Vol. 2, Issue 3 | 2020

NEWSLETTER

GLOBAL PRIVACY ASSEMBLY

GPA
Global Privacy Assembly

Message from the Chair

It is said that we learn more about ourselves during adversity than during easier times.

That feels apt as we consider how the Global Privacy Assembly has responded to this challenging year.

Globally, we have all been asked to answer some difficult questions. Society has faced new and unique problems, and many of the proposed solutions have involved using people's data in novel ways: from track and trace systems and mobile phone apps to employers collecting staff's temperatures as they enter a building. I know from speaking with GPA colleagues that this has been a similar picture around the world.

The GPA has responded at pace to these unprecedented questions and queries, facilitating the sharing of best practice and providing a forum for discussion and collaboration. We have chaired two international workshops alongside the OECD to discuss challenges and share experiences, and our COVID-19 taskforce has played a crucial role in enhancing information sharing and capacity building for our members.

The result is that our privacy community has demonstrated to the wider world its pragmatism and value in these toughest of times.

That work continues as we look ahead to our Closed Session conference in October. It was crucial that 2020 was not a year dominated solely by the pandemic, and the Executive Committee was committed to finding a way to further the progress and continued modernisation of our Assembly that we advanced in Tirana last year.

The virtual conference we have organised will provide an opportunity for us to continue the GPA's evolution. Across three days of online sessions, we will hear from the working groups delivering on our policy strategy objectives, talk specifically about the how members have worked with governments to respond to the challenges prompted by COVID-19, and consider the resolutions that remain our community's common position on where we stand on key issues.

This conference will be different in many ways, but it remains a crucial landmark in our calendars, and an important opportunity for you to shape the future of our community.

There's a wealth of information in this newsletter about the conference, including the importance of registering as early as possible.

You will notice too that our newsletter itself continues to move forward. We have responded to your feedback, and the result is a bumper edition, with much to inform and inspire during this critical period. However, please continue to share your feedback with us.

I hope it continues to be a valuable read, and I look forward to speaking with you more at our conference.

Regards,
Elizabeth Denham CBE
Information Commissioner, UK

Inside this issue:

GPA Closed Session 2020

At your desk

The Global Privacy Assembly (GPA) Executive Committee and Secretariat are delighted to announce the Global Privacy Assembly 2020 Closed Session – At your desk.

This year, for the first time, the GPA membership will be brought together online for the annual conference, which will be held over three days, each day consisting of a three-hour online session from 11:00-14:00 (UK Time):

- **Tuesday 13 October 2020**
- **Wednesday 14 October 2020**
- **Thursday 15 October 2020**

All the information you need for the **Global Privacy Assembly 2020 Closed Session – At your desk** is included on the GPA website.

Register today

globalprivacyassembly.org/gpa2020
@PrivacyAssembly
secretariat@globalprivacyassembly.org

Come together to debate and celebrate the considerable achievements and success of our community initiatives this year, and help shape the future of the GPA.

Day 1, Tuesday 13 October

The Closed Session opens with a warm welcome from the Chair of the GPA, Information Commissioner, Ms. Elizabeth Denham, immediately followed by the Accreditation of this year's new Members and Observers.

The agenda then moves to the Strategic Direction Closed Session event. Chaired by the GPA Strategic Direction Sub-Committee, the session focuses on the GPA's three strategic priorities and key achievements over the year, including the progress, deliverables and outcomes of the 2019-2021 GPA Policy Strategy:

Assessing progress against the three GPA Strategic Priorities:

- **Advancing global privacy in the digital age;**
- **Maximising the GPA's voice and influence; and**
- **Capacity Building.**

Day 2, Wednesday 14 October

This session is dedicated to a review of the activities and deliverables of our ground-breaking GPA COVID-19 Taskforce from May to September 2020, and its significant impact in aiding the GPA community to deal with the privacy issues arising from the COVID-19 pandemic.

This session includes the launch of a Compendium of Best Practices, bringing together authorities' good practice initiatives in response to COVID-19.

Day 3, Thursday 15 October

This is the GPA Core Business Session, which includes a spotlight on the:

- **Adoption of Working Group Reports and Annual Report of the Executive Committee;**
- **Executive Committee Elections;**
- **GPA Resolutions, discussion and adoption;**
- **GPA Rules on the GPA Voice;**
- **The new GPA Reference Panel; and**
- **Statement of the Next Conference Host**

Have your say, register today

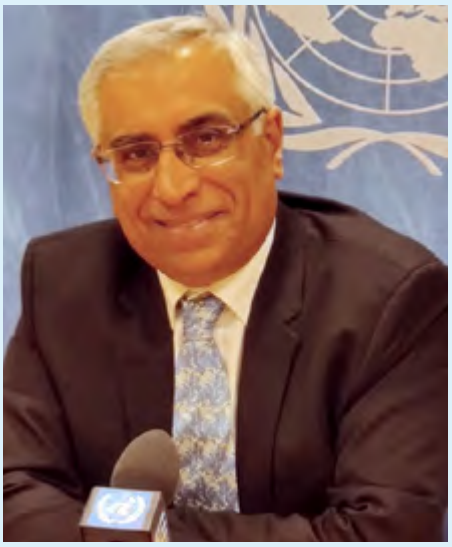
The registration deadline is now extended to 30 September 2020. If you have not yet registered, please email the Secretariat for the link to the registration form at secretariat@globalprivacyassembly.org.

GPA Closed Session 2020
At your desk

globalprivacyassembly.org/gpa2020
@PrivacyAssembly
secretariat@globalprivacyassembly.org

Horizon scanning

Data Subject Rights – Privacy as an Enabling Right – Where are we now? Safeguards and Remedies



Professor Joe Cannataci, UN Special Rapporteur on the Right to Privacy writes exclusively for the GPA on the landscape regarding privacy rights in 2020

The defining feature of 2020 has been the COVID-19 pandemic. It is hard to think of an aspect of our world and our lives that has not been affected in some way by this virus. Human rights, including the right to privacy, also have been severely and adversely affected by the pandemic.

In the COVID-19 public health emergency, the priority is to save lives. The need to arrest the spread of a potential epidemic is a time where the public interest may sometimes be socially valued above the right to privacy and other rights, such as freedom of movement and freedom of association. But responses to the COVID-19 virus and respecting human rights including the right to privacy, are not incompatible. International and regional frameworks for human rights and data protection already equip States to effectively combat the COVID-19 virus and respect the rights of their citizens.

The fight against the continued circulation of the COVID-19 virus, has seen individuals' data become a key tool for governments and scientists. We have seen also many debates about the funnelling of personal and health data to power strategies, and the erosion of rights and civil liberties in the name of combating the virus.

However, the use of information and of technology in managing public health emergencies is not new. Containing the spread of disease for public health reasons has always provided a legitimate legal basis for the processing of data. The COVID-19 pandemic is no different in this regard. The International Health Regulations (2005) (IHR) – a legally binding agreement between 196 countries, requires signatory states to report "an event that may constitute a public health emergency of international concern."

But what is of concern are reports of how personal and health data are being collected and used, and the degree of intrusion and control over citizens, **possibly to little public health effect**.

Interferences with the right to privacy should be legal, necessary and proportionate to the objective pursued, "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (Universal Declaration of Human Rights (UDHR), Art. 29(2)).

International legal instruments, including Article 4 of the International Covenant on Civil and Political Rights and Article 15 of the European Convention on Human Rights, recognise the occasional need of governments during a period of crisis, for a limited time and for a specific purpose, to have special powers – powers which normally would be considered infringements or violations of fundamental human rights and freedoms.

"Manual" contact tracing to enable contagion to be arrested and contained is standard practice in epidemics. While contact tracing is privacy-intrusive, it can be classified as a necessary measure.

The fight against the continued circulation of the COVID-19 virus has seen individuals' data become a key tool for governments and scientists

We know that some governments and tech companies have expanded the traditional manual process of contact tracing by using technology to track individuals who have tested positive for COVID-19, and by extension, every individual with whom they may have come in contact. We know also that that technology driven contact tracing has become, in some places around the world, disturbingly close to incessant and omni-present surveillance.

The quantity and nature of data generated as a product of managing the pandemic, has resulted in a significantly increased volume of health-related data being processed, and in more comprehensive and complete profiles of both patients and their contacts. The interests in this data are various, varied, and unequal, and pose increasingly challenging

legal, ethical and human rights issues.

The sensitivity of the data merits specific protection to provide the deserved respect to the right to privacy, as per UDHR Article 12.

The WHO commits to only publishing data which is anonymised. Under the IHR, signatories are encouraged to share data to assist preventing the spread of any global pandemic. Article 45 specifies the data protection requirements that such data must meet, including the removal of any personal identifiers and locators.

> **...what is of concern are reports of how personal and health data are being collected and used...the degree of intrusion and control over citizens, possibly to little public health effect**

At the regional level, but with significant international influence, the GDPR and Convention 108 recognise health data as a 'special category of data'. In Convention 108, the processing of health data is permissible only where appropriate safeguards are enshrined in the law. The GDPR provides more scenarios in which health data may be processed, but has increased restrictions, and permits EU Member States to "maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health." In March 2019, the Committee of Ministers of the Council of Europe adopted the Recommendation on the protection of health related data which contains principles intended to protect health related data, incorporating both Convention 108 and the revised Convention 108+.

In 2019, my Taskforce on Health Related Data led by Professor Dr Nikolaus Forgò developed a Recommendation presented to the UN General Assembly in October 2019, which included provisions addressing the legitimate processing of health-related data carried out in the public interest.

In the light of the above, it is reasonable to assert that there is sufficient guidance available for any country collecting health data as part of their COVID-19 response, and it is clear moreover, that the use of data either consensually or non-consensually obtained, has to be demonstrably lawful, necessary and proportionate in a democratic society.

In relation to the use of modern technology in checking the pandemic spread, privacy engineering has not always been given its due importance.

