



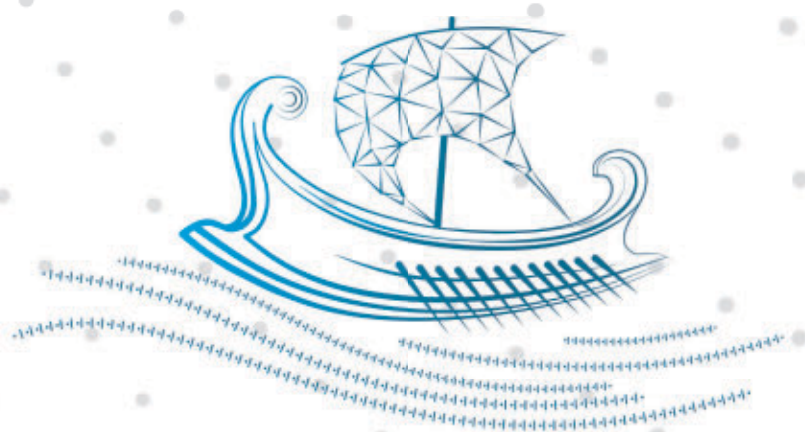
41ST INTERNATIONAL CONFERENCE
OF DATA PROTECTION AND PRIVACY COMMISSIONERS

CONVERGENCE AND CONNECTIVITY

RAISING GLOBAL DATA PROTECTION STANDARDS IN THE DIGITAL AGE

21-24 October 2019
Tirana - Albania

— CONFERENCE REPORT —



41ST INTERNATIONAL CONFERENCE
OF DATA PROTECTION AND PRIVACY COMMISSIONERS



TABLE OF CONTENTS

Overview of the week	04
Foreword	05
Closed Session	06
Open Session	10
Annex A: Side events	36
Anex B: 2019 Global Privacy and Data Protection Awards	53
Anex C: Special thanks to the Programme Advisory Committee (PAC)	55
Annex D: Acknowledgements	56

OVERVIEW OF THE WEEK

Event overview of the week , Tirana

Date	Time	Event	Venue
Sunday 20 October 2019	19:00-20:00	Closed Session Welcome Cocktail	National Museum
Monday 21 October 2019	09:00-18:00	Closed Session Cultural Tour	Palace of Congresses
Tuesday 22 October 2019	09:00-14:00 14:30-18:00	Closed Session Side Events	Palace of Congresses
Wednesday 23 October 2019	09:00-17:30 19:30-22:00	Public Session Concert show Gala Dinner	Palace of Congresses
Thursday 24 October 2019	08:45-13:30 14:30-18:00	Public Session Side Events	Palace of Congresses
Friday 25 October 2019	09:00-18:00	Side Events Social Activities	<i>Venues in Tirana District</i>

41st INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS¹

CONVERGENCE AND CONNECTIVITY RAISING GLOBAL DATA PROTECTION STANDARDS IN THE DIGITAL AGE

OCTOBER 21 – 24, 2019 | TIRANA, ALBANIA

The 41st International Conference of Data Protection and Privacy Commissioners was held from 21 to 24 October 2019 in Tirana, Albania, attracting more than 700 hundred delegates from across the world. It constituted one of the most valuable annual international events to share information in the privacy and data protection field. The Conference stressed the need for convergence and cooperation, not only among global regulatory authorities, but also among governments, civil society and industry considering that dramatic advances in digital technology continue to challenge law and regulations, business models and democracies around the world.

Data protection has taken a giant leap in the past two years. The world's data protection and privacy authorities came together in Tirana to set priorities for the coming year. The conference focused on how best to make laws speak to one another, and how to maximize potential in people's connected lives while maintaining high standards of data protection and privacy.

This report reflects the historic progress made towards regulatory cooperation and high data protection standards. Members of the ICDPPC agreed a framework that continues to strengthen the group's position building on a policy strategy that sets out a clear vision for the organization for the next two years. The Conference decided to change its name as agreed by the Closed Session and it will from now on be referred to as the "Global Privacy Assembly (GPA)" For the purposes of this report, it will be referred to as ICDPPC, as the name change to GPA only come into effect shortly after the conference. The name GPA reflects the year-round activity of this community, rather than a once-per-year conference. Further reporting about the event may be found on the GPA website.

¹Remarks made in summary of the 41st International Conference of Data Protection and Privacy Commissioners



CLOSED SESSION

The International Conference of Data Protection & Privacy Commissioners (ICDPPC) is a recognized international community of privacy and data protection authorities. Throughout its 41-year history, the conference has met each year, bringing together data protection authorities from local, national and international levels, to share knowledge and to offer support.

This year's Conference was one of the most defining in ICDPPC history. The closed session – which is open only to accredited members and observers of the ICDPPC – was held on Monday October 21 and Tuesday October 22, 2019 at the symbolic Tirana Palace of Congresses. The closed session focuses on the ordinary and discretionary business of the Conference.

As the GPA community continues to grow, the 41st ICDPPC admitted the following members to the Conference: Chilean Transparency Council, Chile;



The Closed Session was preceded on 20 October 2019 by the 55th Meeting of ICDPPC Executive Committee.

Commission Nationale pour la Protection des Données à Caractère Personnel, Gabon; Autorità Garante per la Protezione dei Dati Personali, San Marino; National Agency for the Protection of Personal Data, Sao Tome and Principe; OECD Data Protection Commissioner (the latter without voting rights).

The challenge was for the Conference's Closed Session on AI to focus on the practical issues of mobilizing the ICDPPC 2018 AI Declaration, in the session titled "From Theory to Practice" which invited experts from industry, standards and engineering, and regulation to offer their analysis. A speech and presentation by Dr. Ing. Konstantinos Karachalios, Managing Director IEEE SA, may be found [here](#).

They came together to discuss the principles outlined in the AI declaration, and offered their views before a robust debate took place by also involving the audience through a Q&A session.

The audience was fully engaged and offered challenging, critical questioning, with members also highlighting the need to collaborate and coordinate efforts. This was reinforced by audience members on several occasions, when discussing the power imbalance between the leaders in AI development and its use in industry, and the regulatory community.

The session called for collaboration between the regulatory community and the engineers, data scientists and practitioners, who ultimately, are building the modern data enabled world around us.



The session on the Future of the Conference (FOTC) Matters on Monday afternoon represented a key moment for the membership which adopted a new name and logo, Global Privacy Assembly (GPA). This work was led by the Executive Committee member from Mexico, the INAI, and was the result of extensive consultation with the membership ahead of the Annual

Meeting. During this session, the membership also adopted a background paper on the interpretation of the autonomy and independence criteria in the conference accreditation process as well as adopting the FOTC Working Group recommendation on the creation of a contact group with external stakeholders which will be named GPA Reference Panel.

The closed session of the 41st International Conference of Data Protection & Privacy Commissioners (ICDPPC) adopted a number of high-level resolutions addressed to their respective governments. These resolutions are important as they signal the general direction in which the global community of regulators is heading and provide a glimpse into their evolving perspectives on some of the most pressing data protection issues of the day. The Adopted Resolutions of this year's conference were:

Resolution on the Conference's strategic direction and first ever Policy Strategy.

By this resolution, the Conference adopts a Conference Strategic Plan that includes among its strategic priorities: advancing global privacy in a digital age, maximizing the Conference's voice and influence, and capacity building for the Conference and its members.

Resolution to support and facilitate regulatory co-operation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the digital economy.

This resolution emphasizes the need for continued collaboration between data protection and consumer protection authorities at both domestic and international levels, with a view to fostering better protection for citizens and consumers in the digital economy.

Resolution to address the role of human error in personal data breaches.

This resolution focuses on security safeguards that are appropriate to take against human error, which may include building a workplace culture where privacy and personal data security are treated as organizational priorities, establishing robust and effective data protection and privacy practices, procedures and systems, and adopting monitoring and auditing mechanisms.

Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights.

This resolution advocates that governments around the world should reaffirm a strong commitment to privacy as a fundamental human right, vital to the protection of other democratic rights. It also calls upon businesses to show demonstrable accountability by actively respecting privacy and other human rights across all commercial activities as a key aspect of legal compliance, corporate social responsibility and an ethical business approach.

Resolution on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement.

The Conference resolves to continue to encourage efforts to bring about more effective cooperation in cross-border investigation and enforcement in appropriate cases. This includes continually contributing their knowledge and expertise to a new permanent online public repository section on the ICDPPC website that links to publicly available enforcement cooperation resources.

Resolution on social media and violent extremist content online.

Highlighting the terrorist attacks which took place in Christchurch, New Zealand in March 2019, the Conference resolves to urge social media providers to take steps to stop the dissemination of terrorist and violent extremist content using their platforms, while continuing to protect freedom of expression.

The ICDPPC Executive Committee, among its other responsibilities, assesses the applications from member authorities to host the next conference. In early 2019, the Committee announced that the next conference will be hosted in Mexico by the National Institute for Transparency, Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) (INAI). After Mexico, annual conference will take place the following year in New Zealand. Elections were held during the closed session proceedings of the 41st ICDPPC. Elizabeth Denham CBE, UK Information Commissioner, was confirmed as ICDPPC chair for a further two years. Marguerite Ouédraogo Bonane, President of the CIL, Burkina Faso was re-elected to the Executive Committee. Eduardo Bertoni, Director of Access to Public Information Agency, Argentina was elected to the Executive Committee.



CONVERGENCE AND CONNECTIVITY

RAISING GLOBAL DATA PROTECTION STANDARDS IN THE DIGITAL AGE

Open Session

On Wednesday 23 October and Thursday 24 October 2019, the Open Session of the 41st International Conference of Data Protection and Privacy Commissioners was held at the Palace of Congresses in Tirana.

