



GPA
Global Privacy Assembly

NEWSLETTER

Volume 9 • Issue 2 • Philippines • 2026

Protection Supervisor - Data Breach Awareness C
Cyberattack Exercise PATF CIA
Data Breach Awareness Security Incident



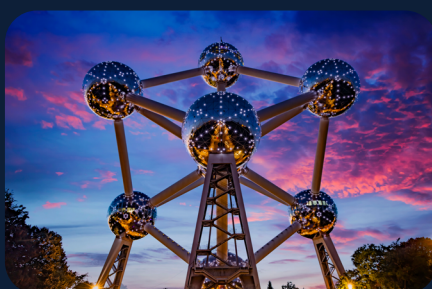
**EDPS on challenges to
personal data breach
management**



Get to know your
Executive Committee
Paul Vane



48th Global Privacy Assembly
Annual Conference



Building trust in the digital
age



Table of Contents

3

Update from the Chair

Philippe Dufresne
Chair of the Global Privacy Assembly
and Privacy Commissioner of Canada

5

Get to know your ExCo

Paul Vane
Jersey Information Commissioner

7

In Conversation with

EDPS on challenges to personal
data breach management

10

Welcome to the four newest members of the Global Privacy Assembly!

11

Meet our member

Building trust in the digital age

13

48th Global Privacy Assembly Annual Conference

Update from the Chair

Philippe Dufresne

Chair of the Global Privacy Assembly and Privacy Commissioner of Canada

Dear colleagues,

I would like to express my appreciation to all of the member data protection and privacy authorities who have reached out to share ideas and feedback with me during my first eight months as Chair of the Global Privacy Assembly (GPA). I am also grateful for the support and expertise of the GPA Secretariat at the National Privacy Commission in the Philippines, and of my colleagues on the Executive Committee (ExCo). They have been instrumental in helping me to integrate into my role and are actively collaborating to advance our shared vision to promote and enhance global cooperation and dialogue on privacy and data protection issues.

I am excited to work with you to evolve this Assembly, to strengthen the impact of our collective voices, and to provide more value for the entire membership. Some of the recent initiatives that the GPA Chair, ExCo, and Secretariat have been focused on include:

New ExCo subcommittees

To help progress the work of the ExCo and the functioning of the GPA, the ExCo has established four subcommittees, each with 2026-specific mandates and objectives.

The **Strategic Direction Subcommittee**, as set out in the GPA Rules and Procedures, will coordinate the strategic direction of the GPA, including leading engagement with members to develop the GPA Strategic Plan.

The **Accreditation Subcommittee** is responsible for reviewing accreditation applications. It has already revised the application and assessment forms for both member and observer applications to strengthen the reporting process to members.

These new forms have been implemented and will be available on the GPA website soon.

The **Host-Selection Subcommittee** will select the host for the 50th Annual Conference in 2028.

For the first time, the ExCo has established a **Financial Audit Subcommittee** aimed at providing increased financial transparency and accountability to GPA membership fee collection and expenditures, and at strengthening the GPA's financial position. The Secretariat recently launched a Terms of Reference to solicit bids for an external financial auditing firm.

The mandates and action plans for the subcommittees are available on the GPA's new member-only webpage.

Member's access webpage

The Secretariat recently launched a [members-only space on the GPA website](#) where you can view and download documents such as draft resolutions and supporting materials, award applications, and ExCo minutes. The intention is to continue to develop this exclusive space to facilitate collaboration among members, observers, working groups, and the Secretariat.

Welcoming a new ExCo member

Last month, GPA members elected a new ExCo member to fill a vacated seat until the 2027 Closed Session. I would like to thank the five authorities who put forward their candidacy, and congratulate the **Office of the Data Protection Authority of Guernsey** for being elected as our newest Executive Committee member.

Please join us in welcoming their representative, **Commissioner Brent Homan**, into this important leadership role.

On behalf of ExCo and the Secretariat, I would like to thank Dr. Lela Janashvili for her service and the expertise that she has shared with the GPA. I would also like to express my gratitude to the Secretariat for their advice and guidance, and their support to ensure a democratic and transparent election process.

48th GPA Annual Conference

The 48th GPA Annual Conference (GPA48) will take place during the week of November 16, 2026, co-located in Brussels, Belgium, with the IAPP Europe Congress 2026.

The convergence of the 48th GPA Annual Conference with the IAPP Europe Congress 2026 in Brussels will create opportunities for rich, dynamic programming and engagement to learn and build relationships within the data protection and privacy community. I am grateful for the support of the IAPP as well as the European Commissioner and the European Data Protection Board.

