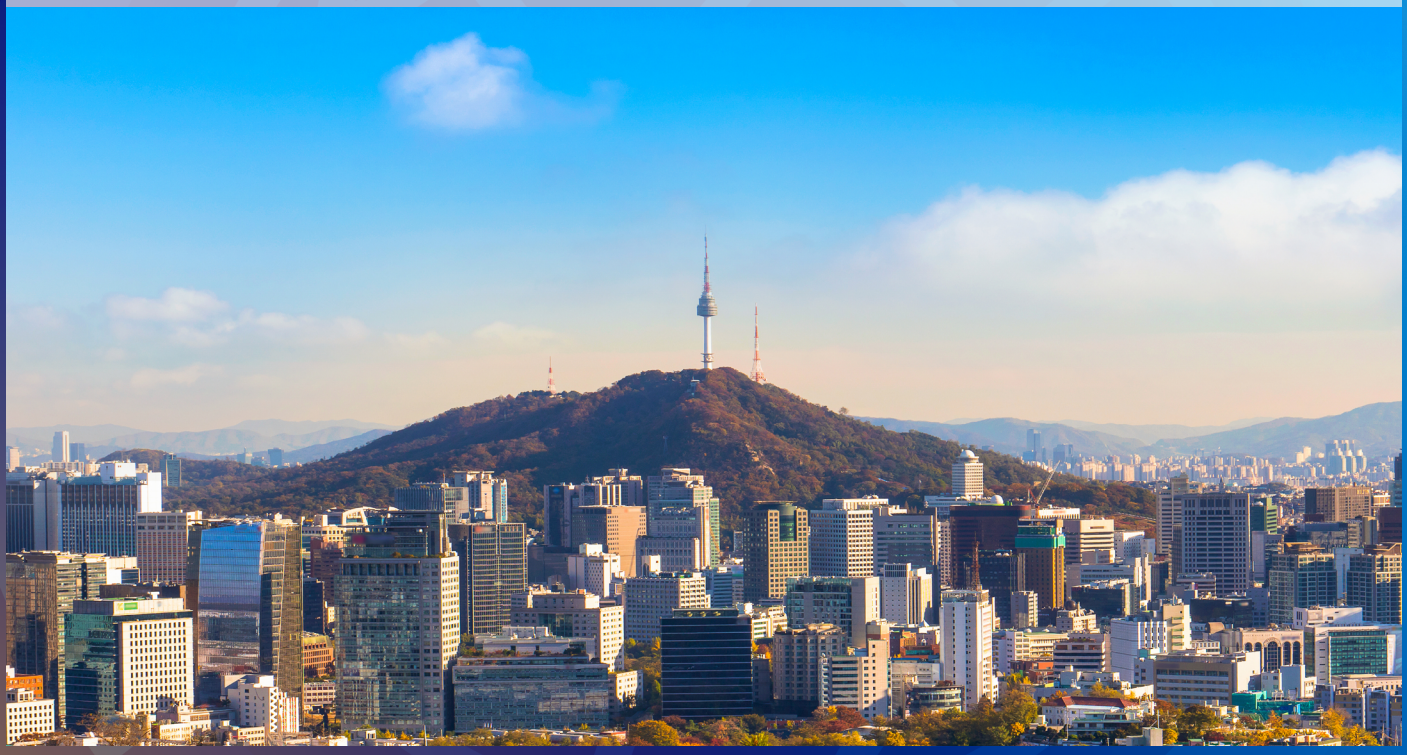
GPA
Global Privacy Assembly

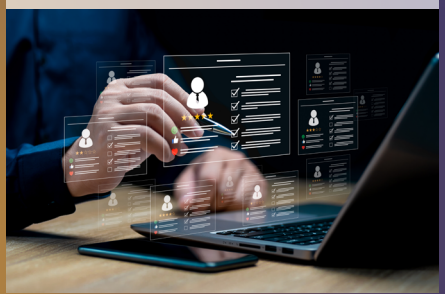
NEWSLETTER

Volume 8 • Issue 1 • Philippines • 2025

South Korea to Host the 47th Global Privacy Assembly in September of This Year



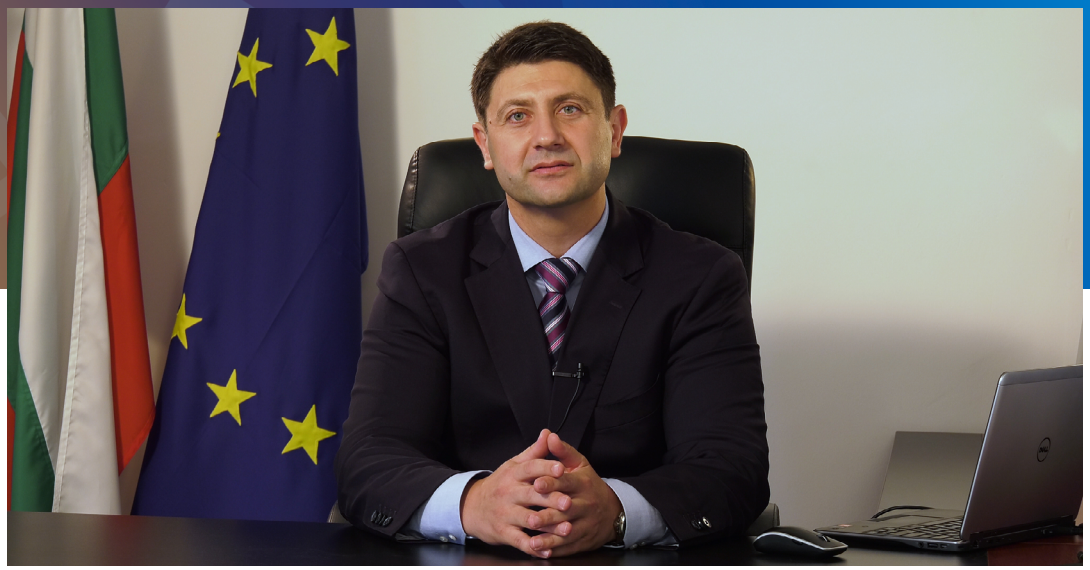
What is good AI practice in the employment context?



Highlights of the 46th Global Privacy Assembly, Jersey, Channel Islands

Data Protection Authority - Somalia

Table of Contents



Ventsislav Karadjov

Chairman

Bulgarian Commission for Personal Data Protection

Ventsislav Karadjov has been Chairman of the Bulgarian Commission for Personal Data Protection since April 2014. After two terms as Vice-Chair of the Article 29 Working Party, he was elected unanimously for Deputy Chair of the European Data Protection Board (EDPB) in May 2018. Since October 2023, he is a Member of the Executive Committee of the Global Privacy Assembly.

Mr Karadjov is a graduate of Sofia University's Faculty of Law and holds a Master's degree in Law, with specialization in Public Jurisdiction.

He began his career as a legal adviser and Programme Director at the Transparency International, Bulgarian chapter. He has also held various senior legal and management positions on projects concerning anti-corruption and the creation of functioning democratic institutions for international institutions such as the European Commission, the US Agency for International Development, the Organisation for Security and Co-operation in Europe, and the UN Development Programme. Throughout his career Mr Karadjov has worked as advisor to the Minister for Internal Affairs in the field of international public security activities and anti-corruption and Chief Expert Associate to the 41st and 42nd National Assembly on matters related to the control of security services, special surveillance devices and access to data retained by public security bodies.

