks and efforts to mitigate the risk of said cyber threat. The work done by the SWG also contributes to the efforts of the GPA to operate as a 'year-round' organization with initiative to actively engage on issues in a pragmatic and relevant way. Further, the engagement and collaboration with external stakeholders contribute to the GPA's strategic priority to maximize the assembly's voice and influence.

On Monday 27<sup>th</sup> June 2022, the GPA published the material produced on the GPA's "Updates from Working Groups" page: <https://globalprivacyassembly.org/news-events/updates-from-working-groups/>. The material was also shared via the GPA's social media platforms and simultaneously published by other members of the IEWG in their communication channels.

(Check for Annex 2,3,4 and 5)

#### FRT Current Status

Between 2021-22 the IEWG-AIWG FRT sub-group developed a set of principles and expectations for the appropriate for the use of personal information in FRT. As mentioned above, this project was mandated by the GPA's [resolution on](#) FRT at the virtual Assembly in 2020.





The principles are informed by desk-based research, literature reviews, input from the GPA membership (in response to a survey on FRT), and contributions from external stakeholders including FRT users, developers, lawmakers, and civil society (as part of a consultation).

Recognizing the significant risks that FRT can pose, especially in certain circumstances, the principles set a high bar for use of FRT, and require robust assessment of risk and demonstrable compliance from organizations procuring and implementing such technology.

The sub-group submitted the principles to the GPA Secretariat as a resolution for adoption at the Closed Session in Istanbul, Turkey, in October 2022.

- *Adtech*: This webinar was open to all GPA members in October 2021. The IEWG leveraged this event to explain to participants briefly the purpose of closed enforcement sessions and how a topic with several data protection and privacy implications that many GPA members are likely grappling with across the globe was discussed. Then, ICO representatives presented the Adtech topic, policies and enforcement actions related to this topic that were undertaken by several authorities and potential key privacy concerns.

### Current Status

An Adtech Subgroup was created and met for the first session in March 2022. It aims to demystify the Adtech ecosystem, and four lines of action were determined:

- 1- AdTech Ecosystem – Research on the players and structure of programmatic advertising
- 2- Key Technology – Research into the key technologies underpinning AdTech
- 3- Harm caused to individuals – Research into the de-facto privacy harms
- 4- Compilation of regulations and policies – Principles, policies etc.

Members of the IEWG volunteered to contribute in line of action that interest them, under the leadership of the secretariat that coordinating all activities related to this sub-working group.

- *Data scraping*

### Current Status

On February 2022 a Closed Enforcement Session to follow up on the Data Scraping initiative was held. In this session, a skeleton of the Data Scraping letter was presented with the purpose to set expectations around the minimum measures SMCs and other websites should implement to mitigate the privacy impacts from data scraping.



After the session, the Office of the Australian Information Commissioner (OAIC) received comments and suggestions from other members of the IEWG. Currently, the scope and the skeleton of the Letter are being finalized.

- *Smart Glasses:*

Smart glasses are wearables that enable collection, recording and sharing of information that the wearer sees. They can be connected to a smart phone and require the user to login via a social media account on their phone to access the smart glasses app.

This raises several questions regarding the privacy of the wearer and especially that of individuals whose personal information is captured while in proximity of the wearer.

The Technology Analysis Directorate (TAD) of OPC Canada conducted a technical analysis of a new brand launched recently in the market. The analysis attempted to understand the flow of data that the smart glasses generate and if it is compliant or not with standard privacy protection principles.

*Current Status:*

On June 2022, the OPC Canada shared their technical analysis on a Closed Enforcement Session, many authorities discussed the topic. Currently, the IEWG members are considering potential follow-up actions.

## **Transnational Case Map**

(For more information, please refer to Annex A)

The "Transnational Case Map" seeks to identify all the cases that IEWG members have enforced with transnational implications in the **past two years**. Such cases can include administrative fines, Administrative orders or any other kind of enforcement actions. that impacted jurisdictions beyond its borders.