Smartphone apps have become a widely deployed method of applying digital technology to contact tracing. My point is that privacy should be considered from the beginning of the process, starting with the engineering of the app. An example of a promising practice in response to the COVID-19 situation that embeds privacy in design, is DP-3T (Decentralized Privacy-Preserving Proximity Tracing), an open-source protocol, for Bluetooth-based tracking in which an individual phone's contact logs are only stored locally, therefore no central authority can know who has been exposed. A number of States, such as Austria, Estonia, Germany and Switzerland, already have announced that their national apps are based on this protocol.

Some apps (eg Australia's COVID Safe and France's Stop COVID-19) have a centralised design, with the infected person uploading both their phone's ID code and the phone IDs of their recent contacts to a central server. Although these IDs are anonymised, officials can see the entire network of contacts. Other apps, for example, Germany, are decentralised, and data about a phone's recent interactions stay on that phone. An infected user uploads only their own anonymized ID to a central database; all phones with the app regularly load the list of infected users to check for a match with phones with which they have been in proximity recently. This design means data about users' social networks are less vulnerable to hacking or exploitation.

In 'traditional' contact tracing, the patient's most comprehensive repository of private information, his or her smartphone, is not accessed or sequestered. With the evidence that some countries have contained COVID-19 using time-honoured public health methodologies without recourse to smartphone APPS, geo-location or other technologies , the regular or constant access to a device such as a smartphone, or monitoring of the user's whereabouts and contacts through smartphone technologies, raises the question whether this is a necessary and proportionate measure.

The data and technological design privacy concerns raised by COVID-19 manifest in an environment already replete with privacy challenges. The jury is still out as to what extent governments are processing health and other data such as travel and location data, in accord with human rights and data protection instruments. The evidence which my mandate collects will probably not be sufficient for at least a year from now for us to make a definitive judgement as to whether and which Governments have been getting things right. Which is why I encourage everybody to continue to send us more information about COVID-19 and privacy in their region or country.

Focus

Artificial intelligence and privacy: best practices for data protection compliance

Simon McDougall, Deputy Commissioner for Regulatory Innovation and Technology at the Information Commissioner's Office, UK, discusses new guidance published to enable good practice in AI

There has been an immense growth in the use of Artificial Intelligence (AI) over the past few years in areas such as online retail, banking and healthcare. We have also seen how the COVID-19 pandemic has driven innovation in the use of AI and data to help curb the global health crisis.

AI offers opportunities that could bring marked improvements for society. But it's clear that the use of the technology has implications for privacy, data protection and people's information rights.

That's why the UK Information Commissioner's Office (ICO) has identified AI as one of its top strategic priorities and has published guidance on artificial intelligence and data protection as part of its commitment to enable good practice in AI.

The guidance and framework are the culmination of two years of research and consultation

Understanding how to assess compliance with data protection principles can be challenging in the context of AI. From the exacerbated, and sometimes novel, security risks that come from the use of AI systems, to the potential for discrimination and bias in the data, it is hard for technology specialists and compliance experts to navigate their way to compliant and workable AI systems.

The guidance recommends best practices and technical measures that organisations can use to mitigate those risks caused or exacerbated by the use of AI. It also acts as a roadmap to data protection compliance for those individuals designing, building and implementing AI systems.

As well as offering AI and data protection guidance and support to organisations across the UK, we are also using the guidance as a tool for the ICO to develop its own framework for auditing AI compliance with data protection obligations. The framework:

- gives the ICO a clear methodology to audit AI applications and ensure they process personal data fairly, lawfully and transparently;
- ensures that the necessary measures are in place to assess and manage risks to rights and freedoms that arise from AI; and
- supports the work of the ICO's investigation and assurance teams when assessing the compliance of organisations using AI.

The guidance and framework are the culmination of two years of research and consultation by Professor Reuben Binns and the ICO Technology team. We have also listened to a wide range of stakeholders who provided feedback to us throughout.

As innovation and use of AI is growing and evolving, the ICO will continue to focus on AI developments and their implications for privacy, offering tools that encourage privacy by design to those developing and using AI.

We will keep seeking feedback on the guidance to help us to achieve this goal and we encourage members of the Global Privacy Assembly to provide comments.

For more information visit ico.org.uk.

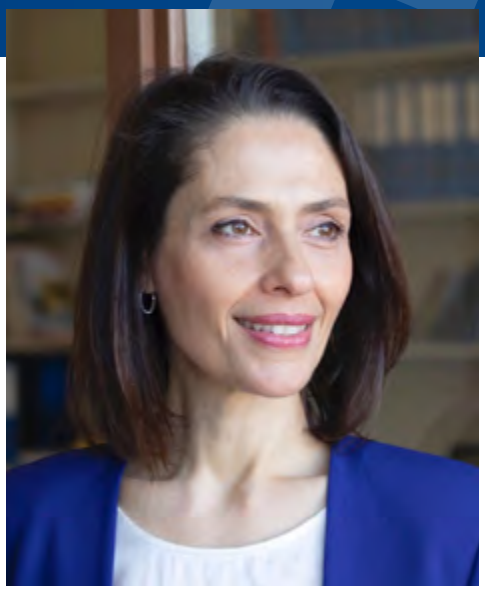
During September the ICO is running a technology month, a campaign set up to highlight how the ICO is working to improve data protection practices in the digital economy. More information at @ICOnews or follow #icotechmonth on Twitter.

TECH MONTH

Case study

Ethics and digital solutions for health monitoring - COVID-19 and the New Normal

Professor Effy Vayena, Co-Chair of the WHO Working Group on AI and Ethics and Professor of Bioethics at the Swiss Federal Institute of Technology reveals the findings of recent research for the GPA community



The last six months have made clear that digital health applications can impact on the progress we make in managing the pandemic. They also showed us that in the rush to develop and deploy the most useful digital tools during a state of global emergency, we face unprecedented ethical challenges. I am using the example of digital proximity and contact tracing apps to illustrate some of these challenges and the way forward.

Building the new normal is an opportunity to get things right

As governments around the world started developing proximity and contact tracing apps (PCT), the public and scholarly debate on their use has been predominantly framed as a matter of hard trade-offs. The use of apps that can help trace those exposed to infected cases is expected to come at a significant cost of privacy. Policy makers and citizens would have to choose between public health and personal privacy, or between privacy and freedom of movement, or re-opening the economy.

This framing seems intuitive. Numerous scandals of privacy breaches, commercialization of data people thought were private, unlawful sharing of health data and questionable deals between tech companies and health care institutions for health data uses have scared our experience of the digital life. Lack of quality assurance systems for health apps (except for those designated as medical devices) and obscure privacy policies that users cannot negotiate add to the sense of exploitation and that whatever utility is on offer by a digital health app, it will require sacrificing privacy.

This framing of competing values and trade-offs, however, is problematic in at least two ways. First, it is not just privacy that is threatened by these technologies. Other values, including autonomy, solidarity, equity and public trust, are also threatened. Second, by focusing exclusively on privacy we end up with a zero-sum game approach to it, foregoing the option to develop systems that optimize for all values instead of trading one against another. Our collective interest lies in protecting simultaneously individual privacy, autonomy, and public trust along with the public's health. For example, acceptance of public health interventions (e.g. a PCT) is dependent on whether people trust their health authorities. If people fear for their privacy or are subjected to discriminatory practices as a result of a public health intervention they use, their trust will be broken, and the success of the public health measure will be undermined.

The commitment to all ethical values is the way to view the challenges and respond to them. This commitment also served as the backbone of most recent ethics guidelines on proximity tracing apps that was issued by the World Health Organization. I was privileged to chair the expert group that worked on this the guidance. Drawing on the WHO guidance and my own research in the issue of digital proximity and contact tracing system I highlight three significant issues:

PCT apps should not be mandated, nor should citizens be unduly incentivized to use them. There are opposing views on the value of voluntary use of digital public health interventions as well as the role incentives can play on their uptake. Those favoring mandatory use of apps often cite the importance of the uptake of such apps that in turn can increase their effectiveness in disrupting viral transmission chains. They argue that contributing to the common good by way of helping control the spread of the virus should be mandated. However, this position underplays first, the risk of data exploitation, as their appropriate use may be hard to secure; second, the digital divide even within wealthy nations where not everyone possesses high tech devices on which the apps run; third, the limited evidence to date that PCT systems are effective in the control of the pandemic.

Although the uncertainty about the effectiveness of these systems should not stifle their development or prevent their deployment, it certainly makes mandating their use even more questionable.

The testing and evaluation of PCT apps before deployment and its continuous monitoring afterwards is critically important. The technical performance of PCT apps, for example their accuracy and security, the rates of false positives and false negatives in contact identification, the role of other factors, such as face-coverings, testing strategy etc. in different contexts remain unknown, and so far there is no universally-accepted standard by which to evaluate these parameters. Even less is known about the effectiveness of PCT apps. Results of effectiveness analyses will more accurately direct policy options on PCT and are critical for earning public trust and acceptability of digital interventions, and ultimately their wide-spread use. In the meantime, inflated expectations about what they can actually contribute should not be used to defend their forceful introduction.

The diversity of actors involved in the development of PCT, the technological complexity of proximity tracing systems and how they are embedded within regular services in our mobile devices, create a higher need for clarity and openness. In addition, as PCT systems will automatically apply risk scores of exposure, and in some cases make determinations for follow-up action (eg quarantine) such determinations should be explainable. These requirements apply equally to state and non-state actors involved with the PCT apps.