The conference welcomed over 700 delegates, including members and observers of the ICDPPC, as well as private and public sector attendees, academia, civil society representatives and journalists. They engaged in an inclusive, cross-disciplinary and interactive debate on convergence and connectivity.

DAY 1 | Wednesday, 23 October

Day one of the open session started with the Albanian Information and Data Protection Commissioner, Mr. Besnik Dervishi. In his address, he highlighted that *"We live in a time where personal data are said to be the solution to any problem, implying that every aspect of life and our relations provide an opportunity for the data market. Companies in the world control our data and it is our responsibility as Commissioners to guarantee protection to every individual."*



Mr. Dervishi invited the **UK Information Commissioner and Chair of ICDPPC Elizabeth Denham CBE** to take the floor. She welcomed attendees at the public

session and on behalf of the conference, thanked Commissioner Dervishi and his team, as well as the ICDPPC 2019 Programme Advisory Committee co-led by Commissioner Dervishi and Mr. Peter Hustinx, non-Executive Board Member to the UK ICO and former European Data Protection Supervisor. She provided a brief summary of what transpired at the Commissioners' closed-door session. She noted that "privacy" has become "mainstream." People around the world expect more information about how their data is handled. She stressed the importance of future international collaboration and regulatory cooperation to develop shared strategies and high data protection standards.



Commissioner Denham also highlighted the increased focus on the role of data protection as a relevant consideration in competition analysis by international regulators. She noted that the International Data Protection and Privacy Commissioners' Conference, and the ongoing assembly of global regulators, resolved to be more transparent in the future with respect to the regulated community and other interested parties.



She added that a new name and logo for the group would be announced before the 2019 conference concludes, reflecting the continued growth of the conference.

Before proceeding to other substantive discussions, Commissioner **Denham** introduced a film tribute to the **late Giovanni Buttarelli**, who passed away in August. Giovanni served as European Data Protection Supervisor, host for the 2018 Data Protection and Privacy Commissioners' Conference, and was widely recognized as a thought leader in the field, especially on the subject of data protection and ethics. He was an inspiring figure in the international data protection and privacy community, a great friend and inspiration to many, and truly a giant in the privacy community.

Opening Address

EDI RAMA | Prime Minister

The Prime Minister of the Republic of Albania, **Edi Rama** offered a warm welcome to attendees: *"We're at an important moment for our civilization," Rama said, "which faces the most threatening attack on personal data and on personal lives."* He pointed to the delegates and attendees as the ones who will help protect human dignity and personal information. *"We have to fight,"* he said. *"We're living in an era with shamelessness, an era when it's no longer shameless to be acting and saying shameful things, fighting shamelessness is the core. I value this network and the knowledge that comes from all of you"* he stated.



PANEL DISCUSSION

Panel I: Global convergence in data protection law: where are we converging and what progress are we making towards common standards?

The panel explored what convergence means in practice and debated the value of both further developing common standards and work on making laws interoperable.



Moderator: **Graham Greenleaf**, Professor of Law & Information Systems, University of New South Wales, Faculty of Law



Chawki Gaddès, Head of the Tunisian DPA (INDPDP), and President of the Francophone Association of Personal Data Protection Authorities (AFAPDP)



Bruno Gencarelli, Head of International Data Flows and Protection, European Commission



Dr. Felipe Rotondo, Member of the Executive Council of the URCDP



Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong, China



Jan Kleijssen, Director of Information Society and Action Against Crime (Council of Europe)



Noboru Yamaji, Commissioner for International Cooperation, Japan PPC



Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales, Faculty of Law, opened the discussion by noting: *“40 years ago development was near complete on the first two international data protection agreements: the OECD guidelines and Council of Europe Convention 108. Both of these instruments responded to a fundamental question with which we still grapple today: how can the flow of personal data between countries be facilitated by common standards for data protection agreed between groups of countries.”*

On this premise, the first panel of the Conference’s Open Session addressed the issue of convergence and interoperability in a positive way, bringing together perspectives from each of the main regions of the globe that are developing instruments and techniques to deal with the issue, identifying convergence of approaches, and suggesting how they can be further strengthened into common standards.

Chawki Gaddès, Head of the Tunisian DPA (INDPDP), and President of the Francophone Association of Personal Data Protection Authorities (AFAPDP), addressing in this panel global convergence in data protection law, said that:… We also find the foundation for convergence in much broader standards, initially adopted at a regional level, but which are now being adopted more universally, I speak of course of Convention 108. Convention 108+ in its preamble states, I quote: *[...that it is necessary to secure personal autonomy based on a person’s right to control of his or her personal data and the processing of such data.] It is thus a case which explains the assertion “convergence must be done around common values and in networks and spaces, to claim thereafter certain universality”.*

Bruno Gencarelli, Head of International Data Flows and Protection at the EU Commission said that such convergence was already a reality. There was also general discussion around the fact that the **Council of Europe’s Convention 108+** was already a leading international data protection pact that has been agreed to by 26 COE member states and one non-member. *“When I started working on privacy issues six or seven years ago, I’d be faced with three observations: First, privacy is a sort of European obsession. It is a question of culture, of history, etc. Second, nobody cares anymore about privacy. It is an outdated topic in the digital era. Third observation, there is no need for legislation in this area. Industry will figure it out; it is too complex for legislation. We are talking about truly universal values and a truly global trend.”*

Dr. Felipe Rotondo, Member of the Executive Council of the URCDP, added to the panel that: *“in this matter it requires an open mind in order to foster data protection effectiveness. Free and safe data flows are needed and that is vital to promote trust in the data protection global system.”*

Hong Kong Privacy Commissioner Stephen Wong described the differences between Hong Kong and mainland China privacy regimes and cybersecurity laws. *“There are two different legal systems within one country. Indeed, the*

Hong Kong data protection legislation is one of the oldest in the region.” He added, “Data has been used as a weapon in Hong Kong to attack opponents, holding different opposing or ill-founded views.” He noted that mainland China observed a “sectoral” approach to privacy, while Hong Kong adopts a comprehensive approach more like the EU. While Hong Kong does not have data localization requirements, this is not the approach taken in mainland China and highlighted the complex status of the various mainland China cybersecurity laws and sectoral regulations.

Wong added, “So we are proposing legislative reforms, which are the result of significant changes that have taken place recently, in particular the GDPR in Europe implemented a year ago, also the recent cases, data breaches cases in particular in Hong Kong that we investigated.”

Jan Kleijssen, Director of information Society and Action Against Crime

explored what convergence means in practice and elaborated on the work needed to make laws interoperable. Growing public awareness of the consequences of data abuse together with the global rollout of AI applications will generate strong pressure for global legally binding data protection standards. Convention 108 offers the best response, he added. “Modernized Convention 108 sets higher standards. I am personally convinced it will. I see two main reasons for this. The first, I think, is a greater awareness of the risk of data manipulation. Cambridge Analytica and other scandals that have appeared have raised awareness of what can happen with personal data. Second, new developments, I am responsible for the work we do on artificial intelligence and I think that AI and other technologies are going to be a catalyst in this factor. Artificial intelligence for the good, trusted artificial intelligence will require trusted and unbiased data, therefore, for these systems to work properly, the exchange of trusted data and safeguards to ensure that what comes out of these applications, will benefit the society”

Noboru Yamaji, Commissioner for International Cooperation, Japan

PPC, introduced some of the initiatives that are being taken in the field of international cooperation. *“We as PPC, would like to work together with all the Authorities on the establishment of a global system that goes beyond the legislative framework that exist at the moment in the fellow countries like the United States or European Union.”*

Marc Rotenberg, CEO of EPIC

during his commentary, stressed the importance of enforcement as the necessary next steps in order to globalize GDPR. He said: “Civil society is watching closely to see what steps will be taken under the GDPR, to give meaning to this most critical legal framework. The challenge for this global framework, I would suggest, will be adoption of the Council of Europe Convention. It needs to be ratified by more countries around the world to give it the global force that is intended”. He described the OECD privacy guidelines originally adopted in 1980 and some changes made in 2013. “Enforcement, adoption, implementation. That is how we give meaning to global privacy frameworks. But I think there is more work still to do”. He raised two questions to the audience:

1. Will we stop technologies of mass surveillance or will we simply regulate their use?

2. Will we allow surveillance capitalism to capture more of the information economy or will we establish rules to safeguard the dignity and autonomy of the individual?

He advocated for a moratorium on facial recognition technology, and for a moratorium on mass surveillance, as well as for study of the embedded biases in the use facial recognition technology.

PANEL DISCUSSION

Panel II: Addressing the global privacy challenge of data driven business models

Data protection and privacy have never been more in the public eye, but focus is often not on the laws that provide protection but the issues that directly engage the public. Abuses of personal data for political campaigning, massive data breaches, hidden surveillance/observation, and concerns about the impact of surveillance capitalism all drove the debate.



Moderator: **Elizabeth Denham CBE**, UK Information Commissioner, ICO and Chair of ICDPPC



Sally Hubbard, Director of Enforcement Strategy, Open Markets Institute, USA



Simon Hania, Data Protection Officer, Uber

Carole Cadwalladr, Investigative Journalist and Features Writer, The Guardian and The Observer



John Edwards, New Zealand Privacy Commissioner



In this panel addressing “the global privacy challenge of data driven business models,” the journalist and civil society panel members and one privacy commissioner issued their respective views on the role of US tech companies. Moderator, Elizabeth Denham spoke of the reasons why we are debating this topic. *“We are debating this topic not in just one jurisdiction, and in fact it is not just regulators. It is companies too, it is the media too, it is journalists, and it is civil society. We are all concerned about the potential of business models and their corporate and legal duty to act responsively”.* She added, *“We are not dealing with one company at a time. We are increasingly dealing with an ecosystem and we need to find new ways to do that. Our work is getting harder. It is not all about the law. It is about ethics, it is about individual expectations, it is about the trust that companies and public bodies need to retain of their citizens and consumers. And I think everybody in this room knows that we never get to rest. We need to figure out where the red lines are”.* As a regulator, she said, we have to answer the lawmakers on the ultimate question, which is how do we support the innovation and at the same time protect people and maintain our humanity.