The following information can be consulted per case:

- Jurisdiction
- Data Protection Authority
- Year in which the investigation was initiated
- Year in which the enforcement measure was imposed
- Case number / name

- Type of institution of the data controller/processor
- Description of the case
- Enforcement tool imposed
- Transnational implication of the case
- Enforcement cooperation mechanisms used (if any)
- Technologies involved in the case (if any)
- Hyperlink to the case

The map is published for the first time, the co-chairs of the IEWG seek to update it each year with new information. Hence, in the first months of the year, the IEWG Secretariat will be sending IEWG members the same questionnaire seeking to update the cases that DPA had over the previous year. That's why we consider the transnational Case map to be a living document and a dynamic tool.



Last but not least, this exercise also helps convey current convergence between data protection legislations worldwide.

### **Enforcement Cooperation Handbook**

The IEWG is in the process of collaborating with the DCCWG to administer a short survey to GPA members to obtain successful examples of enforcement cooperation, barriers faced and solutions developed to overcome them. Additional examples will be added to the Enforcement Cooperation Repository to serve as further concrete guidance for authorities wishing to engage in collaboration.

**(See Annex 6)**

### **Enforcement Repository**

The repository is a digital library on the GPA website that centralizes links to publicly available and non-confidential resources of value to the global community of data protection and privacy enforcement authorities.



In order to develop and maintain this important tool, it has been decided during the last GPA conference in Mexico to establish a steering committee that will lead and coordinate the management of the repository.

The Turkish and the Filipino authorities volunteered to co-lead the steering committee of the enforcement cooperation repository. They held their first meeting in June 2022 and launched two actions: 1- identification of all broken links in the repository and 2-liaise with the GPA secretariat to circulate a call for new resources from all GPA members.

### **Conferences**

In their efforts to promote the IEWG and its activities, the co-chairs participated in several international conferences such as the Privacy Symposium-Venice, the Global IAPP-Washington D.C and the CPDP 2022 in Brussels. In the same vein, three media interviews flowed from the above conferences and allowed the IEWG to highlight its mandate, history and activities.

Additionally, in line with priority 3 of the work plan, we are eager to work with other members of the privacy community worldwide. For example, we have initiated discussion with EDPB, GPEN, APPA and AFAPDP representatives for a potential coordination and cooperation with the IEWG. Currently, the IEWG is preparing a joint capacity building session on “Dealing with Investigative Backlogs” that will be held at this year’s Assembly.

### **Governance Meeting**

On October 2021, the governance meeting was held to finalize the first term of the IEWG. ICO UK handed over the secretariat to the Superintendence of Industry and Commerce of Colombia (SIC) and shared experiences learned during the last two years. The new co-chairs were appointed: Superintendence of Industry and Commerce of Colombia (SIC), Office of the Privacy Commissioner of Canada (OPC), Norwegian Data Protection Authority (Datatilsynet) and Office of the Privacy Commissioner for Personal Data, Hong Kong, China (PCPD). ICO and OPC commissioners expressed their satisfaction for all the work undertaken in the last period.

## **Forward looking plan 2022-2023**

During the second semester of 2022 and in 2023 the co-chairs and the secretariat of the IEWG look forward to work on and strengthen the ongoing projects, such as:

- Capacity building workshops (with our members and with other regional networks).
- Display the Transnational Case Map in different scenarios so that it can begin to fulfil its role as a source of information for the community.
- Continuing the four lines of work of the AdTech SubGroup.



- Finalize follow-up actions on the data scraping and smart glasses closed enforcement sessions and on the FRT resolution.
- Identify the important and urgent topics for our closed enforcement sessions and carry out at least four sessions chaired by a diverse range of IEWG members.
- Help our members to better understand and use our recently updated Cooperation Handbook, and add further case studies.
- Maintain and promote the enforcement cooperation repository.
- Develop and implement tangible cooperation and coordination with other networks in the privacy realm or other areas whose activities are complementary to or/and overlapping with IEWG's activities.
- Subject to adoption of a draft Resolution on 'International Cooperation Capacity Building for Improving Cybersecurity Regulation and Understanding Cyber Incident Harms' at the Assembly in October 2022 - take steps to better understand the remits of GPA members on cybersecurity, and explore collaborative options.

## Conclusion

The IEWG has progressed to maintain its Closed Enforcement Sessions initiative and has demonstrated its importance by convening various authorities around the world to address different issues.