Until his election as CPDP Chairman, Ventsislav Karadjov was a member of the Central Election Commission of the Republic of Bulgaria.

Mr Karadjov has been awarded as "Jurist of the Year" 2018.

Message from the Chair

Commission for Personal Data Protection of the Republic of Bulgaria (CPDP)

Dear colleagues, it is clear for everyone and largely debate at our Annual conference in Jersey last year that artificial intelligence is reshaping our world, driving advancements across multiple sectors like healthcare, finance, education, retail, employment, and social media. From virtual assistants, chatbots, and recommendation engines to autonomous vehicles and healthcare diagnostics, AI is transforming how we live and work. In healthcare, for instance, AI can analyse patient data for early disease detection and help develop personalized treatments, raising privacy concerns around the handling of sensitive health information.

AI is also being used by both fraudsters and professionals in the financial sector. As fraudsters exploit AI to identify and manipulate vulnerabilities, financial institutions have responded with more intrusive KYC procedures to prevent fraud. However, these measures often require collecting significant amounts of personal data, leading to privacy concerns. Similarly, in the retail sector, AI personalizes shopping experiences by analysing user behaviour and purchase histories. Employment platforms now rely on AI-driven, automated decision-making to screen candidates and predict job performance—necessitating increased transparency and more robust data safeguards.

