GPA 2025 SEOUL

47TH GLOBAL PRIVACY ASSEMBLY

Insight&Takeaways

15-19 September 2025

Seoul, Republic of Korea

Personal Information Protection Commission

Foreword

The 47th Global Privacy Assembly (GPA), held in Seoul under the overarching theme "**AI in Our Daily Lives: Data and Privacy Issues**," brought together approximately 1,200 participants across 65 countries. The Assembly served as a platform to examine both the opportunities and emerging risks presented by artificial intelligence, while further advancing discussions on trust-based data governance.

The cross-border nature of AI combined with the rapid pace of technological change present challenges that cannot be addressed by any single country alone. In this context, this year's Assembly underscored the importance of stronger cooperation among DPAs, the active engagement of industry and civil society, and ongoing efforts toward enhancing international interoperability.

Since receiving unanimous support from GPA members in 2023, the Personal Information Protection Commission (PIPC) of the Republic of Korea has undertaken two years of dedicated preparation, culminating in the successful convening of this Assembly. Notably, the Assembly in Seoul featured significantly broadened participation from a diverse range of regions—including Asia, the Middle East, Africa, and Latin America—thereby contributing to a more representative and balanced global dialogue on privacy governance.

GPA 2025 Seoul was particularly meaningful as a forum where DPAs, industry, academia, and civil society harmoniously came together to shape the future direction of privacy governance in the AI era. A key development was the advancement of the "Joint Statement on Trustworthy Data Governance for AI," led by PIPC and CNIL with the participation of 20 DPAs. This initiative contributed to building international consensus on the role of DPAs and on privacy frameworks that support trustworthy innovation.

The most significant outcome of this Assembly lies in the continued progress toward more inclusive global privacy governance. It is our hope that the discussions and outcomes documented in this paper will serve as a valuable foundation for the development of interoperable global privacy frameworks, as the GPA and the international community move forward together.

GPA 2025 Seoul Secretariat

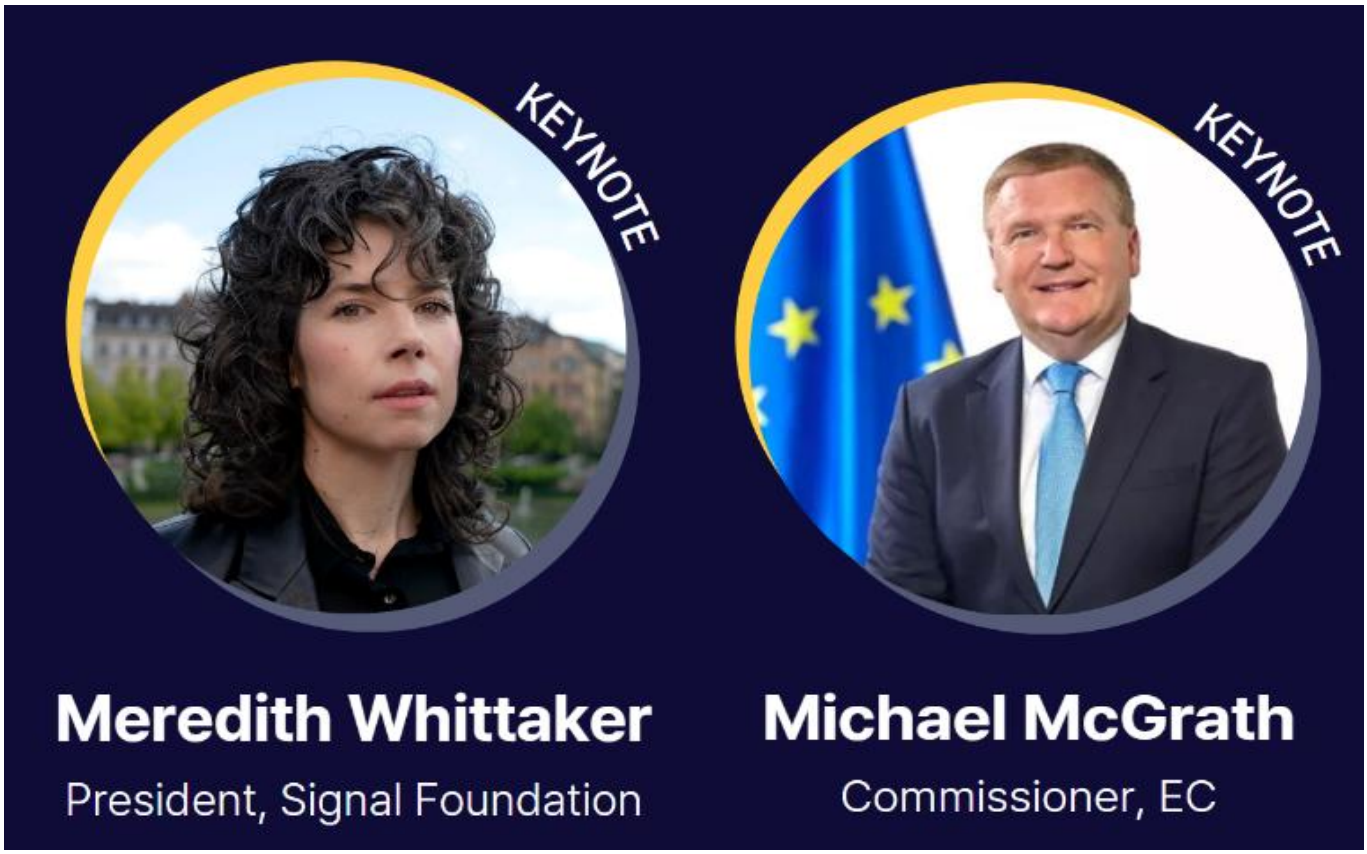
This white paper compiles the discussions and outcomes from the 47th Global Privacy Assembly in Seoul in 2025. It is intended as a reference document to facilitate broader sharing of the issues discussed at the Assembly. Please note that in the course of editing and translation, there may be limitations in fully conveying all nuances, and the views summarized herein does not necessarily represent those of any individual speakers or their affiliated organizations.

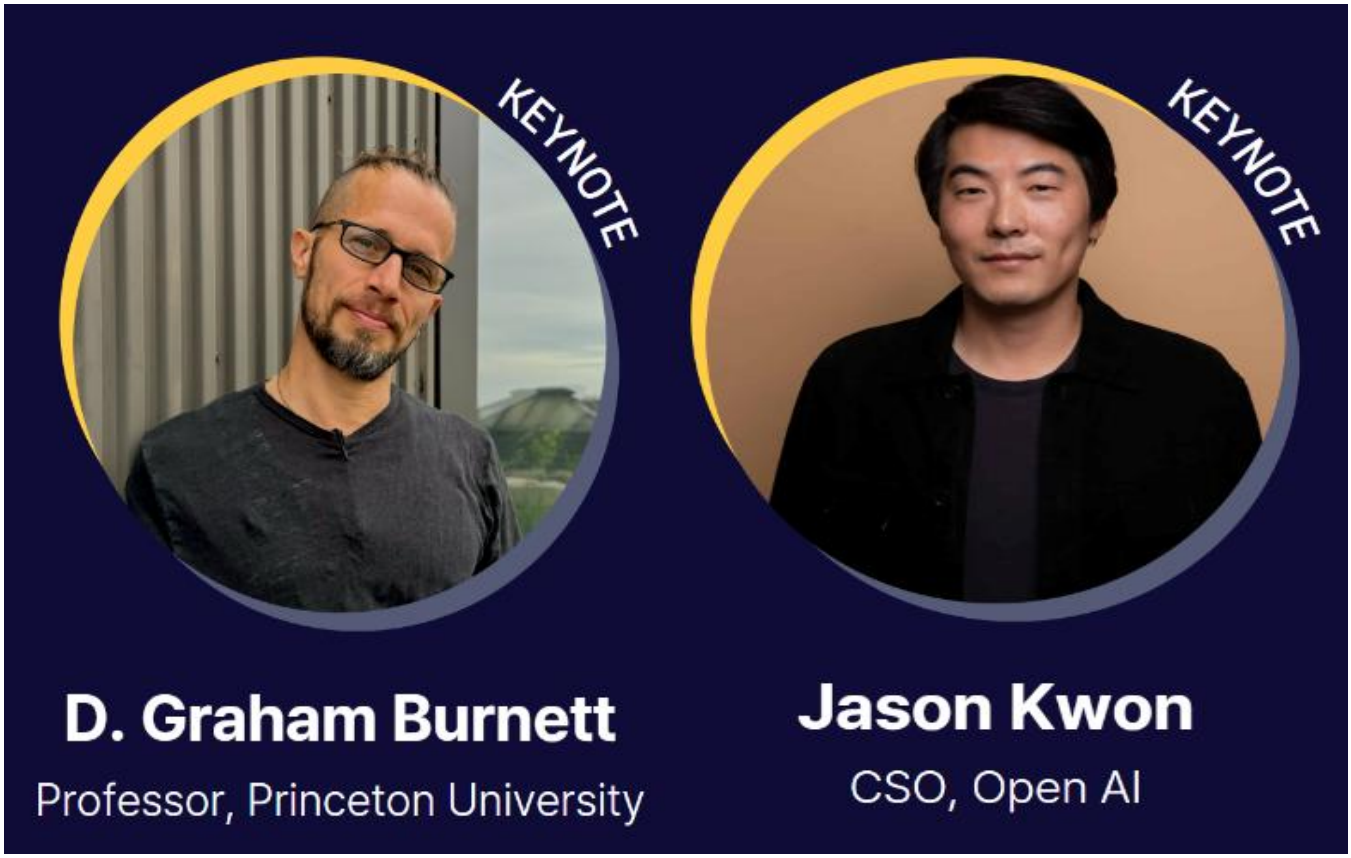

GPA 2025 SEOUL
15-19 SEPTEMBER 2025
SEOUL, KOREA
47TH GLOBAL PRIVACY ASSEMBLY
SEOUL, KOREA
47TH GLOBAL PRI


GPA 2025
SEOUL

Contents

GPA 2025 Keynote Speakers and Session Speakers





47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 1

Global Data Governance in the AI Era

Moderator

Haksoo Ko
Chairperson, PIPC, Korea

Panelists

John Edwards
Information Commissioner
ICO, UK

Marie-Laure Denis
President
CNIL, France

Simon Chesterman
Professor
National University of Singapore

Julie Brill
Harvard Innovation Lab
Fmr FTC Commissioner
Fmr Microsoft Executive

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 2

Pseudonymization of Personal Data to Facilitate Innovation

Moderator

Joe Jones
Research&Insights Director
International Association of Privacy Professionals

Panelists

Adeline Tung
Director of Policy & Technology
PDPC, Singapore

Chris Taylor
Director of International Regulatory Cooperation
ICO, UK

Isabelle Vereecken
Head of the Secretariat
EDPB

Vikash Chourasia
Scientist D
Ministry of Electronics and Information Technology, India

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 3

Synthetic Data in Practice: Opportunities and Challenges

Moderator & Presentation

Khaled El Emam
Canada Research Chair, Medical AI at the University of Ottawa

Panelists

Sungkyu Jung
Professor
Seoul National University

Jörn Wittmann
Group Privacy Ambassador
Volkswagen Group

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 4

Lawful Bases for Processing Personal Data for Purposes of AI

Moderator

Bojana Bellamy
President, Centre for Information Policy Leadership

Panelists

Anu Talus
Chair
EDPB

Beatriz Anchorena
Commissioner
AAIP, Argentina

Dale Sunderland
Commissioner
DPC, Ireland

Byoung Pil Kim
Professor
KAIST

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 5

Agentic AI and Privacy

Moderator

Yong Lim
Professor, Seoul National University College of Law

Panelists

John Edwards
Information Commissioner
ICO, UK

Jules Polonetsky
CEO
Future of Privacy Forum

Kate Charlet
Head of Global Privacy, Safety, and Security, Google

Yoochul Kim
Head of Strategy Division
LG AI Research

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 6

Mechanisms and Policy Instruments to Support AI Innovation

Moderator

J. Trevor Hughes
CEO, International Association of Privacy Professionals

Panelists

Bertrand du Marais
Commissioner
CNIL, France

Des Hogan
Chairperson
DPC, Ireland

Stefano Fratta
Vice President
Meta

Yeonjea Kim
Chief Privacy Officer
Kakao

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 7

Enhancing Interoperability in Cross-Border Data Transfers

Moderator

Philippe Dufresne
Privacy Commissioner, OPC, Canada

Panelists

Presenter
Christopher Kuner
Professor
University of Copenhagen

Immaculate Kassait
Data Commissioner
ODPC, Kenya

Yuji Asai
Commissioner
PPC, Japan

Alex Joel
Professor
American University's Washington College of Law

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 8

Capacity Building for DPAs: Filling the Gaps

Date

Thursday, 18 September 2025

Moderator

Elizabeth Denham
Chair, JDPA, Jersey

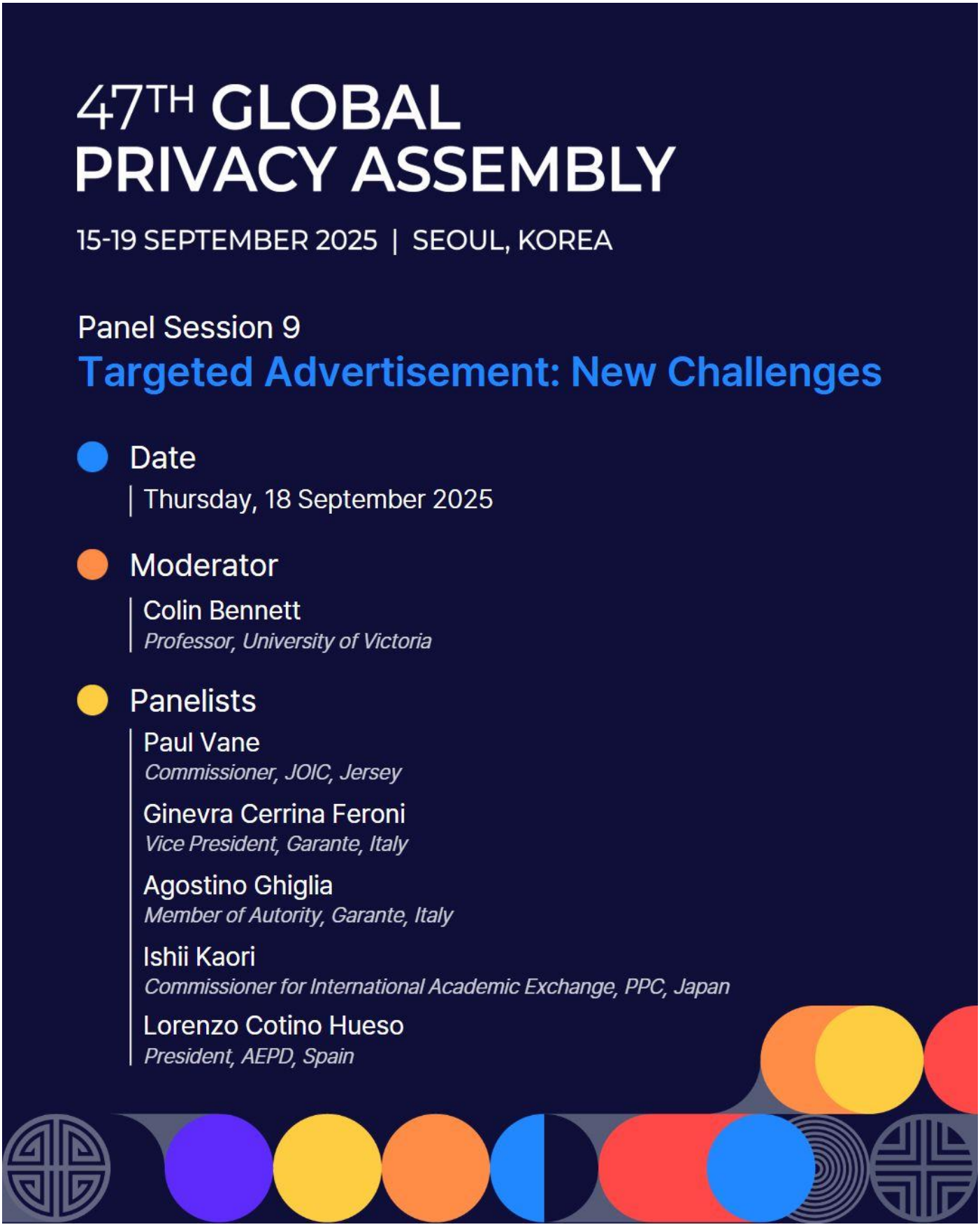
Panelists

Haksoo Ko
Chairperson, PIPC, Korea

Alexander White
Commissioner, OPC, Bermuda

Andreas Hartl
Deputy Commissioner, BfDI, Germany

Lew Chuen Hong
Commissioner, PDPC, Singapore


47TH GLOBAL
PRIVACY ASSEMBLY
15-19 SEPTEMBER 2025 | SEOUL, KOREA
Panel Session 9
Targeted Advertisement: New Challenges
Date
Thursday, 18 September 2025
Moderator
Colin Bennett
Professor, University of Victoria
Panelists
Paul Vane
Commissioner, JOIC, Jersey
Ginevra Cerrina Feroni
Vice President, Garante, Italy
Agostino Ghiglia
Member of Autority, Garante, Italy
Ishii Kaori
Commissioner for International Academic Exchange, PPC, Japan
Lorenzo Cotino Hueso
President, AEPD, Spain

