Vol. 3, Issue 2 | 2021

NEWSLETTER

GLOBAL PRIVACY ASSEMBLY

GPA
Global Privacy Assembly

Message from the Chair

At last year's Closed Session, I spoke about the three aspects that are central to our Assembly's progress: continued modernisation, collaboration and community.

These themes continue to drive our work.

In March, the GPA Executive Committee met to consider our Assembly's strategic direction for the next two years. This is an important part of our continued modernisation, as we focus our priorities on the areas where we can have the most impact and retain the most relevance. As I discuss in more detail later in this newsletter, we as data protection and privacy authorities are at a pivotal moment: if data protection looks too much like a barrier, we risk being left behind. I urge all members to read and consider the Strategic Plan 2021-2023 once it is circulated.

Our strategy is a result of collaboration across the Assembly, with the views of members from around the globe represented. We are greater when we stand together. This shone through when we issued our first GPA Executive Committee Joint Statement in March.

The statement on the use of health data for domestic and international purposes provided timely guidance on an issue that is critical for governments, public sector organisations and private businesses around the world. The flexibility to respond to such an important issue that has arisen between our conferences is an important one: the GPA is now truly an influential forum year round.

If the Joint Statement showed how our Assembly can speak with one voice, then the launch of the GPA Reference Panel showed how we will listen. The panel will provide a valuable resource of experts to inform our views and work at our request on specific items, and allow us to be a greater part of the privacy conversation beyond our regulatory community.

That sense of community is reinforced in the results of our GPA Census, showing the truly global reach of the Assembly. The results provide a vital insight into the way the data protection landscape is changing.

All of these themes will be part of our Global Privacy Assembly 2021 conference later this year. The event will be the first hybrid conference, held both in person and online, and I am looking forward to what promises to be an exciting and important moment in our group's continued history.

Thank you for your continued support during this pivotal time for data protection and privacy, and for helping to make our community one that is so supportive, practical and relevant.

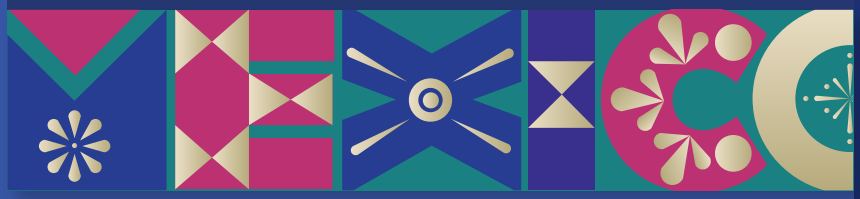
Elizabeth Denham CBE
Information Commissioner, UK

In this issue:

GPA

Global Privacy Assembly

(43° Asamblea de Autoridades)



18 - 21 OCT 2021

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Towards the 2021 Global Privacy Assembly

Blanca Lilia Ibarra Cadena, President Commissioner, National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), Mexico provides an update on preparations for the GPA 2021

During the health emergency due to the COVID-19 pandemic, online activities have become essential for the world's population, adopting the utilisation of virtual conference platforms as one of the main mechanisms for holding meetings and mass events.

However, we should not overlook the importance of having various international personal data protection and privacy authorities sharing a physical forum that will facilitate the exchange of knowledge and ideas to provide solutions for emerging issues in the field and in the context of the health crisis.

> **"For the general theme of this edition of the GPA, it has been decided to maintain the proposal presented last year: "Privacy and Data Protection: A human centric approach"."**

For this reason, INAI has proposed holding the 2021 edition of the Global Privacy Assembly (GPA) in a hybrid format. This format will allow for data protection authorities and other participants who wish to attend in Mexico City, as well as those who participate virtually, to have the same benefits, as well as the ability to take full advantage of the knowledge that will be shared during the event.

It is important to point out that, regarding the face-to-face event, INAI and its contractors will, at all times, comply with the control measures focused on the prevention of COVID-19 infection that have been recommended by the World Health Organization (WHO) and the Mexican authorities, such as social distancing, open spaces, limiting the number of people in face-to-face spaces, among others.