> **The commitment to all ethical values is the way to view the challenges and respond to them**

Undoubtedly, the urgency to control the pandemic coupled with the appeal of digital technologies create a favorable attitude towards them and perhaps the temptation to underplay the challenges they raise. Striking the right balance between enthusiasm and caution is not an easy feat (Ref: Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. Lancet Digital Health 2020, Gasser U et al). A procedural principle that can help with the balancing exercise, namely the establishment of independent oversight bodies for PCT apps. Such institutions carry the responsibility to review the progress of PCT, monitor its impact on the epidemic as well as on people's rights and freedoms, the necessity of its continuous use or its termination. Oversight is not only critical for public accountability but also for galvanizing and sustaining public trust to public health interventions. The independence of the oversight is necessitated by the fact that all actors involved in PCT apps have vested interests in their promotion. This includes state public health actors, whose legitimate role in public health interventions does not necessarily translate into the trustworthiness of the intervention. The novelty of PCT, its scalability and potential impact on the pandemic requires continuous monitoring and assessment.

Building the new normal is an opportunity to get things right.

GPA key upcoming dates 2020

- **30 Sep** Registration closes for the GPA 2020 Closed Session – At Your Desk
- **30 Sep** Deadline for the review of all Working Group Reports and GPA Resolutions
- **30 Sep** 15:30-17:00 (BST) Policy Strategy Working Group WS1 Webinar
- **5 Oct** Documents for the Conference are circulated to the GPA community
- **8 Oct** 61st Executive Committee Meeting
- **12 Oct** 11:30-13:00 (BST) International Enforcement Cooperation Working Group Webinar
- **13-15 Oct** Virtual GPA 2020 Closed Session – At Your Desk
- **28 Oct** 10:00-11:30 (UTC-GMT) Digital Citizen and Consumer Working Group Webinar

Check our website for more information: globalprivacyassembly.org

In conversation with

Ms. Ada Chung, Privacy Commissioner at the Office of the Privacy Commissioner for Personal Data in Hong Kong, China

In an exclusive interview for the GPA, Ms. Ada Chung, the new Hong Kong Privacy Commissioner talks about her role and the work of the PCPD going forward

As the newly appointed Privacy Commissioner at the Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong, briefly inform us about your background and your hopes/vision for the Office of the Privacy Commissioner coming into this role.

I am very honoured to be appointed by the Chief Executive of the Hong Kong Special Administrative Region of China as the Privacy Commissioner for Personal Data, Hong Kong, China with effect from 4 September 2020. Coming from a legal and public administration background, I had served as the Registrar of Companies and held various posts in the Department of Justice, including Principal Government Counsel and Deputy Law Officer (Civil Law). In my capacity as the Registrar of Companies, I contributed to the rewriting of our Companies Ordinance and spearheaded the implementation of the new Companies Ordinance in Hong Kong.

Given the significant technological changes in the past few years, in my view, the protection of personal data privacy has become more important than ever, both locally and in the international arena. One of the priorities in taking up my new role is to amend the local privacy legislation, namely, the Personal Data (Privacy) Ordinance (PDPO), to, among other things, empower the office of the Privacy Commissioner for Personal Data to exercise a wider range of enforcement powers to better protect personal data privacy in a virtual world. I also wish to foster the PCPD's relationship with other data protection authorities worldwide and enhance our cooperation and collaboration in the years to come.

> 'Water can float a boat, so can it swallow the boat' – We are all facing big challenges over the next few years; data can help us all to navigate them, but we need to recognize the risks and harm it may also cause

Tell us about the Office of the Privacy Commissioner for Personal Data in Hong Kong.

Established in August 1996, the PCPD is an independent body set up to oversee the implementation of, and compliance with, the provisions of the PDPO, which came into operation in the same year. The PDPO is one of Asia's earliest comprehensive set of data protection laws. It underwent major amendments in 2012, to include regulation of direct marketing to protect personal data privacy. The PDPO is applicable to both private and public sectors, including the government.

The Privacy Commissioner is the primary driving force advocating personal data protection/privacy innovation in Hong Kong. The PCPD provides support and expert input to the Government on any policy initiatives in the area. Other than being a regulator, the PCPD is also an educator and a facilitator of the protection of personal data privacy. The PCPD works with the Government and relevant stakeholders in the community to consult their views on any new initiatives, including proposed legislative amendments, and is primarily responsible for implementing and enforcing any new requirements or regulations in the area.

Please highlight both the current and future challenges for the PCPD, and any significant barriers to progress that lie ahead.

Personal data privacy finds its presence in almost all facets of our lives. So are the challenges that we face as a regulator. As data sees no borders, contravention of personal data privacy laws involving Internet intermediaries overseas but affecting local citizens requires better international collaborative efforts in order to tackle this. In

this context, Internet doxing is a classic example.

Neither does the virus see borders. The outbreak of COVID-19 has created a new normal under which almost everything goes digital. The extensive collection of personal data resulting from various measures taken by governments to fight the virus and the sometimes less-than-transparent personal data management have aroused fear of surveillance under the name of pandemic control. The pandemic accelerated the pace of digitalisation and the massive use and transfer of personal data, making it even more pressing to better protect privacy online for all walks of life.

Only with trust, and proper compliance, can we work together for the common good

As the world is adapting to this new paradigm, the PCPD believes that in addition to compliance with privacy laws and regulations, data ethics is no less important. We need to go back to the basics. We need data controllers to be respectful and fair to individuals. We need them to exhibit transparency and explainability to garner trust. Only with trust, and proper compliance, can we work together for the common good.

Looking into the future, the PCPD will take concerted efforts to assist the Hong Kong SAR Government to make the necessary legislative amendments to enhance our regulatory capability.

To conclude, please give your views on the important opportunities that lie ahead for the PCPD as a key player in the international data protection and privacy community and with regard to the role of the Global Privacy Assembly.

I am a co-chair of the Permanent Working Group on Ethics and Data Protection in Artificial Intelligence (AI) under the Global Privacy Assembly. The development of AI creates significant challenges and risks to the respect for, and protection of, personal data privacy. Working with the other co-chairs and with the collective effort of this Working Group, I hope we can enhance the international community's attention to the importance of the responsible use of AI so that proper ethics and data protection would not be brushed aside while advancing technological development. It is important that AI serves humans but not the other way round, sacrificing our core values.

As data sees no borders, mutual assistance among data protection authorities is imperative to the enhancement of the protection of personal data privacy. I believe that data protection authorities can mutually benefit from sharing experience and expertise – joint enforcement collaboration and the formation of common positions to make our voices heard in the international community. Our co-operation and collaboration in the international arena would be more important than ever.

Let me conclude by quoting a famous Chinese proverb: 'Water can float a boat, so can it swallow the boat'. We are all facing big challenges over the next few years; data can help us all to navigate them, but we need to recognize the risks and harm it may also cause.

The GPA Secretariat — Your central contact point

If you are interested in getting more involved in the GPA's work, by joining one of the Working Groups, or volunteering to be a future Assembly host, please get
in touch with the Secretariat at
secretariat@globalprivacyassembly.org

For more information on the GPA, visit our website at globalprivacyassembly.org

Follow us on Twitter
@PrivacyAssembly

Get to Know Your ExCo...

Elizabeth Denham, Information Commissioner, Information Commissioner's Office (ICO), UK, Chair of the Global Privacy Assembly

Tell us a little about the ICO, and its regulatory role in the UK?

The ICO is an independent regulator, with a remit that extends across all sectors: we are responsible for regulating business, government, law enforcement, intelligence services and more. The issues on my desk can vary from police use of facial recognition technology to criminal misuse of data, from the use of data in the adtech real-time bidding system to how the UK's health service can better share data.

Our approach is focused on working alongside organisations, protecting individuals' rights by helping organisations to make changes and improvements to comply with the law before mistakes happen or data is misused.

That is important, because our UK research shows that when people have heard about a data breach, they have lower levels of trust and confidence more broadly in organisations using their data. Lower trust can lead to a reluctance to share personal data that can undermine the potential benefits of the digital economy.

This year has brought unique challenges for everyone. How has COVID-19 impacted the ICO?

Responding to the challenges brought by COVID-19 has been a key focus for us this year. Society has faced new and unique problems, and many of the proposed solutions have involved using people's data: from track and trace systems and mobile phone apps to employers' wanting to test staff. I know from speaking with GPA colleagues that this has been a similar picture around the world.

I have been very proud of the way my office has worked in challenging circumstances. We have had to work differently, with all of our office space closed and staff working just as hard from home, and an increased workload brought by the response to the pandemic. We have had to reassess our priorities to reflect these exceptional times, and to recognise the increased pressures organisations face.

> **Globally, we also need to find bridges that bring together our different laws and allow for better collaboration...My view is that accountability can be such a bridge**

But fundamentally we are the same regulator: proportionate, pragmatic, and focused on both enabling innovation and protecting people's information rights.

I have also appreciated the support of international colleagues. The GPA has now organised two international workshops alongside the OECD, to discuss challenges and share experiences, as well as broader work to enhance information sharing and capacity building for our members.

So often we are asked similar questions, and combining our expertise helps us reach the answers more efficiently.

What are your key priorities/ projects for this year?

My teams closely monitor current trends, recent complaints and requests for support, to assess where and how we should focus to have the greatest impact to protect the public and support economic growth and innovation.

Our six priorities in the coming months are:

- protecting our vulnerable citizens, with particular regard to the risks, issues and opportunities presented by COVID-19;
- supporting economic growth and digitalisation, including for small businesses,
- shaping proportionate surveillance;
- enabling good practice in Artificial Intelligence, including the recent publication of our AI guidance;
- enabling transparency, both in data protection and through access to information, which we also regulate; and
- maintaining business continuity and developing new ways of working as we continue to evolve as a regulator.

How will the UK's law change as a result of Brexit?

The UK brought the GDPR into UK law in the Data Protection Act

2018, and that is the law we are responsible for regulating.

Parliament will decide how we approach our legislation outside of the EU, how we pursue adequacy with the EU, and how we shape our relationship with the rest of the world.

The UK government has made a clear commitment to high data protection standards equal to those of the EU, as part of an independent policy on data protection.

That does not come as a surprise. It reflects the international trend of ever higher standards or privacy protections, and it reflects the strong UK tradition – stretching back to the 1980s – of appreciating the value of data protection laws as an enabler of innovation and responsible trusted processing.

What do you believe are the main issues that will impact on the global data protection and privacy agenda in the future?