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Panel Session 10

Developing Mechanisms for Cooperation and Collaboration among DPAs and Stakeholders

Date

Friday, 19 September 2025

Moderator

Clarisse Girot
Head of Division for Data Flows, Governance and Privacy, OECD

Panelists

Wojciech Wiewiórowski
Supervisor, EDPS

Philippe Dufresne
Privacy Commissioner, OPC, Canada

John Edwards
Information Commissioner, ICO, UK

Ada Chung Lai-Ling
Commissioner, PCPD, Hong Kong

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Fireside Chat

Impact of AI on Healthcare Services and Privacy

Moderator

Ho Bae
Professor, Ewha Womans University

Panelists

Ran Balicer
Chief Innovation Officer
Clalit

Sooyong Shin
Chief Research Officer
Kakao Healthcare

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 1-A

Newly Establishing and Institutionalizing DPAs

Moderator

Denise Wong
Deputy Commissioner, PDPC, Singapore

Panelists

Janghyuk Choi
Vice Chairperson
PIPC, Korea

Michael Webster
Privacy Commissioner
OPC, New Zealand

Pansy Tlakula
Chairperson
IRSA, South Africa

Taylor Reynolds
Practice Manager
World Bank

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 1-B

10 years of Data Protection in Humanitarian Action

Moderator

Massimo Marelli

Head of Data Protection Office, ICRC

Catherine Lennman

Delegate for International Affairs and Francophonie
FDPIC, Switzerland

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 1-B

10 years of Data Protection in Humanitarian Action

Panelists

Beatriz de Anchorena
Titular (Head)
AAIP, Argentina

Carmen Casado
Director
World Food Programme (WFP)

Youngsu Jong
Senior Deputy Director
PIPC, Korea

Immaculate Kassait
Commissioner
ODPC, Kenya

Hiroshi Miyashita
Professor
Chuo University

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 1-B

10 years of Data Protection in Humanitarian Action

Panelists

Cosimo Monda
Director of the Maastricht European Centre on Privacy and Cybersecurity, Maastricht University

James De France
Managing Legal Counsel and Head of the Data Protection Office, IFRC

Alex Novikau
Chief Data Protection and Privacy Officer, UNHCR

Wojciech Wiewiórowski
Supervisor EDPS

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 1-C

Rethinking Data Protection Law in the Age of AI

Moderator

Gabriela Zanfir-Fortuna
Vice President, Future of Privacy Forum

Panelists

Carly Kind
Privacy Commissioner
OAIC, Australia

Christopher Kuner
Professor
University of Copenhagen

Sangchul Park
Professor
Seoul National University

Monika Tomczak-Górlikowska
Group Head of Privacy
Digital & AI Governance, Prosus Group

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 2-A

Youth Privacy: Mechanics

Moderator

Michael Harvey
Commissioner
OIPC, BC Canada

Remarks

Melissa Holyoak
Commissioner
FTC, USA

Panelists

Sanghee Park
Commissioner
PIPC, Korea

Leanda Barrington-Leach
Executive Director
5Rights Foundation

Elaine Fox
Head of Privacy
Europe, TikTok

Hilary Ware
Global Head of Privacy and Online Safety
Apple Inc.

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 2-B

Redress and Interoperability of Data Protection

Moderator

Amy Kato
Consumers Japan

Panelists

Guido Scorza
Board Member
Garante, Italy

Hiroshi Miyashita
Professor
Chuo University

Javier Ruiz Diaz
Advisor
Asia-Pacific Digital Consumer Dialogue

Natascha Gerlach
Director
CIPL

Byoungil Oh
President
Korean Progressive Network Jinbonet

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 3-A

Re-Using Health Data

Opening Remarks & Moderator

Clarisse Girot

Head of Division for Data Flows
Governance and Privacy, OECD

Moderator

Limor Shmerling Magazanik

Senior Policy Analyst
OECD

Keynote

Khaled El Emam

Professor
University of Ottawa

Closing Remarks

Cheongsam Yang

Director-General
PIPC, Korea

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 3-A

Re-Using Health Data

Panelists

Nitin Dhavate
DPDAI Compliance Head APMA
Novartis

Soyoung Yoo
Professor
Asan Medical Center

Sooyong Shin
Head of Research
Kakao Healthcare

Gráinne Hawkes
Deputy Commissioner
DPC, Ireland

Michael Harvey
Commissioner
OIPC, BC Canada

Mark Taylor
Professor
Melbourne Law School

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 3-B

Data Governance for EdTech

Moderator

Bertrand du Marais
International Affairs Commissioner
CNIL, France

Keynote

Jasmina Byrne
Legal Officer
CNIL, France

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 3-B

Data Governance for EdTech

Panelists

JongYoun Rha
Professor
Seoul National University

Zelda Gerard-Besset
Legal Officer
CNIL, France

Patricia Kosseim
Commissioner
IPC, Ontario Canada

Ivy Grace T. Villasoto
Division Chief
NPC, Philippines

Cari Benn
Chief Privacy Officer
Microsoft

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 4-A

Mastering Investigation Strategies and Choosing the Right Enforcement Tools

Moderator

Brent Homan
Commissioner, OPDA, Guernsey

Panelists

Ada Chung Lai-Ling
Commissioner
PCPD, Hong Kong

Janghyuk Choi
Vice Chairperson
PIPC, Korea

John Edwards
Information Commissioner
ICO, UK

Philippe Dufresne
Privacy Commissioner
OPC, Canada

Dale Sunderland
Commissioner
DPC, Ireland

Immaculate Kassait
Data Commissioner
ODPC, Kenya

47TH GLOBAL PRIVACY ASSEMBLY

15-19 SEPTEMBER 2025 | SEOUL, KOREA

Parallel Session 4-B

Empowering Data Subjects through Data Portability Mechanisms

Moderator

Carly Kind
Commissioner, OAIC, Australia

Panelists

Anu Talus
Chair
EDPB

Michael Webster
Privacy Commissioner
OPC, New Zealand

Taehoon Lim
Professor
Korea University

Jaewon Sun
Chief Executive Officer
Merakiplace

Keynote 1: Meredith Whittaker

President, Signal Foundation

As AI and data use expand, privacy is being structurally undermined. Legal, technical, and societal responses are required to ensure user control and transparency.

As the use of AI and data continues to expand globally, the scope of personal data collection and usage has grown rapidly, heightening the importance of privacy protection more than ever before. However, concerns were raised as to **whether technological developments are genuinely functioning in a manner that adequately safeguards user privacy**, calling for a **fundamental reassessment**.

While privacy is frequently emphasized as critically important in the AI era, it was noted that, in practice, privacy protections have been gradually weakened. Since the 1990s, although encryption technologies have been liberalized, their benefits have been concentrated largely in corporations and governments, while user privacy has not been sufficiently protected. As encryption expanded across commercial activities such as online payments, stock trading, and authentication, corporate profits increased, and governments utilized data held by companies for surveillance purposes.

Following the Snowden disclosures, positive developments such as the widespread adoption of HTTPS encryption, full-device encryption on mobile devices, and the expansion of Signal's end-to-end encryption (E2EE) were acknowledged. Nevertheless, it was emphasized that **encryption should be understood not as the completion of privacy protection, but as its starting point**.

Currently, privacy was assessed as facing two major threats. One is government demands for backdoors under the pretext of crime prevention and child protection, and the other is the expansion of agentic AI integrated into operating systems. As AI becomes embedded within operating systems, boundaries between applications are eroding, and continuous collection and transmission of user data is becoming the default structure. Examples such as Microsoft's Recall feature and server-side data transmission by Siri were cited.

These changes are occurring without explicit user consent, and due to structures in which refusal of operating-system-level monitoring leads to a restriction on device usability, user consent is practically becoming a must. As a result, operating systems are no longer neutral platforms, and users' substantive control is being weakened.

The speaker stressed that **privacy erosion should not be justified in the name of technological progress. Genuine privacy protection requires legal, technical, and societal efforts to proceed in parallel.** It was proposed that data access by AI be controlled at the development level, with application-specific access boundaries, and that operating system and AI model developers transparently disclose the datasets accessed by AI and the purposes of data collection. It was reiterated that encryption remain a fundamental prerequisite for privacy protection and that it must be implemented substantively rather than merely as a formality.

Keynote 2: Michael McGrath

Commissioner for Justice, European Commission

AI innovation and personal information protection are not conflicting values, but can mutually reinforce one another.

This keynote speech drew on the EU's experience in AI policy and regulation to demonstrate that AI innovation and personal information protection are complementary rather than conflicting, and to discuss the need for and direction of international cooperation.

The speaker evaluated the GPA as a central platform through which data protection and privacy authorities have shared expertise and experience, and contributed to shaping global standards. The importance of independent supervisory authorities with sufficient resources and capabilities in the data protection field was emphasized, noting that the EU's AI regulatory framework has evolved in close linkage with its existing data protection regime.

To promote AI innovation, the EU has established an "AI Continent Action Plan," and has been striving to advance public AI infrastructure and enhance data availability. Through these efforts, foundations are being laid for startups and small and medium-sized enterprises to leverage AI technologies. Key priorities include expanding AI use in strategic sectors, developing cloud and AI legislation, and advancing Data Union Strategy.

The phased implementation of the EU AI Act, risk management obligations for general-purpose AI, and implementation of provisions on prohibited AI practices were also explained. The European Commission is strengthening transparency and safety through a Code of Practice for general-purpose AI, and is supporting stakeholders through the AI Pact network and service desk.

Given AI's close connection to consumer rights, the EU is reinforcing transparency requirements and human oversight obligations in automated data processing. While enforcement of consumer protection using AI tools is expanding, discussions are also underway on Digital Fairness Act to ensure that consumers can be connected to human agents when necessary.

As AI is inherently data-driven, strong personal information protection was emphasized as an essential precondition. The GDPR forms the foundation of the EU's digital legal framework, while the AI Act provides governance for high-risk AI systems in areas such as transparency, cybersecurity, and data accuracy. Stakeholders agree on the need to respect GDPR principles, and the importance of consistent enforcement and the provision of practical guidance by regulators was reaffirmed.

He concluded by **reiterating that AI innovation and privacy are mutually reinforcing values, and that the EU continues to pursue harmony between data protection, innovation, and the protection of fundamental rights.** It was expressed that, with GPA at the center of expanded international cooperation, AI innovation can ultimately serve the interests of citizens worldwide.

Keynote 3: D. Graham Burnett

Professor, Historian of science, Princeton University

In the age of AI, protecting privacy is not simply a matter of regulating data. It requires societal and policy responses aimed at protecting and restoring attention.

In his keynote address, Professor Burnett examined how, in the age of artificial intelligence, human attention has been commodified by technology and capital, and he proposed a new approach to restoring privacy and human dignity. He characterized the phenomenon by which digital platforms and technology companies extract time, emotion, and focus through algorithms and data collection and convert it into economic value as "human fracking." This structure, he argued, deepens loss of attention, erodes literacy, contributes to social disruption, and mental exhaustion, and structurally weakens individual privacy.

The speaker highlighted that the rise of AI is reshaping human consciousness and the structures of attention, opening a new phase in which even the inner realms of experience are being commodified. Rather than mimicking human consciousness, AI acts more like a mirror of it, with the result being that human experience and judgment are increasingly dependent on technological systems. In this context, he emphasized that the control and protection of attention has become a central task for human flourishing.

As a response, Professor Burnett proposed **"Attention Activism,"** an **international movement to resist structures that exploit human attention.** This movement rests on three pillars: **Study**, Organizing, and Sanctuary. Study refers to the recovery of existential learning and reflection; **Organizing** denotes the process of building solidarity among activists and scholars around the world; and **Sanctuary** involves redefining public spaces such as schools, libraries, and museums as places that protect attention.

He further argued that privacy should not be understood merely as a form of restriction or avoidance but should be reinterpreted as a "pathway" to deeper understanding and relationship. Just as the industrial revolution gave rise to the politics of labor, today the **politics of attention** are emerging, and **privacy protection policies must serve as core instruments for safeguarding this new order.**

In closing, Professor Burnett posed two questions: How can privacy policies and regulations contribute to the creation of sanctuaries for attention? And how can communities of attention activism expand their work in support of privacy protection? Through these questions, he underscored the need for social solidarity and institutional responses to protect human attention and dignity.

Keynote 4: Jason Kwon

Chief Strategy Officer (CSO), OpenAI

In the age of AI, privacy is not just a technical challenge or regulatory compliance issue. It is a core value of a human-centered AI ecosystem focused on giving users more control and building trust.

Jason Kwon noted that privacy protection has become a key priority for industries amid rapid advancements and the widespread adoption of AI. He outlined OpenAI's technological and institutional measures and future directions to address privacy challenges. He underscored that **privacy is not merely a compliance matter; it should become a core value grounded in human dignity, autonomy, and respect for exercising individuals' rights, laying the foundation for building trust across the AI ecosystem in the age of AI.**

He explained that ChatGPT's global proliferation demonstrated AI's potential and the grave responsibility it carries. In this context, OpenAI has implemented a range of privacy-safeguarding measures, focusing on giving users greater control over their data. For example, OpenAI introduced temporary chats, enabling users to interact with AI without having their conversations being trained on AI training, data controls giving developers and enterprise users the option to opt out of training on business data, and other internal policy improvement cases to increase transparency in how data is used.