I am sure you remember the heated debate we have had on social media. AI-powered algorithms there determine the content users see and can be weaponized for misinformation. Deceptive design patterns further manipulate user behaviour, making it harder for individuals to protect their data and make informed choices. Meanwhile, AI-enhanced surveillance systems, equipped with facial recognition and behavioural analytics, offer new opportunities for public safety but also escalate risks of mass surveillance and privacy violations. In education, AI is being used to personalize learning experiences, raising questions about how student data is handled and safeguarded.

The Global Privacy Assembly has recognised these emerging issues and taken a proactive stance through resolutions adopted during its latest Annual Conference back in 2024. These resolutions address the abovementioned areas. By focusing on surveillance and privacy, the GPA acknowledges the rising concern over the use of AI-driven facial recognition and behavioural analytics, anticipating future risks to privacy. Their resolutions on regulating neuroscience and neurotechnology reflect a forward-looking perspective, as these fields increasingly use AI to analyse and manipulate cognitive and emotional responses. Similarly, the emphasis on managing global data flows demonstrates the GPA's understanding of the growing reliance on cross-border data sharing in a highly interconnected world. By promoting certification mechanisms, the GPA seeks to create frameworks that ensure the secure transfer of personal data while fostering trust between nations, businesses, and individuals.

These resolutions illustrate the GPA's proactive approach in shaping global privacy frameworks creating a roadmap for international cooperation and privacy protection in an era defined by rapid technological advancement. By anticipating the impact of AI and other emerging technologies, the GPA underscores the importance of balancing innovation with the protection of individual rights ensuring transparency, security and fairness in this evolving digital landscape.

What is good AI practice in the employment context?

UK Information Commissioner's Office

The high data protection and privacy risks associated with AI in the employment context have the real possibility to change livelihoods or career prospects, as it could carry discrimination for employees and for those on other contractual arrangements such as gig workers and contractors. Continued focus on this matter from the GPA is important.

In 2024, the UK Information Commissioner's Office (ICO) has worked on implementing the GPA Resolution on Artificial Intelligence and Employment. We led the GPA in adopting this resolution in 2023, working closely together with our joint Main Sponsors the Federal Commissioner for Data Protection and Freedom of Information (BfDI), Germany and the Data Protection Authority (Garante), Italy.
We've assessed the employment and recruitment contexts that could engage AI, including the development and deployment of AI.

The resolution also describes the risks that people may encounter and the serious harms that may follow as a result of the failure to mitigate those risks. These risks may also entail infringement of other fundamental rights and freedoms, including human dignity, equality of rights, or unfair discrimination.

The use of AI to infer emotions and biometric data is considered particularly risky and should not be used except in limited circumstances subject to robust testing.

We've been clear that there is no regulatory lacuna. The source of data used to train AI models needs to be considered carefully and its compliance with data protection and privacy laws.

In the UK, we've worked with the UK Institute of Future of Work on their AI Regulatory Forum on algorithmic impact assessment. We've also engaged with the Trades Union Congress on the AI and Employment bill draft, and we share knowledge gained from the GPA and other international fora with regulators at domestic level. This work has also helped inform our approaches to AI, including our 2024 consultations on Generative AI.

We aim to cooperate more closely with GPA members on these issues and also with other sectoral regulators such as labour and health authorities.

Next steps

We are running a GPA member survey (**https://forms.office.com/e/DStFuEiSDv**) about the follow-up to the GPA Resolution on AI and employment. This survey has been discussed with the GPA AI Working Group members and remains open for all Resolution Co-signatories and GPA Members until 04 April 2025. All members can alternatively share their updates about this resolution's impact in their jurisdiction by email to the UK ICO: **international.team@ico.org.uk** by the same date above.