This is an opportune time to think about the future. The COVID-19 pandemic has brought an acceleration in the uptake of digital services in months that I would otherwise have expected to take years. Our lives are online now, from recreation to education, from evenings talking to friends and families to our own GPA Closed Session in October.

Whether we are ordering a meal or getting a medical diagnosis, data is now less the trail that we leave behind us as we go through our lives, and more the medium through which we are living our lives.

This accelerated progress brings benefits sooner, but it brings risks sooner too. And data is at the centre of that, the fuel that drives these innovations.

It is our job, as regulators or data protection authorities, to encourage people's confidence in innovation. But that is not easy. The questions we are being asked are getting ever more complex, and we cannot answer them alone.

There is also a question of whether we have the right tools at our disposal. The ICO benefits from strong, credible enforcement powers, which allows us to seize data in cloud servers or make no-notice inspections of business premises, and make it a criminal offence to falsify or conceal evidence that we need for an investigation into a data breach. These are essential powers for a modern regulator in the digital world.

Globally, we also need to find bridges that bring together our different laws and allow for better collaboration. We need to enhance our ability to cooperate in policy and enforcement work, and ease tensions between trading alliances. My view is that **accountability** can be such a bridge. An example is the Artificial Intelligence Working Group resolution, to be brought to this year's Closed Session. We have been able to discuss a complex issue like AI, in the context of a multitude of different legislative regimes, and still find common ground on how we can work together.

Identify both the challenges and opportunities for the Global Privacy Assembly and how can we continue to ensure the GPA makes a real difference?

Let's talk challenges first.

Data protection is more complex, as we have discussed. As regulators and authorities, our workload is greater, with so many of the big international issues featuring a central privacy element, from fair elections to keeping children safe online, from crypto currencies to facial recognition technologies. And then there is the global pandemic to contend with. There might be a temptation to turn inward, and see international cooperation as an aspect we simply do not have capacity to support.

We must not let that happen. We are united within the GPA by a common priority right now. We face very similar questions: of translating our laws in a facilitative way to enable innovation; of finding the balance between supporting our societies and economies, while protecting key rights; and of appreciating the long-term impact that our privacy decisions will have.

> **We have had to reassess our priorities to reflect these exceptional times, and to recognise the increased pressures organisations face**

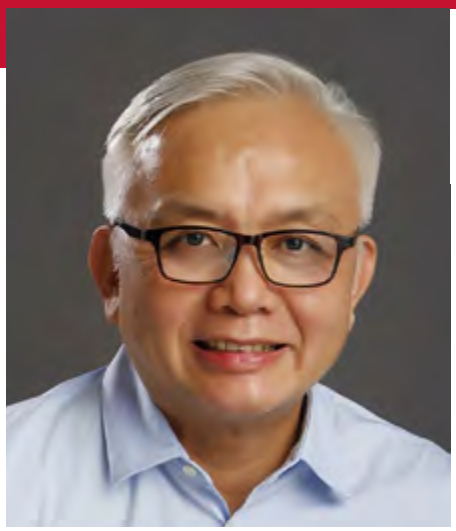
In that respect, our forum for sharing good practice and expertise has never been more relevant. Our work in shaping a Global Privacy Assembly over the past few years has been defining. Our group has never been better equipped to contribute positively to the practical and policy questions we face.

Take facial recognition technology. We all face similar questions, and similarly high stakes. A resolution at this year's Closed Session allows us to share our thoughts, and show a united position on aspects like the value of privacy by design principles and transparency.

As well as greater collaboration, there is also an opportunity for the GPA to have a greater international voice. There will be a resolution at the Closed Session pointing us toward a more active voice on emerging global issues, promoting a global regulatory environment. I believe that could prove a defining moment in the GPA's evolution.

GPA COVID-19 Taskforce Update

GPA COVID-19 Taskforce Paves Way for Fostering Much-Needed International Collaboration



Commissioner Raymund Liboro, Chair of the COVID-19 Taskforce, highlights the role and significant achievements of the Taskforce to date

As the crisis continues to hang on the horizon, the National Privacy Commission (NPC) has taken on an international duty to protect personal data by gathering data privacy regulators and champions around the world to deal with COVID-19 threats that undermine their cause.

The NPC, serving as an example for its collaboration with national authorities in dealing with the pandemic, was tasked in April 2020 to lead the newly formed COVID-19 Taskforce of the Global Privacy Assembly (GPA).

The Taskforce's strategy is aimed at strengthening jurisdictions' roles as an enabler and protector of the use of personal data. To effectively take on these roles, the Taskforce created two subgroups: the Sub-Group on Emerging Privacy Issues, which focuses on compiling best practices on pressing privacy and data protection issues; and the Sub-Group on Capacity Building, which focuses on engagement through webinars and collaboration with various privacy networks.

With these groups, the Taskforce sets the priorities for data privacy authorities (DPAs), which are to survey privacy policy and technology trends, share and explore best practices with other jurisdictions and the private sector, and address current and emerging challenges.

Weeks forward from its creation, the COVID-19 Taskforce has held five robust discussions based on an earlier survey of the most pressing concerns members need to address: privacy-by-design principles, contact tracing and the important role of DPAs in a period that is putting data privacy and protection principles to the test.

Starting tracing efforts with transparency

The first webinar, held on 6 July 2020, tackled the leading contact-tracing solutions around the world. The discussion aimed to give guidance to members and observers whose countries are at the exploratory or initial stage of adopting these applications.

Steps taken to safeguard users' privacy in contact tracing were expounded by technical experts from two of the world's largest technology companies — Apple and Google. Each shed light on the functionalities of their respective technologies and how these augment and accelerate traditional contact-tracing efforts.

An overarching principle in the development and operation of such apps, it was emphasized, is the establishment of transparency at the beginning of the process. The level of transparency aimed for is where users are confident that they are in full control of their personal information. This is enabled by a full, clearly written privacy disclosure that specifies who has access to the data, who can use this, and how.

A policy discourse followed, with privacy regulators, namely, the Information Commissioner's Office, UK, the Federal Data Protection and Information Commissioner of Switzerland and the Personal Data Protection Commission of Singapore, that have successfully applied data protection by design in contact-tracing apps.

DPAs' multiple roles in a crisis

In the second webinar, titled "Enablers and Protectors: The Role of DPAs Confronting COVID-19 – Contact Tracing and the Recovery Response," the many roles of DPAs were underscored.

> **The Taskforce's strategy is aimed at strengthening jurisdictions' roles as an enabler and protector of the use of personal data**

Amid the new emerging challenges, the role of DPAs transcends regulatory function to being an influencer in contact-tracing policies of the public. As several issues have posed questions on proportionality and transparency requirements, privacy issues on location tracking and surveillance, DPAs must also rethink how to set more practicable policies with consideration of scenarios in the future, beyond COVID-19.

In the third webinar which was jointly conducted with the Centre for Information Policy Leadership, contact tracing was again a central topic as economies gradually reopen.

Based on the survey conducted by the COVID-19 Taskforce, 80% of members voted contact-

tracing and location tracking as the top pressing privacy issue of jurisdictions and organizations, with the handling of employee data in work-from-home or return-to-work situations coming in second (76%), and handling of children's or students' data associated with the use of e-learning and online schooling technologies, third (60%).

> **DPAs must also rethink how to set more practicable policies with consideration of scenarios in the future, beyond COVID-19**

For contact-tracing efforts to be rolled out successfully, full transparency must be ensured from the outset. Governments have to enable data subjects to see the entire picture of a contact -tracing process, and be able to zoom in on each aspect in order for them to make informed decisions in assessing whether an intrusive measure leads to lower rates.

In this regard, it was agreed that DPAs have a critical role in guiding epidemiological authorities how to best establish and sustain transparent tracing operations.

Importance of DPO guidance

Meanwhile, the fourth webinar, held on August 25 in collaboration with the International Association of Privacy Professionals, revolved around the adoption of security, privacy and safety measures in the workplace.

Specifically, the talk laid on the table the steps companies are taking to address the privacy risks and challenges facing their different working arrangements: the protection of personal data in digital transactions and transfer of data; policy responses to the pandemic; and the coordination of the private sector with government.

Such discussion stands relevant as businesses and governments are judged by their customers and stakeholders based on their ability to ensure that they not just operate within the bounds of the law but also go the extra mile to institutionalize global best practices.

Crucial in shepherding businesses and government offices toward establishing a privacy-compliant working environment under the new normal are the data protection officers (DPOs). Like DPAs, DPOs must by now be prompted to move forward and deal with challenges with a new sense of purpose, that is to prevent their cause as data privacy advocates from being a casualty in the war COVID-19.

Moving forward

The next dialogue was a workshop held jointly by the GPA and the Organization for Economic Co-operation and Development (OECD) on 16 September. This event centred on recently gained learnings and reflected on how these can be leveraged in anticipation of future data protection and privacy challenges in the road to recovery.

In October, the team aims to collect global best practices and subsequently hold a high-level meeting where the team will assess the practicability of these practices.

The four webinars and the GPA/ OECD workshop conducted so far, showed the many pressure points that demand continued collaboration in the international community. The NPC, as Chair of the Taskforce, hopes to sustain engagement with GPA members, bilateral partners, and other potential international partners in ensuring that communities uphold as basic a human right as data privacy.

You can hear from Commissioner Liboro and the work of the GPA COVID-19 Taskforce at the virtual GPA 2020 Closed Session – At your Desk Conference on Day 2, Wednesday 14 October 2020, GPA COVID-19 Taskforce Session.

Regional Perspectives

The African Network of Personal Data Protection Authorities (RAPDP)

Marguerite Ouedraogo Bonane, President of the RAPDP, explains the origins and importance of this network for the African region

The Formation of the African Network of Personal Data Protection Authorities (RAPDP)

The African Network of Personal Data Protection Authorities (RAPDP) was established in September 2016, in Ouagadougou during the 2nd African Forum on the Protection of Personal Data, and has 13 members: South Africa, Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gabon, Ghana, Mali,

Morocco, Sao Tomé and Principe, Senegal, Chad and Tunisia.