As for the general theme of this edition of the GPA, it has been decided to maintain the proposal presented last year:

"*Privacy and Data Protection: A human centric approach*".

This decision is based on a simple fact: with the advances in technological innovation and the automated processing of personal data, the human being must continue to be the main actor in decision-making and the one who exercises control over his/her personal information.

In the specific case of the GPA's Open Session, the aim will be to achieve co-existence between the development of new information technologies and the protection of human rights, specifically the right to the protection of personal data. For this reason, a programme is being prepared with keynote speakers and parallel sessions for national and international experts from different sectors to present their ideas and experiences, focusing on the central theme from different perspectives: digital economy and e-commerce, regulatory convergence, accountability, data analysis, regional and international cooperation, among others.

In addition, for the first time, various virtual activities are being considered, which will enable participants to interact with the panelists in order to share relevant, cutting-edge information. These activities will take place on the margins of the open session for all participants.

It is also envisaged that during the breaks between conferences, virtual and networking activities will be held to capitalise on the opportunities for open discussion.

In order to successfully carry out these activities, an interactive and user-friendly online platform will be available for this edition of the GPA. This will allow a secure digital interaction among the Assembly attendees.

For all of the above, we would like to extend an invitation to all member authorities and interested parties to participate in the next edition of the Global Privacy Assembly, which will take place in a hybrid format from **October 18 – 21, 2021 in Mexico City and on the digital platform.**

Horizon Scanning

The FTC's post-pandemic privacy approach

Rebecca Kelly Slaughter, Acting Chair, Federal Trade Commission (FTC), US, writes exclusively for the GPA

The COVID-19 pandemic has had a transformative impact on the world, including on privacy. As the virus proliferated, many people shifted major parts of their lives—work, education, shopping, entertainment, and healthcare—almost entirely online, bringing privacy and data concerns to the forefront. I've experienced this transformation in my personal life, as well as in my role as a Commissioner and more recently as Acting Chair of the Federal Trade Commission (FTC).

> **"The pandemic has highlighted the need for strong legislation at the federal level as more of our work, our children's education, and even our social interactions are taking place online."**

For the FTC, the pandemic has put a spotlight on many existing privacy challenges: educational technology, health apps, remote work, and broadband privacy practices. With vaccination on the rise in the United States, we are now looking toward the post-pandemic future, keeping in mind the privacy gaps exacerbated by the pandemic and the broader issues of equity, including, especially in the American context, racial justice.

As I see it, our future will be shaped by our answers to two urgent questions: What major privacy issues will consumers confront? And what tools will we, global privacy authorities, use to address these and other ongoing issues for the benefit of all? As Acting Chair, I am excited to lead the FTC as we emerge from these challenging times and begin to answer these questions. I'm looking forward to engaging with our Global Privacy Assembly (GPA) colleagues on these issues as we use all of our tools to protect privacy and prevent data abuses.

Major Issues

• Algorithmic Discrimination

With more people online during the pandemic, companies have collected—and used—more personal data for more purposes. I know that the GPA has been concerned with the increasing use of algorithms and automated decision-making and the potential for algorithmic discrimination. I share this concern, and this is an area that the FTC will be looking at more intensively.

I've previously noted that, when we focus on the most troubling examples of flawed algorithms in the marketplace, there is a clear list of factors that contribute to discriminatory or unsavoury outcomes: faulty inputs, faulty conclusions, a failure to adequately test, and proxy discrimination. We must take care that existing discrimination is not replicated, exacerbated, or potentially 'hidden' inside algorithmic logic.

Our staff will be actively investigating the use of algorithms, and we will continue to look for ways to address other AI-based consumer issues. The starting point to delivering algorithmic justice is increased transparency and accountability to mitigate discriminatory effects. Transparency means that developers and deployers of AI should make sure that AI decisions are explainable and defensible. With proper transparency, academics, advocates, and third parties can then test for discriminatory outcomes. But transparency must not put untenable burdens on consumers. And transparency must be accompanied by, at a minimum, accountability and proper remedies. The companies that benefit from algorithms must also have the responsibility to ensure they are conducting regular audits and impact assessments. And we have to ensure there is proper redress available for faulty or unfair algorithmic decisions. The goal is to minimise and ideally end discriminatory outcomes from algorithmic decisions.