Guardian journalist **Carole Cadwalladr**, who led the Guardian’s investigative work on Cambridge Analytica, echoed concerns about the harmful effect tech platforms have on people and democracies around the world, noting that Facebook recently changed its policies to allow for political advertisements even if they contain misinformation. *“The vast power and opaque nature these companies have and the profound impacts they’re having in countries around the world”* is immense, she said. *“It’s vital that we continue to interrogate them.”* Carole Cadwalladr further explained how she got to know the Cambridge Analytica, going back to particularly focus to what happened in the referendum in Britain and also to some degree in the US elections. *“Last year I wrote about Cambridge Analytica and Facebook and data and I started looking into it a bit more, and the more I found out, the more unsettled I was because I discovered that this wasn’t a data company per se, it was a military contractor.”*

And I wrote this first article about Cambridge Analytica and I had a stroke of luck at that point.” Cadwalladr explained that this stroke of luck involved regulators starting to look at the issue, after the article was published.

Businesses in Europe worry more about getting data-processing bans than being fined for privacy breaches, Uber’s data-protection officer Simon Hania said, as a block on handling data would hit their revenue stream harder. *“In our company at Uber we are focusing in efficient transport. Being data driven is key to enable that.”*

The Uber executive commented on the discussions at the privacy conference about the effectiveness of different remedies for data-protection breaches. *“The point actually also is that these technologies can be used for multiple purposes. They can be used to influence an election process but they can also be used to influence behaviors on the road”*

Regulators in Europe have been going after companies that have non-compliant policies according to the EU’s strict General Data Protection Regulation with fines that could add up to 4 percent of their global annual turnover, he said, but other remedies could work equally well to force companies to be GDPR-compliant.

His own company had felt the force of direct action, he said: *“Uber had to deal with a case about sexual assault claims in recent times, which were reported in the media. And the use of the hashtag ‘delete Uber’ had an even bigger effect. No fine could have had that effect,”*

When asked if people should be more informed about their data rights and choices, Hania said it was up to companies and data protection authorities to deal with this.

“Data processing is too complex and dynamic — I don’t know that we can make people informed and let them make choices. In my role as DPO, I want to steer the organization to do the right thing.”

New Zealand Privacy Commissioner **John Edwards** noted his small country has a history of welcoming innovative business but warned that big tech platforms are causing “enormous social harms.” He referenced the effect of this year’s horrific terrorist attack in Christchurch during which 50 Muslims were shot dead while the terrorist live streamed the attack on Facebook. “The focus on free expression over other things, like privacy,” he said, is a global challenge. *“Freedom of expression like freedom of privacy is a fundamental human right. A human right we have because of our humanity. They are a fundamental feature of our dignity and they exist in balance with each other. But what we see is a co-option and an elevation of some rights for commercial purposes. So freedom of expression suits an enormous absolute approach, suits some digital business models because it reduces the administration costs and*

absolves them from responsibility; in fact the focus on freedom of expression over values such as privacy diminishes and undermines privacy protection."

Regulators, both data protection authorities and competition watchdogs, need to do more to protect citizens' data and privacy rights. **Sally Hubbard**, director of enforcement strategy at U.S.-based campaign group the Open Markets Institute, said that: *"the only true way to measure a regulator's effectiveness is to ask: 'Have we stopped the harm? Have we stopped the business models that allow the harms to take place? Have we prevented these abusive practices from happening again?'"* The answer to all of these questions is "no".

Competition authorities also need to reflect on their role and their failure to proactively prevent Big Tech firms from becoming dominant in the first place and from abusing that position subsequently. **Hubbard** took aim at the FTC's \$5 billion settlement with Facebook, saying it was *"an abdication of the regulator's power"* because *"the deal does nothing to protect consumers and does not change the way the company operates."*

"The consequences of harmful business models are born disproportionately by vulnerable people and the people who are creating these business models are the most privileged in American society" Hubbard said.

Keynote address

Brad Smith, President and Chief Legal Officer of Microsoft

Brad Smith, President and Chief Legal Officer of Microsoft provided a passionate keynote address in support of a *"third wave"* of privacy protection going beyond earlier waves based on notice/choice and access/control. He explained how the third wave of privacy should be predicated on specified baseline rules, specific rules for new technologies, integration with other laws and be embodied in a new global privacy pact. He also called for new industry initiatives to ensure privacy for new technologies.



in the year 2010”, Smith said.”. This creates both unprecedented opportunities and unparalleled challenges, perhaps especially for the protection of privacy. “Data has the secrets that will unlock many of the world’s most pressing problems. At the same time the benefits of data are growing, the risks are increasing as well. We need to address these risks” said Smith.

Smith told regulators at the conference how these new developments need to be viewed in the context of prior technology changes and efforts to advance privacy protection. Governments in Europe first and then around the world led privacy’s first wave, ensuring that people had notice about the collection of their data and the right to consent to its use. But the rapid expansion of Internet services, he added, led to people being inundated with more privacy notices than time to read them. This led to a second wave of privacy protection through the ground-breaking adoption of the GDPR this past decade, giving people the right to go online and see the data collected about them and address how it is being used.

But as the creation and storage of data continues to explode, will this be sufficient to protect the privacy rights of people? *“A third wave will be needed to establish more regulatory rules to govern privacy”. Smith said.*

“Data has the secrets that will unlock many of the world’s most pressing problems. At the same time, the benefits of data are growing, the risks are increasing as well. We need to address these risks”

Discussion Commentary

Eduardo Bertoni, Director, National Authority of Personal Data Protection and Access to Public Information, Argentina

“What kind of laws are we talking about? Laws that are going to protect the commerce; laws that are going to protect the citizens; laws that are going to give guidelines only to the business sector? Therefore, we need a discussion on that. For sure, for the protection of privacy, we need laws to protect privacy, but what does that mean more concretely? In addition, I cannot find very good answers. Not because Brad [Smith, Microsoft] didn’t give the answers but because I think that’s a complicated issue.”



PANEL DISCUSSION

Panel III: Data protection and competition as converging digital regulation: from theory to practice

Much has been said about data protection and competition in the digital sphere, issues of merger, consolidation, divestment and innovation all interact. But how are the regulators in these different spheres starting to join up their activities in practice? If competition regulators make decisions to impose restrictions or break up big tech, how will this also improve privacy and data protection?



Moderator: **Wojciech Wiewiórowski**, European Data Protection Supervisor



Ulrich Kelber, Commissioner, BFDI, German Federal Commissioner for Data Protection and Freedom of Information



Orla Lynskey, Associate Professor of Law, Department of Law, London School of Economics



Rohit Chopra, Commissioner, FTC, USA



Giuseppe Busia, Secretary General of the Italian Data Protection Authority



Maria Ioannidou, Commissioner, Hellenic Competition Commission and Senior Lecturer in Competition Law, Queen Mary University

On the antitrust panel, the European Data Protection Supervisor, **Wojciech Wiewiórowski** called for a stronger cooperation in different fields of application that share converging issues and aims. *“Regulators are organized very differently from country to country. But we start to find out that the topics we touch, the tools that we want to use are more and more similar.”*

“Data accumulation in the hand of few large companies shall be a big strategic priority for the privacy and data protection community.”

Ulrich Kelber, Commissioner, German Federal Commissioner for Data Protection and Freedom of Information, said that the cooperation and exchange of data protection supervisory authorities with other competent authorities such as Antitrust are necessary orders to ensure a coherent application of the law. *“The power granted by the GDPR in the European Union to data protection authorities and the antitrust powers of competition authorities, are effective tools that can complement each other in the fight against the abuse of data power”*. It is now a matter of exploring the limits of cooperation and making the most effective views of legal possibilities he added.

“It is now a matter of exploring the limits of cooperation and making the most effective views of legal possibilities. This is the only way we can guarantee the digital self-determination of our citizens.”

Orla Lynskey, Associate Professor of Law, Department of Law, London School of Economics, said that *“Competition and data protection are interdependent. We currently see that there are some blind spots or gaps in competition analysis and that they have a significant impact on the effective enforcement of data protection.”*

FTC Commissioner Rohit Chopra addressed the intersection of data protection and competition. He noted that the Federal Trade Commission was a unique privacy agency that has jurisdiction over both data protection and competition as part of its consumer protection responsibilities. He explained that his focus on these topics concerned the use and abuse of power over data. *“For me, it is all about abuse and misuse of power. And I live in a country that has always been a hotbed of innovation, of creativity and entrepreneurship. But I fear that we are moving away from that as our consumers and our businesses have fewer choices about how they will get to market and we are seeing venture capital drying up in so many sectors and I’m worried that our economy is in many ways looking more and more like that in China, where politically connected*

few companies really hold all the cards". Chopra noted that he hoped to see companies compete on the grounds of privacy. He is acutely focused on the remedies available for privacy violations. "We have to think about remedies that actually fix the problem... We want the market place competing on privacy" he said. He also talked about his recent dissent in a case that involved by far the largest privacy financial penalty ever imposed, reiterating his belief that the outcome was still not punitive enough.

Big Tech firms *"need to get used to the idea that they can be prosecuted by more than one regulator, and by more than one law, for the same practices."* warned Rohit Chopra.