The objectives of the organization are to create a framework for cooperation and exchange between members and organizations regarding data protection, to include the private sector and civil society, and foster the sharing of ideas and experiences on emerging data protection issues.

In addition to the General Assembly, the Network includes an Office and a Permanent Secretariat

Member countries remain convinced that cooperation is the only way to better protect personal data and privacy

provided by the National Commission for the Control and Protection of Personal Data, (CNDP) Morocco.

In terms of nurturing influence in Africa, the RAPDP leads engagement with:

- African states, with a view to encouraging them to legislate on data protection and establish independent authorities to ensure that people's data processing rights are respected; and
- Organizations, such as the African Union, to play a leadership role in encouraging African states to accede to the Malabo Convention (the African Union Convention on Cyber Security and Personal Data Protection).

Current priorities for the Network focus on increasing the visibility and presence of the RAPDP on the international stage, including:

- consolidating the partnership with different organisations – African Union, Council of Europe, OIF (The Organisation Internationale de la Francophonie), GSMA, etc.;
- continuing to uphold Africa's voice within these organizations; and
- organising side events at international events.

The major challenges for the Network include; promoting access to technical, financial and human resources in order to achieve our objectives, to lift the language barrier that currently exists with members speaking Portuguese, English and French, and to establish a culture of privacy and personal data protection, particularly on both the Internet and social networks.

As part of the fight against COVID-19, the RAPDP issued a statement reminding States and

Marguerite Ouedraogo Bonane, President of the RAPDP, President of CIL, Burkina Faso and member of the GPA Executive Committee

those responsible for processing personal data of the need to ensure compliance with the fundamental principles of data protection and privacy. This was promoted by all member countries.

Each Member Authority of the Network has taken the initiative to play its part in the fight against the pandemic, ensuring respect for privacy and personal data. The CIL of Burkina Faso, which chairs the Network, organized, with the support of the United Nations Development Programme (UNDP), zoom communications on "COVID and the Protection of Personal Data" for health authorities and members of the Network. Also, the RAPDP member authorities have organised communication/ awareness-raising activities, compliance support, training and cooperation.

Moreover, the CIL of Burkina Faso and the CNDP of Morocco, members of the GPA COVID-19 Taskforce, have shared with the members of the global taskforce the experience of the African Data Protection Authorities.

RAPDP achievements

The RAPDP has adopted a five-pillar action plan:

- Putting in place high-performance work tools;
- Enhanced visibility and presence of the network on the international stage;
- Cooperation with African and international institutions;
- Promoting privacy and personal data; and
- Development of synergy and cooperation between members.

And has established three working groups, on:

- Identity management;
- Capacity building; and
- Cooperation with the African Union and other organizations.

In light of the global operation of companies like Google, Apple, Facebook, Amazon, Microsoft (known as GAFAM), member countries of the RAPDP remain convinced that cooperation is the only way to better protect personal data and privacy.

The vision for the RAPDP in the long term is to: promote the right to the protection of personal data in Africa by enacting legislation and establishing independent authorities with substantial powers and means, to strengthen the capacity of members through access to adequate technical, financial and human resources, and to harmonize privacy and data protection laws and practices.

Strategic Direction Sub-Committee Overview 2019-2020

Information and Privacy Commissioner, Angelene Falk, Chair of the GPA Strategic Direction Sub-Committee (SDSC) highlights the crucial role of the SDSC this year and the priorities ahead

2020 has been a year of unprecedented challenges and opportunities for our global community.

Last October in Albania, the GPA adopted an ambitious Strategic Plan which set out our Policy Strategy to allow the GPA to work towards a global regulatory environment with clear and consistently high standards of data protection. This was a significant moment for the GPA, outlining our commitment to identify and engage on emerging issues and work collectively on regulatory solutions.

Looking back over the past year, I cannot recall a bigger year for our community. The global COVID-19 pandemic has brought unprecedented challenges which have caused us to adapt both our working styles and our regulatory priorities. However, across the GPA community I have seen our resolute focus and commitment to delivering our Strategic Plan.

The Executive Committee established a strategic direction sub-committee that has been tasked with supporting the Executive Committee in overseeing the GPA's progress in relation to its strategic priorities, particularly the co-ordination and review of the Policy Strategy actions. I am very pleased to have had the opportunity to chair this sub-committee.

Our work has been focused on ensuring that internally the GPA is working towards a global regulatory environment with clear, consistently high standards of data protection, and externally we are seen as a united forum speaking with one voice.

Reviewing Policy Strategy progress

One of the Strategic Direction Sub-Committee's (SDSC) main objectives is to coordinate and review the delivery of the Policy Strategy. A key part of this has been linking in with all working group chairs, particularly those working groups with allocated Policy Strategy actions.

> **Looking back over the past year, I cannot recall a bigger year for our community**

The SDSC has had the opportunity to meet with working group chairs to engage in 'deep dive' discussions into working group workplans. These meetings brought to life the important work done during the year, allowing working group chairs to engage with the SDSC, as well as giving them the opportunity to link in with each other where their work was complementary.

I am very much looking forward to standing behind our working group chairs as they present on their achievements over the past 12 months at the Closed Session.

Enhancing the GPA voice year-round

The Strategic Plan also identifies that a mission of the GPA is to be an outstanding global forum, providing leadership at an international level in data protection and privacy. The GPA has committed to maximising its voice and influence by being an active forum which engages on privacy and data protection issues year-round.

The Executive Committee tasked the SDSC with developing a clearly documented and transparent mechanism for the GPA to enhance its influence by speaking on issues as they emerge throughout the year. A proposal was circulated to the GPA membership for consultation, and received diverse and positive support for the proposed mechanism.

Engaging externally with international organisations

The GPA continued to be represented by its observers at international organisations:

- NPC Philippines at APEC;
- CNIL France at OECD;
- EDPS, EU at the Council of Europe and
- OPC Canada at the UN Counter-Terrorism Committee.

While the number of events might have reduced this year because of the current global circumstances, our observers continued to engage where possible. A key part of the SDSC's role is to develop and direct key messages for GPA external engagement. To this end, the sub-committee has this year developed slide decks for observers to use as they represent the GPA externally, and templates for observers to report back on their engagement. The regular 'Observers on the road' feature in the GPA newsletter has enhanced the visibility of the valuable work our observers do.

Working Group highlights

Future of the Conference Working Group

Director of International Regulatory Strategy at the UK Information Commissioner's Office, Paula Hothersall, Chair of the Working Group on the Future of the Conference, reviews progress over the past year and presents an update on work yet to be completed ahead of the 2021 Annual Meeting

As members will recall, the Working Group on the Future of the Conference (FOTC WG) was established in 2018, subsequent to a consultation in 2017, about the future direction of our community. These strategic consultations resulted in the adoption of the Resolution on a Roadmap on the Future of the Conference at the 40th Annual Meeting. The Resolution mandated the FOTC WG with five workstreams; three of which were concluded at the 2019 annual conference in Tirana, including the helpful background paper on the criteria of autonomy and independence which has been a valuable resource for the Executive Committee in the Accreditation process this year.

Key outputs of the Working Group in 2020 have been:

- conclusion of the work to investigate provision of a secure online platform;
- further work to explore the establishment of the Secretariat as a separate legal entity.

Members will be aware of the survey conducted by the Working Group earlier this year which sought to establish the desire for, and possible type of, secure online platform that would best meet members' needs. With low numbers responding to the survey the results were inconclusive. Moreover, it was recognised that a driver for this work – to provide a mechanism for increased sharing of information on our regulatory approaches – continues to be met by the work of the International Enforcement Cooperation Working Group (IECWG). During a meeting held at the beginning of June, the FOTC WG has, therefore, reached the decision to conclude its work on this issue.

> **The most significant output this year was … a new paper exploring the implications of establishing the GPA Secretariat as a separate legal entity**

However, the most significant output this year was the development of a new paper exploring the implications of establishing the GPA Secretariat as a separate legal entity. We will provide an update on this at this year's virtual Closed Session. Importantly, the outbreak of the COVID-19 pandemic and the move to an online conference has meant that the Working Group needed to be realistic about what could be achieved within the limits of a virtual meeting on a matter of some legal and financial complexity. Therefore, at our June meeting, we also reached the decision to recommend to the membership to postpone until 2021, the important decision on the creation of a more stable GPA Secretariat. In the meantime, we will focus our efforts on additional analysis of financial models – including exploring external sources of funding – for the funding of the GPA Secretariat so as to ensure members can make a fully informed decision next year.

Overall, we are pleased with the progress made and I would like to thank all members of the Working Group for the time and effort dedicated to this strategic pillar of the GPA's work, aimed at laying stable foundations for our community.

The Membership of the Working Group on the Future of the Conference currently consists of 16 delegations – including an Observer authority – truly reflecting the cultural and legal diversity of the Assembly. The ICO has been providing the Chair function during 2019-2020, but is keen to have a co-Chair, ideally from a region other than Europe, to lead the WG.

All GPA members are cordially invited to get in touch through the GPA Secretariat (secretariat@globalprivacyassembly.org) should they have an interest in joining the Working Group or acting as co-Chair. If you wish to know more, please visit the Working Group project page on the GPA website.

Working Group highlights

Global frameworks and standards – evolution towards global policy, standards and models for data protection and privacy

A Focus on the work of Policy Strategy Working Group Work Stream 1

Policy Strategy Working Group Work Stream 1 (PSWG1) is chaired by the Information Commissioner's Office, UK, and was established following adoption of the Resolution on the Conference's strategic direction at the 41st ICDPPC conference in Tirana, Albania in 2019, including the new Policy Strategy, and derives its mandate from this.

A pivotal moment for the GPA, this set out a new level of ambition for the GPA as it aimed to transform into a year-round assembly that added real value to privacy and data protection debates, with a clear focus on regulatory cooperation.

