GPA Global Privacy and Data Protection Awards 2023

Entry Form

To submit an entry to the GPA Global Privacy and Data Protection Awards please complete and email this form to secretariat@globalprivacyassembly.org **no later than 9 June 2023.**

Note: GPA member authorities can submit as many entries as they wish, but a separate form should be used for each different entry, submitted by the deadline above.

Languages: The GPA documentation Rule 6.2[1] applies.

1. CONTACT DETAILS FOR THIS ENTRY

Privacy/Data Protection Authority:	Office of the Privacy Commissioner for Personal Data, (Hong Kong), Office of the Privacy Commissioner of Canada, Norwegian Data Protection Authority (Datatilsynet), and the Superintendence of Industry and Commerce (Colombia)	
Person completing this form:	Daniela Alejandro *First name*	Angarita Londono Congote *Last name*
Job title:	Alejandro - Advisor to the Deputy Superintendent for the Protection of Personal Data Daniela - International Affairs Professional	
Email address:	Alejandro - alondono@sic.gov.co Daniela - dangarita@sic.gov.co	

2. ELIGIBILITY

By submitting this entry, I confirm that (*please tick all boxes to confirm)*:

☒ The Authority is a member of the Global Privacy Assembly

☒ The initiative described in this entry was undertaken since January 2022.

☒ I am aware that the information in the entry (other than the contact details in 1(a) above) will be publicised by the GPA Secretariat.

3. CATEGORIES

Please indicate which category you wish to enter.

*Please tick **one;** please use a separate form for each category you wish to enter:*

☐ Education and Public Awareness

[1] GPA Rules and Procedures, Rule 6.2 'Assembly documents':
Without prejudice to section 4.2, Assembly documents, including accreditation and observer applications may be submitted in English or in another language. In the latter case, the documents shall be accompanied by an English version. Members with the ability and the resources to do so are encouraged to translate proposed resolutions and other Assembly documents such as the Assembly Rules and Procedures.

☐ Accountability
☒ Dispute Resolution and Enforcement
☐ Innovation
☐ People's Choice

4. DESCRIPTION OF THE INITIATIVE

a. Please provide a brief summary of the initiative *(no more than 75 words)*

The "Transnational Case Map" seeks to identify all the cases that IEWG members have had with transnational implications. 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.

b. Please provide a full description of the initiative *(no more than 350 words)*

The "Transnational Case Map" seeks to identify all the cases that IEWG members have had with transnational implications. 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 with the one where the

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.

Types of Transnational Implication
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

c. Please explain why you think the initiative deserves to be recognised by an award *(no more than 200 words)*

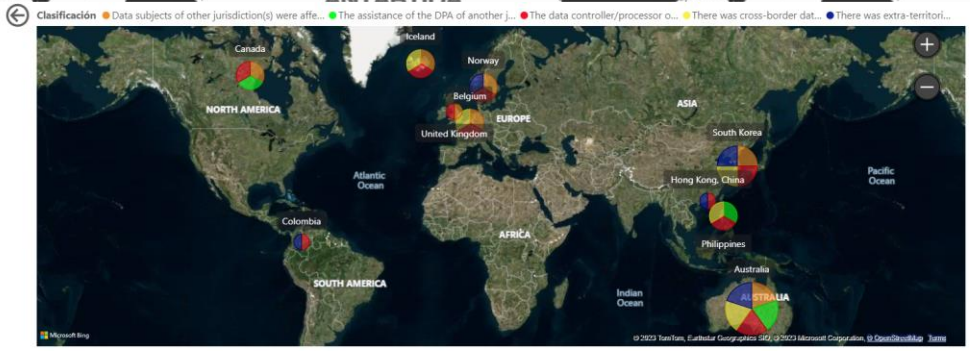
The Transnational Cases Map should be rewarded not only for its innovative way of making information on enforcement tools available to the community, but also for being an ideal tool for teaching personal data protection authorities about each other.

The Transnational Case Map is a constantly evolving product. This is due to the fact that it is intended to be updated year by year with transnational cases. In this way, enforcement tools are being taught, analyse 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:

i) Transnational data protection investigations.
ii) Data protection convergence.
iii) Cooperation between Data Protection Authorities.
iv) Enforcement tools.

d. Please include a photograph or image, if you wish *(This will be published with your entry on the GPA website. The image can be pasted into the box below, be sent as an attachment or a link may be provided)*



Types of Transnational Implication

- *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.)*
- *The assistance of the DPA of another jurisdiction was required or sought*
- *Data subjects of other jurisdiction(s) were affected*
- *There was cross-border data transfer*
- *The data controller/processor operated in more than one jurisdiction*

Jurisdiction

- *United Kingdom*
- *South Korea*
- *Philippines*
- *Norway*
- *Iceland*
- *Colombia*
- *Canada*
- *Belgium*
- *Australia*
- *Hong Kong, China*

Jurisdiction

- ☐ *Hong Kong, China*
- ☐ *Australia*
- ☐ *Bruselas*
- ☐ *Canada*
- ☐ *Colombia*
- ☐ *Iceland*
- ☐ *Norway*
- ☐ *Philippines*
- ☐ *South Korea*
- ☐ *United Kingdom*