• Facial Recognition Technologies

Another pressing issue is the increasing development and deployment of facial recognition technologies. Like algorithmic decision making, facial recognition technology can also exacerbate existing racial disparities. There are some obvious privacy implications in facial recognition, such as being able to identify someone from just a photograph. But there's also disturbing evidence that these

technologies are less accurate at identifying non-white individuals, which has led to documented cases of wrongful arrests of Black men. In our enforcement actions against Facebook and Everalbum, we have challenged their default use of facial recognition technology, and we will continue to look for violations in this area.

- **Children's Privacy**

Finally, protecting young people's privacy will remain a significant part of the FTC's agenda. As schools shifted to virtual learning models during the pandemic, children and teens spent much of their school and non-school hours online. Ed-tech and other services used by children and teens are not going away after the pandemic ends. At the FTC, we are currently reviewing our Children's Online Privacy Protection Act rules. We also recently sent orders requesting information from nine major social media and video streaming firms to obtain a better understanding about these companies' practices including information that may reveal how these firms are targeting and categorizing children and families.

> **"Our future will be shaped by our answers to two urgent questions: What major privacy issues will consumers confront? And what tools will we, global privacy authorities, use to address these and other ongoing issues for the benefit of all?"**

Applying the FTC's Tools

As market conditions and firm conduct around privacy evolves, so too must the FTC's enforcement approach. There are several areas I am prioritising as we move forward. First, as we consider how to resolve investigations, we must focus on deterrence of future violations—both by our defendants and by other participants in the market. In order to have effective deterrence, we need to fully understand the benefits that companies may get from violating the law, not only financial gains but also growth, opportunity, and competitive advantage. Once we better understand the benefits companies get, then we can pursue a remedy that ensures that companies would find these violations unprofitable.

Second, we should focus on accountability at a corporate and, whenever appropriate, individual executive level. Here, we should understand how close the violations were to the core of a business and how executive accountability could change that corporate culture. Further, transparency measures, such as publishing assessments and even including potential whistleblower protections, could help to reduce problematic practices.

Third, we should focus on helping current victims. The FTC often seeks monetary remedies in our consumer protection cases, such as repaying consumers the money they lost and disgorgement of ill-gotten gains. Finding a monetary remedy in privacy cases, in which consumers may have paid little or no money for a service, is a challenge. In cases for which monetary relief is hard or impossible to determine, we need creative approaches to address consumer harm, such as disgorgement of ill-gotten data, meaningful notice, and renewed opt-in for existing consumers. One recent example is our action against Everalbum, where, instead of disgorging monetary benefits, we required the disgorgement of a different benefit: the algorithms based on allegedly improperly collected data.

I should also mention a significant structural advantage that the FTC has: We have both a privacy and a competition mission. We will be thinking carefully about the overlaps between our privacy and antitrust work. We must take note that many of the largest players in digital markets are there because of their access to and control over consumer data. These dual missions are complementary, and we should apply both the privacy and competition lenses to problems in digital markets.

In addition to case-by-case enforcement, we can apply our rulemaking authority to pervasive privacy problems. Clear rules can provide a guide for honest businesses and strong deterrence for would-be rule-breakers. Congress has given the FTC several important authorities to write rules to help protect consumers and promote competition. It is time we look at how rules might provide relief from novel harms in the digital economy as well as traditional scams, with the goal of making our work more efficient and potent. To that end, I have created a new rulemaking group within the FTC to streamline our process, strengthen existing rules, and undertake new rulemakings to prohibit unfair or deceptive practices and unfair methods of competition. The FTC has long innovated in how it uses its existing authority to protect privacy, and this is another tool with which we must be creative.

Even as we take an aggressive approach with our existing statutory mandate, we are closely eyeing the prospect of more direct federal privacy legislation in the United States. The pandemic has highlighted the need for strong legislation at the federal level as more of our work, our children's education, and even our social interactions are taking place online. The urgency of comprehensive data privacy legislation with meaningful limitations on the collection and use of data and prohibitions on discriminatory practices, dark patterns, and data abuses has never been greater. The FTC stands ready to enforce a federal privacy law. In the meantime, we will use our existing tools strategically and creatively to protect consumers, particularly the most vulnerable.