Highlights of the 46th Global Privacy Assembly, Jersey, Channel Islands

28 October 2024 to 1 November 2024

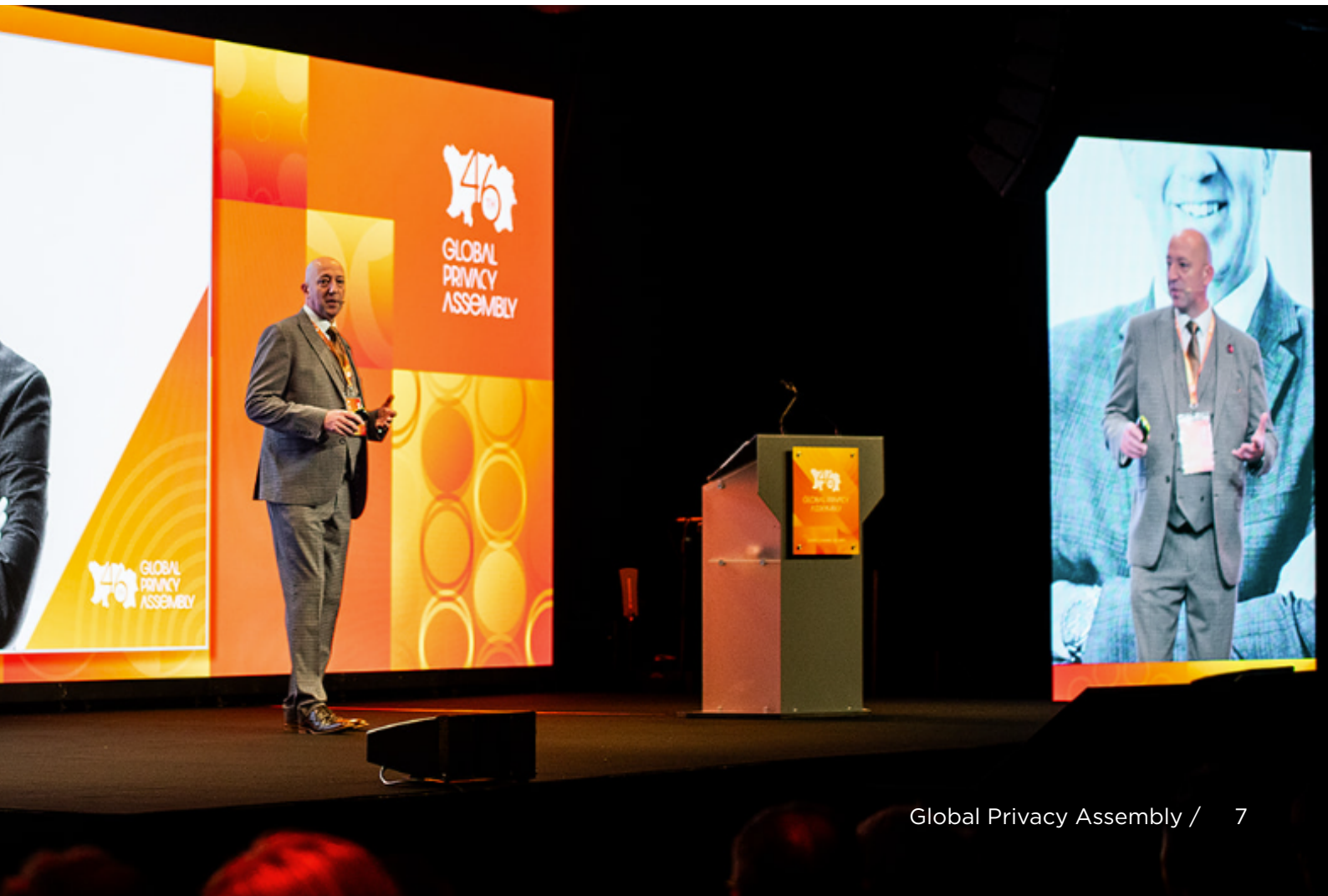
by Paul Vane, Information Commissioner of Jersey

Reflecting on the 46th Global Privacy Assembly, I am thrilled and deeply honoured to have welcomed international colleagues and friends to the beautiful island of Jersey.

Together, we delved into our conference theme of 'The power of i,' exploring the future of privacy, the transformative impact of AI, the protection of society's most vulnerable and the dynamic world of data sharing between government and the third sector. It was an unforgettable experience filled with inspiring discussions and thought leadership.

Amongst many outcomes and action points, we agreed to further explore the following:

- Develop a global standard for data transfers, investigate privacy-enhancing technologies, and strengthen collaboration between financial services regulators and data protection authorities.



- Educate businesses to view data protection as meaningful in situations where people lack a voice and consider cultural and individual factors when applying principles.
- Ensure indigenous communities have a consistent seat at the table, develop new data governance principles, establish a working group within the Global Privacy Assembly and engage directly with indigenous populations.
- Prioritise data privacy as a human right, address biases in data handling, build trust across diverse communities, promote transparency and consent, evolve company cultures to prioritise ethics and privacy, hold tech companies accountable, involve diverse community representatives in policy development, and educate the public on data privacy rights.
- Seek early adopters for a digital privacy charter for schools, implement the '3E' strategy (Educate, Engage, Empower) for children's privacy education, advocate for a digital media literacy strategy and provide support to regulators and innovators globally.
- Map vulnerable populations, make communications more user-friendly, improve design practices and review the age assurance code.
- Explore data trusts in various sectors, assess data governance practices, ensure compliance with data protection regulations, and educate the public on personal data management.
- Establish a connected car working group, ensure data serves users' interests, evaluate the necessity of connected features, use 'live and smart' labels, and encourage responsible data practices.
- Find solutions that reconcile privacy protection with innovation, create a flexible approach to data minimisation and consider proportionality in data collection.