I know that many of you are eager to book your travel and accommodations. We are still confirming if there will be a welcome event on the evening of November 15, but the dates and venues for the Closed Session and Open Programme are firm.

- The GPA Chair and ExCo, with the support of the GPA Secretariat, will host the Closed Session for GPA members and a limited number of official observers on Monday, November 16, and Tuesday, November 17 at the [Albert Borschette Congress Centre](#), European Commission.
- On Wednesday, November 18, and Thursday, November 19, a GPA Open Programme will be offered as part of the IAPP Europe Congress 2026 at the [SQUARE Brussels Convention Centre](#).

All GPA Closed Session attendees will have access to the entire IAPP Europe Congress, including the GPA Open Programme.

More information can be found on the [conference webpage](#), including details on the registration process for GPA Members. The website will continue to be updated as full program details are confirmed.

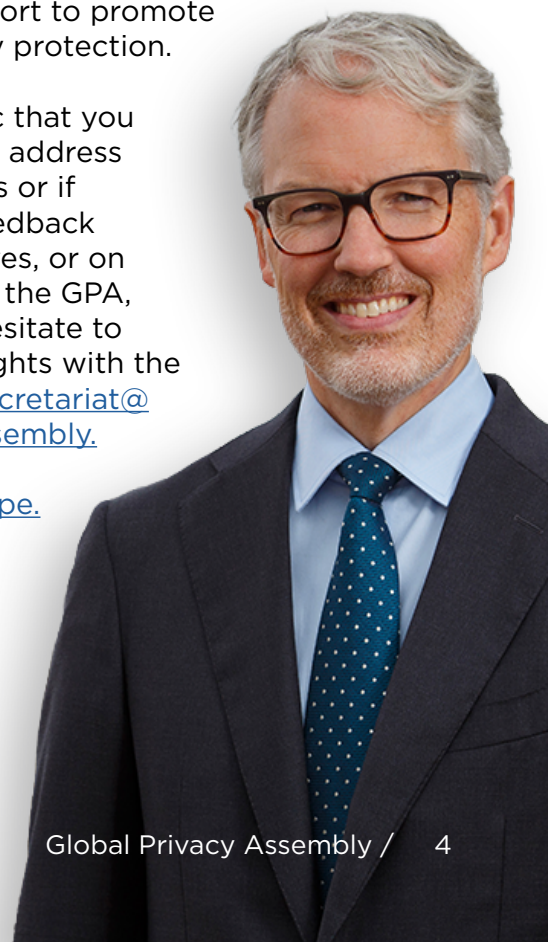
Privacy and Human Rights Award

I was saddened to learn about the sudden cancellation of RightsCon 2026 in Lusaka, Zambia that was to take place at the beginning of May. The cancellation has delayed the announcement of the winner of the 2026 [Privacy and Human Rights Award](#), which the GPA created in collaboration with Access Now, the organizer of RightsCon. We will announce the 2026 Award recipient in the near future.

Conclusion

This is just a snapshot of the work of your ExCo and Secretariat to support the GPA and its vision to help empower members to achieve their respective mandates, and advance a united global effort to promote data and privacy protection.

If there is a topic that you would like me to address in future updates or if you have any feedback on these initiatives, or on the operation of the GPA, please do not hesitate to share your thoughts with the Secretariat at secretariat@globalprivacyassembly.com, or with me directly at Philippe.Dufresne@priv.gc.ca.



Paul Vane

Jersey Information Commissioner

As Jersey's Information Commissioner, I am immensely proud to be serving as a Member of the Executive Committee of the Global Privacy Assembly. Serving on the committee is not only a great honour for me personally but also a major step in cementing Jersey's place as part of the international data protection community.

How did you become involved in Privacy and Data Protection?

I've been interested in security, regulation and most importantly, safeguarding individuals, for as long as I can remember. I've always been fascinated by people, what makes them tick and what drives them to behave in certain ways and that carries naturally into data protection and privacy. That's why I've always insisted we're people protectors, not data protectors. My professional background has always, to some extent, been related to regulation and law enforcement. In my early career I worked as a Compliance Manager and Policy and Legal Manager at the Jersey Financial Services Commission. Prior to that, I was a police officer for the States of Jersey Police, honing investigation skills I still use today. It was by chance and luck I fell into data protection and it was a subject I'd always been keen to find out more about. I happened to bump into esteemed former commissioner Emma Martins at a seminar in Jersey and at the time, Emma was recruiting. As I was preparing for the interview, it became very clear data protection wasn't just about complaints but it was human rights related. It was all about people and that peaked my interest. I gave it my all for the interview, got the job and 22 years later, I'm still here! My passion for our subject is what drives me. I wouldn't want to do any other job outside of this field. Data protection and privacy is all encompassing and touches every aspect of people's lives. I also love the fact every day is different.