The UN Special Rapporteur on the Right to Privacy

In an exclusive for the GPA, Professor Joe Cannataci reflects on his tenure as UN Special Rapporteur on the Right to Privacy

Very early in my role as United Nations Special Rapporteur on the right to privacy, I said "Privacy has never been more at the forefront of political, judicial or personal consciousness". Little did I know how some issues would grow in significance or how others, such as the COVID pandemic, new laws, judicial rulings, and inquiries into corporate use of personal data, would exponentially heighten political, judicial or personal awareness of privacy.

Space does not allow me to dwell at length on any of these matters, but I highlight the significant effect of the European General Data Protection Regulation; the updated Convention 108; the Investigatory Powers Act of Great Britain and Northern Ireland; the US CLOUD Act; the Indian Supreme Court's 2017 Puttaswamy Judgement, and the 'Schrems' decisions of the Court of Justice of the European Union, COVID Apps, amongst others, upon the privacy landscape.

The mandate has an important complementary role with data protection and privacy commissioners worldwide to raise significantly the global standards of privacy. This shared commitment to advance privacy was formalised at the International Conference of Data Protection and Privacy Commissioners, on 27 October 2015, in Amsterdam.

> **"An important issue in information policy and governance is the appropriate weighting given to the use of data for the benefit of society and to the need to protect fundamental rights, like privacy and autonomy."**

UNITED NATIONS HUMAN RIGHTS SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

Priority themes

My priority themes throughout were Security and Surveillance; Big Data and Open Data; Health Related Data; Corporations' use of Personal Data, and Privacy and Personality sought to safeguard individuals' privacy in the overall complex web of information flows in society. The first major initiatives of the state surveillance thematic strand were the establishment of the annual International Intelligence Oversight Forum (IIOF) and the development of the 'Draft Legal Instrument for Government Led Surveillance'. Both, in their own way, successfully provoked debate and action to protect citizens' privacy.

Privacy, freedom of expression and freedom of access to information are essential to the universal and overarching fundamental right to dignity and the unhindered development of one's personality. As inaugural Special Rapporteur on the right to privacy, I sought to increase understanding of the right to privacy as fundamentally important for the autonomy and the ability of individuals to identify and choose between options in an informed manner throughout their lives.

The theme of children's privacy was added in 2017-2018 to the initial list of priorities, to examine the important contribution of the right to privacy. It followed the work on 'gender perspectives of privacy' which shone a light on the privacy concerns of many citizens about the way in which gender was the basis for infringements upon their dignity and reputation – sometimes irrevocably.

An important issue in information policy and governance is the appropriate weighting given to the use of data for the benefit of society and to the need to protect fundamental rights, like privacy and autonomy. This tension has been at the crux

of the challenges posed by the COVID virus to the right to privacy of individuals and communities. The UN SRP Task Force on Health Data 2019 Recommendation on the Protection and Use of Health-Related Data and its accompanying Explanatory Memorandum, was, quite fortuitously, a very timely report for the advent of the pandemic in 2020.

Some particular issues identified early in the mandate, such as smartphones as compellable witnesses, have only grown in significance. For example, the number of sexual assault victims willing to proceed with their cases, even very strong cases, has reportedly dropped due to the 'digital strip search' nature of handing over their phones.

> **"Privacy is everybody's right and its protection should not depend on the passport in your pocket or your location anywhere around the world."**

Big data issues continue to weigh heavily on privacy, particularly the growing reliance on artificial intelligence (AI). This provided the impetus for the Recommendations on AI which is intended as a common international baseline for data protection standards regarding AI solutions, especially those to be implemented at the domestic level.

Safeguards and remedies

The safeguards and remedies available to citizens can never be purely legal or operational. The complexity of important issues such as Indigenous Data Sovereignty means that law alone is not enough. Cultural change based on an appreciation of human rights and their contribution to achieving economic and social equality is required. It is now opportune for example, for a global discussion to determine the type of information policy most suitable for maximising the protection of, and minimising the risk to, individuals' privacy arising from the data collected about them by corporations, and accessed from there, by governments.