In brief summary of the Open Session content, our first session on Innovation saw futurist Nik Badminton emphasising that while technology isn't moving faster, the noise and data are increasing. He urged a shift in mindset from 'what is' to 'what if,' highlighting the long-term impact of technology. A fireside chat on AI also discussed the need for a mindset change to handle advanced analytics, the role of ethics, and the impact on human rights. It highlighted the complexity of new laws, the lack of skills and resources among Data Protection Authorities (DPAs) and the need for global principles to ease regulatory tensions.

In the second session on the Individual, Douglas Kruger spoke about the importance of elevating individuals to elevate humanity, warning against the contraction of human freedom due to complex systems. A youth panel discussion emphasised the importance of hearing young voices on privacy issues, such as cyberbullying and facial recognition. The session called for more education on privacy and for regulators to engage with younger generations. We also heard parallel sessions focusing on mental health, highlighting the need for transparency and the importance of collaboration between DPAs and NGOs. Another session on defining privacy harms stressed the need for a holistic approach and collaboration between privacy and safety teams.

The third session on Independence talked about 'Regulatory Cousins' highlighting the rise in global data protection legislation and the need for a cohesive digital policy.

In terms of the themes of Intercultural and Indigenous, Massimo Marelli's keynote on data privacy

in humanitarian crises emphasised that data protection is not just a compliance exercise but a fundamental aspect of humanity, ensuring accountability and transparency. Collaboration between data protection authorities and humanitarian organisations is crucial for meaningful applications of these principles.

We discussed indigenous data protection frameworks and noted the lack of international discussion on indigenous experiences and how these communities face harms from unauthorised data collection. Indigenous knowledge must be included in AI systems, with attention to misuse risks.

Back to the theme of the Individual, the panel on privacy education focused on empowering children to navigate the digital age, the collective responsibility of adults to protect children's rights and the need for young people to be involved in the conversation.

We discussed accessible privacy, highlighting the dual nature of technology, which can both enable and pose risks to disabled, vulnerable, and socially marginalised individuals. Some communities have unmet data protection needs and are often abandoned after data breaches and suffer negative impacts. Privacy and accessibility coexist, supporting other human rights.

Moving on to the theme of Integrity, the panel on data trusts emphasised their importance in governing data and building confidence in data usage, highlighting that data quality is crucial for AI. Jersey's unique trust laws could lead in data trust innovation, in an arena where balancing data access and commercial value in health research presents both challenges and opportunities.

The discussion on trust and safety for automobile innovation highlighted an urgent need for transparency and honesty in data practices for connected cars. Developing IoT good practice principles is essential for ethical and sustainable use. Data should serve people, not replace them, and manufacturers must consider long-term consequences.

The final session on Information featured a podium debate on data minimisation, discussing its role in protecting individual freedoms and supporting innovation, competition and trust. While some argue strict data minimisation principles are incompatible with innovation, a flexible approach is needed. Context and proportionality are essential in interpreting these principles.

To close the conference, Martine Wright MBE's fireside chat brought the focus back to the human, sharing her journey post-2005 London bombings and highlighting the privacy and data protection challenges she has experienced. Ms Wright advocated for better support systems and using one's voice to fight for rights.

It is fair to say that we packed a lot into a busy week, but the important thing now is for us to focus on those key outcomes and actions and ensure we don't forget them. We set out with the intention of building a roadmap for the future, and that is what we now have. It is incumbent on us all as GPA members to make good progress on the issues identified.

Finally, I must say a huge thank you to all the speakers, sponsors, contributors and all those involved behind the scenes for making GPA Jersey 2024 a conference to remember. Your hard work and efforts are greatly appreciated.

Data Protection Authority Somalia

Background

As the Somalia Data Protection Authority (DPA), we represent a country emerging from decades of instability. During this period, a significant amount of personal data was held by the private sector without regulation or oversight. This absence of a legal framework led to widespread privacy violations, leaving individuals vulnerable to threats against their privacy rights. Recognizing the urgent need to address these issues, Somalia took decisive action to safeguard its citizens data. In March 2023, Somalia enacted its first Data Protection Act and in February 2024, the Somalia Data Protection Authority was established.