OpenAI developed 'Privacy Filter' as a tool to enhance its privacy protection features. For its frontier models, 'Privacy Filter' is used inside the organization to significantly reduce the processing of personal data and model training. OpenAI will open-source the 'Privacy Filter' to build a safer AI ecosystem.

To respect users' rights, users can now have a simple, human-like conversation about OpenAI's privacy policy and quickly learn how to exercise their rights. The speaker also emphasized that OpenAI aims to deliver tools that provide parental controls and detect harmful content to keep young people safe online. These are part of OpenAI's endeavors to enhance user protection when using its AI models.

He also emphasized that **AI should advance in ways that enhance human capabilities and provide greater freedom. To this end, he emphasized that guardrails should put users in control, protect their data, and be built with security and accountability at their core**. He added that conversations between people and doctors, or lawyers, are legally protected as confidential. While legal frameworks for AI were not built the same way, interactions with AI should also be protected to empower users.

Last but not least, the speaker **reaffirmed that privacy is not just a technical challenge but a future of human dignity, autonomy, and respect for the individual, and a collective endeavor toward progress. At the same time, he said industry, regulators, academia, and civil society should come together to build a sustainable and effective framework for privacy protection**. He concluded that OpenAI will remain committed to advancing technology that honors human dignity.

Panel Session 1

Global Data Governance in the AI Era

Discussion Panel

Haksoo Ko: Chairperson, Personal Information Protection Commission (PIPC), Korea (Moderator)

John Edwards: Commissioner, Information Commissioner's Office (ICO), UK

Marie-Laure Denis: President, Commission Nationale de l'Informatique et des Libertés (CNIL), France

Simon Chesterman: Professor, National University of Singapore, Singapore

Julie Brill: Harvard Innovation Lab; Former FTC Commissioner; Former Microsoft Executive

Keywords

Cross-border data flows, regulatory fragmentation, interoperability, privacy principles, international cooperation

Purpose and Backgrounds

As AI technologies proliferate, the ways in which data are generated, used, and transferred are changing rapidly, while legal and institutional regulations remain largely jurisdiction-based. The expansion of large-scale data use and automated processing structures is increasingly revealing mismatches between existing regulatory frameworks and technological environments. These changes raise new challenges in data protection, accountability, and regulatory coherence, increasing the need for comparative analysis and discussion of national policy responses and cooperation models. This session was convened to share these concerns and identify common challenges.

Key Message

The session confirmed a shared understanding that the limitations of a single regulatory framework necessitate cooperation among supervisory authorities, trust-building, and application-oriented international cooperation to advance both personal data protection and technological innovation.

Main Discussion Points

Participants recognized that while both the local and global dimensions of data are expanding, law and regulation remain limited by their application primarily at regional and jurisdictional levels. Several factors were identified as making a single regulatory model difficult: many countries are positioned more as "rule takers" than "rule makers," resulting in relatively high levels of under-regulation; asymmetries exist between stakeholders' levels of attention and their policy influence; and in certain regions, lack of access to technology itself is perceived as a greater concern than AI misuse.

France shared that **data protection authorities must continuously consider how to align technological innovation with privacy protection**, and introduced institutional mechanisms—such as data intermediation mechanisms and detailed guidelines—that combine the dual objectives of promoting data provision and reuse while protecting individual rights, especially privacy. The UK also shared its interest in pursuing policy approaches that regulate without undermining innovation. The U.S. noted that active state-level legislation creates a complex landscape with diverse and inconsistent regulations from an industry perspective, while also observing that companies themselves want data to be protected safely in the context of AI and privacy.

In a context where many principles and guidelines already exist, participants agreed that **the key policy issue is less about establishing additional principles and more about how existing norms are applied and enforced in real policy environments and technical operations**. Accordingly, the focus of regulatory discussions is shifting from adding principles to implementation and execution. It was emphasized that **without cooperation among regulators across multiple jurisdictions and sectors, it will be difficult to secure practical regulatory effectiveness**. At the same time, participants noted that the institutional forms such cooperation may take—and the extent to which coordination is feasible—remain tasks to be further identified through future policy discussions.

Panel Session 2

Pseudonymization of Personal Data to Facilitate Innovation

Discussion Panel

Joe Jones: Research & Insights Director, International Association of Privacy Professionals (IAPP)

Adeline Tung: Director of Policy & Technology, Personal Data Protection Commission (PDPC), Singapore

Chris Taylor: Director of International Regulatory Cooperation, Information Commissioner's Office (ICO), UK

Isabelle Vereecken: Head of the Secretariat, European Data Protection Board (EDPB)

Vikash Chourasia: Scientist D, Ministry of Electronics and Information Technology, India

Keywords

Pseudonymized data, de-identification, anonymized data, industry use cases, training data

Purpose and Backgrounds

As demand for data use across industries, especially in AI and big data, continues to grow, **pseudonymization is emerging as a key tool for enabling AI training and data analysis**. At the same time, however, pseudonymization's status and limitations arise from a lack of legal definitions, jurisdictional disparities in regulatory approaches, and gaps in understanding of the technique. This session identified jurisdictional differences in legal frameworks and regulatory approaches to pseudonymization, and explored how pseudonymized data is currently used across public-sector and industry use cases to assess its potential and constraints. It also focused on examining where pseudonymization is positioned along with anonymization and other privacy-enhancing technologies (PETs).

Key Message

Pseudonymization can serve as a tool to mediate personal data protection and data utilization, but its effectiveness depends on jurisdictional frameworks and interpretations, as well as on technical and organizational competence. In this sense, establishing guidelines to give clarity, building trust, and taking sector-specific approaches are required to facilitate the use of pseudonymized data.

Main Discussion Points

Regulatory approaches to pseudonymization vary across jurisdictions, but it is widely recognized as an assistive tool that enables data use with privacy safeguards in place. Singapore has published a series of guidelines emphasizing simplicity and clarity in regulations, introducing pseudonymization as one of the basic de-identification techniques. The country also supports the experimental use of pseudonymization through regulatory sandbox programs. The United Kingdom sees pseudonymization as a lawful safeguard and uses pseudonymized data in the medical and public health sectors, with the separated storage of additional information. The EU views pseudonymization as both a data minimization measure and a means that is aligned with privacy by design (PbD). Judicial precedents clarify that whether pseudonymized data constitutes personal data depends on the context and recipient. India takes a flexible approach in which specific techniques are not stipulated by law. In the Indian legal context, pseudonymization may be included among legal safeguards, but the country has adopted a structure in which the specific application of techniques falls within the remit of sectoral regulators.

In practice, pseudonymization is not a single technique; it is combined with trusted execution environment (TEE), security data environments, and PETs. The main challenges to pseudonymization come from insufficient understanding of the technique, capacity gaps across organizations, and an immature organizational culture. Panelists **repeatedly argued that the criteria for what constitutes anonymized data are strict yet unclear, blurring the line between pseudonymization and anonymization**. To address these challenges, panelists emphasized the **importance of sharing criteria by providing guidelines on PETs and through international cooperation**. They also noted that **regulators should signal that pseudonymization and other PETs are trustworthy and respected**, encouraging industry to build trust in them. Moreover, they argued that **an approach that reflects industry-specific characteristics** rather than a one-size-fits-all application of general law is more effective. Panelists agreed that **the broader adoption of pseudonymization hinges on technical safeguards, interpretation, trust, cooperation, and a phased-in approach.**

Panel Session 3

Synthetic Data in Practice: Opportunities and Challenges

Discussion Panel

Khaled El Emam: Professor, Medical AI at the University of Ottawa, Canada (Moderator)

Sungkyu Jung: Professor, Seoul National University, Korea

Jörn Wittmann: Privacy Ambassador, Volkswagen Group

Keywords

Synthetic data, obstacles to introducing technology, data quality, safety assessment, AI training

Purpose and Backgrounds

Synthetic data is one of the Privacy-Enhancing Technologies (PETs) that **mimics the statistical properties of real data to enable data scalability, mitigate bias, and strengthen personal data protection**. This session aimed to improve understanding of synthetic data and review its roles and limitations in building trustworthy AI systems, sharing relevant guidelines and industry use cases.

Key Message

Synthetic data has been discussed as an enabler for both privacy protection and data utilization, but precise criteria for safety assessment and whether it is subject to regulation remain open discussions.

Main Discussion Points

Synthetic data generation guidelines have been published in the United Kingdom, Singapore, and Korea, **but an international consensus on its safety and whether it is subject to personal information has not yet been reached. The lack of metrics, safety, and utility examination criteria was identified as a key challenge**. In particular, the legal interpretation of whether synthetic data constitutes personal or anonymized data, and whether it is subject to regulation, varies across jurisdictions. Moreover, membership inference attacks, attribute disclosure vulnerability, and other potential re-identification assessments are not technically feasible. In this context, panelists discussed **the need for regulators to establish quantitative assessment criteria and develop standards**.

In Korea, the public sector has increasingly used synthetic data, but safety examination criteria are not yet sufficiently established. Korea's guidelines do not automatically classify synthetic data as anonymized; however, a review of its purpose-setting, generation methods, safety assessment, and deliberation procedures is required to determine whether it is properly anonymized and has low re-identification risk. For synthetic data that is open to the public, a fully synthetic approach, stringent safety criteria, and risk-type-specific monitoring are required. However, panelists argued that examination frameworks are not keeping pace with utilization in practice.

An industry-side panelist noted that synthetic data complements real data, not as an alternative. For training AI systems for autonomous driving, the motor vehicle industry uses synthetic data to generate diverse scenarios quickly and cost-effectively, but it cannot fully replace real-world data. Ultimately, unobfuscated original data is required to fully reflect reality and human behavior. In this regard, panelists agreed that synthetic data is a tool to boost efficiency and safety, but it cannot replace real data. Balancing the use of synthetic and real data is ultimately needed, depending on the purpose and risk levels.

Panel Session 4

Lawful Bases for Processing Personal Data for Purposes of AI

Discussion Panel

Bojana Bellamy: President, Centre for Information Policy Leadership (Moderator)

Anu Talus: Chairperson, European Data Protection Board (EDPB)

Beatriz Anchorena: Commissioner, Agencia de Acceso a la Información Pública (AAIP), Argentina

Dale Sunderland: Commissioner, Data Protection Commission (DPC), Ireland

ByoungPil Kim: Professor, KAIST, Korea

Keywords

AI training data, web scraping, legitimate interest, user data, secondary use, purpose change

Purpose and Backgrounds

This session was convened in response to the growing demand for large-scale high-quality data driven by rapid advances in AI technologies. It examined the **lawful bases under which publicly available data or existing user data may be used for AI training**, and **how such practices can be aligned within a reasonable and flexible regulatory framework**. Given the divergent legal interpretations and ongoing uncertainties across jurisdictions, the session aimed to share regulatory approaches, guidelines and case examples, and to explore the direction of an appropriate personal data processing framework for the AI era.

Key Message

Personal data processing for AI training and deployment should continue to be grounded in established data protection principles, while requiring interpretations and applications that reflect the technological characteristics of AI systems and the level of associated risks.

Main Discussion Points

Discussions focused on jurisdictional practices regarding **personal data use in AI training**, the application of the purpose limitation principle, the permissible scope of sensitive data processing, and practical principles to support responsible implementation.

With respect to **regulatory approaches**, the European Data Protection Board (EDPB) has presented views on issues such as model anonymity, the applicability of legitimate interests, the impact of unlawfully collected data, and is developing criteria for assessing the risk of re-identification. Ireland's Data Protection Commission (DPC) has engaged with companies from the early stages of AI development to review risk mitigation measures and, in some cases, has requested orders to suspend training activities. Argentina has complemented monitoring efforts with capacity-building initiatives, including an AI Observatory and self-assessment tools. Korea's Personal Information Protection Commission (PIPC) has accumulated guidance on the use of publicly available data and AI privacy risk management through public-private consultative bodies.

The **purpose limitation principle** was reaffirmed as a **foundational requirement** in AI environments. At the same time, **a degree of flexibility** in defining and designing purposes may be recognized where appropriate risk mitigation measures (such as pseudonymization or anonymization, deduplication, and the exclusion of sensitive data) are implemented. In particular, when relying on **legitimate interests**, it was noted that careful balancing of risks and benefits must take into account **sector-specific contexts.** Participants also highlighted the need to expand discussions beyond training datasets to include the use of real-time runtime data, especially as agentic AI systems become more widespread.

On **sensitive data processing**, the session shared that the EU GDPR permits limited use under Article 9 only where special legal grounds and enhanced safeguards apply, alongside a Korean case involving sanctions for unauthorized use. Given the significant tension between technical necessity and the protection of fundamental rights, there was broad recognition that the processing of sensitive data requires a clear legal basis, robust risk assessment, and strong protective measures.

With regard to **principles to be considered in the development and operation of AI models**, the participants emphasized the need for a comprehensive governance approach supported by a multidimensional impact assessment encompassing privacy by design (PbD), transparency, fairness and bias management, security, data quality management, and the reinterpretation of data subject rights. It was also noted that, in light of emerging risks associated with the widespread adoption of open-source models and model reuse, end-to-end monitoring and regular reporting mechanisms are increasingly important. Multi-agent-based logging and verification structures were also discussed as a promising tool for strengthening transparency and accountability going forward.

Panel Session 5

Agentic AI and Privacy

Discussion Panel

Yong Lim: Professor, Seoul National University, Korea (Moderator)

John Edwards: Information Commissioner, Information Commissioner's Office (ICO), UK

Jules Polonetsky: CEO, future of Privacy Forum (FPF)

Kate Charlet: Head of Global Privacy, Safety, and Security, Google

Yoochul Kim: Head of Strategy, LG AI Research

Keywords

agentic AI, autonomy, interaction with external systems, complexity, opacity

Purpose and Backgrounds

Unlike conventional generative AI systems that primarily respond to user prompts by producing content, **agentic AI systems are designed to perceive their environment, formulate plans, and take actions on behalf of users**. This shift introduces substantive changes in how personal data may be collected, used and shared. **As agentic AI is rapidly moving toward commercialization, the session examined the new privacy risks arising from heightened data accessibility, limited human oversight, and the potential for long-term data retention.** Drawing on experiences from regulators and industry, discussions focused on the technical and institutional foundations needed to ensure the responsible design and operation of autonomous AI systems, and on identifying key privacy challenges and response directions.

Key Message

Since agentic AI automates decision-making in ways that make traditional privacy protection models difficult to apply as is, the session underscored the need for policy, institutional, and technical measures across the entire lifecycle of training and operation.

Main Discussion Points

Agentic AI was described as a class of AI systems that combine autonomy, adaptability, and integrated reasoning, planning, and execution capabilities. These systems are distinct from generative AI in that they generate physical or digital outcomes through environmental awareness, goal-setting, tool selection, and task execution. Agentic AI may operate either as a task-specific tool performing discrete functions or as a higher-level intelligence structure that integrates and coordinates multiple agents. Owing to these characteristics, its potential applications are expanding in dynamic industries such as healthcare, finance, and manufacturing.

