International Enforcement Working Group

Report – August 2023

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 **(PCPD)**

Table of Contents

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 2022 – July 2023.

Heading towards its fourth 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 virtual GPA in 2020, with a total 35 official members, 3 observers and 3 members in the process of membership approval including many from regions not previously represented in the IEWG, such as: Latin America, Asia and Africa.

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. It has been sought in recent times that the approach will be more practical than theoretical, and this has been reflected in the publication of guides and manuals to materialize the cooperation; also in tools that allow sharing the importance of privacy 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 Safe Space Framework and Capacity Building Sessions, the active participation of members at the designated subgroups that focuses on Data Scrapping, Credential Stuffing, AdTech, the Enforcement Cooperation Repository, Cybersecurity etc.

Moving forward, and in line with the strategic priorities of the GPA from 2023 - 2025, the IEWG will look to maintain the momentum of its work, while also broadening its scope with a particular focus on: capacity building; further increasing the regional and linguistic diversity of the group; and exploring opportunities, with the Digital Citizen and Consumer Working Group, for operationalising cross-regulatory cooperation, including with other networks such as: Global Privacy Enforcement Network (GPEN), Asia Pacific Privacy Authorities (APPA), IberoAmerican Data Protection Network (RIPD), Association francophone des autorités de protection des données personnelles (ADAPDP), 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 41st 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 the reach out of other networks of data protection and privacy enforcement authorities.

In its third year (2021-2022), the IEWG advanced the goals of its thematic sub-working groups which culminated in the publication of guidance on Credential Stuffing and in the identification of principles that should govern the use of personal information in Facial Recognition Technology. The IEWG launched the Transnational Case Map which highlights in an innovative manner enforcement cooperation activities that have a transnational impact around the world.

In its fourth year (2022-2023), the IEWG completed and/or advanced goals in its multiple work streams. The year commenced with a highly successful Capacity Building workshop held in Istanbul where DPAs exchanged strategies and experiences on managing backlogs. Owing to the success of this workshop another has been planned for GPA Bermuda to cover Breach management and enforcement. The IEWG focused on maintaining the momentum of the WG's multiple work streams. Achievements included the final draft of the Data Scrapping letter, our Closed Enforcement Sessions regarding extra-territorial enforcement, cybersecurity, UK ICO's investigation on facial recognition technology company PimEyes, social media platform Tik-Tok and LLM ChatGPT, and began updating the Transnational Case Map with 2022 cases, among others.

Membership

From 2021 until 2023 the Superintendence of Industry and Commerce of Colombia (SIC) is in charge of the Secretariat, and the following authorities 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 2020 -2021 to 35 official members, 3 observers and 3 members in the process of membership approval (Spain, Kenya and Morocco) in 2022-2023.

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 2021-2023:

- ***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 - Develop 'safe space' enforcement cooperation frameworks focused on multinationals.
    - Objective 2 - Use of and evaluation of the framework in practice.
    - Objective 3 – Develop an annual "transnational case map" for authorities to use in order to learn from other colleague's work.
- ***Priority 2 – Tools***: Build on the previous work of the 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 – Analyse global PEA networks and make recommendations on coordination.
    - Objective 2 – Promote and strengthen the communication channels between PEA of each region.

- Objective 3 – Develop existing and new mutual observation agreements.
- Objective 4 – Improve our communication outreach for more of our members to participate in the activities put in place.
- Objective 5 – Translate to the best of our abilities and capacities of the products, conferences and different activities the group may have.

Liaison with the Strategic Direction Sub-Committee

In 2022-23, the IEWG continued to regularly update the Strategic Direction Sub-Committee (SDSC) on the progress of its work, in written quarterly reports. In March and August 2023, the IEWG participated in the ninth and tenth meeting of the SDSC to provide:

- further detail on the activity undertaken to advance the 2022-23 Strategic Plan (including the further development of the closed enforcement sessions, updates to the Transnational Case Map, and engagement with other networks);
- updates on aspects of the IEWG work with key links to the broader social, political, and economic debate (including work on Credential Stuffing, Data Scrapping, and interventions of chairs in press conferences and panel of other networks and AdTech); and

The IEWG co-chairs were pleased to receive positive feedback from members of the SDSC. Our next meeting with the SDSC is schedule for August 4th 2023.