This requires engagement with all stakeholders, especially civil society, to bring home to lawmakers and the corporate sector, citizens' and users' expectations of improved privacy protection. I stress the need for a citizen focus to achieve recognition if not remedy, for those individuals whose privacy has been infringed, and for those whose privacy is vulnerable.

Future challenges require ongoing action based on evidence and a clear, comprehensive vision of privacy. The value of privacy in urban spaces for example, needs to be assessed when considering all the intrusive technology that can be deployed in so-called smart cities to meet individual and collective expectations of privacy, in both public and private spaces. Engagement is also required with the technical community to promote the development of effective technical safeguards, including encryption, to put 'privacy by design' genuinely into practice.

Privacy and its protection is everybody's right

Apart from extremely useful unofficial visits to several other countries, I carried out official country visits in Argentina, France, Germany, Korea, the UK and the USA. When read together, the updated versions of the country visit reports should provide useful examples of good practices as well as insights into the complexities, trials and tribulations that privacy protection faces across all regions of the world.

COVID-19 put an end to plans to carry out more visits in countries as diverse as Nigeria, the Philippines and others but the common template adopted in the country visit reports should help readers compare apples with apples, oranges with oranges. It should not be difficult to discern the common thread that runs across my recommendations to all countries visited: privacy is everybody's right and its protection should not depend on the passport in your pocket or your location anywhere around the world.

> **"The mandate has an important complementary role with data protection and privacy commissioners worldwide to raise significantly the global standards of privacy."**

Multiple consultations with multiple stakeholders, such as civil society, academics and individuals, the corporate world, and data protection and privacy authorities, provided invaluable insights captured in the reports on all the subjects mentioned above made to the United Nations Human Rights Council and General Assembly. Throughout I have been assisted by the expertise and support of many individuals and organisations. The Taskforces for thematic action streams were composed of highly experienced and unpaid volunteers who provided invaluable research and background for my reports to the Human Rights Council and General Assembly. I thank the international community of privacy and data protection authorities in particular, and I wish the GPA and all its members and observers, a safe and successful 2021.

SRP reports are available on the SRP webpage. Enquiries can be made to Prof. Elizabeth Coombs at ecoom02@sec.research.um.edu.mt

Balancing data sharing, innovation and governance in the digital society – Safeguarding individuals' data protection and privacy

Andrea Jelinek, Chair of the European Data Protection Board (EDPB), gives an overview of the safeguards and legal frameworks in place in the EU to uphold data protection and privacy standards in the digitised society

The EU's data protection legal framework is a key enabler of a data economy: innovation and new technologies will not be successful if they are not trusted and trust can only be achieved by respecting existing data protection legislation. The data protection regulators have a key role to play in making sure individual rights are respected in a quickly digitalising society.

> **"The data protection regulators have a key role to play in making sure individual rights are respected in a quickly digitalising society."**

The European Data Protection Board aims to uphold data protection standards in our evolving digital economy. The EDPB recently published its Strategy and Work Programme for the coming years with four pillars providing a clear account of EDPB objectives and focus. One such key objective is to monitor new and emerging technologies and their potential impact on fundamental rights and the daily lives of individuals.

The EDPB safeguards data protection principles through guidance, consistency opinions and decisions, and legal advice to the European Commission. Recent examples of when the EDPB's legal advice was called for was in consultation on the COVID-19 related Digital Green Certificate (DGC), the future ePrivacy Regulation, on the Data Governance Act (DGA) and the draft of the UK adequacy decision.

In the joint EDPB-EDPS opinion on the DGC, the Board underlined that any measure adopted at national or EU level that involves processing of personal data must respect the general principles of effectiveness, necessity and proportionality. Therefore, any use of the Digital Green Certificate by the Member States other than enabling free movement within the Union must have an appropriate legal basis in the Member States' law and all the necessary safeguards must be in place.

Furthermore, the EDPB affirms the new regulation must expressly include that access to and subsequent use of individuals' data by the Member States once the pandemic has ended is not permitted. At the same time, the application of the DGC must be strictly limited to the current COVID-19 crisis.