At the same time, **autonomous execution and interaction with external environments introduce new risks, including unintended data collection, expanded security vulnerabilities, and weakened user control. Where decisions such as reservations or payments are automated, existing consent mechanisms (such as cookie banners or terms-and-conditions-based models) may no longer function effectively.** Additional risk factors discussed included long-term memory, the collection of bystander information, and the possible use of sensitive data in sectors such as healthcare and finance. These architectures, characterized by broad API access and autonomous execution, may complicate the identification of responsible actors. However, participants also noted that **accountability can still be anchored through existing data protection frameworks, including the controller-processor principles under current privacy laws.**

In response, the session discussed the **growing importance of proactively embedding safeguards throughout both training and operational stages, including enhanced transparency, strengthened user control, privacy by design (PbD), and use of data protection impact assessments (DPIAs).** Participants considered standardized APIs and governance tools that allow permitted data, purposes, and retention rules to be configured in machine-readable form; technical measures such as federated learning, synthetic data, on-device processing, and least privilege access; as well as policy mechanisms including data minimization, enhanced visibility into inference processes, and calibrated human oversight. Furthermore, the session highlighted the need for **early-stage collaboration between regulators and industry to design safety and transparency** into agentic AI models, supported by innovation-enabling regulatory instruments and guidelines.

Panel Session 6

Mechanisms and Policy Instruments to Support AI Innovation

Discussion Panel

J. Trevor Hughes: CEO, International Association of Privacy Professionals (IAPP) (Moderator)

Bertrand Du Marais: Commissioner, Commission Nationale de l'Informatique et des Libertés (CNIL), France

Des Hogan: Chairperson, Data Protection Commission (DPC), Ireland

Stefano Fratta: Chief Privacy Officer & Vice President, Meta

Yeonjea Kim: Head of Privacy & Vice President, Kakao

Keywords

Regulatory sandbox, prior consultation, co-regulation, legal uncertainty, self-regulation

Purpose and Backgrounds

The gap between the rapid pace of AI technological development and the slower speed of regulatory reform has generated legal uncertainty and regulatory blind spots, which in turn hinder private-sector innovation. In this context, establishing a trustworthy and flexible legal and institutional framework has emerged as a key challenge. Policy tools such as **regulatory sandboxes and prior adequacy review were discussed as mechanisms to complement ex post regulatory approaches** by enabling early-stage cooperation between government and industry, thereby **mitigating legal uncertainty**. This session aimed to examine how such institutional tools can operate in ways that promote AI innovation while maintaining legal certainty and public trust.

Key Message

There was a shared understanding that regulatory authorities should function not merely as enforcers, but also as facilitators supporting industrial development amid technological change. While the effectiveness of regulatory sandboxes and prior adequacy review mechanisms was acknowledged, the need to ensure coherence across the broader regulatory ecosystem was emphasized.

Main Discussion Points

With regard to the **objectives of regulation and the role of supervisory authorities**, participants shared the view that **regulation should simultaneously pursue market development and the realization of the public interest**. In rapidly evolving technological environments, regulations must reflect stakeholder needs and interests. At the same time, concerns were raised that existing norms—including the EU GDPR—have struggled to keep pace with technological change, leading to gaps between on-the-ground practices and legal interpretation, as well as regulatory vacuums arising from a lack of precedent. Accordingly, regulatory authorities were encouraged to move beyond an enforcer and instead engage in gathering stakeholder input, promoting research and investment, and supporting industrial development amid technological change.

In terms of **proactive regulatory responses and collaborative tools**, examples were shared in which authorities took anticipatory measures—such as requests to halt large language model training—while also addressing real-world challenges jointly with companies through **regulatory sandboxes**. Even in the absence of clearly established AI legislation, cooperation has been pursued with authorities responsible for the Digital Services Act to coordinate joint regulation and reduce overlapping requirements, demonstrating the dual role of regulators as both watchdogs and facilitators.

From an industry perspective, regulatory sandboxes and prior adequacy review mechanisms were evaluated as providing spaces to reduce legal uncertainty and experiment with new data processing methods. Experiences such as joint testing and application of technologies such as multi-party computation with regulators, as well as resolving uncertainties under personal data protection law prior to service launch through consultation and flexible interpretation were shared. **However, it was also noted that engagement with a single regulator alone may lead to confusion if other authorities adopt divergent interpretations, underscoring the need for coordination and consistency across the regulatory ecosystem**. Beyond ex ante review of individual services, the importance of promoting self-regulation to encourage companies to develop and adhere to their own internal standards was also discussed.

Panel Session 7

Enhancing Interoperability in Cross-Border Data Transfers

Discussion Panel

Philippe Dufresne: Privacy Commissioner, Office of the Privacy Commissioner of Canada (OPC), Canada (Moderator)

Christopher Kuner: Professor, University of Copenhagen, Denmark (Presenter)

Immaculate Kassait: Data Commissioner, Office of the Data Protection Commissioner, Kenya

Yuji Asai: Commissioner, Personal Information Protection Commission (PPC), Japan

Alex Joel: Professor, American University Washington College of Law, USA

Keywords

Data transfers, adequacy decisions, interoperability, data localization, international standards

Purpose and Backgrounds

The proliferation of AI services now calls for reshaping the global data distribution order. The international community agrees on **the need to facilitate cross-border data transfers**. However, it also calls for limiting such data transfers to safeguard privacy and national security. Meanwhile, AI-powered data processing practices are making the existing data transfer order more complex, as they involve large-scale data transfers in real time, and more and more entities are shifting to cloud-based environments. Against this backdrop, **establishing interoperable, free, and secure cross-border data transfer mechanisms has come to the fore**. This session discussed how AI and other emerging technologies are reshaping perspectives on cross-border data transfers and explored potential approaches to making these transfers safe and seamless.

Key Message

Various cross-border data transfer mechanisms are available, but we need to use them in the jurisdictional context, not in a one-size-fits-all manner. Panelists highlighted that transparency and accountability are core values of cross-border data transfer mechanisms.

Main Discussion Points

Cross-border data transfer is deeply intertwined with national security, sovereignty, and global order, and it is a complex task that requires international trust and legal stability. Panelists noted that jurisdiction-specific application of data transfer regulations limits data flows, stifling innovation and economic activity. In this context, **building a framework for cross-border data transfers that is implementable in practice is needed**, rather than relying on perfunctory regulations or checklists. As data localization policies are cited as a key challenge in the AI landscape, panelists discussed the need for data protection authorities (DPAs) to set international norms in an unbiased manner.

Adequacy decisions, binding corporate rules (BCRs), standard contractual clauses (SCCs), and consent from data subjects are institutional means for enabling cross-border data transfers. **Each country is seeking the best combination of the aforementioned mechanisms.** Some countries are exploring ways to modernize their privacy laws to ease regulatory burdens and reduce legal uncertainty. A privacy-by-design (PbD) approach to transborder data transfers was also discussed from a consumer perspective. Panelists also reviewed the roles of cooperation frameworks, cross-border privacy rules (CBPR), data privacy frameworks, and other multilateral mechanisms, grounded in common values shared by democratic countries.

Meanwhile, as legal frameworks rapidly evolve across jurisdictions, it is increasingly challenging to gain a clear understanding of these shifts and apply them effectively. Panelists **suggested we should avoid blindly following any particular legal framework when assessing cross-border data transfer frameworks in other jurisdictions**. For small and medium-sized enterprises and civil society organizations, the costs and time required to build data transfer infrastructure remain burdensome. To mitigate limitations, they shared the need for outreach and cooperation. Overall, **transparency and accountability were reaffirmed as the core values underpinning the cross-border data transfer mechanisms**, and panelists noted that capacity building of DPAs and international cooperation are beginning to take root as prerequisites for creating a trust-based environment for cross-border data transfers.

Panel Session 8

Capacity Building for DPAs: Filling the Gaps

Discussion Panel

Elizabeth Denham: Chairperson, Jersey Data Protection Authority(JDPA) , Jersey

Haksoo Ko: Chairperson, Personal Information Protection Commission (PIPC), Korea

Alexander White: Commissioner, Office of the Privacy Commissioner (OPC), Bermuda

Andreas Hartl: Deputy Commissioner, Federal Commissioner for Data Protection and Freedom of Information (BfDI), Germany

Lew Chuen Hong: Commissioner, Personal Data Protection Commission (PDPC), Singapore

Keywords

Technical expertise, filling the gaps, talent acquisition

Purpose and Backgrounds

As AI has been integrated across public services, commerce, and day-to-day life, it has created ever-growing complexities in data processing mechanisms and undermined the enforcement capacities of data protection authorities (DPAs). Moreover, we are now seeing growing capacity gaps among approximately 148 DPAs worldwide due to disparities in available resources, competencies, and experience with AI and other new technologies. **Such disparities among DPAs may directly affect the effectiveness of respecting data subjects' rights and ensuring global consistency, as AI knows no borders**. In this regard, this session explored ways to bridge growing gaps and foster capacity building among DPAs by sharing experiences and identifying potential solutions.

Key Message

To build DPAs' capacity, concrete action plans were proposed: ensuring consistent responses to AI and emerging technologies, fostering regional and international cooperation, and securing expertise.

Main Discussion Points

To proactively address issues arising from AI and emerging technologies, panelists shared their experiences. With the advent of generative AI, DPAs began establishing dedicated teams or units to address emerging issues, understand how generative AI works, and develop guidelines. Recognizing that abstract principles cannot reduce business uncertainty, panelists explained how they introduced principle-based approaches, provided consultation, and implemented operating review schemes for new technologies. In this line of work, a combination of technical and administrative competence was identified as a key factor.

From a regional and international cooperation perspective, establishing a DPA's identity and organizational design in the early phase, capacity building, and seeking divergence were identified as major challenges. Through bilateral or multilateral cooperation and other working groups, DPAs share their AI work, ethics, and governance. In this workstream cycle, DPAs' hands-on, accumulated experience can translate into effective legal interpretation and working-level applicability.

To ensure consistency in capacity across DPAs, panelists are using consultative bodies, working groups, and other communication channels. Panelists discussed building a centralized repository to support small and less-experienced DPAs, allocating resources available, establishing a division for regulatory sandbox programs, providing stakeholder consultation, and operating pilot programs for new technologies as solutions.

Panelists reaffirmed the importance of continuous learning of AI and emerging technologies, taking interdisciplinary approaches, talent acquisition and staff training **to secure expertise**. To that end, panelists discussed the social relevance of DPAs' work and the importance of an environment where job seekers learn new technologies, which can be a significant advantage in attracting talented people.

Panel Session 9

Targeted Advertisement: New Challenges

Discussion Panel

Colin Bennett: Professor, University of Victoria, Canada (Moderator)

Paul Vane: Commissioner, Jersey Office of the Information Commissioner (JOIC), Jersey

Ginevra Cerrina Feroni: Vice President, Garante per la Protezione dei Dati Personali (Garante), Italy

Agostino Ghiglia: Member of the Authority, Garante per la Protezione dei Dati Personali (Garante), Italy

Ishii Kaori: Commissioner for International Academic Exchange, Personal Information Protection Commission (PPC), Japan

Lorenzo Cotino Hueso: President, Asociación Española de Protección de Datos (AEPD), Spain

Keywords

Behavioral advertisement, consent, transparency, protection of vulnerable groups, dark patterns

Purpose and Backgrounds

Regulation of targeted advertising constitutes a **complex domain** that combines the use of anonymized and pseudonymized data, the classification of online identifiers as personal data, and the deployment of AI-based advertising technologies. In interconnected environments spanning the web, apps, and advertising platforms, **personal data processing structures are technologically complex** and driven by strong economic incentives. The introduction of generative AI and automated technologies is bringing structural changes to the advertising ecosystem and to all stakeholders, including data subjects. This session sought to discuss the expanding regulatory scope and impacts of new technologies in targeted advertisement, as well as future challenges such as awareness-raising and education.

Key Message

Targeted advertisement, due to its complex data processing structures involving multiple actors and increasing sophistication through AI, is raising the level of difficulty for privacy supervision and policy design.

Main Discussion Points

As the legal and technical complexity of targeted advertisement regulation increases, recalibration of regulatory and enforcement standards and awareness-raising initiatives targeting both users and industry were identified as mid- to long-term priorities.

Approaches treating online identifiers such as IP addresses and device identifiers as personal data are becoming more widespread, and the **need for dedicated governance of AI-based advertising technologies is being reviewed**. While technological innovation may generate economic benefits, it can also conflict with privacy protection. To ensure transparency in targeted advertising, participants argued that **effective and balanced enforcement should be achieved through clear legal standards** rather than prohibition-centered approaches.

Discussions also addressed the increased risk of personal identification through data combination, **highlighting the need for stricter safeguards for vulnerable groups such as children and elderlies**. Enforcement case on TikTok's targeted advertising was cited as demonstrating the necessity for data subjects to **retain substantive control** over their data, and additional **protective measures for minors** were emphasized. The need for consumer education in **aging societies**, validation of the effectiveness of prior-consent models, and the limitations of consent tied to access to essential services were also discussed.

Targeted advertisement such as **behavioral advertisement** was identified as requiring heightened caution and being justifiable only under conditions of transparency and lawfulness. The **"consent-or-pay" model**, which conditions service access on the provision of personal data, was widely viewed as problematic for its commodification of personal data. It was also noted that there was substantial opposition on the model at public consultations. As a policy direction, it was proposed to **apply privacy-by-design at the design stage**, provide clear and comprehensible **notice** to users, and impose responsibilities on advertisement providers regarding data minimization and tracking governance.

Panel Session 10

Developing Mechanisms for Cooperation and Collaboration among DPAs and Stakeholders

Discussion Panel

Clarisse Girot: Head of Division for Data Flows, Governance and Privacy, OECD (Moderator)

Ada Chung Lai-ling: Commissioner, Privacy Commissioner for Personal Data (PCPD), Hong Kong

Philippe Dufresne: Privacy Commissioner, Office of the Privacy Commissioner of Canada (OPC), Canada

John Edwards: Information Commissioner, Information Commissioner's Office (ICO), UK

Wojciech Wiewiórowski: Supervisor, European Data Protection Supervisor (EDPS)

Keywords

Regulatory overlap, policy coherence, joint forums, information sharing, enforcement coordination

Purpose and Backgrounds

With the deployment of AI, personal data has become increasingly implicated at regulatory intersections involving consumer protection, competition, cybersecurity, intellectual property, online safety, and finance. Regulatory overlap, conflicts, and fragmentation arising at these intersections can undermine the effectiveness of personal data protection and constrain technological innovation and economic activity. **Securing policy coherence and coordinated enforcement through cooperation among regulatory authorities has therefore emerged as a key task**. This session focused on sharing cooperation cases across existing and emerging regulatory intersections and examining their achievements and limitations to explore future directions for cooperation mechanisms.

Key Message

As regulatory intersections are expanding due to AI deployment, cooperation among regulatory authorities was discussed as an essential condition for ensuring effective personal data protection and policy coherence.

Main Discussion Points

Overall, **while cooperation among regulatory authorities has become an essential condition for policy coherence and mitigation of duplication and conflict**, further reinforcement areas were identified as necessary such as **legal basis, resources, expertise, and operational procedures to ensure stable functioning**.