Working Group Activities

SAFE SPACE FRAMEWORK/CLOSED ENFORCEMENT SESSIONS

In 2019-20, the IEWG took the first steps towards establishing itself as an active forum for enforcement cooperation on live and pressing issues. It did so through the development of safe space sessions. These provided a confidential environment for IEWG members to discuss emerging privacy and enforcement matters of global impact and explore collaborative opportunities.

The framework (developed by the UK ICO with support from the GRA and the EDPS) documents what the safe space sessions are and how and why they're run. It puts a structure around the sessions to make them more replicable and accessible for any IEWG member to participate or lead. It does this by:

- establishing three principles that underlie the development of sessions:
  - Global – focusing on issues of global impact,
  - Practical – encouraging consideration of options for cooperation,
  - Inclusive – urging proactive consideration of ways to engage members;
- setting out a flexible timetable for sessions across the year;
- explaining how to prepare to lead a session, including selecting an appropriate topic, setting objectives for the session, carrying out research and preparing background materials;

- describing how to run a session, including the provision of a template slide pack, and recommendations for chairing a discussion; and
- providing a process for following-up a session, including reviewing objectives, circulating a meeting note, and establishing sub-groups where appropriate.

Nowadays, regarding the 2022-23 work plan the same framework of the Sessions has been used; however, the terminology has changed. *'Closed enforcement session'* is the new name for the IEWG's safe space sessions, this new concept provides a confidential environment for IEWG members to discuss emerging privacy and enforcement matters of global impact, and explore collaborative opportunities., without losing the essence of the original Safe Space Sessions.

The IEWG conducted the following Closed Enforcement Sessions during the reporting year:

- November 10th 2022 - Extraterritorial Enforcement Cooperation.
- February 2nd 2023 – UK ICO's investigation on the facial recognition technology company PimEyes
- May 11th 2023 – DPA actions regarding Tik-Tok and ChatGPT.
- June 29th 2023 – Cybersecurity.

ADTECH SUBGROUP

An Adtech Subgroup was created in April 2022 following the first session in March. With this meeting, the group was officially formed, 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.

Currently the lines of action are seeking for champions leaders, until finding those, the secretariat is leading all this matters.

DATA SCRAPPING

With issue linkages to the 'global incident' session chaired by the PCPD Hong Kong in May 2021 regarding the Facebook data scraping incident, in June 2021, the OAIC led a safe space session on the topic of data scraping – the practice of extracting data from websites and public facing access points. The session's objectives were to raise awareness of the issue, better understand members' policy and enforcement positions, and gauge appetite for cooperative action. Participants discussed relevant aspects of their domestic laws and closed enforcement cases to help inform how to characterize instances of data scraping and considered whether joint regulatory intervention of some form would

be appropriate. Following the session, several IEWG members indicated appetite to be party to further work to consider and progress joint activity on the topic, and the OAIC has established an IEWG subgroup for that purpose.

Current Status

After working with our members, gathering some feedback, OAIC and the OPC circulated the final draft of the *Data Scrapping Joint Statement* in July 2023. The *Joint statement on data scraping and the protection of privacy* is endorsed by the members of the IEWG from the following jurisdictions: Australia, United Kingdom, Switzerland, New Zealand, Jersey, Colombia, Norway, Hong Kong, Morocco, Argentina, Mexico, and Canada. The Joint Statement was issued in August 2023. It was also directly sent to various companies running social media platforms.

TRANSNATIONAL CASE MAP[1]

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.

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 was once again submitted for the Global Privacy Assembly 2023 Awards for the *Dispute Resolution and Enforcement* category. This year, we have asked once again our members to submit all the cases that in 2022 the DPA had regarding transnational implications. The updates to the map are being worked on.

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

CYBERSECURITY

At the 44th GPA in Istanbul in October 2022, the GPA adopted a resolution on cybersecurity. This tasked the IEWG with developing an understanding of the remits and responsibilities of GPA members in relation to cybersecurity, and exploring possibilities for international cooperation.