"We have to think about privacy as a clear point on which companies compete. We want that marketplace competing on privacy and not having 'take it or leave it' contracts where more and more data is vacuumed up."

Tech firms are subject to scrutiny from data, competition, and e-Commerce/digital markets regulators around the globe but their investigations often focus on different parts of the same problem. For example, competition authorities are concerned about how firms exploit the number of users they have, as well as the ubiquity of their platforms, to coerce people into accepting services or be barred from them. Data regulators, on the other hand, are more interested in the fact these practices put users' personal information at risk because they have been forced into agreements that give tech firms license to sell it to anyone.

Chopra suggested both data protection authorities and antitrust regulators should consider ways of opening up the market for innovative new entrants to gain a foothold and flourish. "Increased competition ensures a fairer market and better consumer choice, so we should look at ways of making that happen," he said. To increase competition, Chopra suggests regulators need to look at what technology is available via open source; have clear rules and bans on some practices by tech companies; and push for individual liability when prosecuting tech firms for data misuse.

Giuseppe Busia, Secretary General of the Italian Data Protection Authority, noted one very important issue that *"if we consider only the economic perspective, the economic point of view, then we have in many cases an unbalanced relation between the user and the company, because the data can be reused many times"*. In his intervention, Busia stressed the key importance of cooperation between data protection authorities and competition regulators because of the interplay between data protection and competition on two levels: the first, is the need to protect consumers' personal data; the second, is the fact that concentration of personal data in the hands of one company can represent

an unfair competitive advantage on the market. He concluded by stressing the importance of embedding data protection in competition, therefore going beyond a purely antitrust approach.

Maria Ioannidou, Commissioner, Hellenic Competition Commission, elaborated on the concept of digital agoraphobia, the fear of the marketplace. Consumers are losing their trust in their transactions online. *Taking an example, she further explained on the topic "The Greek Competition Commission only has powers to apply competition law; it's not the same with the consumer markets authority in the UK or Australia, so the question is: do we want to convert competition authorities into a type of super regulator; do we need something else?"*

Keynote address

Jamie Bartlett, Senior Fellow, UK Demos

Jamie Bartlett, second keynote speaker of the first day of open session, is the author of bestselling book "People vs. Tech" and BBC series presenter of "Secrets of Silicon Valley". He elaborated on how data rights are key to securing other rights in the future. In a world of total connection and datafication, whoever controls data controls people's sense of reality, and even their experience of the physical world, "will rob the poor their peace of mind". Bartlett mentioned how elections are an obvious example of that. *"The regulations and laws we have about elections need to be sufficient for people to think that this is a free and fair election. How do the regulators run an election in a free and fair way when every single person receives different messages, every day millions of messages that will be posted online or targeted online at people through personalized devices and often machine-generated? I don't think we are really ready for that yet".*

Jamie Bartlett echoed his comments on what will happen, if in future the wealthy pay for a "privacy premium" and avoid the profiling and algorithms of the 2020s, and the poor have little choice. In the future, the rich will be able to afford to pay for a privacy premium, the new inequality of the future will be caused by data. He added that almost every problem will have a data element, he suggested that data regulators may necessarily become regulators of everything.



" I think the inequality of the future is not just going to be about stuff and money, will always be about that too, but it will also be about freedom of mind, clarity of thought and attention and if that is left purely to the free market then the inequality will grow and will cement other existing inequalities."

DAY 2 | Thursday, 24 October



In his welcoming keynote address, **Erion Veliaj**, Mayor of Tirana, stressed the fact that various international organizations, such as the United Nations or the World Bank, have put cities' development at the top of their priorities. He continued by encouraging data protection and privacy authorities to also focus on cities. *I'll encourage you when it comes to data protection and data collection and data management and data security and privacy, please include the cities. It's the cities that gather a lot of data about transport, the city that has all this wealth of data that can be put in good use when it comes to people using car shares or people using bike shares or people using other methods in the sharing economy".* Because local authorities collect and use many categories of data, which can be used for the effectiveness of city management.



Peter Hustinx, co-chair of the Programme Advisory Committee introduced the final day's activities and described the purpose of the gathering, i.e. to raise global privacy standards and promote global convergence. *"I've had the pleasure to have been co-chairing the Programme Advisory Committee for this conference and I can only say that it's been a very smooth and pleasant cooperation because in the end it is all about bringing us together and making us all more effective as privacy and data protection community."* He also noted how appropriate the symbol of Illyrian Liburnia was as we handle tradition and innovation; *the concept of which is: In a sea of data, Liburnia, an ancient Albanian symbol, navigates safely through the digital network. The symbolism of its sail is composed of 41 connecting dots".*

Keynote address

Christopher Docksey, Hon. Director General, European Data Protection Supervisor and Data Protection Authority of Guernsey

Christopher Docksey, Hon. Director General, European Data Protection Supervisor and member of the Data Protection Authority of Guernsey delivered a keynote focused on the “Accountability” principle, what it means and how it can be achieved. Accountability is the key when dealing with compliance in multiple jurisdictions. He pointed out that the benefits of accountability are undeniable as long as it is applied in practice: towards a real and concrete accountability, rather than formal or on paper. *“Accountability has moved data protection from being an adjective to a verb. What we had was an adjective, a definition [of] who is the person responsible. Now we have a verb, an activity, what is the responsible person doing.* He suggested this was a somewhat new concept in data protection regulation (in Article 24 of GDPR). *“The EU enshrined the accountability principle in Article 24 and Christopher Docksey says that article 24 is his favorite article of the GDPR. I think it’s mine to, to be honest.”* Sometimes, he said, **it is not the processing that is the problem so much as the lack of transparency to users** Docksey spoke about the blossoming of data protection accountability across the globe, the philosophy behind accountability and the toolbox that can be used to demonstrate it.



“One pragmatic way of understanding accountability is to see it as a toolbox, full of useful tools.”

Docksey emphasized the inclusion of the accountability principle in data protection legislation, and the need for controllers and regulators to embrace this fundamental principle to 'give life' to data protection compliance and regulations.

Docksey described "accountability" as companies implementing necessary internal mechanisms to achieve and demonstrate compliance.

Christopher Docksey closed with this quote from the late Giovanni Buttarelli:

"Not everything that is legally compliant and technically feasible is morally sustainable."

PANEL DISCUSSION

Panel IV: Accountability – the global bridge to support high standards of data protection?

Even when not explicit in the law, accountability is implicit in most privacy and data protection laws. How do we bridge the gap between the expectation of authorities and the companies that must be accountable? How can authorities' enforcement approach ensure accountability drives high standards of data protection and what role for responsible and answerable data stewardship? How do we ensure accountability is scalable and flexible and supports high standards in SMEs, particularly tech start-ups? What is an effective enforcement approach in this context?



Moderator: **Andrea Jelinek**, Chair, European Data Protection Board and Director of the Austrian Data Protection Authority (DSB)



Marty Abrams, Information Accountability Foundation (IAF)



Caroline Louveaux, Chief Privacy Officer at Mastercard



Daniel Therrien, Privacy Commissioner of Canada



Bertrand Du Marais, Commissioner of the CNIL, France



Ailidh Callander, Legal Officer, Privacy International



The “accountability” discussion was elaborated in the panel moderated by **Andrea Jelinek, Chair of the EDPB and Director of Austria’s DPA**. She explained that an “accountable” organization needs to put in place policies, procedures and technical measures to achieve compliance, and be able to demonstrate compliance. *“In Europe, naturally the GDPR is our point of reference and the GDPR expressly incorporates accountability as a requirement. The controller has to put in place appropriate technical and organizational measures to ensure compliance and she or he has to be able to demonstrate compliance with the regulation.”* For protecting personal data today and in the future, accountability is key.

The incorporation of the accountability principle in the GDPR is a key change compared to the Data Protection Directive and is a fundamental shift in approach Jelinek noted.

Accountability is key in addressing data privacy, and it is not just the responsibility of a regulator to hold companies to account, they have to be proactive and demonstrate accountability themselves. Christopher Docksey, honorary director general at the European Data Protection Supervisor (EDPS), defines accountability as “actively developing compliance and being able to demonstrate compliance.”

Marty Abrams, Information Accountability Foundation (IAF) later distinguished “accountability” from compliance on the basis that the former seeks to achieve justice and fairness in addition to legal compliance. *“Accountability takes us beyond compliance, beyond a technical application of the law and to do that I would like to start with one of the values [...] in a 2015 paper on ethics where Giovanni Buttarelli said: “Data should serve people”.*

Accountability is a process, a continuous responsibility for the processing of personal information which is proactive and demonstrable. It is a toolbox, accompanied by specific mechanisms, such as having a privacy officer, privacy by design and default, impact assessments, breach notification and certification. And it is a philosophy, of being a responsible and ethical steward of personal information. Accountable organizations understand, and are committed to, the work they have to do, he said.

Caroline Louveaux CPO of MasterCard explained her company's Corporate Data Responsibility initiative. *“We have an issue when those requirements diverge because all our products and services are being designed centrally and then deployed locally and obviously we have an even bigger challenge when those requirements keep changing over the conflict with each other.”*

Daniel Therrien, Privacy Commissioner of Canada spoke of his agency's investigations of Equifax and Facebook regarding the alleged inadequacy of their accountability programs, including alleged failures of internal monitoring.

Regulators believe that, for the most part, companies have good intentions about preserving data privacy and about being accountable: The problem, however, is that policies and procedures often have gaps in them, and they are not properly implemented, understood, monitored, or revised. *“Accountability is necessary but it is not sufficient. We find that large organizations for the most part have developed detailed policies and procedures but upon close examination these policies often have significant gaps.”* “True accountability means ensuring that the measures you say are in place to ensure data privacy and consumer protection are working. The only way to make such a claim is to constantly check and review, and not enough organizations do this,” said Daniel Therrien, Canada's Privacy Commissioner.