About the Authority

The DPA's mandate is to oversee the implementation and enforcement of the Data Protection Act, ensuring compliance with national and international standards. Since the establishment of the institution, the authority has been focusing on public awareness, stakeholder engagement, policy development and building institutional capacity so that the DPA can achieve its core objectives, which includes:

1. Safeguard personal data from misuse, breaches, and unauthorized access.
2. Encourage best practices in data management and security.
3. Facilitate secure data-sharing frameworks to support public services and governance.
4. Build public awareness of data protection rights and responsibilities.
5. Ensure Somalia's compliance with international data protection obligations.

Although the DPA aims to achieve above mentioned objectives, the concept of data protection is a new phenomenon in Somalia, therefore our institution faces numerous challenges in establishing a robust regulatory and legal framework.

Challenges

Many citizens and institutions are unfamiliar with the importance of safeguarding personal data, making education and public awareness efforts critical. DPA has been facing difficulties in developing regulatory and compliance frameworks as required for the enforcement of the Act. The institution also struggles with limited infrastructure to effectively regulate data controllers and processors. This includes the absence of advanced systems and tools necessary for monitoring compliance and enforcement.

Another major challenge that hinders the institution's capability is financial constraints, which significantly impact its ability to implement key initiatives, conduct training programs and invest in necessary technologies essential for effective operation. The institution also faces a lack of expertise in the field of data protection and to address this, the DPA tends to engage with its worldwide counterparts that are members of the Global Privacy Assembly (GPA), in order to build its institutional capacity by learning and fostering knowledge transfer through collaboration and strategic partnerships.

Joining Global Privacy Assembly

As a newly formed institution in the early developmental stages, the DPA recognizes the importance of learning from established data protection bodies around the globe. To achieve this, Joining the GPA as an observer in 2024 was a historic milestone for Somalia. After 46 years of GPA´s existence, Somalia officially joined as observer and made its debut at the assembly's annual conference in Jersey, United Kingdom.

This achievement was not only a moment of a national pride but also a testament to Somalia´s commitment to addressing the pressing need for data protection. Through its observer status, the Somalia DPA now has the opportunity to connect with global regulatory bodies, exchange insights and adopt best practices to strength its regulatory framework.

Our participation in the 46th Annual GPA Conference in Jersey was both an invaluable opportunity and a positive experience. It provided us with a platform to learn from global leaders in data protection through workshops, panel discussions and collaborative efforts, we gained critical insights into best practices, policy development, and innovative enforcement mechanisms. As an observer in the GPA, the DPA is laying the groundwork for a robust and effective data protection ecosystem in Somalia.

Conclusion

The establishment of the Somalia Data Protection Authority marks a significant milestone in the country's journey toward safeguarding its citizens' privacy and building a secure digital future. By joining Global Privacy Assembly and collaborating with international regulators, the DPA took a historic step forward. While Somalia is still in the early stages of its data protection journey, the DPA is eager to contribute its unique perspective to the GPA's global work. The country's experience as a post-conflict nation offers valuable insights into the challenges of establishing data protection frameworks in fragile contexts.

In a post-conflict society like Somalia, implementing and enforcing data protection compliance across both public and private sector presents significant hurdles. However, while the road ahead is undoubtedly challenging, the Authority is committed to overcoming these obstacles through strategic partnerships, capacity-building initiatives and sustained public engagement.

As Somalia continues to rebuild and modernize, the DPA will play a vital role in ensuring that data protection becomes a cornerstone of trust, security and innovation in the country's digital transformation. This effort is not just a regulatory endeavor, but a national mission that protects the rights and dignity of every Somali citizen in an increasingly data driven world.

Know Your Importer

DIFC's vision to "multilateralise" data free flows with trust between public and private organisations

Dubai International Financial Centre Authority

The power of i was the theme of the 46th Global Privacy Assembly. One of the key take-aways was about the power of information. In the end, information is the " i " that the GPA Members and Observers protect. The other take away was about international influence.

However, the one " i " that underpins all of the eight " i ' topics of GPA 46 is the **"importer"**. How well do we, as controllers or processors, know our importers (KYI)? Whether the controller or processor is a private company or a public authority, we all share information, internationally, with importers. If we know the importer is unethical or tends to be non-compliant, should we share personal data with them? What are the drivers for those decisions?