The GPA cybersecurity sub-group was established in December 2022 to deliver the resolution's commitments. The sub-group is coordinated by the UK Information Commissioner's Office and currently comprises 16 GPA members. A cybersecurity survey has been conducted amongst the DPAs, and the UK ICO chaired a Closed Enforcement Session in June 2023. A number of short and long term goals for the sub-group have been identified and will be continued to be progressed.

Background

At the Assembly in Istanbul in October 2022, the GPA adopted a resolution on cybersecurity. This tasked the IEWG with developing an understanding of the remits and responsibilities of GPA members in relation to cybersecurity, and exploring possibilities for international cooperation.

A GPA cybersecurity sub-group was established in December 2022 to deliver the resolution's commitments. The sub-group, coordinated by the UK Information Commissioner's Office, comprised 16 GPA members:

- Australia - Office of the Australian Information Commissioner
- Canada – Information and Privacy Commissioner of Ontario
- Canada – Office of the Privacy Commissioner of Canada
- Catalonia – Data Protection Authority
- Estonia – Data Protection Inspectorate
- France – National Commission for Informatics and Liberties
- Gibraltar – Gibraltar Regulatory Authority
- Hong Kong, China – Office of the Privacy Commissioner for Personal Data

- Israel – Privacy Protection Authority
- Japan – Personal Information Protection Commission
- Philippines – National Privacy Commission
- Switzerland – Swiss Federal Data Protection and Information Commissioner
- Uruguay – Personal Data Regulatory and Control Unit
- UK – Information Commissioner's Office
- USA – Department of Justice, Office of Privacy and Civil Liberties
- USA – Federal Trade Commission

In January 2023, the sub-group agreed an action plan to progress its work. The key activities carried out under the action plan were the circulation of an all GPA-member survey, and delivery of an IEWG closed enforcement session on cybersecurity.

Survey

To meet the first commitment in the cyber resolution – developing a better understanding of GPA members' cyber remits – between February and April 2023, the cybersecurity sub-group drafted, circulated, and analyzed responses to an all GPA-member survey.

46 GPA members, from five continents, responded to the survey. This provided a valuable snapshot of the cybersecurity regulatory landscape across GPA member jurisdictions, the extent to which data protection and privacy authorities' (DPAs') competencies overlap with national cybersecurity authorities, and the maturity of cooperation across the regimes. Key findings from the survey were:

- Over three quarters of respondents reported that their jurisdictions have one or more cybersecurity law and cybersecurity authority.
- Just under a third of DPAs have competence, for a range of activities, under their jurisdictions' cybersecurity laws, in addition to responsibilities under their data protection / privacy laws (DP laws)
- This creates overlaps between requirements in DP laws and cybersecurity laws, and between the competencies of DPAs and cybersecurity authorities. For example:
    - Almost all responses indicated the existence of duplicate breach reporting requirements, with varying timeframes and thresholds for reporting.
    - Almost half of respondents do not have responsibility for incident response under DP laws, but it is one of the most common tasks DPAs reported having under their jurisdictions' cybersecurity laws.
- To manage potential conflicts such as these, most DPAs are collaborating with their domestic cybersecurity authorities, particularly their jurisdictions' national CSIRT / CERT (Computer Security Incident Response Team / Computer Emergency Response Team).
- Responses show that collaboration between DPAs and cybersecurity authorities is primarily focused on policy and engagement activity, rather than operational joint working (such as thereat analysis or investigations).

- Key challenges to cooperation are limited resources, and difficulty of engaging cybersecurity authorities.
- Far fewer DPAs collaborate internationally on cybersecurity matters than domestically. Where international collaboration does happen, it is primarily between national DPAs, and occasionally with others such as standards bodies and supranational organizations. Limited resources and lack of legislative power are most often cited as challenges to international cooperation.

To support the GPA membership in better understanding the cybersecurity responsibilities and activities of fellow GPA members, a more detailed report of the survey's findings was circulated by the GPA Secretariat in May 2023. This is also available in the GPA's Enforcement Cooperation Repository, here [add link when live].