Bertrand Du Marais, Commissioner of the CNIL, France added to the panel that: *“Thanks to GDPR, we in Europe have moved from a hierarchical regulatory logic to a conformity paradigm. So we changed the approach, from a controlled regulatory based on prior formalities, to a very static logic; in a dynamic concept and implementation of ongoing processes that evoke a worldwide awareness of data protection.”*

Ailidh Callander, Legal Officer, Privacy International briefly summarized: *“All of us here want to live in a world where technology empowers us and enables us*

and our data is not exploited for profit and power but we know as we've heard throughout this conference that without action and action by all of you, that is not the future."

PANEL DISCUSSION

Panel V: Future challenges for data protection authorities and data protection officers

The challenges for data protection authorities and DPOs alike have never been greater; the portfolio of skills and competence required is broad and deep to be effective enforcers. This demands further professionalization and further debate about how the community can meet this challenge. How can DPAs best network to pool their expertise? How do DPAs ensure they are 'tech savvy' in delivering their core functions, not just a specialism? How should an ethical focus and dimension be integrated? How can AI and new technology help DPAs or DPOs do their job?



Moderator: **Trevor Hughes**, President and CEO, International Association of Privacy Professionals, (IAPP)



Kalinda Raina, Vice President, Head of Global Privacy, LinkedIn



Julie Brill, Corporate Vice President, Deputy General Counsel & Chief Privacy Officer, Microsoft Corporation



Simon McDougall, Executive Director of Technology Policy and Innovation, ICO, UK



Alexandra Jaspar-Leeuw, Director - Belgian Data Protection Authority



Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong, China



Trevor Hughes, CEO of IAPP, moderated the final panel about operationalizing privacy. He pointed out: *“You need privacy program management, you need management structures, actual systems of processes and controls that help give life to data protection. And you need people. You need privacy officers, data protection officers, people who do the work, people who lead the work. And finally you need transparency.”*

Julie Brill, SVP and Deputy General Counsel of Microsoft, spoke of the operational imperatives of data protection, including the likely lack of sufficient resources. She noted that companies need the right technological tools to implement privacy at scale. She also recommended that DPAs establish mediation services to address complaints. *“Right now, I think both companies and regulators are experiencing a very fast changing environment and also both regulators and companies are experiencing very intense and, in my opinion, appropriate scrutiny about what we are doing.”*

The Deputy General Counsel of Microsoft, noted that Microsoft relies on internal ethics boards with respect to AI and facial recognition technologies. These boards comprise engineers, lawyers, and senior executives responsible for business and trust. They look at individual proposals and projects, and use of the company’s APIs for data access.

Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong, China agreed in saying that *“I share the same view that we need to put in more resources, human resources, financial resources and in particular nowadays the technical, the professional, the IT people.”*

Simon McDougall, Executive Director of Technology Policy and Innovation, at the UK ICO, stated that: *“GDPR has brought a series of positive changes. It has a focus on compliance; but the range of services, the way data is being used is changing so rapidly and we should be focused a little more on some of the technological changes. We live in such a data saturated world where there is proliferation of data and personalization of data that is so hard for us to keep up with the new services and the new threats”,* noting that we need to be more data-driven in what we are doing. He concluded by noting the importance for data protection authorities to develop their own data science capabilities, to help pursue cases and to work with those in the tech sector in order to understand where the greatest risks are.

Kalinda Raina, LinkedIn stressed the importance of corporate privacy culture. *“I speak to this from a unique perspective of a company that was originally thought of by two founders in the late 90’s who thought that doing a dating business might be really successful and they quickly failed at it but learned a good lesson which was that trust was essential to relationships.”* She recommended the value of deputizing non-privacy colleagues as privacy champions in their business units.

Alexandra Jaspas-Leeuw, Director of Belgium Data Protection Authority told the audience that the watchdog will prioritize individuals’ rights under the EU’s strict privacy rules to access the data that companies hold on them, as well as scrutinize the legitimacy of data processing.

“We have defined four priority sectors, three GDPR provisions and four practices, which we will scrutinize within the coming five and a half years.” We choose to focus on our telecom sector, the public sector, direct marketing sector and the educational sector. As the GDPR provisions are concerned, we will focus on access rights, legitimacy and the role of the DPO. We will focus on the following topics: online privacy, pictures and cameras, and sensitive data, said Jaspas-Leeuw,

Concluding remarks

Raymond Liboro, ICDPPC Executive Committee member and Privacy Commissioner/Chairman of NPC, The Philippines, took the stage for the final summary of Open Session thematic discussions, noting the importance of cooperation in the international privacy community. *“Attending the ICDPPC and attending all the sessions reminded me of one thing and probably should all remind you of the fact why we’re here; it is because we are in the middle of a revolution;*

it's a digital revolution and it's sweeping across governments, it's sweeping across jurisdictions touching the lives of all our citizens." Concluding he added that the newly agreed strategic plan gives the Executive Committee of ICDPPC a clear direction and that a new Strategic Direction Sub-committee has already been created to oversee the working groups.



In closing, **Elizabeth Denham, ICDPPC Chair** said: *"So it falls to me as Chair to thank our host for their excellent organization, their warm hospitality. This has been a truly global conference. There is an Albanian proverb that is relevant here: "He who leans against a big tree, will always find shade". Well, the ICDPPC is the tree and I think that the progress that we've made this week will make sure that we can continue to benefit from the shade of that tree."*

The Chair announced the new name for the ICDPPC as agreed by the Conference Closed Session will from now on be the "Global Privacy Assembly (GPA)" and that the next conference will be in Mexico City. Dr. Francisco Javier Acuna Llamas, Commissioner President of INAI, introduced a video presentation of Mexico's forthcoming Annual Meeting as the next ICDPPC Host.

Commissioner **Dervishi** thanked the 41st conference speakers who shared their diverse perspectives with the conference, all of them promising to engage in a fruitful collaboration.

With an inspiring closing speech and moving words of gratitude to his staff and all those involved in the organization of the conference for the 41st edition of ICDPPC and for the results that this conference achieved, he concluded: *"Happy that Tirana will remain a landmark in the history of the Conference"*.



Side Events

The 41st International Conference featured side events, which were accommodated in two slots, respectively on Tuesday afternoon, October 22 from 14.30-16.00 and 16.30-18.00 and Thursday afternoon, October 24, from 14.30-16.00 and 16.30-18.00

22 OCTOBER

THE GLOBAL DATA PROTECTION CONVENTION AND YOU

Organized by the Council of Europe

Snapshot interventions on the pros of Convention 108+ by inspirational data protection promoters and defenders.

How is the Convention different from other international frameworks? Is this difference an asset or an obstacle?

Views on the modernized Convention were shared, and borders softened as the focus was on how to facilitate cooperation between DPAs, on what this instrument represents in specific parts of the world, on its broad scope of application and on its 'human rights' flavor and color.

Speakers

Joseph A. Cannataci – UN Special Rapporteur on the Right to Privacy;

John Edwards – Privacy Commissioner, New Zealand;

Jan Kleijssen – Director of Information Society and Action against Crime, Council of Europe;

Sophie Kwasny – Head of the Data Protection Unit, Council of Europe;

Patricia Poku – Executive Director, Data Protection Commission, Ghana;

Omer Tene – Vice President, Chief Knowledge Officer, IAPP;

Jean-Philippe Walter – Council of Europe Commissioner for data protection.

ISO 27701: WHAT YOU NEED TO KNOW ABOUT THE NEW PRIVACY STANDARD

Organized by OneTrust

The ISO 27701 certification for a Privacy Information Management System – the privacy extension of the ISO 27001 – establishes privacy controls and for the processing of personal data, and may likely become the foundation for future GDPR certifications. This panel brought together ISO 27701 experts to detail the new standard and shared best practices for achieving ISO 27701 certification.

Speakers

David Forman – Senior Director, ISO Services, Coalfire;

Markus Gierschmann – CIPP/E, CIPM, Gierschmann Consulting;

Moderator

Andrew Clearwater – CIPP/US, Chief Privacy Officer, OneTrust.

GPEN 'ENFORCING ACCOUNTABILITY'

Organized by Global Privacy Enforcement Network

The GPEN annual face-to-face event was an opportunity for members and interested authorities to discuss practical tools they had put in place to encourage and ensure compliance by data controllers in their own jurisdiction.

PRIVACY BEST PRACTICES AND TRANSPARENCY IN LAW ENFORCEMENT

Organizers: Chief Privacy and Civil Liberties Officer at the US Department of Justice; Chief Privacy Officer, Head of Data Protection Unit at the Danish National Police; and the Data Protection Unit of Europol.

Questions over law enforcement access to personal data have to an increasing degree affected global data transfers for years. For transfers from the European Union to the United States, such questions could upend the EU-US Privacy Shield framework and the European Commission-approved "standard contract clauses." Because of the need to ensure the confidentiality of criminal investigations – most often in the opening stages – facts about data collection, use, dissemination, retention rules, oversight, and privacy-related safeguards historically have been difficult to discern and debate, often resulting in misunderstandings or even mistrust of law enforcement. Yet, over the past few years, several countries have been hard at work in developing best practices to protect privacy, increase transparency, and rebuild public trust, thereby supporting the core government mandate to both protect public safety and privacy. Privacy officers and authorities from across the European Union, United States, and possibly elsewhere examined best practices and lessons learned with respect to efforts to promote privacy and transparency

in connection with law enforcement activity. Further, this event aimed to provide a starting point for ongoing engagement between law enforcement agencies, privacy and data protection supervisory authorities, academia and other stakeholders designed to share best practices, raise insights into the diverse ways in which legal systems protect citizens' rights in the context of law enforcement, and ensure constructive dialogue about ongoing challenges.