Working Group Activities

PSWG1 is responsible for delivering an element of the Policy Strategy relating to the GPA first Strategic Priority for 2019-21 – 'Work towards a global regulatory environment with clear and consistently high standards of data protection'; more specifically Pillar 1 of the Policy Strategy, namely 'Global frameworks and standards' and the 'evolution towards global policy, standards and models for data protection and privacy'.

There are two Pillar 1 Policy Strategy actions, forming the first steps towards that evolution:

- Pillar 1, action 1 – Complete an analysis of current global frameworks for privacy and data protection, including key principles, data subject rights, cross-border transfers and demonstrable accountability standards.
- Pillar 1, action 2 – Consider developing common definitions of key data protection terms.

PSWG1's work plan set out that the group would address action 1 in 2020, and action 2 in 2021.

In 2020, PSWG1 undertook analysis of ten global frameworks for privacy and data protection, covering all the regions of the GPA, identifying common principles and themes according to an agreed list of criteria. The ten frameworks compared were:

- Madrid Resolution
- OECD Privacy Guidelines
- APEC Privacy Framework
- Convention 108
- Convention 108+
- Standards for Personal Data Protection for Ibero-American States
- African Union Convention on Cyber Security and Personal Data Protection
- ECOWAS Act on Personal Data Protection
- EU data protection standards (EU General Data Protection Regulation)
- UN Guidelines for the Regulation of Computerized Personal Data Files

The criteria used to analyse the frameworks were selected in order to fulfil the requirements of the mandated action – to include "key principles, data subject rights, cross-border transfers and demonstrable accountability standards."

Conclusions and next steps

It was clear from the subsequent analysis that there is broad agreement across the frameworks in terms of key principles, a number of core rights and other requirements, and in particular around the role of supervisory authorities. The similarities identified could, as a starting point, assist GPA members by providing an evidence base which emphasises the importance of the common elements found.

The group agreed it would be appropriate to deliver an output for 2020, which highlighted the strong degree of commonality and convergence found between the frameworks. This output/referential document would not only suggest a commitment to shared values between the frameworks and the GPA members who work within them, but could also provide a point of reference for GPA members in their conversations with those they regulate, their governments and wider global stakeholders.

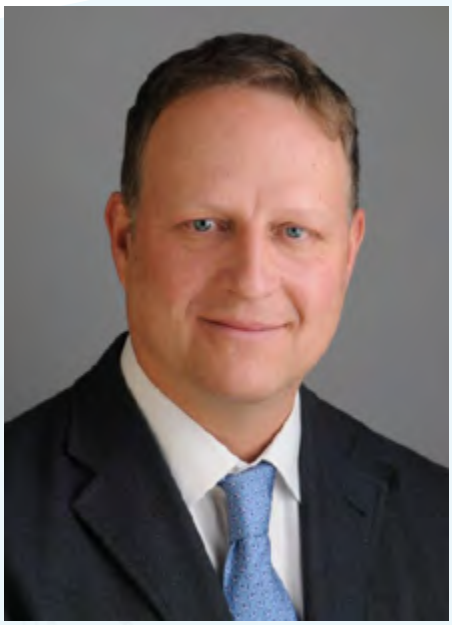
Findings relating to cross-border transfers indicated that while there are broadly similar general principles around the need to protect personal data across-borders, there are a variety of different mechanisms in use. These mechanisms themselves require further analysis in order to reach any substantive conclusions. PSWG1 has therefore recommended carrying out further analysis work on cross-border transfers in 2020-21.

Policy Strategy Working Group Work Stream 1 will hold a Webinar on 30 September 15:30-17:00 (BST) for GPA Members and Observers only, please contact **secretariat@globalprivacyassembly.org** for more information

Working Group highlights

The integral relationship of privacy and data protection to other rights and freedoms

Gregory Smolynec, Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada, Co-Chair of the Policy Strategy Working Group Workstream Three (PSWG3) together with the European Data Protection Supervisor (EDPS), outlines developments to date and phases of work for 2021



The 41st International Conference of the Global Privacy Assembly (GPA), held in Tirana, Albania in October 2019, saw the adoption of the Resolution on the Conference's Strategic Direction and the Strategic Plan. At the core of this Resolution and Strategic Plan is a policy strategy that sets out the 2019-21 vision for the GPA.

Research to inform a new draft narrative which links to global rights-based instruments that enshrine data protection and privacy rights is complete; next steps include external stakeholder engagement before a resolution at the GPA 2021 conference

The Policy Strategy Working Group Workstream Three (PSWG3) is one of three groups established to assist the GPA with the implementation of its new Policy Strategy. This group derives its mandate from Pillar #3 Action IV of the Policy Strategy, which commits to developing a narrative highlighting the integral relationship of privacy and data protection to other rights and freedoms. This narrative will build on the 2019 Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising other Fundamental Rights.

The Policy Strategy recognizes that at a global level, data protection and privacy rights are enshrined in important international rights-based instruments, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The Strategy notes the importance for the GPA of highlighting and clarifying linkages between privacy and data protection with other rights.

In doing so, the narrative will aim to encourage global progress in the recognition of privacy as a fundamental human right. It will help GPA members promote the calls for action outlined in the 2019 Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising other Fundamental Rights.

Current Progress

The PSWG3 has set out a four-phased approach for developing the narrative over a two-year period. Phase 1 involves research and information gathering, followed by the development of a narrative under Phase 2. External feedback on the draft narrative will be received under Phase 3, and Phase 4 will see the narrative finalized for adoption by the GPA membership at the 2021 annual conference.

For its first year of activity, the PSWG3 focused on gathering and collating information from data protection authorities and GPA observer organizations from around the globe.

Based on the information received to date, the group has now begun developing the draft narrative.

The PSWG3 has also identified additional actions that will run parallel to the development of the narrative. These include:

- encouraging GPA members to call on their governments to reform laws as needed to protect broader human rights;
- encouraging members to work with local counterparts on the regulation of political ecosystems; and
- developing a proposal for a privacy and human rights champion award as part of the annual Global Privacy and Data Protection Awards.

In 2020-2021, the PSWG3 will move forward with the final phases of the work. This includes seeking the views of stakeholders, such as international and domestic human rights agencies, the UN Special Rapporteur on the Right to Privacy, civil society groups and other key international stakeholders, such as the Global Alliance of National Human Rights Institutions and Geneva International. Finally, the PSWG3 will recommend a final narrative, to be considered for adoption at the 2021 GPA annual conference.

Working Group highlights

Revitalizing the CIRCABC e-library platform with up-to-date online privacy resources

The Digital Education Working Group reports on the CIRCABC platform

Raising awareness for the concerns of data protection for children, adolescents and adults will increase their capacity to claim their data protection rights in the digital environment. In the light of a tense resource situation, continued sharing of videos published on Data Protection Authorities (DPAs) YouTube channels, of entertaining online games, films and any other teaching medium addressing young people, parents, and educators is a priority for the Digital Education Working Group (DEWG).

The specific workspace created in 2015 on the CIRCABC platform, an information sharing tool provided by the European Commission dedicated to our Working Group, is continuously assessed and updated in order to remain effective and attractive. 37% of the documents made available by DPAs are in English, 34% in French, while many are naturally also published in national languages.

The CNIL (FR) and the CNPD (LU) both acting as administrators of the online library, are currently engaged in a project to update the CIRCABC platform and re-configure it with a new classification by types of teaching and training resources and with additional key categories.

The objective is to go online with the revised library by 30 September 2020.

What is at stake?

There is currently a wide diversity of some 300 uploaded documents, which include videos, comics, school manuals, children's books, vademecum for students/ teachers, online games, short film scenarios, posters on protecting Privacy online, and Guides for parents. In order to improve the quality of the library content, a detailed inventory of the existing resources was performed with members asked to have documents reviewed, updated, deleted or simply replaced in the new folder architecture.

> The COVID-19 pandemic demonstrates more than ever that digital education should have a fixed and important role in schools

The COVID-19 pandemic demonstrates more than ever that digital education should have a fixed and important role in schools. For this reason, we expect an increased and more regular access to CIRCABC with larger numbers of users and contributors, thus creating a very dynamic environment.

How to proceed?

The CNPD has offered to upload updated documents on behalf of the DPAs until 30 September 2020.

Any newcomer just needs to request authorization from the administrators to access the platform (via a simple online protocol) and to complete a questionnaire with the URL of the resources, a short description, and the age groups or target audience.

After the date of 30 September 2020, DPAs will be kindly invited to open individual accounts on the platform or use their dedicated account to add new online material by themselves.

A new governance arrangement with the EU Commission hosting the free of charge CIRCABC Platform service will ensure the back-up of the DEWG to the benefit of all DPAs worldwide.

What next?

There will be a reinvigorated need to share the most relevant online resources in digital literacy and privacy education intended for school curricula, in Codes of Best practices in online learning for schools and teachers, as well as a rapid response guidance in education after the COVID-19 pandemic. Specific events, such as Data Protection Days, Privacy Awareness Weeks, Safer Internet Days or the Annual Global Privacy Awards, will also create opportunities to upload new resources.

An appropriate procedure is available to apply for registration and opening **an ECAS account**. Please ask the DEWG Secretariat (Pascale Raulin-Serrier at **pserrier@cnil.fr**, Jérôme Commodi at **jerome.commodi@cnpd.lu**, Vincent Legeleux at **vincent.legeleux@cnpd.lu**,) regarding any questions related to the CIRCABC platform and registration process.

Working Group highlights

Exploring the intersection and collaboration across regulatory spheres in today's digital economy

An update from the Co-Chairs of the Digital Citizen and Consumer Working Group, the Office of the Privacy Commissioner of Canada, and the Office of the Australian Information Commissioner

The Digital Citizen and Consumer Working Group (DCCWG), established in 2017, arose out of the recognition that traditional lines separating privacy, consumer protection and competition have rapidly begun to blur – or outright disappear – in today's digital economy. The group seeks to explore and better understand these intersections, and to foster greater collaboration across regulatory spheres, holistically realizing superior privacy and consumer outcomes for individuals across the globe.