What have been the key landmarks on your Career and Data Protection Journey?

I moved to the JOIC in 2004 and held the position of Deputy Commissioner from 2004 until 2021. Always keen to further my learning, I studied for a Bachelor of Arts with Honours degree in Social Policy and Criminology from the United Kingdom's Open University, between 2012 and 2018. There have been many industry milestones along the way but those that stand out for me personally, are the Jersey Adequacy assessment in 2008 and our independence from the Government of Jersey. Of course the General Data Protection Regulation, our equivalent Data Protection (Jersey) Law 2018 and its accompanying laws, which changed the landscape. It's hard to believe when data protection law first came into effect, we were still in only the first decade of the internet, so what a change so many of us have experienced. The big game changer after that was undoubtedly the pandemic and how that changed the world. So we've had some pretty huge challenges to contend with across a quarter of a century haven't we!

What are your perspectives on the evolving Global Privacy Landscape?

With Artificial Intelligence now embedded in our operations, supply chains, customer service and decision-making, we are all acutely aware we're without doubt, witnessing one of the most transformative technological revolutions since the invention of the internet. But productivity gains mean little if they come at the expense of customer trust and I believe we stand at a crossroads. One path leads to extraordinary productivity and the other risks eroding trust and confidence if we fail to protect the fundamental rights and principles of data protection and privacy that underpin our digital lives. My belief is privacy and AI aren't opposing forces. They're complementary pillars of trustworthy innovation and the leaders of tomorrow will be those who treat them as such. By working together to ensure privacy is embedded into the heart of AI development and adoption, we can ensure that the future of productivity is one we can all share in — inclusively, confidently, securely, and ethically. I believe in a rapidly changing landscape, it is vital the GPA remains agile enough to tackle the data protection and privacy issues arising from emerging technologies such as AI, facial and emotional recognition technologies and synthetic media. I believe we must also be at the forefront of policy development in areas such as protecting children's data online, securing simple but robust data sharing mechanisms and enforcement of data protection legislation. As a member of the Executive Committee, my role is to contribute the Jersey Authority's voice to furthering those critically important discussions and policy areas. I believe the collective skills, experience and knowledge among GPA peers cannot be underestimated.

Finally, what are your Leadership Insights?

Never underestimate the importance of bringing your team with you, believing in and investing in your team and treating them well. When growing a team, I would advise not doing so too quickly. Allow time for the team dynamic to settle and recruit not just for skillset but for team fit. I think it's hugely important to find the right people and look after them. I look forward to continuing to work with Commissioner Dufresne and the Executive to further the GPA's vitally important work. I can be contacted at p.vane@jerseyoic.org or via LinkedIn.

EDPS on challenges to personal data breach management

2026 will mark ten years since the adoption of the General Data Protection Regulation (GDPR) in the European Union, which introduced clear obligations for organisations to manage and report security incidents involving personal data breaches. Similar requirements exist for European Union institutions (under their dedicated Regulation¹) and worldwide, either explicitly for personal data breaches or for significant security incidents. While these frameworks have led to high-profile enforcement actions and increased public awareness as well as limited fragmentation of law, many organisations continue to struggle with personal data breach management. Most organisations have implemented breach-response procedures to meet notification obligations, yet at the European Data Protection Supervisor (EDPS)² we still observe underlying weaknesses that

hinder timely reporting, heighten risks for individuals, and expose deeper organisational shortcomings.

Over-reliance on IT-centric management

When the handling of security incidents is primarily IT-driven, several issues commonly arise:

- Failure to timely escalate security incidents to the data protection function and management.
- Lack of the *data-subject-at-the-centre* approach, with security incident risk assessment focusing mainly on the effectiveness of mitigation measures to contain the incident rather than reducing harm to affected individuals.

Organisations need stronger cross-functional collaboration and shared risk-management tools. This becomes even more pressing in a technological environment that is increasingly complex (e.g. AI operations) and highly interconnected (e.g. interoperability frameworks).

Incomplete and biased risk assessments where the risks for the organisation prevail over the risk of the individuals

At the EDPS, we recognise that risk assessment is not an exact science, yet many organisations treat it as a purely arithmetic



¹ The EDPS manages the submitted personal data breach notifications framed by the Article 34 and 35 of Regulation (EU) 2018/1725: all European Institutions have a duty to report personal data breaches to EDPS, unless a risk is unlikely to affect the concerned data subjects' fundamental rights and freedoms.