Speakers

Christian Wiese Svanberg – Chief Privacy Officer, Head of Data Protection Unit, Danish National Police;

Étienne Maury – Legal and Policy Officer, European and International Affairs Department, Commission Nationale de l'Informatique et des Libertés (CNIL);

Desislava Borisova – Specialist, Data Protection Function, EUROPOL;

Peter Winn – Chief Privacy and Civil Liberties Officer (Acting), U.S. Department of Justice;

Moderator

Jennifer Daskal – Associate Professor of Law, Washington College of Law, American University.

CLIMATE CRISIS AND DIGITAL RIGHTS: CAN UNIVERSAL RIGHTS TO DIGNITY AND PRIVACY WITHSTAND THE CONSEQUENCES OF CLIMATE CHANGE IN THE COMING DECADES?

Side event organized by the European Data Protection Supervisor

In recent years, one million refugees from conflict zones including Syria endured great personal suffering to seek a new life in the stable democracies of Europe. This contributed to considerable disruption of political discourse in the host countries. Similar events have unfolded in other regions. A typical policy response has been to apply surveillance and control technologies such as collection of biometrics and location tracking. As climate change intensifies and conflict and displacement become more likely, poorer areas of the world will be the hardest hit, placing the notion of universal human rights under greater pressure than perhaps ever before. Multiple tiers of entitlement could emerge, with vulnerable migrants and refugees increasingly the objects of surveillance and control. This panel looked at likely scenarios in the next 10-30 years and how it prevents the fracturing of human rights as collateral damage of global warming.

Speakers

Patricia Adusei-Poku – Executive Director, Ghana Data Protection Commission;

Pam Dixon – Executive Director, World Privacy Forum;

Mario Oetheimer – Deputy Head of Research and Data Unit, EU Agency for Fundamental Rights;

Christina Vasala Kokkinaki – Legal Officer, International Organisation for Migration

Massimo Marelli – Head of Data Protection Office, International Committee of the Red Cross.

Moderator

Christian D’Cunha – Head of Private Office, European Data Protection Supervisor.

FROM REGIONAL TO GLOBAL CONVERGENCE: THE LATIN AMERICAN MODEL

Co-hosted by the European Commission and the Ibero American Data Protection Network

Since their adoption in 2017, the Ibero-American Standards have very well played their role as a blueprint for privacy laws in the region and as a platform for closer cooperation between data protection authorities.

The last years saw many new exciting developments: from Brazil that adopted its first comprehensive data protection legislation to Chile that amended its constitution to introduce the right to privacy and announced the creation of an independent data protection authority, from Argentina where the existing legislation is being modernized to Ecuador where the government tabled the first ever bill in this area.

Similar initiatives have also been taken in many countries of Central America and the Caribbean, from Panama to Barbados or Jamaica. At continental level, the Organization of American States has launched an important initiative towards the modernization of its own data protection principles. It is also remarkable that the first non-member of the Council of Europe that signed the modernized “Convention 108” comes from Latin America: Uruguay.

This shows how regional integration and global convergence can meet, complement each other, and in this way bring new opportunities to facilitate trade and cooperation at both regional level and with international partners.

Speakers

Eduardo Bertoni – Director, Transparency and Data Protection Agency of Argentina;

Jose Ziebarth – Director, Special Secretary of Debureaucratization, Management and Digital Government, Ministry of Economy of Brazil;

Gloria de la Fuente – Commissioner, Transparency Council of Chile;

Andres Barreto – Superintendent, Superintendence of Industry and Commerce of Colombia;

Francisco Acuña Llamas – President of the National Institute of Access to Information, Transparency and Data Protection of Mexico;

Felipe Rotondo – President of the Ibero-American Data Protection Network; Chairperson

Rafael García Gozalo – Head of the International Department at the Spanish Agency for Data Protection.

Moderator

Estelle Masse – Senior Policy Analyst and Global Data Protection Lead at Access Now.

Closing Remarks

Joseph Cannataci – UN Special Rapporteur on the Right to Privacy

INTERNATIONAL ENFORCEMENT COOPERATION WORKING GROUP - for ICDPPC members only

Organized by the Information Commissioner Office (ICO)

The ICO organized a side event that focused on themes familiar to those ICDPPC members already participating in the International Enforcement Cooperation working group (IEC) whose work under the current mandate came to a close in Tirana. The event tried to build an environment for different jurisdictions to exchange expertise, enforcement approaches, and collaborate on joint initiatives. It focused discussions on two organizations as case studies and discussed the potential activities for a permanent working group in the ICDPPC moving forward.

SUPPORT TRAINING ACTIVITIES ON THE DATA PROTECTION REFORM (STAR)

Organized by Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB)

This event introduced and discussed the final results of the STAR project (co-funded by the European Union (EU) under its Rights, Equality and Citizenship

program (2014-2020)) which supports training activities of EU Data Protection Authorities (DPAs) and Data Protection Officers (DPOs) on the EU data protection reform, and especially on the General Data Protection Regulation (GDPR). The panel identified the challenges and best practices around data protection training. The panel then launched the steady-made, easy-to-customize and easy-to-run training materials, (i.e. 11 Microsoft PowerPoint presentations, training scenarios, further supporting forms as well as a handbook for trainers and users of the materials) targeted for DPAs and DPOs and which are freely and publicly available in a digital form at the project's website: <http://www.project-star.eu/training-materials>. During the event speakers guided the audience through the STAR materials and, in form of a discussion, gathered their feedback and experience from training activities thereafter.

Speakers

Paul De Hert – Professor, Vrije Universiteit Brussel (VUB);

István Böröcz – Researcher, Vrije Universiteit Brussel (VUB);

Filippo Marchetti – Senior Researcher, Trilateral Research Ltd. (TRI);

Júlia Sziklay – Head of Department, Hungarian National Authority for Data Protection and Freedom of Information (NAIH);

Gábor Kulitsán – freedom of information expert, Hungarian National Authority for Data Protection and Freedom of Information (NAIH).

GDPR IN THE PRIVATE SECTOR - BURDEN OR OPPORTUNITY?

Organised by Arbour Group

The event looked at practical implementations across multiple private sector companies. The event discussed how to get the Board of Directors buy in and how to establish a plan to a successful implementation that may be duplicated.

Speakers

Vijay Laxmi – DLP, Director of Cyber Security and Privacy, Arbour Group.

Al Berry – VP Connected Health, Arbour Group

DEMYSTIFYING 5G: PRIVACY IMPLICATIONS OF INTELLIGENT CONNECTIVITY IN A CONVERGENT WORLD

Organised by GSMA

The arrival of 5G ushers in a new era of Intelligent Connectivity and is set to transform the lives of citizens and businesses around the world.

Starting from the earliest days of first-generation analogue phones, every

subsequent generational leap has brought huge benefits to societies around the world and propelled the digitisation of more segments of the global economy. The transition to fifth generation (5G) technology – together with the Internet of Things, Big Data and AI – will drive a new step change in productivity and innovation by delivering real-time services across multiple sectors such as entertainment, transportation and manufacturing. With an expected 1.4 billion 5G connections by 2025 and 5G forecast to contribute \$2.2 trillion to the global economy over the next 15 years, 5G's ubiquitous hyper-connectivity will spur diverse next-generation applications such as augmented reality, intelligent transportation systems, optimized industrial processes, remote controlled robots, boosted crop yields and remote surgery. As the mobile industry starts to roll out 5G, it becomes increasingly important to understand what data is generated on mobile networks and how it is used. As part of its role representing the mobile industry globally, the GSMA publishes resources on 5G and has written a seminal report exploring the visions, opportunities & considerations for 5G.

Discussing:

What are the potential use cases of 5G?

How does 5G work?

What is network slicing?

Who is really responsible for security and privacy in a 5G/IoT world?

What data is generated and how is it used?

Where are the privacy challenges?

Speakers

Boris Wojtan – GSMA Director of Privacy, Government and Regulatory Affairs;

Caitlin Fennessy – International Association of Privacy Professionals, Research Director;

Jade Nester – GSMA, Director of Consumer Policy, Government and Regulatory Affairs;

Mikko Niva – Vodafone, Group Privacy Officer and Head of Legal – Privacy, Security and Content Standards;

Simon Hania – Uber, Data Protection Officer;

Simon McDougall – Information Commissioner's Office, Executive Director for Technology Policy and Innovation;

Vikram Raval – GSMA Senior Policy Director, Government and Regulatory Affairs.

AFRICAN NETWORK OF DATA PROTECTION AUTHORITIES

African Network of Data Protection Authorities (RAPDP)

As every year, the African Network of Data Protection Authorities (RAPDP) organized as a side event of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Tirana, an open-session roundtable of Network members and other privacy and data protection stakeholders. The purpose of this roundtable was to discuss privacy and personal data protection of young people on social networks and to share experiences of the supervisory authorities in this field.

23 OCTOBER

BIOMETRICS ROUNDTABLE

The Brookings Institution and the World Privacy Forum co-hosted an invitation-only Biometrics Roundtable. The purpose of the Biometrics Roundtable was to promote a dialogue between the data protection community, the law enforcement community, and key stakeholders in Europe and other jurisdictions. The goal was to facilitate stakeholders' ability to network, ask questions, and learn from each other on matters related to privacy and data protection in biometrics systems, with a focus on those used in law enforcement and government contexts.

Cam Kerry – Brookings, and **Pam Dixon** – World Privacy Forum, co-moderated the event.