The **ICO** introduced the Digital Regulation Cooperation Forum (DRCF), a formal consultative body through which authorities responsible for information protection, communications, competition, and finance jointly coordinate regulation. Cooperation infrastructure has been built by integrating business consultation channels and information portals and conducting joint discussions on generative AI. Demand for inter-agency cooperation is also increasing rapidly in areas such as children's access to harmful content, financial consumer protection, medical devices, and energy. Given the challenges each authority faces in securing AI expertise, the need for joint utilization of shared resources, including personnel, was also discussed.

The **PCPD** described operating structures for investigative cooperation, joint education initiatives, and policy coordination with the police, finance authorities, and broadcasting and communications authorities. Cooperation in addressing identity theft, child protection, and data scraping was presented as success cases of improved response speed and effectiveness. At the international level, efforts such as developing standardized frameworks for data transfers and adopting global joint declarations are proceeding in parallel. Participants emphasized that effective cooperation requires legal grounds for information sharing and institutional clarity regarding roles and responsibilities.

The **EDPS** noted that, following the introduction of the Digital Markets Act, discussion structures involving multiple regulators have been established, but that practical coordination on individual cases remains insufficient. Legal restrictions on information sharing were identified as factors that can weaken cooperation, and participants highlighted the need to institutionalize information-sharing scope and procedures.

The **OPC** shared that while cooperation is being strengthened across areas such as copyright, finance, and child protection, further activation of cross-sector collaboration is needed given the DPA's enforcement and supervisory constraints. Through the Canadian Digital Regulators Forum (CDRF), the OPC has diversified regulatory cooperation, including the publication of a report on synthetic media in digital environments.

Fireside Chat

Impact of AI on Healthcare Services and Privacy

Discussion Panel

Ho Bae: Professor, Ewha Woman's University, Korea

Ran Balicer: Chief Innovation Officer, Clalit, Israel

Soo-Yong Shin: Chief Research Officer, Kakao Healthcare, Korea

Keywords

Healthcare service, pseudonymized data, synthetic data, health data, medical practices

Purpose and Backgrounds

AI technology is impacting healthcare services across the board, from improving diagnostic accuracy in medical imaging to expanding remote medical treatment, enabling personalized care, and streamlining administrative processes. These shifts enhance the accessibility and efficiency of medical services but also introduce new privacy challenges, including large-scale collection of sensitive information, re-identifiability risks during AI training, and risks arising from use beyond the initial purpose. This session aimed to explore how AI is transforming healthcare, share perspectives on future directions, and discuss the sensitivity and need to protect health data, the potential and limitations of synthetic data, and governance issues for trustworthy data sharing.

Main Discussion Points

AI adoption in the healthcare sector has the potential to shift care from reactive to preventive and proactive. Case studies on specific disease detection showed that similar levels of patient identification were possible with analyses of significantly fewer subjects than existing methods. Panelists noted that medical practitioners can devote more time to patient care and decision-making by having AI handle routine, repetitive tasks. However, it was also noted that as AI becomes a core component of healthcare systems, the risk of being targeted by malicious attacks increases. To address this challenge, systematic risk management should be undertaken in collaboration.

While health data is recognized as highly sensitive and subject to strict regulations, there are concerns that undue regulations may stifle innovation. The adoption paths of AI may vary by hospital size, jurisdictional regulatory landscape, and technological infrastructure. Panelists argued that **pseudonymization is a key tool for using health data without obtaining consent**, but it is not standardized across jurisdictions and entities, hindering multi-institutional and multinational research projects. They agreed on **the need to establish international standards for pseudonymization**. They also discussed that **synthetic data is useful for training and testing phases, but real data is still required for clinical validation or safety assessment**.

Regarding AI explainability, ensuring interpretability is important for medical practitioners to understand and explain the rationale behind AI's decision-making, rather than technical mechanisms for patients in detail. For clinical judgement and ethical considerations, black-box AI is insufficient, underscoring the need for explainable AI. **To ensure trustworthy AI, panelists agreed that technical measures, consent mechanisms, transparency, and governance design should work together**.

Parallel Session 1 (1-A)

Newly Establishing and Institutionalizing DPAs

Discussion Panel

Denise Wong: Deputy Commissioner, Personal Data Protection Commission (PDPC), Singapore (Moderator)

Janghyuk Choi: Vice Chairperson, Personal Information Protection Commission (PIPC), Korea

Michael Webster: Privacy Commissioner, Office of the Privacy Commissioner (OPC), New Zealand

Pansy Tlakula: Chairperson, Information Regulator South Africa (IRSA), South Africa

Taylor W. Reynolds: Practice Manager, World Bank

Keywords

Establishment of data protection authorities, independence, accumulation of expertise, capacity building, international cooperation

Purpose and Backgrounds

Across the Asia-Pacific region, the enactment of personal data protection laws has been accompanied by the establishment of new supervisory authorities. Many institutions are confronting challenges related to legal foundations, delineation of powers and responsibilities, and securing organizational capacity and expertise. Supervisory authorities have experienced trial and error in areas such as institutional design, enforcement approaches, staffing and budgeting, and stakeholder engagement. This session aimed to share experiences related to the establishment and early-stage strategies of DPAs, discuss data protection approaches in new technological environments, balance between self-regulation and enforcement, and the role of international cooperation, thereby providing practical insights for newly established or early-stage DPAs and laying the foundation for mutual learning and cooperation.

Main Discussion Points

Common challenges identified included securing **DPA independence, budgets, staffing, and accumulated expertise** amid the rapid growth in the number of DPAs following the enactment of personal data protection laws. Capacity-building discussions within APPA and ASEAN were framed as extensions of these shared concerns, with emphasis on the need for newly established DPAs to define enforcement approaches and institutional identity from the design stage onward.

International and regional cooperation was recognized as having **tangible benefits**, with cases introduced in which **cross-border information sharing and joint responses during complaint handling, investigations, and enforcement proved effective**. Issues such as large-scale breach response, legal questions involving global platforms, determination of whether a data qualifies as personal data, and attribution of responsibility were identified as difficult to resolve within a single jurisdiction, underscoring the value of experience sharing and joint investigative mechanisms.

In terms of **ex ante regulation and promotion of self-regulation**, a structure of **internal Chief Privacy Officer system, guidance and training, sanctions for violations, and institutional improvements were emphasized to collectively create compliance incentives**. A dual structure of support mechanisms enabling companies to establish and effectively operate internal norms complemented by administrative measures to ensure accountability in cases of non-compliance were mentioned as well.

In the context of **development cooperation**, participants shared the view that rather than uniformly applying a single institutional model, **it is more appropriate to support countries in selecting from diverse structures and approaches aligned with their legal systems, administrative cultures, and resource levels**. As multiple models—such as independent authorities and agencies under executive branches—coexist, institutional choices of DPAs were recognized as context-dependent.

Parallel Session 2 (1-B)

10 Years of Data Protection in Humanitarian Action: Building on the past to navigate future challenges for Humanitarian Action in the age of AI

Discussion Panel

Catherine Lennman: Delegate for International Affairs and Francophonie, Federal Data Protection and Information Commissioner (FDPIC), Switzerland (Moderator)

Massimo Marelli: Head, Data Protection Office, International Committee of the Red Cross (ICRC) (Moderator)

Alex Novikau: Chief Data Protection and Privacy Officer, United Nations High Commissioner for Refugees (UNHCR)

Carmen Casado: Director, United Nations World Food Programme (WFP)

James De France: Managing Legal Counsel and Head of Data Protection Office, International Federation of Red Cross and Red Crescent Societies (IFRC)

Wojciech Wiewiórowski: Supervisor, European Data Protection Supervisor (EDPS)

Immaculate Kassait: Data Commissioner, Office of the Data Protection Commissioner (ODPC), Kenya

Beatriz de Anchorena: Head, Agency for Access to Public Information(AAIP), Argentina

Hiroshi Miyashita: Professor of Law, Faculty of Policy Studies at Chuo University, Japan

Youngsu Jong: Senior Deputy Director, Personal Information Protection Commission (PIPC), Korea

Cosimo Monda: Director, European Centre on Privacy and Cybersecurity, Maastricht University, Netherlands

Keywords

humanitarian data, vulnerable populations, international cooperation, global standards, capacity building

Purpose and Backgrounds

Over the past decade, the humanitarian sector has made various efforts to institutionalize data protection and integrate it into operational practice. Since 2015, international organizations and humanitarian actors

have adopted comprehensive data protection frameworks and developed guidance and handbooks tailored to humanitarian contexts, alongside initiatives to translate and disseminate these materials in multiple languages. These developments have been driven by the recognition that data processing needs expand rapidly in crisis situation (such as armed conflict, natural disasters, and infectious disease outbreaks) while the leakage or misuse of such data can pose severe risks to the lives and safety of individuals and communities.

This session aimed to reflect on the institutional progress and experience of the past ten years, assess achievements and remaining gaps, and identify areas requiring further improvement. By doing so, it sought to distill shared lessons for data protection in humanitarian action and strengthen inter-organization cooperation and learning.

Main Discussion Points

Participants repeatedly emphasized that data processed in humanitarian context is closely linked to vulnerable groups, including victims of armed conflict, refugees, stateless persons, and disaster-affected populations. If such information is disclosed or misused, it may lead to devastating consequences, including targeting, violence, or mass atrocities. **In this context, data protection is not merely a matter of safeguarding individual rights, but can be a prerequisite for protecting life itself.** Failures in data protection may result in irreversible harm.

The session also discussed how digital transformation is reshaping humanitarian assistance, with **increasing reliance on technologies** such as messaging platforms, registration applications, and digital identity systems. While **these tools can improve efficiency, they also introduce new risks.** Accordingly, participants highlighted the importance of embedding privacy principles into the design of tools, systems, and applications from the outset, strengthening security measures, and deploying risk management instruments to prevent data from being weaponized or exploited. At the same time, the growing use of technology reinforces the need for privacy education and enhanced capacity building for practitioners working in the field.

In complex environments involving international organizations, states, and both public and private actors, it was noted that **data protection challenges cannot be resolved through a single regulatory framework.**

International organizations may operate under their own regulatory regimes, yet legal conflicts can arise when they collaborate with service providers subject to domestic laws. In such cases, cooperation between data protection authorities and international organizations was identified as important. Approaches discussed included improving predictability through clearer guidance, establishing cooperation based on shared clauses that recognize sovereignty concerns, and strengthening capacity through education on data protection principles and data subject rights.

At both global and regional levels, **international standards** such as Convention 108 were r**ecognized as providing a common language and baseline level of protection**, and can **have practical effect when combined with regional networks**. In federal systems or contexts marked by significant regional disparities, centralized norms alone may be insufficient, underscoring the value of regional collaboration, training initiatives, observatories, and networks for sharing experience and lessons learned.

The session further noted that, in emergency situation where life-saving efforts and privacy protection may appears to be in tension, practitioners face the difficult task of determining priorities. In such circumstances, context-specific operational guidance and procedures are more useful than abstract principle-based norms. **Differences in role allocation and accountability structures between governments and humanitarian actors also vary across countries, requiring cooperation frameworks that take these realities into account.** It was suggested that the direct involvement of data protection authorities in the development of humanitarian handbooks could enhance either practical relevance, while the importance of clarifying responsibility-sharing between governments and humanitarian actors was also underscored.

Finally, participants highlighted the **critical role of education and training**. Data protection should be understood not only as a legal obligation but also as a matter of values and ethics. Practical, action-oriented training and tools are needed to ensure that frontline personnel can acquire relevant knowledge at the right time and make responsible decisions in the field. In this context, education and training were presented as core priorities as they form the foundation for cultivating organizational awareness of data responsibility and building trust.

Parallel Session 3 (1-C)

Rethinking Data Protection Law in the Age of AI

Discussion Panel

Gabriela Zanfir-Fortuna: Vice President for Global Privacy, Future of Privacy Forum (FPF) (Moderator)

Carly Kind: Privacy Commissioner, Office of the Australian Information Commissioner (OAIC), Australia

Christopher Kuner: Professor, University of Copenhagen, Denmark

Sangchul Park: Professor, Seoul National University, Korea

Monika Tomczak-Gorlikowska: Chief Privacy Officer, Prosus Group

Keywords

Principle-based approach, reasonable interpretation, regulatory agility, legal uncertainty, institutional coordination

Purpose and Backgrounds

This session was convened to discuss how existing personal data protection laws should be applied and interpreted in environments where new technologies such as chatbots, AI agents, and automated decision-making are proliferating, and to examine the extent to which institutional adjustments may be required. While core principles and provisions of personal data protection laws were established prior to the widespread adoption of AI, they continue to apply to diverse AI usage cases. Nevertheless, concerns were raised regarding **whether existing norms function sufficiently amid rapid technological change, or whether additional interpretation, supplementation, or amendment is necessary**. The session aimed to assess the balance between maintaining principles and introducing institutional adjustments, and to explore reasonable policy directions between over-regulation and regulatory gaps.

Main Discussion Points

Participants shared the view that **fundamental principles of personal data protection remain valid regardless of technological change, and that the emergence of AI does not automatically replace or negate existing norms**. Personal data protection frameworks are designed on a principle-based foundation that enables adaptation to technological change; thus, the key challenge lies not in creating new principles, but in interpreting and applying existing ones in new technological contexts. Concerns were also expressed that excessive expansion of AI-related regulatory discussions could impose disproportionate regulatory burdens relative to actual risk levels, and that caution is warranted against extending regulatory scope to areas not directly related to personal data protection.

At the same time, it was noted that delays in legal interpretation, guidance issuance, and policy responses relative to the pace of AI development could exacerbate uncertainty in practice. **Regulators were therefore urged to provide clearer and more timely explanations regarding scope and application**, particularly with respect to the respective responsibilities and obligations of AI model developers, service providers, and deploying entities. Such clarity was recognized as contributing not only to compliance, but also to greater predictability for innovation.

Without sufficient understanding of AI system operations and data processing structures, risk assessment and normative application risk becoming overly formalistic. Accordingly, **the need to strengthen technical expertise within DPAs and enhance investigative and analytical tools** was emphasized. Given the uneven application of personal data protection norms across regions, issues of regional disparity and equity were also identified as requiring inclusion in policy discussions.

Korea's efforts to advance AI special provisions allowing limited use of original data for AI development under public-interest purposes and strengthened safeguards were introduced. In this context, **balancing regulatory clarity with flexibility for AI innovation**, and **coordinating potential overlaps and conflicts between the Personal Information Protection Act and related legislation such as a basic AI law**, were identified as key challenges.

Parallel Session 4 (2-A)

Youth Privacy: Mechanics

Discussion Panel

Michael Harvey: Commissioner, Office of the Information and Privacy Commissioner for British Columbia (OIPC), Canada (Moderator)

Melissa Holyoak: Commissioner, Federal Trade Commission (FTC), USA (Remarks)

Sanghee Park: Commissioner, Personal Information Protection Commission (PIPC), Korea

Leanda Barrington-Leach: Executive Director, 5rights Foundation

Hilary Ware: Global Head of Privacy Legal and online Safety, Apple

Elaine Fox: Head of Privacy Europe, TikTok

Keywords

Age assurance, default setting, user control, privacy by design, global alignment

Purpose and Backgrounds

Children and adolescents growing up in digital environments are increasingly exposed to new risks, including extensive data collection, profiling, deepfake, and behavioral analysis. Owing to their developmental stage, they often face greater difficulty in recognizing these risks and exercising meaningful control over their personal information. At the same time, existing legal and technical systems are frequently structured in ways that make it challenging for the youth to understand and effectively exercise their rights.
The session was convened to examine the practical feasibility of protecting youth privacy through measures that can operate effectively in practice, based on the perspective that privacy safeguards must be ensured alongside access to the benefits of technology.