² The EDPS is an independent institution of the EU, responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies, as well as for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data.

exercise. A common misconception - often a bias - is that certain categories of personal data such as contact details, job titles or internal identifiers are inherently harmless and therefore present a low risk to individuals. However, harm stems not only from the data's sensitivity but also from the context of the breach. Even seemingly innocuous data can expose individuals to phishing, targeted scams or unintended inferences, particularly when vulnerable groups are involved.

Organisations therefore need mature breach-response processes capable of assessing both actual and potential harm in context, moving beyond simplistic labels or an over-reliance on the number of affected individuals.

Absence of robust plans to communicate with individuals

In Europe and in many jurisdictions worldwide, controllers must inform affected individuals when a breach presents a high risk to their fundamental rights and freedoms³. Legislation outlines the required content of such notifications.

Despite this, few organisations maintain documented procedures governing breach communication. Clear allocation of roles, predefined templates, or guidance on effective communication channels remain uncommon. Communications often provide vague descriptions of the breach and associated risks, failing to address the specific implications for different recipients. Too frequently, the content focuses on portraying the organisation as the victim, rather than helping individuals understand how to protect themselves.

Organisations must approach breach communication with the same rigour applied to business continuity, prioritising transparency to protect stakeholders and maintain trust.

Failure to learn from past incidents

Many organisations treat breaches as isolated incidents, addressed through a compliance 'tick-box' approach. However, recurring issues - such as repeated device loss or recurring misconfigurations - signal deeper systemic deficiencies. Breaches should instead be viewed as opportunities to strengthen organisational security controls, training and governance.

The EDPS hands-on awareness campaign

These observations highlight the importance of Supervisory Authorities acting as knowledge facilitators. The EDPS incorporated these observations into our awareness campaign, focusing on active participation and learning activities, which was recently awarded by the Global Privacy Assembly.



Our first project, the **PATRICIA** exercise, brings together technicians, security officers and data protection officers to work through a detailed cyberattack scenario. Each participant receives different pieces of information, interpreted uniquely from their professional perspective, demonstrating the necessity of collaboration between functions

³ For EU institutions, communications requirements are provided in Article 35(2) of Regulation (EU) 2018/1725.

that often operate in isolation. By applying internal procedures in a simulated crisis, participants could identify gaps in communication channels, tools and manuals - essential insights for the effective real-world breach management.

The second initiative, the **Data Breach Management Awareness Campaign**, assessed the maturity of organisations' breach-management practices. Selected EU institutions completed two self-assessment questionnaires designed to go beyond verifying the existence of procedures, followed by face-to-face discussions and evaluations supported by the EDPS. Participants gained a clear understanding of weaknesses in their structures and processes and received tailored recommendations to improve compliance, accountability and operational readiness.

The EDPS remains committed to practical training actions that cultivate accountability, clarity and ongoing learning. Such efforts not only ensure regulatory compliance but also reinforce trust in an increasingly data-driven society. Without a consistent learning cycle, organisations risk remaining in a reactive rather than proactive posture towards personal data protection.



Welcome

to the four newest members
of the Global Privacy Assembly!

**Personal Data
Protection
Commission**
(Singapore)

**Office of the
Information
Commissioner**
(Jamaica)

**Superintendence of
Personal Data
Protection**
(Ecuador)

**Saudi Data &
AI Authority**
(Saudi Arabia)

We look forward to working with you to strengthen our collective voice to promote and advance privacy globally, and to learning more about your work!

Building trust in the digital age

PDPC Singapore

Since our establishment in 2013, the Singapore's Personal Data Protection Commission (PDPC) has had a clear mission: balance the protection of individuals' personal data whilst supporting businesses to thrive amidst global developments in the digital economy. As the digital landscape rapidly evolves, so does our work to ensure trust is the foundation upon which innovation and opportunity are built.

Protection and Innovation: Two Sides of the Same Coin

The misconception that data protection hinders innovation is fading fast. As businesses increasingly adopt and integrate technologies and as data use and sharing become more pervasive, we see how protection and innovation mutually reinforce each other, rather than opposing forces.

With emerging technologies like Artificial Intelligence (AI) maturing rapidly, data protection has become a key enabler to building the trust that is crucial for economic growth and progress. Our goal is to build an environment where innovation thrives

precisely because individuals trust how their data is protected and used.