The DCCWG's 2019-2021 mandate focuses primarily on the complex intersection between privacy and anti-trust. To that end, the group's work includes:

Privacy and Competition Deep Dive: To better understand the complementarity and regulatory tensions between privacy and competition, the group has been conducting interviews with anti-trust regulators, which have included the Colombian Superintendence of Industry and Commerce and the US Federal Trade Commission, who shared their valuable perspectives as leading authorities regulating both privacy and competition. Preliminary takeaways for this overarching area of study include:

- Privacy can represent a non-price factor in competition, but is often difficult to define and measure;
- Anti-trust remedies may involve a privacy component requiring consideration or action in that area (eg access to consumer data); and
- Regulatory alignment or tensions will depend on circumstances. A merger can result in increased dominance, decreased competition based on privacy, and the erosion of privacy protection; or the cost of data protection requirements can represent a barrier to entry for smaller companies, thereby increasing the market power of large established players.

That is just the tip of the iceberg, and we look forward to learning more as we continue our anti-trust interviews over the coming months. This work will support our development of collaborative approaches to address this intersection.

Tracking and Facilitating Actual Cross Regulatory Co-operation: The group continues to capture and map concrete examples of cross-regulatory intersection and co-operation between regulators. The impressive extent of intersection-related work around the world is illustrated in the DCCWG's 2020 final report, but to provide just a few interesting examples:

- The Office of the Australian Information Commissioner and Australian Competition and Consumer Commission (ACCC) have established a co-regulatory scheme to enforce Australia's new data portability law, which aims to give consumers greater control over how their data is used and disclosed, in order to create more choice and competition.
- The Norwegian Datatilsynet and Consumer Authorities issued joint guidance on digital services and consumer personal data, aiming to help business operators, developers, marketers and providers of digital services navigate practical issues where consumer protection and privacy issues overlap.
- Recently, the European Commission announced an in-depth investigation into Google's acquisition of FitBit, for which it has been working in close cooperation with the European Data Protection Board. The DCCWG will, of course, follow this case with great interest.

In addition to the above, the DCCWG is also focused on:

- continued sensitization of relevant networks to intersection issues, such as through interventions at APPA, ICPEN and OECD events; and
- in collaboration with the IEWG, the DCCWG will provide a chapter on cross-regulatory collaboration, to support an update to the Enforcement Cooperation Handbook. The DCCWG and IEWG will conduct a survey of privacy, consumer protection and anti-trust authorities to inform this chapter.

We look forward to sharing more at the DCCWG side-event. See you all there, virtually of course.

The Digital Citizen and Consumer Working Group will hold a Webinar on Wednesday 28 October 10:00-11:30 (UTC - GMT) for GPA Members and Observers only, please contact **secretariat@globalprivacyassembly.org** for more information.

Working Group highlights

Creating an environment that supports and catalyses proactive, practical enforcement cooperation

The Co-Chairs of the International Enforcement Cooperation Working Group (IEWG) report on the role of the group in helping to advance a global regulatory environment of high standards of data protection and privacy

The International Enforcement Cooperation Working Group (IEWG) is now a permanent Working Group of the GPA. It is co-chaired by the Office of the Privacy Commissioner of Canada, the UK Information Commissioner's Office, and the US Federal Trade Commission, and has a regionally diverse membership of 16 Authorities.

> **the IEWG facilitated two 'safe space' sessions [which] contributed to the development of two concrete enforcement cooperation initiatives**

The work of the IEWG is integral to the GPA, supporting its strategic ambitions around leadership, collaboration, and fostering a global regulatory environment of high standards of data protection and privacy. The IEWG also has a key role in helping to advance the Assembly's Strategic Direction and associated GPA Policy Strategy. In particular, it has primary responsibility for leading on delivery of the enforcement cooperation element of the Strategy in Pillar 2 - from which the IEWG derived its mandate to form as a permanent Working Group.

Working from this mandate, in its first year of operation, the co-chairs of the IEWG prioritised activities to rapidly put into action the group's refreshed focus on creating an environment that supports and catalyses proactive, practical enforcement cooperation on current and pressing issues. To this end, in the first half of 2020, the IEWG facilitated two 'safe space' sessions, during which members spoke candidly about their key concerns, policy positions, and regulatory experiences in relation to specific global entities and issues.

These sessions – while valuable in and of themselves in supporting the exchange of knowledge and information on live issues – contributed to the development of two concrete enforcement cooperation initiatives:

- a joint investigation into Clearview AI between the Office of the Australian Information Commissioner and the UK Information Commissioner's Office; and
- an open letter with a joint statement on global privacy expectations of video teleconferencing companies, signed by six member Authorities of the IEWG.

Looking ahead, the IEWG co-chairs are leading a programme of work that will continue to strengthen the group's ability to facilitate live enforcement cooperation, while also: developing and enhancing tools to guide and support organisations in their collaboration initiatives; and exploring ways to better coordinate and leverage activities across the global landscape of Privacy Enforcement Authority (PEA) networks.

The International Enforcement Cooperation Working Group (IEWG) will hold a Webinar for GPA Members and Observers only on Monday 12 October, 11:30-13:00 BST, for further information, please contact: **international.enforcement@ico.org.uk**.

Have you thought about contributing to the GPA Newsletter?

We are now planning editorial for the November edition of the Newsletter, please contact the GPA Secretariat if you would like to contribute, and for more information on any of the issues highlighted, contact secretariat@globalprivacyassembly.org.

Working Group highlights

International Working Group on Data Protection in Technology (IWGDPT) – The Berlin Group

Maja Smoltczyk, Berlin Commissioner, provides an update for the GPA on the important work of this group

A lot has happened since the Berlin Group last met in Brussels in the fall of 2019. Due to the rapid spread of COVID-19, which has been keeping us all on edge since the beginning of this year, we had to cancel the spring meeting in Tel Aviv with very short notice. This decision was hard because our hosts, the Privacy Protection Authority Israel, had, very generously, already organized the meeting. However, of course, health comes first and so there was no alternative but to cancel the meeting. I very much hope that we will soon have the opportunity to hold a meeting in Tel Aviv in better times.

The group is currently focusing on Working Papers on Data Portability, Web Tracking in the Targeting Ecosystem, Sensor Networks and Voice-controlled devices

Since the COVID-19 situation did not improve worldwide, we also had to cancel our fall meeting, which the ICO was planning to host in London. Since the ICO is part of the group that will host regular meetings in the future, I am confident that we will catch up very soon. After we had weighed up possible options regarding how to continue the work of the group in these insecure times, the Secretariat decided not to move the meeting to the virtual world by holding a video conference. The

meetings of the working group are characterized by intensive and very detailed work on papers, as well as a rather informal personal exchange. We concluded that a video conference was not the appropriate format for this type of work meeting.

Instead, we have developed a procedure to advance the working papers, which the group is currently working on through a formal written process. During commenting and revision phases, members will have the opportunity to contribute within set deadlines. Where it is useful, rapporteurs can organize virtual meetings in small groups to discuss contentious issues and work on good formulations. The aim is to discuss and revise the drafts in this written process so that final versions of each paper will be ready for adoption at the next meeting, which we hope to hold in spring 2021.

Difficult times like these require new approaches. I think this procedure is a good solution, in order to meet the group's demand to deal with important issues at an early stage.

The group is currently focusing on Working Papers on Data Portability, Web Tracking in the Targeting Ecosystem, Sensor Networks and Voice-controlled devices. I would like to invite all members to contribute with both their experience and knowledge to help us create papers that will – as usual – serve as a solid professional support in our daily work. If you would like more information or would like to get involved in the work as a member of the working group, please contact our Secretariat.

I am pleased to announce an important novelty. After some discussions and a written vote among the members, the Working Group officially changed its name at its last meeting.

From now on, the group will meet under the name **International Working Group on Data Protection in Technology**. The reason why participants of the group had suggested a name change was that the group has not been dealing exclusively with telecommunications issues for a long time. On the contrary, this original topic of the group has receded into the background in past years. The new title honours the current work of the group, which deals with a wide range of issues from all areas of technology. By the way, all those who have learned to love the difficult acronym IWGDPT over the years can be happy, because the Berlin Group will continue to be listed under this abbreviation.

I hope that personal meetings at international level will soon be possible again without any worries because this exchange is an important part of our work. I wish you all good health, and safety in these difficult times.

For more information on the IWGDPT, please email: iwgdpt@privacy.de

Observer on the Road

Latest Update from the GPA Observer at the United Nations (UN) Counter-Terrorism Committee

Daniel Therrien, Privacy Commissioner of Canada, reports as the representative for the Global Privacy Assembly on the work of the UN Counter-Terrorism Committee

The United Nations Counter-Terrorism Committee

The United Nations (UN) Counter-Terrorism Committee's (CTC) work has linkages to data protection and privacy issues. Therefore, the Global Privacy Assembly (GPA) has obtained observer status before this international organization. The Office of the Privacy Commissioner of Canada (OPC) fulfills this observer role on the GPA's behalf. We are pleased to provide the following report on the work of the CTC.

The UN CTC was established by the UN Security Council shortly after the 9/11 attacks and works to bolster the ability of UN member states to prevent terrorist acts both within their borders and across regions.

> **updated technical guidance August 2020… covers a new emphasis on standards for data collection and the importance of non-discrimination, necessity and proportionality**

An executive directorate (CTED), which carries out policy decisions of the CTC, conducts expert assessments of States and facilitates counter-terrorism technical assistance for CTC members.

The Security Council has developed an extensive counter-terrorism framework through the adoption of numerous resolutions, many of which call on member states to make use of technological tools that raise privacy and data protection concerns. At the same time, UN member states are required to effectively counter terrorism while protecting the right to be free from arbitrary or unlawful interference with privacy.