In its latest statement on the future ePrivacy Regulation, the EDPB recalled that under no circumstances can the level of protection offered by the current ePrivacy Directive be lowered. The ePrivacy Regulation should complement the GDPR by providing additional strong guarantees for confidentiality and protection of all types of electronic communication.

The EDPB also asserts that the data protection authorities responsible for enforcement of the GDPR should be entrusted with the oversight of the privacy provisions of the future ePrivacy Regulation. Allowing this will ensure a harmonised interpretation and enforcement of the privacy rules across the EU and guarantee a level playing field in the Digital Single Market.

Similarly, the joint EDPB-EDPS opinion on the Data Governance Act was also built on keeping the integrity of the GDPR's standards, and the roles of the national DPAs to enforce the GDPR and maintain a level playing field.

The protection of personal data is an essential and integral element for trust in the digital economy, and the DGA must be fully in line with the EU personal data protection legislation, and make this unambiguously clear.

An issue that is at the top of the EU's political agenda is the

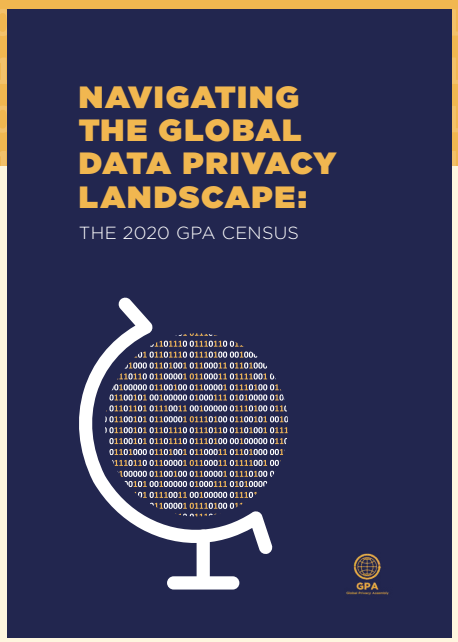
adequacy agreement with the UK. The EDPB was requested to issue two Opinions on the Commission's draft UK adequacy decisions: one on the UK's adequacy under the Law Enforcement Directive (LED); and the second on the draft adequacy decision based on the General Data Protection Regulation (GDPR). The EDPB noted that the UK starts off from an advantageous position vis-à-vis other third countries. The UK has mirrored, for the most part, the LED and GDPR in its data protection framework and when analysing its law and practice, the EDPB identified many aspects to be essentially equivalent. At the same time, a number of important challenges remain and the Board calls upon the Commission to address these in its final decision.

We welcome the Commission's decision to limit the granted adequacy to a specific time period. We also ask the Commission to closely monitor all relevant developments in the UK in the months and years to come and to take action if needed.

The EDPB is determined to help to shape Europe's digital future in line with our common values and rules, while continuing to work to promote regulatory coherence and enhanced protection for individuals.

Navigating the Global Data Privacy Landscape: The 2020 GPA Census

An introduction to the 2020 GPA Census Report and its significance for the GPA and wider data protection and privacy community



Every three years the GPA takes stock of the work of the Global Privacy Assembly (GPA) membership through the GPA Census. This work began in 2017, and the 2020 Census builds upon the work of the first Census in 2017. This Census – based on 2019 data – collected information from 70 GPA members to provide a 'point in time' picture of the policies and delivery approaches that currently guide and regulate data protection and privacy globally.

The GPA Chair Elizabeth Denham has advised that the Census:

"Furthers the work previously done and provides points of comparison as well as new insight into how the approach of member authorities supports the GPA's 2019-2021 strategic priorities."

The Census provides a useful reference tool for those whose business and data crosses jurisdictions and to national policy makers considering new legislative approaches. It also supports member authorities' capacity building and collaboration through dissemination of 'how it's done' in other jurisdictions. Finally, the data in this Census informs the GPA's Working Groups which are charged with delivering activity in support of the GPA 2019-2021 Conference Strategic direction and its successor document (currently under development and to be agreed at the GPA Conference in October 2021).