Closed enforcement session

To meet the second commitment in the cyber resolution – exploring possibilities for international cooperation – the GPA cybersecurity sub-group ran an IEWG closed enforcement session in June 2023. Objectives for the session were to build on the survey by providing a space for capacity building, exchange of expertise, and exploring scope and options for further collaboration and next steps on cybersecurity.

Participants enjoyed a fruitful session with GPA members sharing invaluable experience of a broad range of regulatory activities on cybersecurity, including: development of a single environment for cyber incident notification; operational DPA-CSIRT collaboration and joint onsite inspections; and industry consultation to promote use of privacy preserving techniques in common or high risk cybersecurity products and solutions.

Looking ahead, to build on the work of the cybersecurity sub-group, participants discussed a range of possibilities for further engagement and cooperation on the topic. Some authorities also provided their views in writing after the session to help inform next steps.

Members were in favour of maintaining the momentum built in 2023, and keen to exploit the broad interest in cybersecurity across the GPA, demonstrated by the large number of authorities that participated directly in the cybersecurity sub-group, and contributed via response to the survey.

Authorities generally expressed a preference to maintain use of informal mechanisms to support further collaboration in the shorter-term, but recognized that the global nature of cyber threats, and the common security principles in our DP laws, make cybersecurity an area ripe for further cross-border supervisory cooperation on breaches and incidents.

There was therefore broad consensus on the value of maintaining, and expanding, a community of interested DPAs on cybersecurity, and identifying appropriate opportunities to leverage that resource for tangible operational and capacity building activities.

Recommendations

On behalf of the IEWG, and based on the findings from the work carried out in 2023, the cybersecurity sub-group recommends to the Assembly the following actions for further international activity on cybersecurity:

1. Community of Practice
    - Engage with GPEN with a view to establishing a GPA-GPEN cross-network Cybersecurity Community of Practice. This would allow us to:
        - leverage the GPA's broad membership and appetite for collaboration on cybersecurity, and GPEN's invaluable infrastructure (including secure online forums) and activities (such as teleconferences and practitioner events); and
        - support senior and staff-level (e.g., investigators, technologists) networking, bilateral and multilateral relationship development, and capacity building in relation to cybersecurity.
    - Longer-term, the community may wish to further explore possibilities for:
        - development of joint statements on common cybersecurity concerns and expectations or best practices;
        - further international mapping to build a more comprehensive picture of the full range of bodies with cybersecurity competencies, across regulatory regimes and other sectors; and
        - establishing the community on a more formal footing, such as a GPA Working Group, if appropriate.

2. Convergence and guidance
    - Working towards promotion of convergence and alignment, compare:
        - respective breach report forms, the information requested, and how this informs investigatory lines of enquiry; and
        - strategies and factors in evaluating risk of harm from breaches.
    - Based on this, work towards development of guidance and / or a checklist for investigations of cyber breaches and incidents.
    - Promote the guidance through Cybersecurity Community of Practice-led capacity building sessions, and with other networks via GPEN's Network of Networks initiative.

The IEWG invites the GPA 2023 Closed Session in Bermuda to acknowledge and accept these recommendations in its adoption of the IEWG Annual Report.

ENFORCEMENT COOPERATION HANDBOOK

The GPA's Enforcement Cooperation Handbook was originally created in 2015 and updated in 2016. Based on contributions and experiences of members from across the GPA, it provides guidance and a

common foundation for authorities wishing to engage in enforcement cooperation. It sets out: the issues an authority may face in preparing for, and engaging in, enforcement cooperation; models, approaches, and solutions to address such issues; and how to choose appropriate strategies in different circumstances.

Working with colleagues in the Digital Citizen and Consumer Working Group (DCCWG), the IEWG undertook in 2021 several activities to deliver the objective of updating the Handbook to reflect the wealth of experience gained and lessons learned through enforcement cooperation since it was last updated, both between data protection / privacy enforcement authorities and in a cross-regulatory context. This work has been undertaken by the OPC (overall lead), the SIC and the JOIC, with additional support from the UK ICO.