24 OCTOBER

14.30 - 16.00

LEGITIMACY, FAIRNESS AND NEUTRALITY: DEFINING ETHICAL DESIGN

Hosted by Facebook

In this interactive session, participants engaged in discussion and debate on the topic of ethical design and the changing role of product design. Participants engaged across different disciplines to share their perspective on neutrality, fairness and legitimacy, drawing on models and frameworks developed in concert with academics and with designers from the team at TTC (Trust, Transparency & Control) Labs, a cross-industry initiative driven by Facebook to pursue innovation and research in designing interfaces and controls for data. We will work through a series of design case studies to examine appropriate rule-making mechanisms and the role of ethics through the design lifecycle.

THE NEAR FUTURE OF PRIVACY-ENHANCING TECHNOLOGIES

Hosted by Google

This session examined how privacy-enhancing technologies and other techniques contribute to raising data protection standards for people everywhere. We heard from technologists, academics, lawyers, and representatives from data protection and privacy authorities about how recent advances, when combined with smart regulation, can support data protection principles and enhance privacy for individuals. We asked how stakeholders can work together to continue improving the state of the art and make privacy-protective technologies more widely available.

Speakers

Miguel Guevara – Product Manager, Google;

Alon Kaufman – Co-founder & CEO, Duality;

Aoife Sexton – Chief Privacy Officer, Truata;

István Mate Böröcz – Researcher, Vrije Universiteit Brussel (VUB);

Simon McDougall – Executive Director Technology Policy & Innovation, UK Information Commissioner's Office.

Moderator

Sarah Holland – Public Policy Manager, Google.

WHAT IS ACCOUNTABILITY? ADDRESSING THE CONFUSION, FINDING CONSENSUS

Centre for Information Policy Leadership (CIPL) in collaboration with IAF and the OECD

Organizational Accountability has become a key building block of data protection globally through legislation, regulatory guidance, global standards and privacy management programmes. If properly understood and implemented, it has enormous potential for maximising both privacy protections for individuals and the effective and beneficial use of personal data. Yet, as noted in a recent OECD-CIPL workshop, the concept of accountability is still being questioned as lacking a commonly agreed meaning, as well as generally accepted ways of measurement, effective enforcement, scalability and auditability. This session addressed these concerns to reinforce the relevance of accountability in the digital era. It also explored ways to increase and incentivise the uptake of organisational accountability by organisations. This workshop was intended to provide the foundation for the subsequent session on "Accountability 2.0 – Data Stewardship and Beneficial AI" by the IAF and the OECD.

Speakers

Bojana Bellamy – President, CIPL;

Hielke Hijmans – Director, President of the Litigation Chamber, Belgian Data Protection Authority

Jennifer O’Sullivan – Deputy Commissioner, Irish Data Protection Commission;

Rohit Chopra – Commissioner, US Federal Trade Commission;

Bertrand du Marais – State Counselor, CNIL;

Damien Kieran – Global Data Protection Officer, Legal Director, and Associate General Counsel, Twitter;

Lisa Sotto – Partner, Hunton Andrews Kurth LLP;

William Malcolm – Director Privacy Legal, Google;

Knut Mager – Head Global Data Privacy, Novartis;

Florian Thoma – Senior Director of Global Data Privacy, Accenture.

GLOBAL ENFORCEMENT AND CONSISTENCY

Organised by OneTrust DataGuidance

Enforcement actions are beginning make headlines and highlight the varying aspects that authorities have focused on regarding organisations compliance with global privacy laws. Hear from regulators regarding their priorities and recommendations for demonstrating compliance, as well as how to practically achieve this.

Speakers

Laura Flannery – International Affairs and OSS Operations at Data Protection Commissioner Ireland;

Alan Raul – Partner at Sidley Austin;

Brent Homan – Assistant Commissioner, Office of the Privacy Commissioner of Canada;

Guilherme Roschke – Counsel for International Consumer Protection at Federal Trade Commission.

AI AND DATA PROTECTION: GLOBAL CHALLENGE GLOBAL RESPONSE

Organised by Beijing Normal University & Huawei Technologies Co. Ltd

With the fast development of privacy regulations and AI applications, the data protection is becoming a common priority for the international community. The side event addressed the current status and challenges of AI and data protection, the applicable policies and regulations, the best practices, as well as the global solutions for the data protection and AI applications.

Speakers

Achim Klabunde – Advisor to the Supervisors on Data Protection and Technology, EDPS;

Sophie Kwasny – Head of Data Protection Unit, Council of Europe;

John Kavanagh – Head of Commissioner Private Office, ICO (UK);

Stephen Kai-Yi Wong – Hong Kong Personal Data Protection Commissioner;

John Suffolk – Global Cyber Security and User Privacy Officer, EU Privacy Protection Officer, Huawei;

Shenkuo Wu – Director of International Centre of Cyber Law, Beijing Normal University;

Fabrice Naftalski – Global Privacy Protection Leader, EY;

Joerg Thomas – Director of EU DPO Office, Huawei;

Kevin Wang – Privacy Protection Team Leader, GSPO Office, Huawei;

Alan Tang – Senior Privacy Expert, GSPO Office, Huawei.

Raising awareness and Capacity Building of Personal Data Protection in Asia

Korea Internet and Security Agency

Personal data has become one of key elements in Digital era. Despite the importance of Personal data has enlarged, awareness and capacity of personal data have a room for improvement.

Korea Internet and Security Agency shared their current activities for raising awareness and capacity building of personal data, especially for children and public bodies.

Speakers

Hyun joon Kwon – Vice President of Korea Internet & Security Agency in Korea;

Stephen Kai-yi Wang – Privacy Commissioner for Personal Data, Hong Kong;

Raymund Enriquez – Liboro National Privacy Commission in Philippine.

FIRST RISK-RATING AGENCY FOR DATA SOVEREIGNTY KELONY®

Data sovereignty can only be led by an independent Risk-Rating agency such as KELONY® with its ultimate KELONY®-Assured process. Data are so rich that they can be considered as the gold of the 21st century. In reality, data are much more than that. Data is the most strategic and fundamental asset for human life protection. The ongoing process of digitalization of people's life, ranging from health code to banking code, to tax code and e-mail address, makes individual security more attackable. Personal Data represent an enormous wealth and a crucial part of freedom, identity and security for each of us. Just think, for example, what personal data aggregated into information allow us to do. There are many disciplines that in a fragmented way contribute to data protection, such as Information Security, Cyber Security, ICT, and yet it's not enough to protect the whole which is greater than the sum of its parts. It is necessary to possess the data sovereignty's traits to have full control of it. Risk is the common denominator of data sovereignty and has therefore to be neutralized according to Risk-Rating.

Speakers

Genséric Cantournet – Chairman, KELONY®;

Angela Pietrantoni – General Manager, KELONY® Italy;

Ivo Galligani – Partner, Étoile Level KELONY® Italy

ACCOUNTABILITY 2.0 - DATA STEWARDSHIP AND BENEFICIAL AI

Hosted by Information Accountability Foundation in collaboration with CIPL and the OECD

AI and advanced analytics require accountability 2.0 and its requirement that organisations be fair data stewards. This session on the accountability 1.0 session explored data stewardship, its linkage to OECD Ethical AI guidance, and how it may be enforceable.

Speakers

Martin Abrams – Executive Director, Information Accountability Foundation;

Christopher Docksey – Hon. Director General, EDPS;

Scott Taylor – Associate Vice President, Merck;

Cosimo Monda – Director, Maastricht University European Centre for Privacy and Cybersecurity;

Stephen Kai-yi Wong – Privacy Commissioner for Personal Data, Hong Kong;

Pam Dixon – Executive Director, World Economic Forum;

Christian D'Cunha – Head of Private Office, EDPS;

Elettra Ronchi – Senior Policy Analyst, Science, Technology and Innovation Directorate, OECD.

Steve Wood – Deputy Commissioner, UK Information Commissioner’s Office.

THE BLOCKCHAIN SOLUTION: DATA SHARING FOR A BETTER PROTECTION

Hosted by Consulcesi Tech SA

During the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC 2019), Data Protection Commissioner of Albania, also on behalf of the Executive Committee of the ICDPPC, granted Consulcesi Tech the honor of hosting the Side Event Roundtable “The Blockchain solution: data sharing for a better protection”. The roundtable sets beyond the dualism between data protection and processing: by leveraging the blockchain capabilities for a better data protection, the roundtable delved into a wide range of evolving opportunities such as data monetization and digital identity. The debate involved prominent panelists from top institutions, universities and the tech industry.

Opening Greetings were given by **H.E Edi Rama, Prime Minister of the Republic of Albania.**

Speakers

Massimo D’Alema – President of the Italianeuropei Foundation;

Luigi Neirotti – Associate Partner of Studio Legale Tributario EY;

Kara Sutton – Privacy Policy Manager at Facebook;

Luca Bolognini – Founding Partner at ICT Legal;

Jörn Erbguth – Lecturer at the University of Geneva;

Davide Casaleggio – Founding Partner of Casaleggio Associati.

Moderator

Gianluigi Pacini Battaglia – CEO at Consulcesi Tech.

FUTURE CHALLENGES: HOW LEADERS AROUND THE WORLD ARE ADDRESSING EMERGING PRIVACY ISSUES

Session co-sponsored by Microsoft and Future of Privacy Forum

The online world is designed to collect, use, and share personal data-and as technology gets more complex so do questions of ethics, bias, fairness, and

protection of vulnerable populations. This session explored the evolving role of privacy in addressing these human challenges. Together with a stellar panel of global leaders, participants were invited to provide their input on supporting ethical research, protecting children, responsible advertising, and fairness in machine learning.