Thanks to the efforts of the former secretariat and the co-chairs together with the commitment of all the members of the group, it has been possible to deliver in this last period the ideas and initiatives that began more than a year ago, such as: the guidelines on Credential Stuffing, the Resolution on FRT, the publication of the Updated Enforcement Cooperation Handbook and the launch of the new initiative regarding the Transnational Map, among others.

We are aware that achievements will always lead to new challenges within the same group. One of our main objectives is the diversification of the group and we strongly believe that this starts with the sharing of material and sessions in various languages, as well as encouraging regional efforts and networks that would help to reinforce cooperation through shared experiences and similarities.

Looking ahead, the four co-chairs will maintain their position until 2023, as will the secretariat. During this period, it is expected that more authorities will join this committed and promising group.



## Annexes

### Annex A: Transnational Case Map

**Link:**

<https://app.powerbi.com/view?r=eyJrIjoizDI5Y2YyNmItNGQ4MS00NjRiLWE3MmYtM2RmYzgyYjhlMDU4liwidCI6Ijlk0NzhIZWMyLThkZjctNDk0OC04MGQzLTc0MGExNmUxZGNjYSJ9&pageName=R eportSection>

The “Transnational Case Map” seeks to identify all the cases that IEWG members have had with transnational implications in the **past two years**. Such cases can go from Administrative fines from a DPA, Administrative orders or any other kind of enforcement tool that any of IEWG members have used with implications beyond its borders.

It is common for information to be presented in written form. However, there are several ways of projecting information with the intention of making it not only more accessible but also easier to understand.

The IEWG co-chairs have chosen to develop three maps. The first is intended to show the convergence of data protection regulation. For this purpose, they chose to join with a red line the country where the data protection authority that used the enforcement tool.

A second map aims to colour code the transnational implication(s) of each of the cases. By colour coding the cases this way, this map would ideally provide an overview of the prevalence of the different types of transnational cases that occur over time.

<b><u>Types of Transnational Implication</u></b>
The data controller/processor operated in more than one jurisdiction
Data subjects of other jurisdiction(s) were affected
There was cross-border data transfer
The assistance of the DPA of another jurisdiction was required or sought
There was extra-territorial application of the domestic data protection law (e.g. investigation against overseas data controller/processor; penalties were imposed to overseas data controller/processor, etc.)

And last, but not least, a third map that enables the user to identify by country the specifications of each case reported by the IEWG members. The following information can be consulted per case:

- Jurisdiction
- Data Protection Authority
- Year in which the investigation was initiated

- Year in which the enforcement measure was imposed
- Case number / name
- Type of institution of the data controller/processor
- Description of the case
- Enforcement tool imposed
- Transnational implication of the case
- Enforcement cooperation mechanisms used (if any)
- Technologies involved in the case (if any)
- Hyperlink to the case

The Transnational Case Map is a constantly evolving product. This is since it is intended to be updated year by year with transnational cases. In this way, enforcement tools are being shown, analysed, and compared year by year.

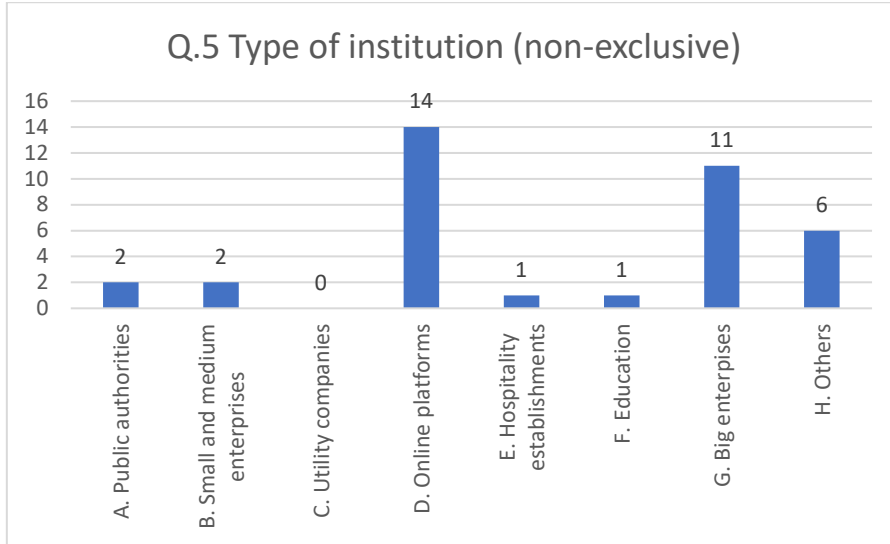
The interactive method of the map helps the privacy community to embrace another source of primary information on relevant topics such as:

- Transnational data protection investigations.
- Data protection convergence.
- Cooperation between Data Protection Authorities.
- Enforcement tools.



Analysis:

**Q5. What type(s) of institution may the controller/processor involved in the case be categorised as?**



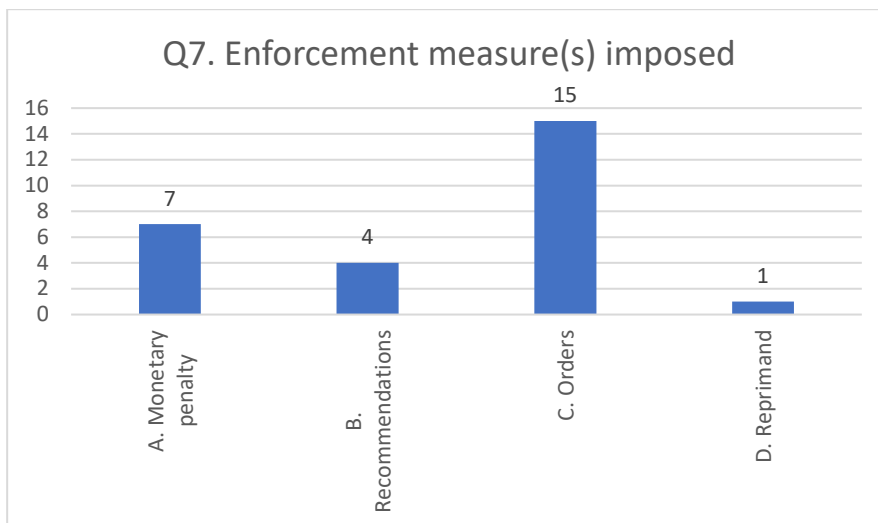
Total number of cases reported: 24

#### Q5. Observations

The most common type of institution being the subject of the reported transnational cases was 'Online platforms' (14 cases), followed by 'Big enterprises' (11 cases). The types listed are not treated as mutually exclusive.

Institutions reported as belonging to the 'Others' category included Airline, Ticket retailer, Financial institution, Facial Recognition company, and Developers of software for education.