To better understand how the Handbook has been used by authorities, what works well and what areas of improvement there might be, the OPC developed a survey which was circulated, key findings from this analysis included:

- Most respondents indicated they had the legal and practical ability to cooperate, including in a cross-regulatory context, but there were limited concrete examples provided of cooperation on specific investigations.
- Most respondents also reported that they had not actually used the handbook to support them in cooperation enforcement projects.
- Many respondents were keen for real-world examples of how to apply the theoretical concepts encompassed in the handbook in practice.

Based on these findings, the updated version of the Handbook was shared with all GPA members at the Assembly of 2021 in Mexico. In this version, the suggestions proposed by all members were sought to be implemented, considering the geographic and legislative diversity of each of the authorities.

New cases of cooperation between authorities were included and reflected in the new handbook, experiences regarding the covid-19 pandemic were shared, and the outlines of "how to understand cooperation" were improved. Memorandums of understanding were shared as an example for authorities to follow, among other topics.

During the first semester of 2023, the IEWG and the DCCWG worked on a survey regarding GPA members' experiences in regulatory collaborations with other DPAs and cross-regulatory collaborations with regulatory authorities in the competition/anti-trust and consumer protection spheres that operate in their jurisdictions. We are now analyzing the result, which we hope to publish soon. Once those results have been socialized we will proceed to take action in the matter, hence updating our cooperation handbook.

CAPACITY BUILDING WORKSHOP ON INVESTIGATIONS' BACKLOG MANAGEMENT

The International Enforcement Cooperation Working Group ("IEWG") organized, in collaboration with the Asia Pacific Privacy Authorities ("APPA"), the Association francophone des autorités de protection

des données personnelles (“AFAPDP”) and the Global Privacy Enforcement Network (“GPEN”), a capacity building workshop on the margins of the 44th Closed session of the Global Privacy Assembly.

During this workshop, the Office of the Privacy Commissioner of Canada (“OPC”), the Information Commissioner’s Office of the United Kingdom (“ICO”), la Commission Informatique et Liberté of France (“CNIL”), the Personal Information Protection Commission of Japan (“PPC”) and the Office of the Privacy Commissioner for Personal Data of Hong Kong (“PCPD”) shared their experiences and strategies regarding the management of investigation backlogs.

The motivation for the topic stems from the fact that most data protection authorities face a daily challenge to manage the influx of a growing number of complaints that outpace existing enforcement capacities. This imbalance translates naturally into the extension of the delays to process complaints and in the emergence of complaint backlogs.

Backlogs can be caused by many factors. Examples include:

• A significant increase in the influx of complaints. For example, the entry into application of the General Data protection regulation (“GDPR”) in Europe caused a 75% increase of the number of complaints filed with the CNIL (from 8000 to 14000).

• The obligation to assess and examine all complaints (where required under law), which can cause valuable resources to be assigned to frivolous complaints and cases with low impact on individuals’ privacy rights.

• The complexity of certain files that may require multi-disciplinary teams and therefore longer timeframes to examine and conclude the corresponding investigations.

• The difficulty, resistance and delays in receiving comprehensive information and documentation from data controllers.

Strategies to manage the backlog

With multiple factors contributing to Backlogs, regulators should consider a series of strategies to avoid, manage and mitigate their occurrence. Strategies shared include:

Reducing the influx of complaints and foster their admissibility

To reduce the influx of the complaints, regulators may educate individuals, manage their expectations (re. available remedies) and provide them with self-service tools to help them file comprehensive and admissible complaints. This can help ensure that complaints received are both relevant and properly constituted, thus avoiding the resource cost of processing complaints that are incomplete or outside of jurisdiction.

PPC Japan also advised that the upfront narrowing of the scope of breaches that warrant notification to the regulator, and setting (and maintaining) firm deadlines to submit breach reports and associated correspondence can also mitigate the length of investigations and provide discipline to the investigation process.

Adjusting complaint-handling processes and the investigation team organization

Privacy Authorities need to decide which risks they are willing to take. Although, all authorities aim to produce the highest quality products, they may consider assuming a greater risk of not exhaustively investigating every complaint and compare it to the risk of having unacceptable complaint delays and backlogs, which can put the credibility and reputation of authorities at risk, and increase risk to individuals by delaying remediation.