This report bears many similarities to the picture reported in the 2017 census, but there are some noteworthy differences in 2020. Most notably, the growth in size of data protection authorities around the world in terms of budgets and personnel indicates the increasing importance of ensuring that citizens' personal data and privacy are protected, and seen to be protected, via the oversight of an independent regulator.

The design of the report is founded in the GPA aspiration, which is to: "create an environment in which privacy and data protection authorities around the world are able to act". The words within this aspiration have been translated into binary code, and we wanted to convey that the report is about data authorities across the world by using the globe visual.

GPA Members and Working Groups have received a copy of the GPA Census 2020 Report.

Case study

A carrot and stick approach to data protection

Bjørn Erik Thon, Director at the Datatilsynet, the Norwegian Data Protection Authority, contributes our case study on innovative practices in safeguarding individuals' data protection and privacy

As a data protection authority in 2021, we must use a wide range of measures to achieve our goals. With complaints and data breach notifications pouring in, there is a risk that we end up as a mere case-handling factory. It is therefore important for us to apply a strategic approach in our work, to have a long-term perspective, and not to be afraid to try innovative working methods.

To ensure compliance, we believe that it is necessary to use a carrot and stick approach. We recently announced our intention to issue a €10 million administrative fine to a social networking application. Additionally, we imposed a ban on the processing of personal data in the Norwegian contact-tracing app, at the height of the pandemic. This demonstrates that we have to use a big stick if necessary. However, the carrot can be equally useful. Our regulatory sandbox promotes that data protection can benefit organisations and society alike. Through our work on data protection by design and default, we aim to provide businesses with instruments that unite the use of technology and the protection of consumer data. To address issues regarding children's data, we have both issued fines and taken on a more proactive role.

Using the stick where it matters the most

One of our biggest cases of 2020 was our investigation into Grindr, a social networking app for gay, bi, trans and queer people. The investigation was sparked by a complaint regarding the app's data sharing practices, coupled with a technical report outlining how sensitive user data was being transmitted to third parties. Taking into account the complexity of the matter, we established an interdisciplinary team with legal, technical, social science, and communications expertise to handle the case.

> "To keep up with the complexities of the ecosystems we regulate, we need to be proactive and innovative. While we need to sanction violations, prevention is better than cure."

For us, the Grindr case is a symptom of a bigger issue, namely the opaqueness and lack of user control in the AdTech industry. This is something we believe needs to be addressed as a matter of priority. To make matters worse, Grindr users belong to sexual minorities at risk of discrimination. Our preliminary findings suggest that Grindr lacked a valid user consent for sharing detailed GPS location and identifiers of its users, which is why we announced our intent to issue an administrative fine of approximately €10 million. Grindr is contesting those findings, and we are now working on a final decision.

Ensuring data protection in a pandemic

In the context of COVID-19, the Norwegian health authorities launched a contact-tracing app in April 2020. The app had three different purposes: contact-tracing, analysing the effect of infection-reducing measures, and research. While the use of the app was voluntary, we were concerned that users could not choose the purpose(s) for which they wanted to provide their data. We also criticised the use of GPS data for contact-tracing. As the data was stored in a centralised, cloud-based facility, this created the potential for mass-surveillance.

Furthermore, the app was launched before the technology for contact-tracing and analysis had been completely developed. Subsequently, large amounts of personal data were collected without there being any practical way of making use of the data. Due to this, we considered the measure disproportionate, also taking into account low public support of the app (14% adoption rate) and the manageable infection rates at the time.

Mid-June 2020, we announced that we would be imposing a temporary ban on the app's

processing of personal data. This immediately led to the health authorities shutting down the app and deleting the collected data. A new version of the contact-tracing app was later released, amending the shortcomings.

Encouraging viable innovation

We recently established a regulatory sandbox to help companies develop data protection friendly artificial intelligence (AI). The sandbox provides free guidance to a selection of companies of varying types and sizes across different sectors. Feedback from both the private and public sector shows that there is uncertainty on how to translate regulatory requirements into practice when developing and deploying AI. Transparency, data minimisation, and fairness were the top three data protection issues in the first round of applications.