#### **Q7. What was the enforcement measure(s) imposed (e.g. sanction, administrative order or other)?**



Total number of cases reported: 24



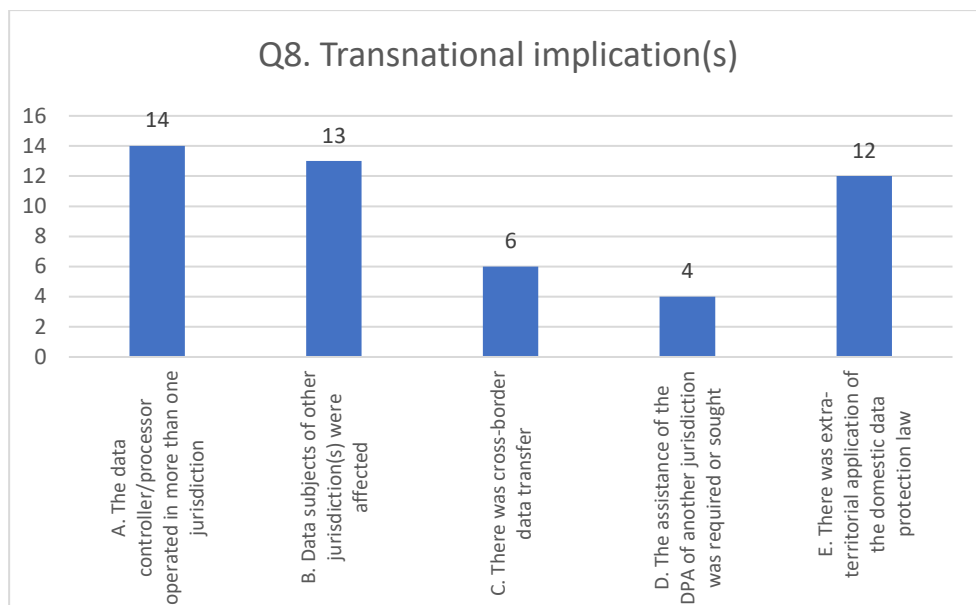
### Q7. Observations

In the 24 reported cases, the most popular enforcement measure imposed was 'Order' (15 cases), followed by 'Monetary penalty' (7 cases)

Order includes, for example, a compliance order to stop processing of personal data, a cease and desist order to remove content, etc. The legal mechanisms behind the orders would vary according to each jurisdiction.

The highest monetary penalties reported was the £20 million monetary fine imposed by ICO UK to British Airways, followed by the £18.4 million monetary fine imposed by ICO UK to Marriot International Inc.

### **Q8. What was the transnational implication of the case?**



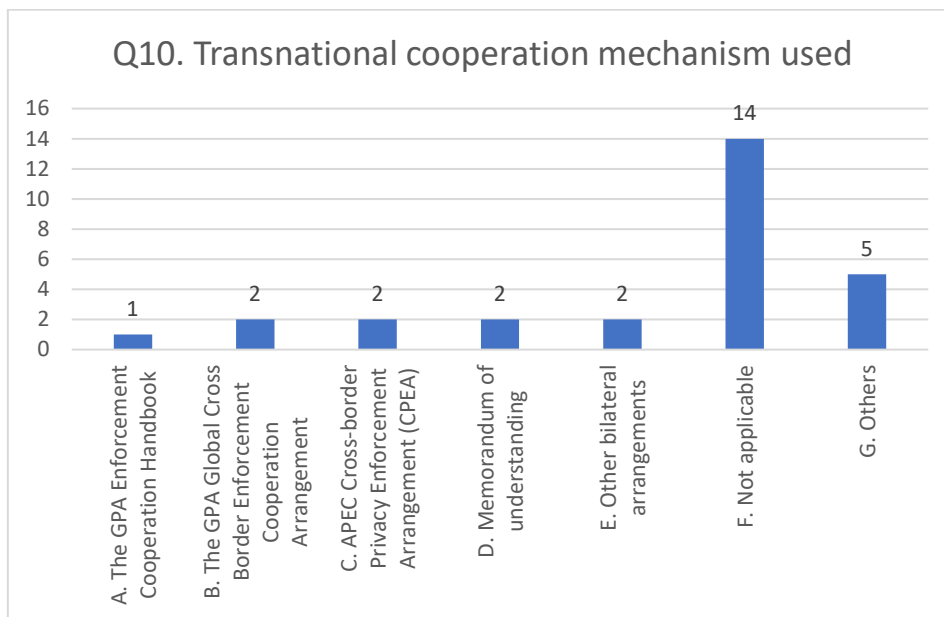
Total number of cases reported: 24

### Q8. Observations

The most reported transnational implications among the 24 cases were 'The data controller/processor operated in more than one jurisdiction' (14 cases); followed by 'Data subjects of other jurisdiction(s) were affected' (13 cases); and 'extra-territorial application of domestic data protection law' (12 cases).

Many cases reported multiple transnational implications. For example, in a data breach incident where the data controller/processor involved operated in another jurisdiction, the data subjects of the other jurisdiction may have also been affected in the case.

**Q.10 If your office engaged in enforcement cooperation with an oversea authority in this case, what transnational cooperation mechanisms (if any) were used?**



Total number of cases reported: 24

### Q10. Observations

Result suggests many transnational cases (14) reported had not involved the use of any transnational cooperation mechanisms. DPAs conducted investigations and imposed enforcement measures in cases with transnational implications, without seeking the assistance of authorities in other jurisdictions or without initiating cross-border cooperation.

Other transnational cooperation mechanism reported included: EU GDPR Cooperation and Consistency mechanism (One-stop-shop), and international relations/ties with the embassy of another country.