To this end, the CNIL shared how they had adjusted the complaints handling process and the organization of the investigative team to include a risk-based triage phase that expediates non-admissible complaints (one third of CNIL's cases are considered inadmissible). They then assign complaints to different teams based on the complexity of the complaints, the novelty of the topics at issue, the degree of impact on individuals and the experience of the investigators in the teams. Along similar lines, two-thirds of OPC's complaints are closed at the early resolution phase. Files are triaged and those of lower complexity or lower privacy impact are generally directed to a team who specialize in expedient resolution.

Similarly, to the extent that discretion allows, a regulator should tailor its efforts and actions to the importance of the complaints - for example: set aside very low priority cases or settle them with a warning or advisory letter without an intensive investigation; assign less experienced investigators to minor cases, and save more skilled investigators and a multi-disciplinary team to more impactful cases. In relation to this point, PCPD Hong Kong shared that it proactively screens out frivolous complaints and attempts to resolve the matters by contacting complainants to raise their awareness on the principles that govern the processing of personal data in Hong Kong. PCPD added that for the sake of greater efficiency, legal counsels are brought in at the early stages of any investigation involving complex or novel issues.

Identifying and automating repetitive tasks

Employ the use of template letters to close recurrent straightforward issues, such as: receiving direct marketing messages, video-surveillance in dwelling, etc.

Adjust the processing capacity to match the influx of cases

Extend the capacity and the efficiency of the investigative team by hiring subcontractors for dedicated complaints resolution functions. It is important to monitor and foster productivity by setting clear contractual requirements for the number of file closures under what timelines and corresponding monitoring indicators. For example, the CNIL outsources 28% of its low-risk complaints to a service provider who was contractually obliged to close the complaints within a two-week timeframe.

Foster and monitor productivity

The UK ICO sets deadlines and Key Performance Indicators (or KPIs) for each stage of the investigative process, leverages its powers to compel data controllers to respond to its requests in a timely manner and has its files' progress monitored by senior managers every two weeks.

PPC Japan noted the importance of dedicated and ongoing training for investigators (especially in light of continuous tech advances) and the efficiency of having all phases of a specific case dealt with by the same employee. On average, each PPC staff member processes 400 cases each year. Similarly, OPC Canada finds that file transfers from one investigator to another should be minimized, as they often cause significant delays with momentum lost while a new investigator familiarizes themselves with a file.

Finally, having files approved by a limited number of individuals should be avoided. Regulators can minimize potential bottlenecks by delegating decisions based on risk, complexity, sensible criteria, etc.

Summary

Several participants opined that this workshop represents the type of event and discussions that should be reproduced among GPA's members either during or on the margins of the GPA conference. This workshop demonstrated how all regulators face similar operational challenges and that sharing their perspectives will allow them to learn from each other's experiences, both successful and otherwise. To that end, it has been further suggested that the IEWG reintroduce the annual in-person GPA Enforcement Collaboration meeting that can then focus on common operational risks, challenges and associated solutions. The IEWG is exploring such an event in the coming year.

Forward looking plan 2023

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

- Capacity building workshops (with our members and with other regional networks).
- Continue developing the Transnational Case Map to display cases with different scenarios so that it can begin to fulfil its role as a source of information for the community.
- Display the map in different scenarios so that it can begin to fulfil its role as a source of information for the community.
- Strengthen the four lines of work of the AdTech SubGroup and nurture ongoing efforts of the Cybersecurity Subgroup.
- Identify the important and urgent topics for our closed enforcement sessions.
- Help our members to better understand and use our recently updated Cooperation Handbook.
- Hold our governance meeting in which the Co-Chairs for 2024-2026 and the Secretariat will be elected.

Conclusion

The IEWG has managed 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 materialise in this last period the ideas and initiatives that have been shaped more than a year ago, such as:

- Multiple Closed Enforcement Sessions on emerging privacy issues
- The Resolution on FRT.
- Final draft of the Data Scrapping Joint Statement.
- Ongoing efforts to nurture the Enforcement Cooperation Handbook.
- Updating our Transnational Map.
- Newly created Cybersecurity working group.
- Capacity building workshops on operational activities.
- Delivering on the GPA's cybersecurity resolution.

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 December of 2023, as will the secretariat.