Main Discussion Points

Participants emphasized that protecting youth privacy **requires more than the articulation of principles. It must be coupled with robust enforcement and strengthened corporate accountability.** Enforcement cases under the U.S. children's Online Privacy Protection Act (COPPA), which clarified corporate obligations, were shared. These included sanctions against companies for transferring children's location or usage data to third parties without valid consent, or for failing to properly flag child-directed content in ways that enabled advertising use. Such enforcement actions were presented as establishing a minimum baseline for youth protection and correcting harmful market practices.

The **limitations of current age verification methods and the need for improvement** were key points of debate. While self-declaration lacks effectiveness, methods like biometric estimation or government ID verification present risks to privacy and accessibility, respectively. Consequently, a risk-based approach combined with international coordination was proposed as a more realistic alternative, rather than a single technical "silver bullet" solution.

The session also examined how excessive or fragmented regulation can paradoxically lead to increased data processing. Varying age brackets and authentication requirements across different jurisdictions may force companies to track and manage user ages with greater precision. It was noted that regulations intended to enhance protection could inadvertently create new privacy risks.

The session further offered a perspective of **recognizing children not merely as passive subjects of protection, but as active subjects of rights.** Korea's initiatives were introduced as examples of expanding mechanisms for children to exercise their rights such as the "Eraser Service." Additional measures under consideration include the authority to request removal of deepfake content, and developing anti-replication technologies. These initiatives were introduced as attempts to substantively guarantee children's right to self-determination. At the same time, participants noted that national initiative alone are insufficient and that greater coherence across international principles and regulatory frameworks is increasingly necessary.

Finally, **the importance of embedding child protection into the technical design phase was underscored.** Design principles such as age-appropriate default settings, data minimization, and protective measures enabled by default ("default on") were presented as more effective than regulation after-the-fact. Technically feasible measures discussed included systems that transmit only age-group information rather than exact birthdates, automated filtering of sensitive content, and requirements for parental approval when creating a new website account.

Parallel Session 5 (2-B)

Redress and Interoperability of Data Protection:

The Consumer Perspective (led by the Asia Pacific Digital Consumer Dialogue)

Discussion Panel

Amy Kato: Director, Consumers Japan (Moderator)

Guido Scorza: Member of the Board, Garante per la Protezione dei Dati Personali (Garante), Italy

Hiroshi Miyashita: Professor of Law, Chuo University, Japan

Javier Ruiz Diaz: Advisor, Asia Pacific Digital Consumer Dialogue

Natascha Gerlarch: Director for Privacy & Data Policy, Centre for Information Policy Leadership (CIPL)

Byoung-il Oh: President, Korea Progressive Network Jinbonet

Keywords

Redress mechanism, interoperability, enforcement cooperation, transparency, and accountability

Purpose and Backgrounds

As digital services and AI are launched simultaneously worldwide, data controllers and processors are everywhere. Against this backdrop, supervisory authorities vary by jurisdiction, making it difficult for them to secure enforcement authority over foreign business operators. Consumers, who are data subjects, find it difficult to exercise their rights under this fragmented structure. Amid these recurring issues, fostering cross-regulatory cooperation, linking procedures, ensuring transparency in providing information, and establishing a user-friendly redress framework are proposed as key tasks for stakeholders. This session aimed to explore how to secure practical, accessible redress mechanisms when a data breach occurs from a consumer perspective, and to foster interoperability of data governance regimes across jurisdictions.

Main Discussion Points

Panelists discussed that **a lack of global enforcement cooperation** is the biggest hindrance to consumer redress. When there are no mutual notification mechanisms for administrative dispositions and agreements governing enforcement cooperation, taking measures against foreign business operators is not feasible. Accordingly, panelists highlighted the need to establish unified regulations and international cooperation networks to integrate enforcement mechanisms. Also, panelists shared the view that regulations alone are not enough to encourage businesses to comply with privacy law and stressed the importance of creating an environment in which consumers choose businesses that prioritize privacy through consumer training.

Information exchange through the Global Privacy Enforcement Network (GPEN), the commonalities between APEC Cross Border Privacy Rules (CBPRs), EU Binding Corporate Rules (BCRs), ASEAN Model Contractual Clauses (MCCs), EU Adequacy Decisions, and EU One-Stop Shop Mechanism were introduced as **the state of play of cross-border redress and interoperability**. The panelist introduced the EU's risk-based approach and the US's harm-based approach by comparing them. The former emphasizes prevention and accountability in the pre-breach phase, while the latter requires data subjects to prove the specific harm caused by a data breach.

Meanwhile, panelists raise concerns that **government-led discussions on interoperability** do not adequately address consumer rights and redress. One of the panelists emphasized the need to strengthen research cooperation from a consumer perspective and develop policies grounded in existing international norms, such as the United Nations Guidelines for Consumer Protection.

Panelists also shared that technological advancements can complement the effectiveness of consumer redress. Ensuring transparency through CBPRs and other certifications, implementing compliance management through automation and AI, and advancing systems to address violations were suggested as measures to encourage businesses to be held accountable and provide users greater predictability in redress.

In Korea, various redress mechanisms exist, such as dispute mediation, data breach reporting, and lawsuits; however, there are limitations. A class-action lawsuit system is not established under Korea's privacy law, with the burden of proof placed on affected data subjects and with cost and time constraints. Accordingly, the need for institutional improvements, including the introduction of a class-action lawsuit system and the strengthening of the data breach reporting center's functions, was discussed.

Parallel Session 6 (3-A)

Re-Using Health Data: Balancing AI Health Innovation and Privacy in a Cross-Border Context (led by the OECD)

Discussion Panel

Clarisse Girot: Head of Division for Data Flows, Governance and Privacy, OECD (Opening Remarks&Moderator)

Khaled El Emam: Professor, University of Ottawa, Canada (Keynote)

Cheongsam Yang: Director-General, Personal Information Protection Commission (PIPC), Korea (Closing Remarks)

Limor Shmerling Magazanik: Senior Policy Analyst, OECD (Moderator)

Nitin Dhavate: DPDAI Compliance Head APMA, Novatis

Soyoung Yoo: Professor, Asan Medical Center, Korea

Soo-Yong Shin: Head of Research, Kakao Healthcare, Korea

Michael Harvey: Commissioner, Office of the Information and Privacy Commissioner for British Columbia (OIPC), Canada

Gráinee Hawkes: Deputy Commissioner, Data Protection Commission (DPC), Ireland

Mark J Taylor: Professor, Melbourne Law School, Australia

Keywords

Secondary use, research for the public interest purposes, PETs, global harmonization

Purpose and Backgrounds

Health data have dual characteristics: i) sensitive data that requires protecting individuals' fundamental rights; ii) a public asset that creates social value. While the secondary use of health data is indispensable for improving public health systems and advancing medical innovation, privacy concerns and jurisdictional differences in systems hinder its use. Today, international joint research projects and international cooperation have become the norm; however, jurisdictional differences in legal bases, consent requirements, and safeguards pose an obstacle to research involving the secondary use of health data. This session explored policy directions to facilitate the responsible use of health data, ensure privacy protection, and enable cross-border collaboration.

Main Discussion Points

Panelists shared that getting access to health data for **secondary use through consent is challenging** because data subjects may have died or moved, or there may be consent bias and under-representation. In this context, consent is not always the optimal approach for public-interest research projects. Panelists discussed the need to identify **additional lawful bases for accessing data, taking into account public interest, risk levels, and the degree of anonymization**. The concept of social license was introduced as another key factor to facilitate the availability of data for secondary purposes. Social license is the acceptance by patients, healthcare providers, the public, and civil society that health data is used in acceptable ways.

Privacy-enhancing technologies (PETs) were repeatedly introduced **as a prerequisite and a viable solution for the secondary use of health data** without patient consent. Anonymization, synthetic data, secure multi-party computation, differential privacy, federated learning, and other PETs are used to minimize privacy risks, thereby making it outside the scope of personal data and enabling its use for research and commercial purposes. Panelists discussed gaps in technical infrastructure, cost burdens, data quality and utility, applicability in medical services, and other real-world limitations. Accordingly, they discussed **the need for multi-layered safeguards, including technical, organizational, procedural, and ethical safeguards, as well as a risk-based approach**.

The importance of international cooperation and standard-setting was shared through use cases from industry and medical institutions. Regulatory disparities across jurisdictions are adding burdens in conducting multinational clinical trials and research projects. To reduce these disparities, industry and academia use federated learning, pseudonymized or anonymized data, build joint analysis models, and strengthen internal governance frameworks. The medical institution **highlighted that creating a feedback loop that research outcomes benefit patients and society is at the core of building trust**. Also, panelists discussed the need for differentiated protection proportionate to data sensitivity and purpose, and for a trustworthy, confidential environment.

Panelists suggested that **governments and regulators need to ensure access to health data, provide clarity, take risk-based regulatory approaches, give concrete guidance and education, and work to publish global guidelines**. They noted that consent should be respected where appropriate and possible, but it should not remain perfunctory. Regulators should build trust by sharing real-world use cases and outcomes, rather than relying on abstract principles. At its core, competence, commitment, and culture were presented as the foundation of trust. Panelists also added that the legitimacy and social license for data use should be continuously reviewed through public-interest tests and social governance.

Parallel Session 7 (3-B)

Data Governance for EdTech: How to protect children's Privacy?

(Hosted by DEWG (CNIL) and UNICEF)

Discussion Panel

Bertrand Du Marais: International Affairs Commissioner, Commission Nationale de l'Informatique et des Libertés (CNIL), France (Moderator)

Jasmina Byrne: Regal officer, United Nations Children's Fund (UNICEF) (Keynote)

JongYoun Rha: Professor, Seoul National University, Korea

Cari Benn: Chief Privacy Officer, Microsoft

Patricia Kosseim: Commissioner, Information and Privacy Commissioner of Ontario (IPC), Canada

Ivy Grace T. Villasoto: Division Chief, National Privacy Commission (NPC), Philippines

Zelda Gerard-Besset: Legal Officer, Commission Nationale de l'Informatique et des Libertés (CNIL), France

Keywords

EdTech, children's rights, data governance, co-regulation, rights-based design

Purpose and Backgrounds

As the expansion of EdTech and the introduction of AI-based learning tools rapidly increase the collection and usage scope of children's data, concerns were raised regarding the need to restructure data governance frameworks to protect children's rights and privacy. Emphasis was placed on ensuring that educational innovation does not occur at the expense of children's data rights, highlighting the necessity of policy approaches that advance technological development alongside rights protection. Based on UNICEF's review of EdTech data governance practices and policy recommendations, this session aimed to explore ways for diverse stakeholders—including the public sector, private companies, educational institutions, and civil society—to establish shared standards and responsibility structures. The session also sought to promote governance models that recognize children not merely as objects of protection, but as rights-holders and participants.

Main Discussion Points

A shared concern was identified that EdTech companies, while leading educational innovation, exert significant influence over children's data. Accordingly, **the need for public–private co-regulation and shared accountability** was emphasized. It was also proposed that the existing GPA e-learning resolution requires updating to adequately reflect contemporary technological environments.

Participants stressed the importance of **developing international common standards and expanding the participation of child data subjects** to ensure children's rights. UNICEF introduced its efforts to develop policy recommendations tailored to diverse stakeholder groups. It was agreed that, rather than collecting children's data without clear purpose, educational objectives should first be defined, followed by decisions on how data can be used to achieve those objectives. The importance of multi-stakeholder cooperation was highlighted, with collaboration among governments, EdTech providers, schools, and civil society identified as a core element.

Practical implementation challenges for embedding children's privacy protection in EdTech environments were also discussed. **Privacy protection was framed as needing to be embedded at the design stage rather than addressed solely through ex post regulation**. Participants emphasized **the need for data processing standards, standardized consent forms, and data minimization principles for AI textbooks and learning platforms**. At the same time, it was noted that the expansion of AI-based education platforms can contribute to reducing learning gaps, positioning the balance between protection and accessibility as a key challenge.

Regulators shared enforcement cases involving the use of children's data for marketing purposes, processing without consent, and facial recognition technologies, underscoring the **role of DPAs**. Countries are establishing institutional foundations for safe EdTech use through guidance issuance, legislative amendments, regulatory sandboxes, and international cooperation, and inter-agency collaboration was identified as a key factor for effective regulation and protection.

Parallel Session 8 (4-A)

Mastering Investigation Strategies and Choosing the Right Enforcement Tools

Discussion Panel

Brent Homan: Commissioner, Office of the Data Protection Authority (ODPA), Bailiwick of Guernsey (Moderator)

Janghyuk Choi: Vice Chairperson, Personal Information Protection Commission (PIPC), Korea

Ada CHUNG Lai-Ling: Commissioner, Privacy Commissioner for Personal Data (PCPD), Hong Kong

Philippe Dufresne: Privacy Commissioner, Office of the Privacy Commissioner of Canada (OPC), Canada

John Edwards: Information Commissioner, Information Commissioner's Office (ICO), UK

Immaculate Kassait: Data Commissioner, Office of the Data Protection Commissioner (OPC), Kenya

Dale Sunderland: Commissioner, Data Protection Commission (DPC), Ireland

Keywords

Investigation strategies, Enforcement Tools, Joint Investigation, Early Response, Prevention-Oriented Approach

Purpose and Backgrounds

This session was designed to examine recent high-profile personal data breach cases and analyze the investigation and enforcement strategies and tools that data protection authorities have applied in practice. Its objective was to trace the key factors behind successful outcomes and distill practical lessons that other authorities can adopt. Rather than serving as a simple exchange of case examples, the session focused on the full enforcement cycle– from the initiation of investigation and the definition of scope, to the selection of investigative tools and the choice of enforcement measures. Through this structured review, the session sought to strengthen a shared foundation for learning among supervisory authorities, enabling them to enhance investigative expertise, establish clearer criteria for tool selection, and improve cooperation mechanisms in an environment of limited resources and rapidly increasing caseloads.

Main Discussion Points

Regarding **enforcement strategy**, it was suggested that **differentiating approaches based on the type** of incident is crucial. For **data breach cases**, an effective approach was shared that focuses on fact-finding and root-cause analysis, utilizing digital forensics and log analysis to clarify the circumstances and scope of the leak. In contrast, for **general infringement cases**, a method was introduced to identify infringement factors structurally by analyzing data processing flows, while simultaneously providing substantiation of violations through technical tools such as traffic analysis. **Clearly defining issues at the outset** and **setting the scope of the investigation within the agency's capacity** were identified as the **primary factors determining the integrity and effectiveness of an investigation**.

In terms of **enforcement measures**, the discussion focused on **strategies that combine corrective orders, recommendations for improvement, and public disclosure orders, rather than limiting actions to administrative fines**. In particular, utilizing **public disclosure** and **media engagement** to induce changes in corporate behavior and raise public awareness was presented as a significant policy tool. At the same time, for new industries and emerging technologies, it was shared that a strategy centered on **prior inspections and prevention** is more effective than an **ex-post, sanction-oriented approach** in reducing the actual likelihood of infringements.