Year in which the investigation was initiated

2016	2019
2017	2020
2018	2021

Data Protection Authority

National Privacy Commission	Norwegian Data Protection Authority (Datatilsynet)	Personal Information Protection Commission of Sout...
European Data Protection Supervisor	Office of the Australian Information Commissioner	Persónuvernd / Icelandic Data Protection Authority
Information Commissioner's Office	Office of the Privacy Commissioner for Personal Data (PCPD)	Superintendence of Industry and Commerce
National Privacy Commission	Office of the Privacy Commissioner of Canada (OPC)	

Description of the case

A Transport Network Company (TNC) were ordered to cease and desist from rolling out its new data processing system namely: 1. Passenger Verification, 2. pilot test of the In-vehicle audio Recording, and 3. pilot test of the in-vehicle video recording. the TNC did not sufficiently identify and assess the risks posed by the data processing systems to the rights and freedoms of data subjects, saying that "only the risks faced by the company were taken into account" in its Privacy Impact Assessment (PIA). In addition the company also failed to mention its legal basis in processing the collected data.

Investigation into EU institutions' use of Microsoft software. Involved a wide-ranging assessment of the licensing agreement. We found a number of serious concerns: Microsoft acting as a controller; ill-defined purpose limitation; non-compliant controller-processor agreement; non-compliant transfer provisions; disclosure provisions contrary to EU institutions' privileges and immunities. In response the EU institutions renegotiated their licensing agreement but concerns remain. We have therefore launched another (ongoing) investigations which is likely to result in corrective measures being taken

A cyber-attack on British Airways in 2018 potentially led to the attacker accessing the personal data of approximately 429,612 customers and staff. This included names, addresses, payment card numbers and CVV numbers of 244,000 BA customers. Other details thought to have been accessed include the combined card and CVV numbers of 77,000 customers and card numbers only for 108,000 customers. Usernames and passwords of BA employee and administrator accounts as well as usernames and PINs of up to 612 BA Executive Club accounts were also potentially accessed. The ICO found BA ought to have identified weaknesses in its security and resolved them with security measures that were available at the time, e.g.: • limiting access to applications, data and tools to only that which are required to fulfil a user's role • undertaking rigorous testing, in the form of simulating a cyber-attack, on the business' systems; • protecting employee and third party accounts with multi-factor authentication. BA did not detect the attack themselves but were alerted by a third party more than two months afterwards. It is not clear whether or when BA would have

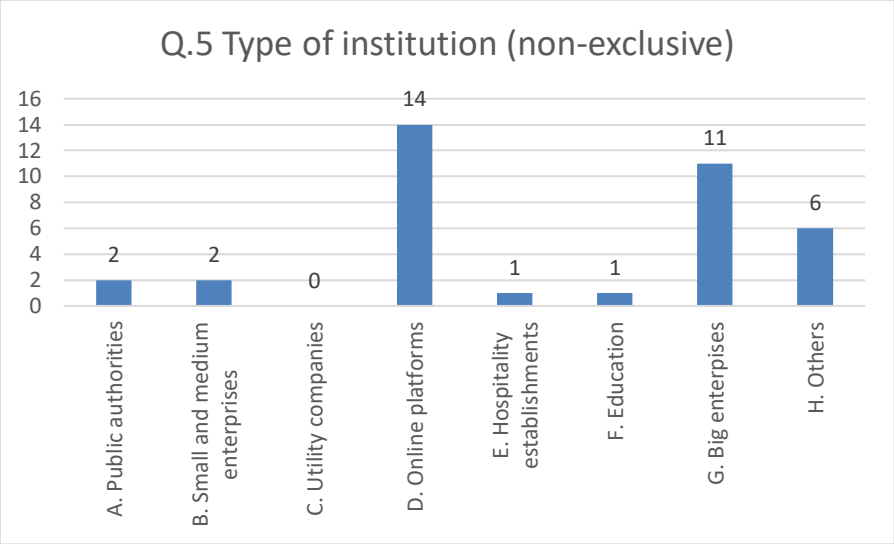
e. Please provide the most relevant link on the authority's website to the initiative, if applicable *(The website content does not need to be in English)*

https://app.powerbi.com/view?r=eyJrIjoiZDI5Y2YyNmItNGQ4MS00NjRiLWE3MmYtM2RmYzgyYjhlMDU4IiwidCI6Ijk0NzhlZWMyLThkZjctNDk0OC04MGQzLTc0MGExNmUxZGNjYSJ9&pageName=ReportSection

f. Please provide any other relevant links that help explain the initiative or its impact or success *(e.g. links to news reports or articles):*