In the Dubai, UAE, the DIFC is exploring KYI by way of the Ethical Data Management Risk Index (EDMRI). The EDMRI is currently DIFC guidance only, telling the user the capacity for an importer to comply with the local and extraterritorial data protection laws. The EDMRI+ , which is supplemental to the EDMRI, complements the overall index the way a TIA might. In addition, the DIFC Commissioner's office is working on a proposal for a multilateral MOU between members of a public / private consortium that among other outcomes, will shape the governance around the content and validity of the EDMRI.

Sharing personal data across borders is an on-going area of risk. Personal data is not only shared with importers in "adequate" or "essentially equivalent" jurisdictions. It is shared beyond those borders, and, arguably, it is shared without borders at all. It goes to importing jurisdictions that don't have data protection laws or that have only recently enacted laws; or where the supervisory authorities are just getting their arms around the rather large task of enforcing these laws; or with importers in jurisdictions where the data protection law has not yet been recognized as equivalent to the exporting one – ***even if the law is in fact equivalent.***

In a large number of data protection laws, adequacy is only one mechanism amongst a few. To this latter point, only 14 jurisdictions in 30 years of "adequacy" vis a vis the EU regime have been recognised as essentially equivalent, and only a few jurisdictions whose laws contain adequacy provisions have actually utilized this capability.[1]

However, in most data protection laws around the world, several other mechanisms exist to address safely sharing personal data across borders, with additional controls and obligations that essentially insert the exporting jurisdiction's law to the importing one.

But regardless of the available mechanisms, there is so much more for exporters to consider, such as:

[1] https://iapp.org/media/pdf/resource_center/global_adequacy_capabilities.pdf

- environmental factors;
- supervision and enforcement efforts of local non-DP regulators;
- access to supervisory authorities and courts to press individual rights;
- access by government authorities and law enforcement, and associated safeguards, such as the implementation of rule of law;
- general accountability and transparency; and
- propensity for corruption in general

Based on the above, it is important on an international level to shift the current information sharing paradigm to something pragmatic and predictable, thereby encouraging compliance rather than making it near impossible or implausible to comply. Laws can be broken and regulators may decline to regulate. It's risky to think otherwise. Exporters need proactive support and guidance to understand that exporting the data protection law to the importing jurisdiction still carries risk, and that "importing due diligence" to know your importer is key.

EDMRI provides guidance on thematic issues that may be valuable to them, as well as an overall rating with recommendations for mitigating such risks. Ideally, all exporters should be looking at these details regardless of the (recognized or unrecognized) equivalence of the law and regime in the importer's jurisdiction, which is only one piece of the multilayered, nuanced puzzle.

DIFC is a smaller jurisdiction with thousands of globally based companies. As such, we are exploring several globally-minded solutions to pragmatically reduce the risks associated with data transfers. In addition, we need support and governance to keep any outcomes fair, objective and accessible. As such, DIFC are also building a Responsible Data Management Consortium for multilateral governance and the authentic exchange of ideas on accountable data processing. We sincerely invite other supervisory authorities and private entities to join the conversation.

If you want to know more, please review FAQs, available here. The KYI and multilateral governance taking shape now in the form of the RDM Consortium is based on our 2022 non-legislative consultation.

If you have any questions, comments or corrections, or if you wish to participate in the RDM Consortium, please let the DIFC Commissioner's Office know by emailing us as commissioner@dp.difc.ae.

South Korea to Host the 47th Global Privacy Assembly in September of This Year

By Personal Information Protection Commission (PIPC) of South Korea

The Personal Information Protection Commission (PIPC) of South Korea will host the 47th Global Privacy Assembly, to be held between 16 and 19 September 2025 at the heart of the dynamic city, Seoul. The PIPC Chairperson Haksoo Ko extends his warm invitation to you to engage in a week of insightful dialogues, collaboration, and cultural exchange.

Overarching Theme: "Artificial Intelligence in Our Daily Lives – Data and Privacy Issues"

Artificial Intelligence has become an integral part of our daily lives, presenting both opportunities and challenges particularly in the realm of data protection and privacy. With the overarching theme "Artificial Intelligence in Our Daily Lives: Data and Privacy Issues" in mind, this year's Assembly will examine the changes brought on by AI technology and the challenges it poses from various data protection and privacy perspectives. To ensure that advancements in AI technology remain trustworthy, establishing robust governance frameworks for data and privacy is essential. This year's discussions will focus on fostering these frameworks and facilitating important conversations around AI.