Speakers

Andrea Jelinek – Chair, European Data Protection Board and Director of the Austrian Data Protection Authority, DSB;

Eduardo Bertoni – Director, National Authority of Personal Data Protection and Access to Public Information, Argentina;

Rohit Chopra – Commissioner, FTC, USA;

Julie Brill – Corporate Vice President, Deputy General Counsel, and Chief Privacy Officer, Microsoft;

Clara Wong – Assistant Legal Counsel of the Privacy Commissioner for Personal Data, Hong Kong, China;

Florence Raynal – Deputy Director, Head of the Department of European and International Affairs, CNIL, France;

Omer Tene – Vice President, Chief Knowledge Officer at International Association of Privacy Professionals, United States;

Rob Van Eijk – Managing Director for Europe, Future of Privacy Forum

Moderator

Cari Benn – Assistant General Counsel, Privacy and Regulatory Affairs, Microsoft.

BUILDING BRIDGES: COMMON APPROACHES TO DATA GOVERNANCE

The U.S. Chamber of Commerce, Information Technology Industry Council & AmCham Albania

Data governance is today at the forefront of the global agenda. Given the continued growth in the global digital economy and the emergence of artificial intelligence, it is critical that policymakers seeking to address foundational issues such as privacy choose to build bridges, rather than moats, across national, regional, and global regimes. Common approaches to data governance, including certifications, interoperable regulations, trade rules, and emerging technology frameworks, such as the OECD's AI Recommendations, are therefore invaluable. This session identified examples and opportunities across multiple forums where policymakers can contribute to constructive bridge building in data governance.

Keynote Address

Raymund Enriquez Liboro – Commissioner, National Privacy Commission of the Philippines.

Speakers

Alex Greenstein – Director of the EU-U.S. Privacy Shield, U.S. Department of Commerce;

Erika Brown Lee – Senior Vice President & Assistant General Counsel, Mastercard

Simon Hania – Data Protection Officer, Uber

Lisa Sotto – Partner, Hunton Andrews Kurth;

Moderator

Guido Lobrano – Vice President for Europe, Information Technology Industry Council.

Closing Remarks

Noboru Yamaji – Commissioner for International Cooperation, Personal Information Protection Commission of Japan.

DATA PROTECTION IN DIGITAL ECONOMY: THIRD COUNTRIES VIS-A-VIS THE GDPR

Hosted by the Information and Data Protection Commissioner's Office of Albania

This session aimed at bringing best experiences of third countries, including Albania, in relation to the General Data Protection Regulation (GDPR) and the latter's impact on digital economy. With the entry into force of this Regulation in May 2018, its widespread influence expanded on many areas, most notably technology and innovation. Technology is a significant catalyst for all social changes. Organizations, companies and public authorities dealing with personal data are responsible for the way the information is collected, exchanged and stored, whether these decisions are made by humans or algorithms. Advanced technology should go hand in hand with every controller's accountability for more security and protection of personal data relating to consumers. Meanwhile digital marketing has evolved rapidly. Customers can be easily reached. Businesses offer "free" services like news, entertainment and search engines, and in return, they collect data and sell ads. The aim of this session was to establish a dialogue between the panel and the audience on the readiness of all stakeholders in the digital world to tackle the challenges and the introductions brought about by the GDPR in third countries while promoting consumer confidence in the digital market. The speakers brought their views, current practices, problems identified and attempted to provide possible solutions for achieving GDPR compliance.

Speakers

Catherine Lenman – Swiss Federal Data Protection Authority (FDPIIC);

Leida Matja – Competition Authority of Albania;

Mirlinda Karçanaj – General Director, National Information Society Agency – (TBC);

Aniss Lahoussine – International Data Protection Expert;

Irena Malolli – Director of Policies and Development Strategies for Telecommunication and Posts, Ministry of Infrastructure and Energy.

Moderator

Pjerina Gaxha – Director of Data Protection Department, Information and Data Protection Commissioner's Office of Albania (IDP).

INN Festival

Innovation Festival 2019 was powered and supported by Innovation Nest which is a Balkan Business Angel Network based in Albania, aimed at supporting, investing, incubating and developing new technologies ideas on WB6 industries and enterprises, helping them in being innovative, competitive and internalized.

INN Fest 2019 is designed to be the most important regional conference for innovation and technology. The 2-day festival (24th & 25th October), with a final reception where all ICDPPC delegates were invited, brought together successful CEOs, entrepreneurs and leaders of the regional marketplace, building so a bridge of support and communication for the new business/startup ideas seeking investment.

Website: fest.innovationnest.org

Pictures from the side events





2019 Global Privacy and Data Protection Awards

In their third year, the Awards celebrate the achievements of the entire ICDPPC community and shine a light on good practice. They were celebrated with a special ceremony on the occasion at the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Tirana, Albania.

Elizabeth Denham CBE, Chair of ICDPPC and UK Information Commissioner, said: *"The awards celebrate the creative ideas, the practical innovations and the brilliant people we are privileged to call part of our community. I hope the winners not only take home their award but also the pride that goes with that – to have been recognized by your peers."*

This edition's winners per category were:

Education and Public Awareness Award

Winner: Data Protection Authority of the Canton of Zurich, Switzerland

Project: Educational Resources for Children aged 4-9 years old

Dispute Resolution and Enforcement Award

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

Project: Inquiry into the Ministry of Social Development

Innovation Award

Winner: European Data Protection Supervisor (EDPS)

Project: Website Evidence Collector Tool

Accountability Award and People's Choice Award

Winner: Agencia Española de Protección de Datos (Spanish DPA)

Project: FACILITA_RGPD Tool

Albanian Information and Data Protection Commissioner's Award

This year's conference, a dedicated award under the initiative of the host authority and with the support from the GPA Secretariat, was given to Giovanni Buttarelli to recognise his outstanding contribution to the protection of personal data and privacy. Besnik Dervishi, the IDP Commissioner, handed the award to Wojciech Wiewiorowski, Acting European Data Protection Supervisor, who highlighted Giovanni's legacy in the data protection and privacy community.



From left to right): Bruno Baeriswyl, Privacy Commissioner, Data Protection Authority of the Canton of Zurich; John Edwards, New Zealand Privacy Commissioner; Wojciech Wiewiorowski, Acting European Data Protection Supervisor; Mar España Martí, Director of the Agencia Española de Protección de Datos (AEPD); Besnik Dervishi, Albania IDP Commissioner; Thomas Zerdick, Head of IT Policy Unit at the EDPS.

More information on the awards and all the entries is available at the GPA website.

Special thanks to the Programme Advisory Committee (PAC) and ICDPPC Executive Committee

The host acknowledges the invaluable work of the Open Session Programme Advisory Committee (PAC), co-chaired by Peter Hustinx, former European Data Protection Supervisor, and currently non-Executive Director at the ICO and Besnik Dervishi, Information and Data Protection Commissioner of Albania, who contributed to appointing the final speaker line-up and content of the Open Session agenda of the 41st ICDPPC. More information on the Programme Advisory Committee is available at the dedicated conference website: www.privacyconference2019.info The organizer of the 41st ICDPPC also recognizes the hard work carried out by the Executive Committee (comprising members: Canada OPC, EDPS and Bulgaria's DPA, and IDP Albania, UK ICO, Burkina Faso's CIL, Philippines NPC, Australia's OAIC, and Mexico INAI) as they devoted significant time and resources to preparing decision-making in the 2019 Conference.

You may find below a list with all PAC's members:

41st ICDPPC Programme Advisory Committee (PAC) 2019

Peter Hustinx	Former EDPS and Former Head of Dutch Data Protection Authority	The Netherlands
Besnik Dervishi	Commissioner Albania IDP (Albanian Information and Data Protection Commissioner's Office) Host Authority, ICDPPC 2019	Albania
Chawki Gaddès	Head of Authority, INPDP Tunisia and Chair ad interim of the AFAPDP	Tunisia
Steve Wood	ICO (UK DPA), Deputy Commissioner	UK
Noboru (Nobi) Yamaji	Commissioner for International Cooperation, PPC, Japan	Japan
Sophie Kwasny	Head of the Data Protection Unit, Council of Europe	France/International

Marc Rotenberg	CEO, EPIC Public Voice	USA/International
Isabel Davara F De Marcos	Partner and Founder of the law firm Davara Abogados	Mexico
Marty Abrams	Executive Director, Information Accountability Foundation	USA/International
Graham Greenleaf	Professor of Law & Information Systems, University of New South Wales, Faculty of Law	Australia
Omer Tene	Vice President and Chief Knowledge Officer at the International Association of Privacy Professionals (IAPP) Affiliate Scholar at the Stanford Center for Internet and Society and Senior Fellow at the Future of Privacy Forum	Japan
Francisco Acuña Llamas	President of INAI (Mexican Access to Information/Privacy Authority)	Mexico
Gabriela Zanfir	Senior Counsel, Future of Privacy Forum	International

Acknowledgements

The host also acknowledges the irreplaceable, tireless and dedicated work of the GPA Secretariat throughout the planning of the 41st ICDPPC Conference: Hannah McCausland, Annabelle McGuinness, Christine Ferguson, Fabiana Marinaro, Debora Biasutti, and Victoria Cetinkaya.

Special thanks to Boga & Associates law firm for providing valuable consultancy and assistance to the host for the preparation of this report. The host also wishes to thank all the partners that gave their support for the organization of this Conference. Conference partners are listed below:

Our partners

Diamond Partner



Platinum Partner



VIP Dinner Host



Gold Partner



Silver Partner



Associate Partner



Supporting Partner



Media Partner





41ST INTERNATIONAL CONFERENCE
OF DATA PROTECTION AND PRIVACY COMMISSIONERS

privacyconference2019.info