IEWG 2022 Transnational Case Map – Statistical Analysis Appendix

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



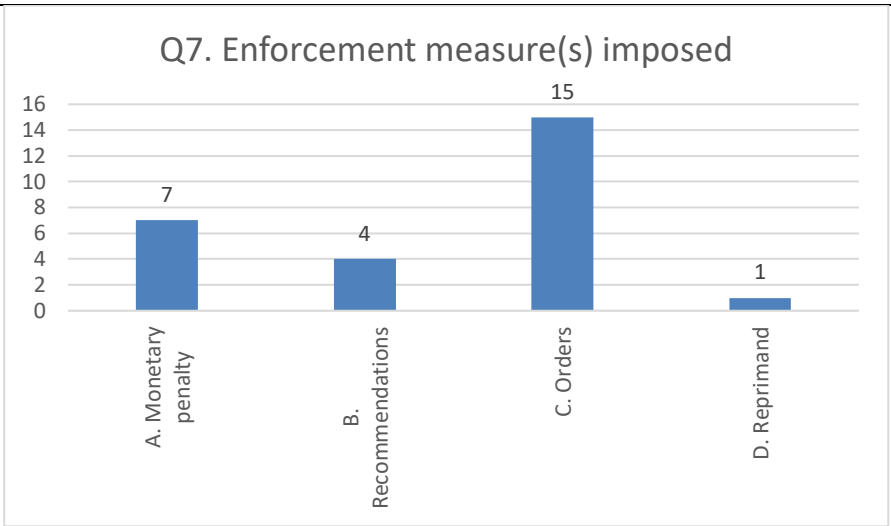
Total number of cases reported: 24

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

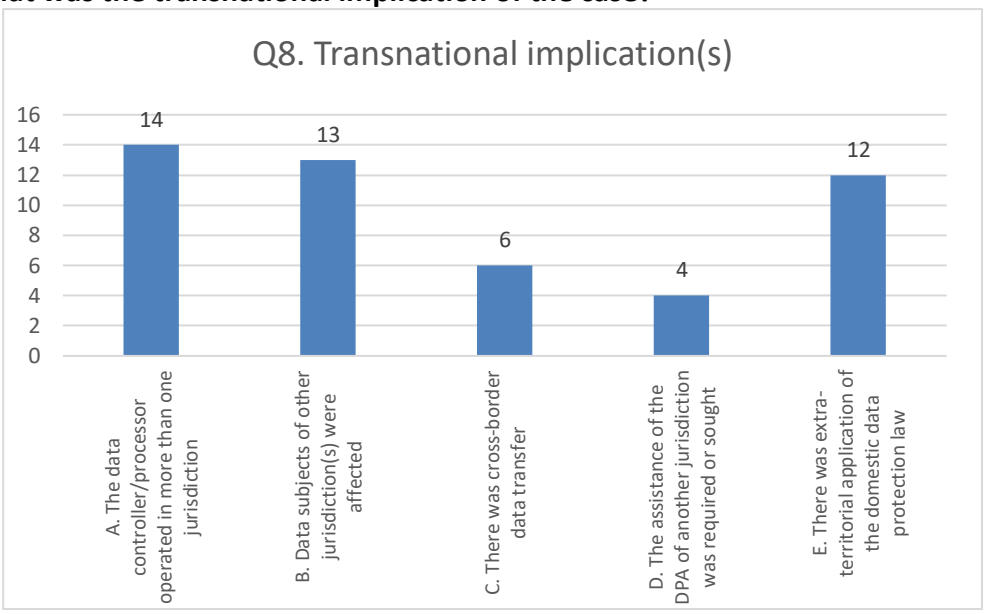
Q7. Observations

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?



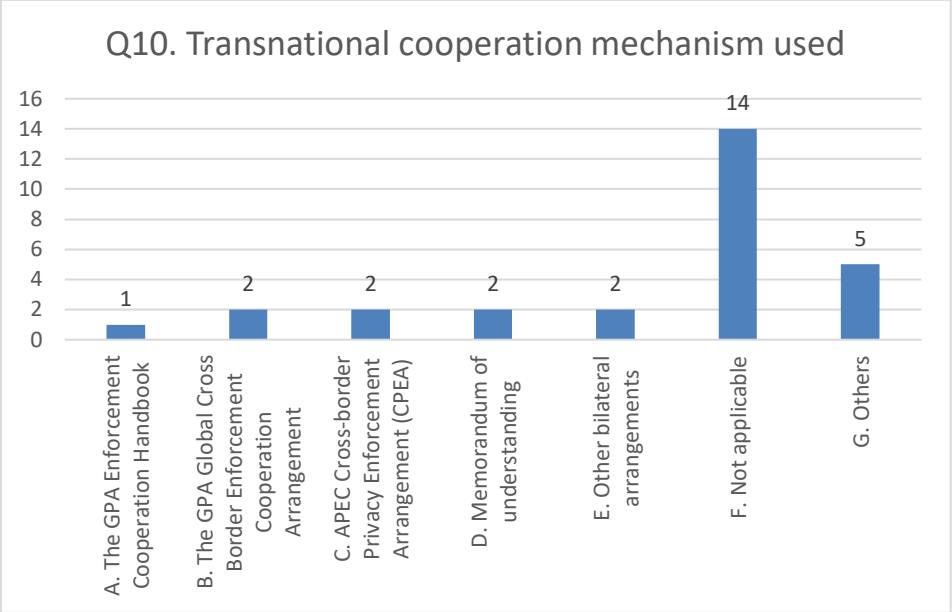
Total number of cases reported: 24

Q8. Observations

The most commonly 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.