Observations on behalf of the Global Privacy Assembly

The CTC and CTED are mandated by the Security Council to assess the implementation of the council's counter-terrorism framework by member states and to collect good practices in this area in compliance with international human rights, humanitarian and refugee law.

They have been actively pursuing efforts to this effect.

Of particular note, in December 2018, a special meeting of the CTC reviewed a proposed addendum to the Madrid Guiding Principles, a practical tool for member states to stem the flow of foreign terrorist fighters. During the special meeting, the OPC recommended the Principles be clarified to explicitly note that their implementation must be done in a manner that respects international human rights law. This should include privacy and data protection principles of necessity, proportionality and independent oversight.

The Addendum to the Principles that was adopted following this meeting was the first document produced by the CTC that addresses matters related to privacy and data protection in detail.

In its most recent report to the UN Security Council, the CTC highlighted that efforts to ensure compliance with international human rights obligations while countering terrorism continue to be a priority for member states and the CTC. However, recent developments and related Security Council resolutions have raised new challenges in this area.

The report noted that many counter terrorism practices, such as enhanced surveillance, the international exchange of watch lists and reliance on biometrics have human rights implications. These practices can raise serious issues with respect to the rights to freedom of expression and privacy. The CTC and CTED have considered steps to guard against such human rights infringements, including the use of independent oversight mechanisms.

The UN CTC hosted a virtual open briefing on its updated technical guidance in August 2020. The new edition of the guidance synthesizes international resolutions, standards and norms so member states can meet their counter-terrorism obligations and prepare for UN assessments. It covers a variety of counter-terrorism strategies (terrorist financing, border security, etc.) with new emphasis on standards for data collection and the importance of non-discrimination, necessity and proportionality.

Additionally, a working group

(which the CTED co-chairs) launched a project to identify, collect, and analyze existing standards and good practices on collecting, analyzing, processing, storing and sharing data for counter-terrorism purposes. This project will recommend legal provisions related to such efforts that comply fully with international human rights, humanitarian and refugee law. The recommended provisions will be used for the preparation of national data protection legislative frameworks.

The CTC and CTED are committed to working with the GPA membership on its forthcoming recommendations to ensure that adherence to fundamental data protection obligations and universal human rights commitments such as the right to privacy are formally incorporated into international counter-terrorism efforts.

Meet our Member

President Felipe Rotondo of the Regulatory and Control Unit of Personal Data of Uruguay (URCPD)

Data Protection in times of health emergency – The Uruguayan Approach

Protection of personal data: regulation and authority

Law No. 18.331 of 11-VIII-2008 is Uruguay´s general law on the protection of personal data, with adjustments provided by Law No. 19.670 of 15-X-2018.

Its first article states: "The right to personal data protection is inherent to the human person, which is why it is included in art. 72 of the Constitution of the Republic". The latter establishes: "The enumeration of rights, duties and guarantees made by the Constitution does not exclude others that are inherent to the human personality or derive from the republican form of government".

This Law created the National Authority: Regulatory and Control Unit of Personal Data. It was accompanied by provisions that gave the Authority control and sanctioning powers, and a structure comprised of a three-member Executive Council, and an Advisory Council to the Executive Council.

It also provides administrative and jurisdictional guarantees, based on the principles of:

1. Truthfulness and purpose limitation – data must be accurate and not excessive ('minimization'), limited to the purpose for which it was obtained, and deleted if no longer necessary;
2. Lawfulness – in the way it is obtained and processed, without discrimination and that the data subject knows its usage, communications, etc;
3. Confidentiality;
4. Security; and
5. Accountability of the controller and processor, considering appropriate technical and organizational measures – privacy by design, by default, impact assessment, and to demonstrate its effective implementation.

The Uruguayan regime was considered adequate by the EU in 2012. In 2013, Uruguay became the first non-European member of Convention 108, also signing its amendment protocol.

Our work so far

The focus of our work to date has included: Promotion and awareness raising i.e., the school initiative "Tus Datos Valen"; Governance and capacity building i.e., training, guidelines, national and international events; Strengthening and positioning of our organization i.e., our annual review and other documents, the "Coffee Talks" cycle; and building international relations, with our Presidency of the Ibero-American Network, GPA membership, and participation in the Convention 108 T-PD Committee.

Health emergency, new challenges, and the rule of law

This health emergency is an exceptional situation that requires immediate and appropriate measures within the rule of law, which cannot be considered in isolation. People´s rights are not absolute – except life – and this obviously depends on health, our Constitution provides that "all inhabitants have the duty to take care of their health, as well as to assist in case of illness".

This is consistent with the Universal Declaration of Human

Rights, art. 29 and the American Convention on Human Rights, art. 30.

> Protection of personal data is not an obstacle to emergencies but rather marks the ethical and legal path to follow in respect of a fundamental human right

Regarding the consent of the data subject, it must be informed, explicit and, written in the case of sensitive data (such as health data). There are exceptions – exercising the functions of 'Public Authority' or the fulfillment of a legal obligation. It permits the processing of sensitive data for reasons of general interest according to law or if the requesting body has a legal mandate to do so.

The protection of personal data is not an obstacle to emergencies but rather marks the ethical and legal path to follow in respect of a fundamental human right.

Opinions and recommendations of the Regulatory and Control Unit of Personal Data (URCDP) in relation to the health emergency

The emergency was declared by the Government on 13 March 2020.

On 20 March, the Unit issued Opinion 2/020 clarifying the role of the Ministry of Public Health, and the application of principles and conditions in cases of exceptions to consent.

On 15 April 2020, the Unit issued "Recommendations for the processing of personal data in the face of the national health emergency situation", and on 9 June 2020, Resolution N° 35/020, in order to reaffirm the respect for this right regarding contact tracing.

Finally, on 18 June 2020, an instruction on the use of temperature control was issued.

Lines of work, a forward look

The Unit is developing four projects going forward.

1. "Regulation Update" – updating the legislation, drafting a compendium of legal provisions, and publishing various guidelines.
2. "Educational Content and Direct Action for Citizens" – agreements with educational authorities, and the inclusion of data protection in the curricula.
3. "Governance and Capacity Building" – publication of documents, and "National Data Protection Week", as well as a "Coffee Talks" cycle.
4. "Participation in the International Community" – ongoing work at the Ibero-American Network and the GPA, and in international engagement.

For more information on the URCPD, please visit the website.

Access the latest data protection and COVID-19 guidance and resources from GPA members and observers at:

globalprivacyassembly.org/covid19

GPA
Global Privacy Assembly

COVID-19 TASKFORCE

Your GPA News Highlights

For each edition of the GPA Newsletter, this section features GPA News Highlights for your information and review

September is here and unfortunately, the world is still gripped by the COVID-19 pandemic. However, the GPA has not stood still during this time. The GPA Community has shared knowledge and expertise throughout the year to aid in the global response to the data protection and privacy issues raised by this pandemic. With the annual conference imminent, we reflect below on the successful initiatives achieved by the GPA this year and those awaiting your review and adoption in the upcoming GPA 2020 Closed Session – At your Desk.

The GPA Response in 2020 to issues raised by the COVID-19 pandemic

Since the publication of the June Newsletter, the GPA COVID-19 Taskforce, led by Raymund Liboro, Privacy Commissioner of the Philippines National Privacy Commission and GPA's Executive Committee member, has organised two webinars and the follow-up OECD-GPA Workshop. At these events, the GPA global community shared their own experiences, and opportunities for innovation and best practice, together with input from representatives from government, academia, the private sector and civil society. Thereby, driving practical responses to the data protection and privacy challenges arising from the COVID-19 pandemic, and providing a valuable opportunity to engage and review the lessons learnt from each other in these unprecedented circumstances.

At the COVID-19 Taskforce Session on Day 2, Wednesday 14 October of the Closed Session, the Taskforce will be launching the COVID-19 Compendium of Best Practices. The draft Resolution on COVID-19 Resolution On The Privacy And Data Protection Challenges Arising In The Context Of The COVID-19 Pandemic will be considered for adoption on Thursday 15 October, Day 3 – Core Business Session at the conference.

Further GPA initiatives this year regarding the response to the COVID-19 pandemic have included the Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic issued on 27 March 2020.

On 21 May, the GPA Executive Committee issued its Statement about contact tracing measures being implemented around the globe. This recognises the importance of public trust and confidence in the handling and protection of personal information as a necessary precondition for their success. Emphasising the value in achieving privacy by design when developing new technologies in the interests of protecting public health.

And the launch of the GPA COVID-19 Response Repository provides valuable one-stop shop access to the latest guidance, Statements and information from GPA members for GPA members.

The Strategic Direction Sub-Committee and GPA Working Groups

The GPA's Strategic Direction Sub-Committee (SDSC) led by Angelene Falk, Information Commissioner for the Office of the Australian Information Commissioner and GPA's Executive Committee member, continues to drive the GPA's current priorities: please refer to our Strategic Plan (2019 – 2020) and Policy Strategy. The GPA will have the opportunity to discuss the priorities, achievements and forward looking plans of the GPA Working Groups on Tuesday 13 October, Day 1 – Strategic Priorities session, prior to the adoption of the Working Group reports on Thursday 15 October, Day 3 – the Core Business session.

Several Working Groups will be holding webinars for the GPA community only, please contact the secretariat for more information at secretariat@globalprivacyassembly.org.

Joint Statements on Emerging Global Issues

The GPA Executive Committee has proposed a Resolution on a new mechanism to enable the GPA as a whole to make its voice heard outside of the Closed Session on emerging issues with significant privacy implications. The proposal includes a suite of options to cater for different scenarios that might arise outside of the Closed Session and will be discussed for adoption on 15 October in the Day 3 – Core Business session.

Call to Members

All Resolutions proposed by the membership for 2020, will be reviewed for adoption on 15 October, Day 3 – Core Business Session at the conference. We look forward to receiving your comments and prospective co-sponsorship details by 30 September 2020.