For **inter-agency cooperation** and **international joint investigations**, **key factors** included **cooperation built on trust, the setting of clear common goals, and prior agreement on the timeline and scope of the investigation.** The success of these efforts was attributed to clarifying objectives and schedules before the joint investigation and delegating roles based on differences in enforcement powers, thereby increasing efficiency. Furthermore, it was shared that **early detection through constant monitoring** and the rapid initiation of preliminary inquiries led to more effective enforcement.

Finally, in investigations involving large digital platforms, it was underscored that **keeping the investigative scope narrow and well-defined, while applying legal standards based on existing case law and guidelines, is vital for managing technical complexity.** It was also noted that by approaching cases through established doctrines (such as protection obligations in the design and default setting stages, protective measures for cross-border transfers, and the Schrems rulings) authorities were able to secure predictability and clarity in both the investigation and the final enforcement process.

Parallel Session 9 (4-B)

Empowering Data Subjects through Data Portability Mechanisms: New Experiment

Discussion Panel

Carly Kind: Commissioner, Office of the Australian Information Commissioner (OAIC), Australia

Anu Talus: Chairperson, European Data Protection Board (EDPB)

Michael Webster: Privacy Commissioner, Office of the Privacy Commissioner (OPC), New Zealand

Lim Taehun: Professor, Korea University, Korea

Sun Jaewon: CEO, Merakiplace, Korea

Keywords

MyData, data portability, right to self-determination, technology standardization, service innovation

Purpose and Backgrounds

Data portability is a privacy right that empowers data subjects to have control over their data and transfer it to the service they want. It has the potential to enable customized services, foster competition, drive data-driven innovation, and enhance transparency. To effectively establish the MyData initiative, technology standardization, public-private cooperation structures, awareness-raising, and participant roles and responsibilities should be implemented in parallel. This session aimed to review the significance of data portability rights as a key mechanism to strengthen data subjects' rights to self-determination, and to share adoption cases and implementation outcomes to explore conditions for broader adoption.

Main Discussion Points

Panelists agreed that **the right to data portability gives data subjects control over their data and offers a means that has the potential to support innovation and greater competition**. However, the right to data portability is not widely used. Panelists suggested next steps to foster the right to data portability: **reviewing the definition and policy objectives, achieving standardization, and ensuring data subjects' participation**.

Australia has the Consumer Data Right (CDR) scheme. It was first deployed in the banking sector and has since been extended to the energy sector. However, the user adoption rate remains low, and customers prefer alternative methods for transferring data between providers, such as screen scraping. The Australian government is currently undertaking a reset of this scheme to promote the Consumer Data Right as a privacy-protecting measure.

The European Union has added multiple layers to the framework for data transfer rights through the Data Act and the Digital Markets Act (DMA), building on the GDPR. The GDPR does not exclude data from transfer rights based on the legal basis for processing, and not all entities are designated as very large online platforms (VLOPs), also known as gatekeepers, under the DMA. In this sense, the scope of regulatory application may vary on a case-by-case basis. To further improve the effectiveness of data portability rights, the panelist emphasized the need to lay the institutional and technical groundwork, raise awareness, and improve understanding of data portability.

New Zealand is currently establishing a Consumer Data Right (CDR). It is similar to Australia's approach to data portability. Both the data holder and the accredited requester must obtain explicit customer authorization; otherwise, information cannot be shared. The panelist suggested that the problem definition and policy objectives should be clarified before adopting the right to data portability.

In Korea, panelists emphasized the need to increase interconnectedness among the financial, public, and medical sectors and to strengthen cross-regulatory cooperation to enable more data subjects to benefit from data portability rights. Panelists agreed that standardization for data transfer systems is essential for seamless service delivery, but there are concerns that it might make the systems rigid. In the healthcare sector, panelists noted that data fragmentation, insufficient participation, security concerns, infrastructure limitations, and other constraints exist, but the MyData initiative could enable new business models and deliver tangible value.

Personal Information
Protection Commission

Press Release

Expanding Support for the Joint Statement on Trustworthy Data Governance for AI: Twenty Data Protection Authorities Commit to Innovative and Privacy-Protecting AI

September 17, 2025

At the Global Privacy Assembly (GPA) Seoul 2025 (15-19 September, 2025), twenty data protection authorities (DPAs) – Australia, Belgium, Bulgaria, Canada, Croatia, Finland, France, Germany, Hong Kong, Ireland, Italy, Korea, Netherlands, New Zealand, Luxembourg, Macao SAR, Spain, Poland, Sweden, and the United Kingdom – signed the Joint Statement on Building Trustworthy Data Governance Frameworks to Encourage Development of Innovative and Privacy-protecting AI (Joint Statement).

The Joint Statement was initially signed by the Office of the Australian Information Commissioner (OAIC), the Personal Information Protection Commission (PIPC), the Information Commissioner's Office (ICO), the Commission Nationale de l'Informatique et des Libertés (CNIL), the Information Commissioner's Office (ICO), and the Data Protection Commission (DPC) at a side event, co-organized by the CNIL and the PIPC, to the AI Action Summit in Paris last February.

Building a Reliable Governance Framework for Trustworthy AI

The Joint Statement highlights the numerous opportunities offered by AI across various fields. At the same time, it also sheds light on several risks, including concerns over data protection and privacy, discrimination and bias, disinformation, and AI hallucination.

To ensure AI is compliant with the current legal frameworks, the DPAs advocate incorporating data protection principles by design in the approach to AI systems, establishing robust data governance and anticipating risk management.

The statement also underscores the increasing complexity of data processing by AI and emphasizes the diversity of actors involved, and the need for a regulatory framework adapted to technological advancements.

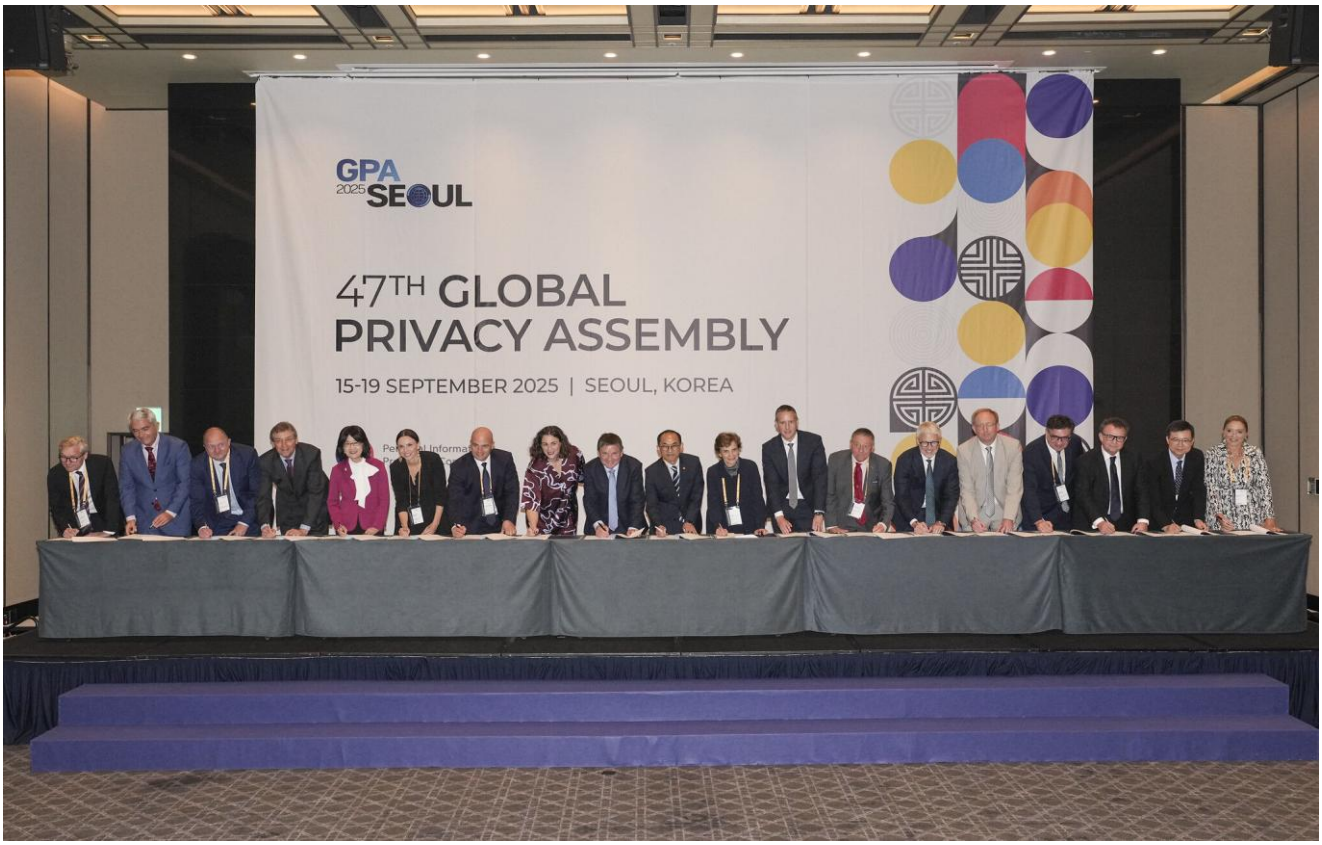
Commitment to Addressing Legal Uncertainties Raised by AI

Twenty DPAs recognize their leading roles in shaping data governance to address challenges raised by AI and committed to:

- clarify legal bases for the processing of data by AI;
- share information and establish appropriate security measures;
- monitor the technical and societal impacts of AI by involving various actors;
- encourage innovation while reducing legal uncertainty;
- strengthen cooperation with other competent authorities (consumer protection, competition, intellectual property).

On the occasion of the GPA Seoul 2025, a joint signing ceremony was held on 17 September 2025. At the ceremony, the DPAs gathered together to formally express their support, marking an extended global commitment to innovative and privacy-protecting AI.

Taking this opportunity, the DPAs reaffirmed their shared commitment to the Joint Statement and expressed their hope that more like-minded DPAs will join this meaningful initiative.



[Full Text]

Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI

17 September 2025

1. Artificial intelligence (AI) presents immense opportunities for the benefit of humanity, innovation in science, the economy, and society as a whole. AI also poses significant risks with respect to the protection of fundamental rights such as data protection and privacy, but it also poses risks of discrimination, misinformation and hallucination that are often caused by the inappropriate processing of data.

2. We recognize the need to fully cultivate public trust and harness the transformative benefits AI could bring. We recall that AI should be developed and deployed in accordance with data protection and privacy rules and other norms. This includes embedding privacy-by-design principles into AI systems from the initial planning stage and implementing robust internal data governance frameworks. These frameworks should incorporate technical and procedural safeguards for effective management and mitigation of risks throughout the entire lifecycle of an AI system.

3. Moreover, we recognize that in the current environment surrounding AI development and deployment, data processing has become exceedingly complex. Indeed:

a. It is developed and deployed across many different sectors, including health, public services, public security, human resources, and education;

b. It involves a great number of stakeholders scattered all over the world and complex value chains, including dataset creators, model providers, dataset and model hosting platforms, integrators, annotators, system deployers, and end-users;

c. It operates at large scale with AI technologies necessitating vast amounts of data that are at the core of these systems;

d. It implies complex data processing that poses significant challenges for its control and increases the needs for transparency to foster the protection of privacy and other fundamental rights; and

e. It evolves at a very fast pace with major scientific and technological breakthroughs being recorded on a daily basis.

4. Citizens' and businesses' need for answers and legal certainty is therefore increasingly pressing in order to enable the development of AI within trustworthy data governance frameworks. At the same time, the application of rules should provide a sufficient degree of flexibility for various innovative efforts to take place consistently with the protection of privacy and personal data. We recognize therefore the importance of supporting players in the AI ecosystem in their efforts to comply with data protection and privacy rules and help them reconcile innovation with respect for individuals' rights.

Highlighting data protection authorities' leading role in shaping data governance to address AI's evolving challenges, we commit to the following:

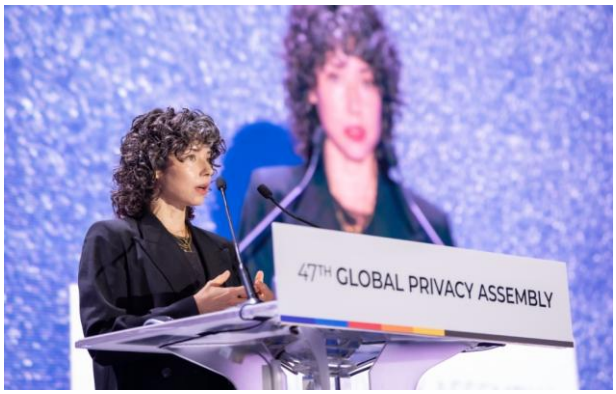
5. To foster our shared understanding of lawful grounds for processing data in the context of AI training in our respective jurisdictions. Clear standards and requirements should be developed to ensure that AI training data is processed lawfully, whether based on consent, contractual necessity, legitimate interest, or other legal justifications. In doing so, attention should be paid to various relevant factors, including the specific purposes of AI development, the characteristics of the requisite data, the reasonable expectation of data subjects, and associated risk mitigation strategies.

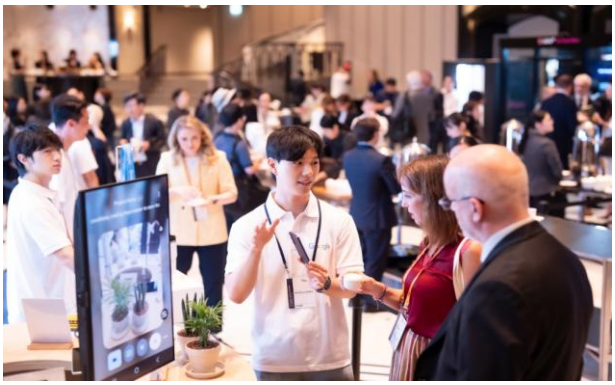
6. To exchange information and establish a shared understanding of proportionate safety measures based on rigorous scientific and evidence-based assessments and tailored to diversity of use cases. The relevance of these measures should be regularly updated to keep pace with evolving AI data processing technologies and practices.

7. To continuously monitor both the technical and societal implications of AI and to leverage the expertise and experience of Data Protection Authorities and other relevant entities, including NGOs, public authorities, academia, and businesses, in AI-related policy matters when possible.

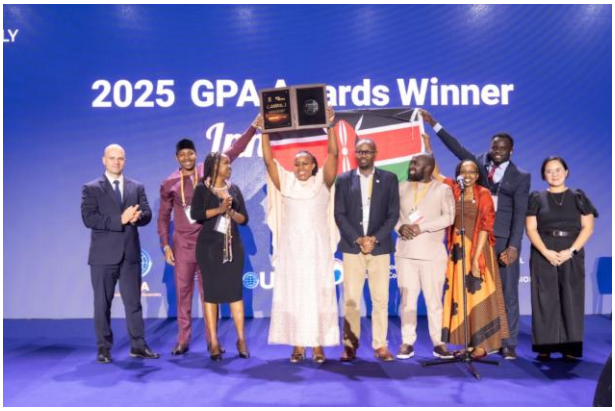
8. To reduce legal uncertainties and secure space for innovation where data processing is essential for the development and deployment of AI. This may include institutional measures, such as regulatory sandboxes, as well as tools for sharing best practices. These measures and tools should be grounded in public trust and be consistent with principles of privacy and data protection.