Engaging Programs and In-Depth Discussions

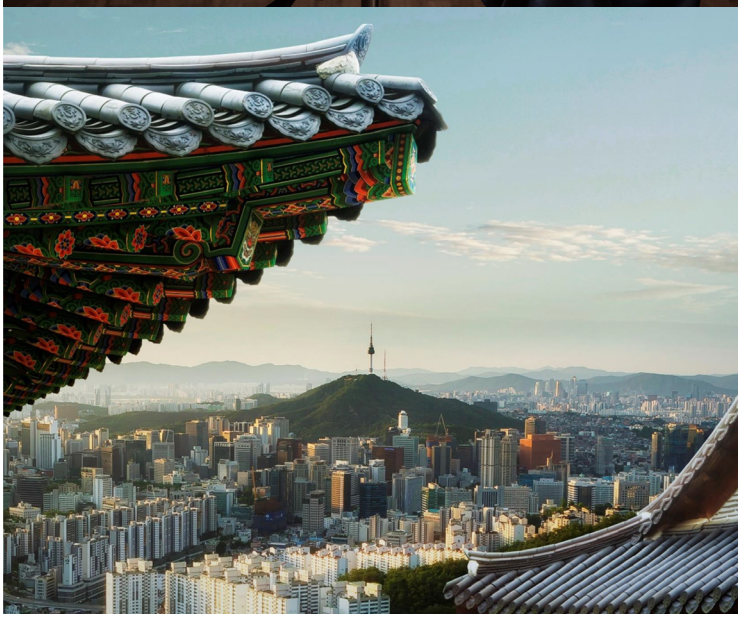
The 47th conference will kickstart with a Welcome Reception on Monday, 15 September. On this day, there will be pre-event activities such as a site visit to certain Korean companies that are at the forefront of technology as well as exciting cultural events. During the first two-day Open Session, the Assembly will tackle a wide array of pressing issues related to data and privacy challenges in the age of AI and will entertain the idea

of establishing a global framework for AI and data governance. These topics will be introduced through a few keynote speeches, setting the stage for thought-provoking and forward-thinking conversations. Attendees will also have a chance to explore the evolution of emerging AI technologies, such as AI agents and humanoids, while gaining insights into the complex issues these innovations bring. Additionally, the program will include engaging panel discussions led by experts, exploring the applications of AI in pivotal fields like healthcare and legal services, with a focus on making these conversations inclusive and relatable for diverse audiences. There will also be sessions that cover crucial topics such as cross-border data transfers and safeguarding children's personal information in the context of AI, reinforcing the need for international cooperation in addressing these issues.

This year's Assembly will present a valuable opportunity to explore fresh perspectives on the evolving landscape of data protection and privacy, with rapid technological progress taking place and also with the widespread adoption of privacy and data protection laws in a growing number of geographic jurisdictions. The dynamic setting of Seoul will surely provide an ideal backdrop for discussions on the challenges and opportunities of data governance in the age of AI. The event will also feature sessions showcasing case studies and best practices in enforcement, encouraging global knowledge-sharing and collaborative discussions.

Experience the Vibrant Culture

Seoul, the capital of South Korea, seamlessly blends its deep historical legacy with a dynamic modern culture. Established as the capital during the Joseon Dynasty in 1392, the city has evolved over centuries into a bustling metropolis.



Beyond the conference room, you will have the opportunity to immerse yourselves in the rich culture of Korea. From Seoul's celebrated culinary scene and K-pop music to its time honored traditions and innovative technology sector, the city offers a captivating blend of the old and the new. Cultural activities will provide a glimpse into Korea's heritage as well as new dynamic energy. You can also go hiking on a trail amidst the city's landscape that blends nature with Seoul's modern skyline.

Join Us in Seoul

We look forward to welcoming you to the Grand Hyatt Hotel in Seoul for the 47th Global Privacy Assembly. Providing a great view of the city, the venue is situated near the older part of downtown Seoul, and also offers proximity to modern hubs of the city such as Gangnam.

Open Session will take place on 16 and 17 September, followed by Closed Session for GPA members on 18 and 19 September. Registration for the event will open soon.

Stay tuned for more updates on the agenda and keynote speakers at **https://gpaseoul.kr**

For more information, please contact the International Cooperation Division of the Personal Information Protection Commission at **pipc@korea.kr**

GPA

Global Privacy Assembly

globalprivacyassembly.org

globalprivacyassemblygpa

privacyassembly