Singapore plays an active role in shaping regional dialogue and fostering a shared understanding of how protection and innovation can progress together. This is seen in our active participation in regional and international forums, and most notably our hosting of the Personal Data Protection (PDP) Week alongside the IAPP Asia Forum, where we bring the data protection ecosystem together to explore how responsible use of data can unlock potential for all.

Through its anchor events ranging from data protection to Privacy-Enhancing Technologies (PETs) and AI, this year's [PDP Week](#) gathered more than 2,000 data protection professionals, industry leaders, regulators and policymakers from over 30 countries in Singapore to share honest conversations about the current and future state of the data protection landscape.

These conversations, and the scale and diversity of participation, reflects the region's



shared recognition that trust, assurance, and clarity are not barriers – they are what powers innovation.

Collaborative Approach to Global Challenges

Collaboration is not just something we do – it is also how we think. We believe in building convergence where we can, whilst respecting that different jurisdictions have different social and cultural norms. Data protection and privacy are universal values, but how they are expressed and implemented will naturally vary based on local contexts and priorities.

Similarly, this collaborative spirit shapes our international work. Since July 2024, we have served as Secretariat of the Asia Pacific Privacy Authorities (APPA) Forum and chair both the APPA Governance Committee and Technology Working Group. We will continue to facilitate dialogue amongst data protection authorities across the Asia-Pacific region, coordinate responses to shared challenges, and help build capacity amongst emerging data protection authorities.

Within ASEAN, Singapore chairs the Working Group on Digital Data Governance. Together with regional partners, we are strengthening data governance frameworks, developing robust data ecosystems, and facilitating trusted cross-border data flows that support regional economic integration. The ASEAN Data Management Framework and ASEAN Model Contractual Clauses (MCCs) are good examples of what members of ASEAN have achieved through these efforts.

We are also Deputy Chair of the Global Cross Border Privacy Rules (GCBPR) Forum's Global Forum Assembly, helping to guide the development and implementation of this leading global certification system to facilitate more responsible data transfers.

Deepening Partnership Through GPA Membership

We have been regular participants at the Global Privacy Assembly's annual conferences since our establishment, contributing to discussions on emerging privacy challenges. At the 47th Global Privacy Assembly in Seoul,

we presented updates on the APPA Forum's work and facilitated productive exchanges between the GPA and APPA networks.

Now, we are excited to deepen this partnership as a GPA member. We see this as a natural progression in our international engagement and reflects our commitment to contribute meaningfully to global discussions.

What do we bring to the table?

We aim to contribute fresh perspectives drawn from Singapore's experience as a global city-state deeply integrated into international systems. We want to share insights from our regulatory journey, learn from global best practices, and forge productive collaborations within the broader GPA network.

We are particularly interested in advancing discussions on AI governance, promoting interoperable frameworks and privacy enhancing technologies to facilitate responsible data use and sharing, and supporting capacity building amongst data protection authorities worldwide. On privacy-enhancing technologies specifically, we have worked with organisations across diverse sectors – from fintech, adtech to building management companies – exploring practical applications of PETs in real-world contexts. These experiences have given us valuable insights into the opportunities and challenges of implementing PETs. We are keen to advance this work through the GPA, exchanging learnings with other data protection authorities and contributing to discussions on how PETs can enable more responsible data sharing whilst maintaining strong privacy protection.

Here is what we believe: as data protection challenges grow more complex and interconnected, no single authority can tackle them alone. The GPA provides an invaluable platform for collective action, knowledge exchange, and policy coordination. We are excited to contribute to this vital work, bringing Singapore's collaborative approach and regional insights to help build a better, more trusted global data protection ecosystem.

48th Global Privacy Assembly Annual Conference

Get ready for the **48th Global Privacy Assembly (GPA) Annual Conference**, co-located in Brussels with the **IAPP Europe Congress 2026** – a week bringing together global experts shaping the future of privacy, digital policy, and data governance.

Why participate

- Full access to both **GPA** and **IAPP Europe Congress** programmes
- Rich, dynamic programming with diverse perspectives
- Engage with international leaders in privacy, digital, and data governance
- Insights into emerging privacy trends and collaborative opportunities

Event highlights

- **Closed Session – November 16 and 17**
 - Strategic discussions, GPA updates, future planning, and the GPA Awards.
- **Open Programme – November 18 and 19**
 - Keynotes, panels, and full access to the IAPP Europe Congress experience.

Registration

Registration information is available on the [GPA conference webpage](#). Full programme details will be available soon.

Special thanks

We extend our gratitude to the **IAPP**, the **European Commission**, and the **European Data Protection Board** for their support.





GPA

Global Privacy Assembly



privacyassembly



globalprivacyassembly



privacyassembly