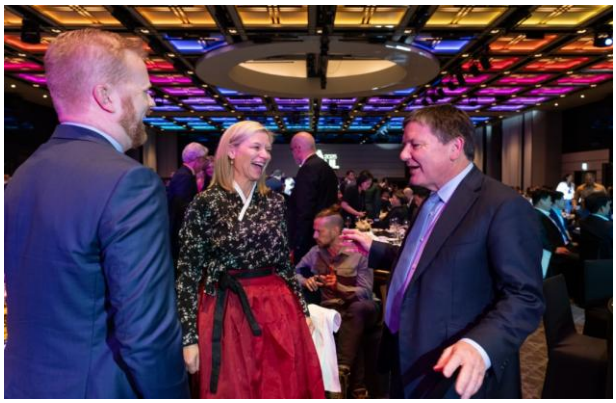
9. To strengthen our interactions with relevant authorities, including those in charge of competition, consumer protection and intellectual property, to facilitate consistency and foster synergies between different applicable regulatory frameworks to AI systems, tools and applications. Dialogues involving diverse players in the AI ecosystem should also be encouraged.

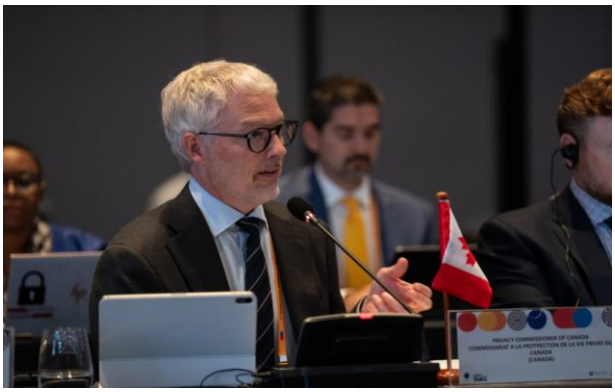

47TH GLOBAL PRIVACY ASSEMBLY

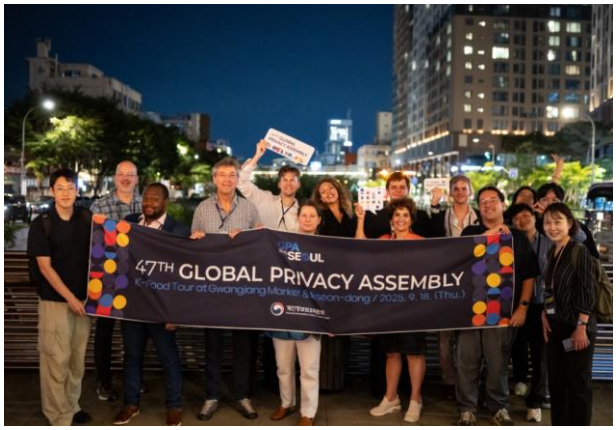


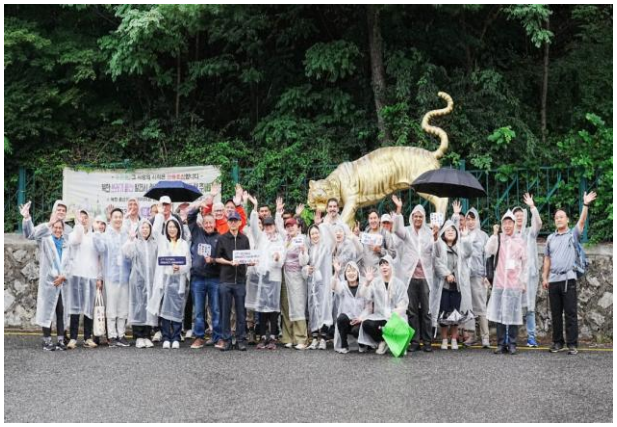

Giovanni Buttarelli Awards 2025
GPA
NATIONAL
PRIVACY
COMMISSION


2025 GPA






SEOUL
47TH GLOBAL PRIVACY ASSEMBLY



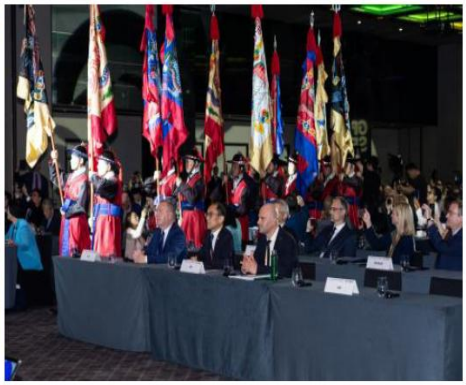
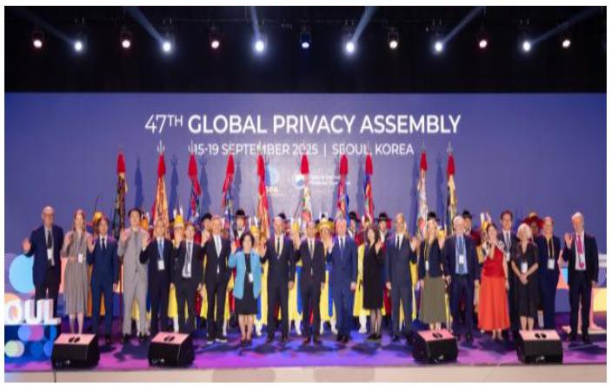




Congratulatory Message
Lee Jae Myung

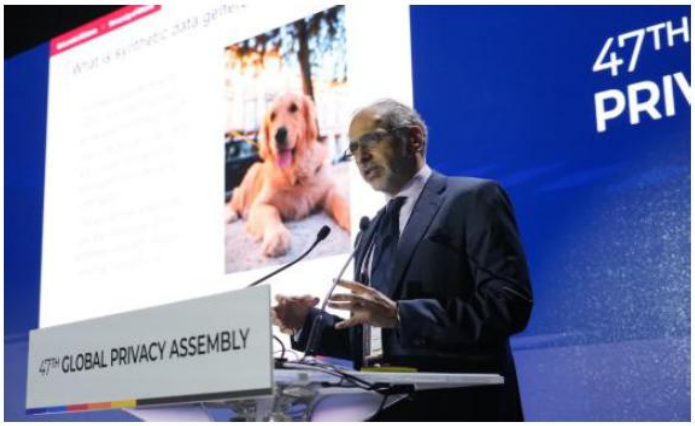
GPA 2025 SEOUL

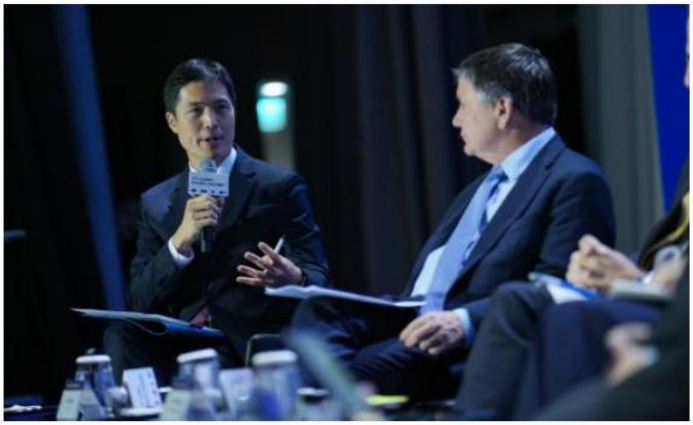
GPA 2025
SEOUL

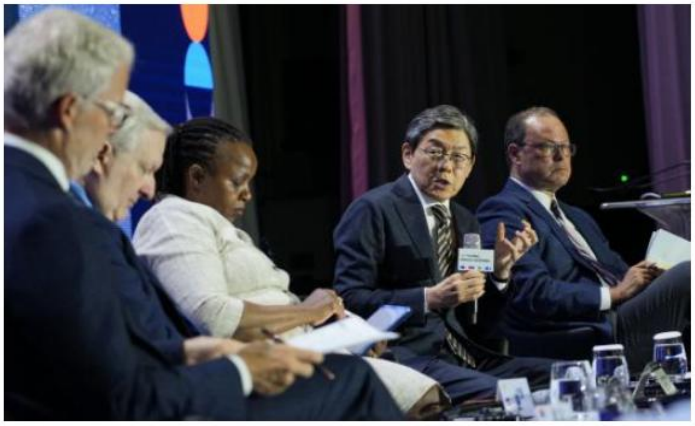
GPA 2025
SEOUL


47TH GLOBAL PRIVACY ASSEMBLY

47TH GLOBAL PRIVACY ASSEMBLY

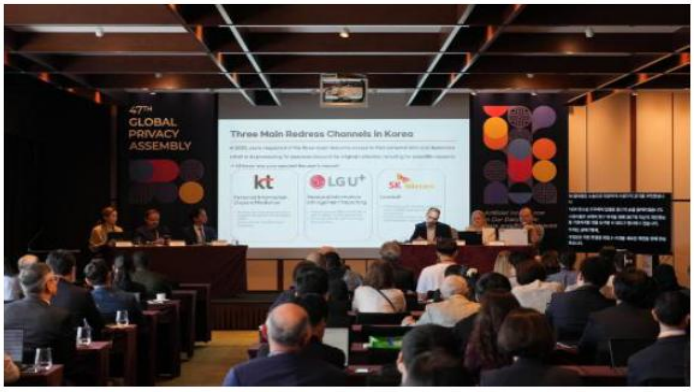

GPA 2024 SEOUL

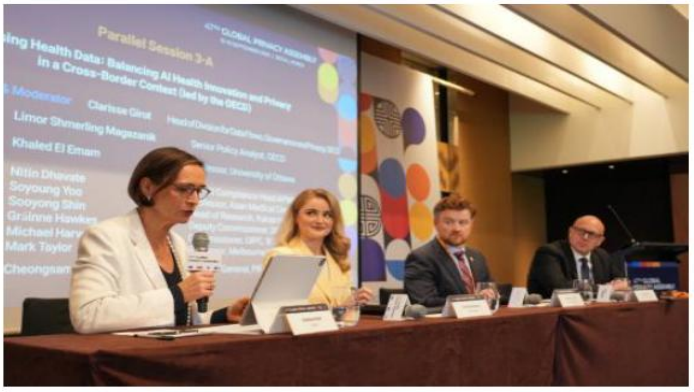

47TH GLOBAL PRIVACY ASSEMBLY

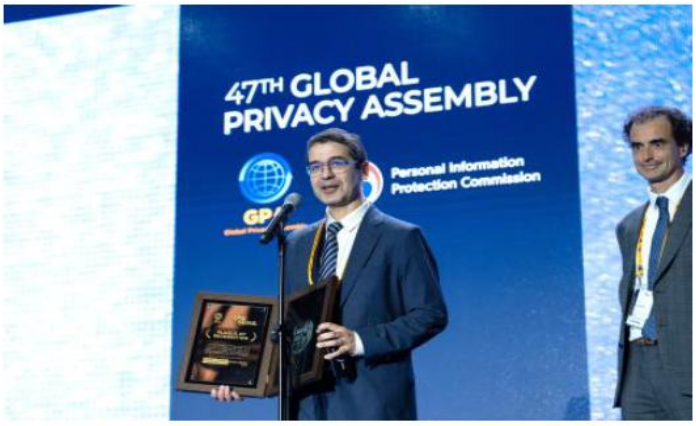




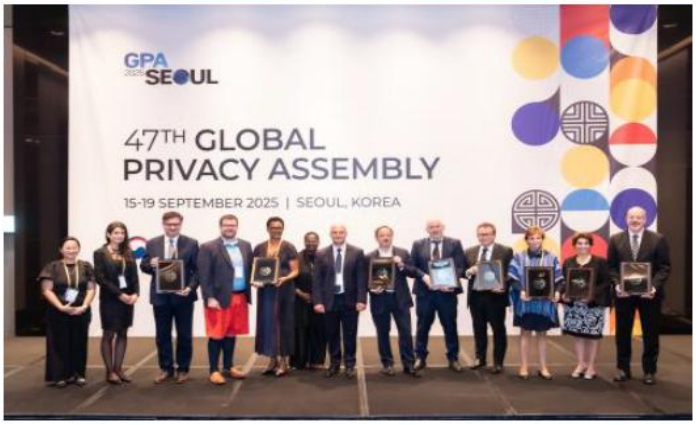

47TH GLOBAL PRIVACY ASSEMBLY
GPA
Personal Information Protection Commission


47TH GLOBAL PRIVACY ASSEMBLY
Three Main Redress Channels in Korea
kt
LG U+

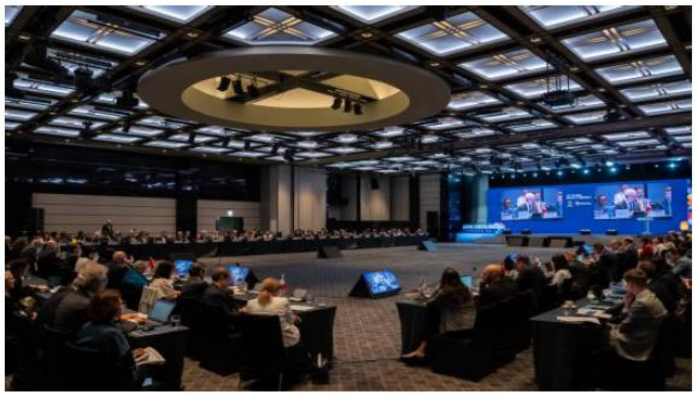

Parallel Session 3-A

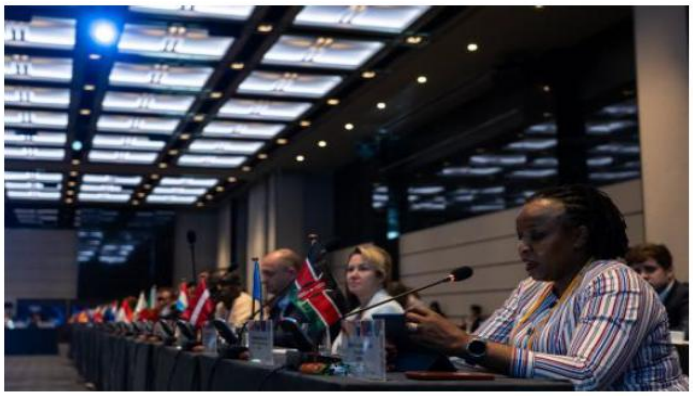

47TH GLOBAL
PRIVACY ASSEMBLY
Personal Information
Protection Commission


GPA Awards & Gala Dinner


GPA
SEOUL
47TH GLOBAL
PRIVACY ASSEMBLY
15-19 SEPTEMBER 2025 | SEOUL, KOREA


GPA
SEOUL
47TH GLOBAL
PRIVACY ASSEMBLY
15-19 SEPTEMBER 2025 | SEOUL, KOREA





GPA 2025 SEOUL

Personal Information Protection Commission