We will use best practice examples and insights from the sandbox projects to help organisations implement AI in a good way that incorporates data protection requirements. The goal is to promote the development of innovative AI solutions that, from a data protection perspective, are both ethical and responsible.

The sandbox is a new way of working for us, allowing us to go deeper into specific use cases and cooperate with stakeholders to help develop compliant solutions. The sandbox is also a way for us to learn more about AI and how organisations work with data protection on a practical level.

Fostering data protection by design

Profiling and personalised services have become part of our daily lives. Users expect services to be secure and to safeguard their data protection rights in an effective manner. Businesses taking data protection seriously build trust and have a competitive advantage.

Data protection by design and default is an essential concept in this regard. Our experience over the years has shown us that where data protection by design is not observed, irreparable damage can sometimes be the consequence. That is why we believe in promoting it as a proactive measure.

> **"The sandbox is a new way of working for us, allowing us to go deeper into specific cases and cooperate with stakeholders to help develop compliant solutions."**

Together with external stakeholders and experts, we have developed guidelines and checklists for software development with data protection by design and by default. Through our involvement in the development of the European Data Protection Board's guidelines on the matter, we were able to discuss with and learn from other data protection authorities to leverage each other's expertise. We also host an annual competition on data protection by design to encourage organisations to put the guidance to practice.

Children's data warrants special protection

Children are encountering continual technological innovation, which brings with it complex risks and opportunities. New forms of data collection by businesses, parents, and the public sector can jeopardise children's rights.

In recent years, we have detected particular issues with how schools process students' data. We have fined schools for data breaches where they have failed to adequately secure children's data or even inadvertently published the data online. Another particular issue is the increased use of educational tools, sometimes applied without schools understanding how they work or which risks they entail. To put these issues on the agenda, we have organised several roundtable conferences with stakeholders, which we believe has had a positive effect in making visible the need for coordination and data protection expertise in the school sector.

Du bestemmer ("You Decide") is an online teaching resource about data protection and digital responsibility for children aged 9 to 18. The objective of the website is to increase awareness, reflection, and knowledge about data protection and the choices young people make when using digital media. The website is a collaboration between ourselves and the Norwegian Directorate for Education and Training.

Looking ahead

To keep up with the complexities of the ecosystems we regulate, we need to be proactive and innovative. We will therefore continue to look for ways to promote compliance at the development stage of systems and services. While we need to sanction violations, prevention is better than cure.

The GPA Strategic Plan 2021-2023
An evolution not revolution

Elizabeth Denham, GPA Chair and UK Information Commissioner, emphasises the importance of shaping the next chapter of the GPA's story on relevance

The GPA, and the ICDPPC before it, is a story. And every story has chapters. There's a chapter on a group being formed. A chapter on a group becoming truly global. A chapter on the group finding its place in the wider world.

The chapter we have written is one of evolving and modernising to meet the challenges of a data-driven age. We've found the structure to make the GPA effective. We've found the topics to make the GPA relevant.

But now we must shape the next chapter of our story. How does that structure, that modernisation, work in the real world? How does equipping our Assembly for a digital-driven world work in practice?

> **"The plan the Executive Committee has set out retains our three strategic priorities but adapts them for our changing world. And it is accompanied by a clear implementation plan, to ensure we continue to have a practical impact."**

And crucially, how will people outside of our regulatory, privacy commissioner community, respond to our story? Because if those outside of our community do not see value, do not see action, then the next chapter of our story will be one of irrelevance.

Writing this next chapter was the focus when the GPA Executive Committee held the Strategic Direction Development Workshop 2021-2023, in March.

The Strategic Plan 2021-2023 will shape our story and priorities over the next two years in the eyes of the wider community. And we approach it at a pivotal moment: if data protection looks too much like a barrier, we risk being left behind. Either we are an essential part of the solution, or we lose our voice.

With that in mind, the Executive Committee has focused our next chapter on relevance.

The strategic plan builds on the solid foundation we have in place, and on the progress made through the work of our GPA Working Groups and the GPA membership in the last two years. Our vision, mission and priorities remain truly relevant, and so our new plan is one of evolution not revolution.

But we must respond to the changing world. The pandemic has resulted in significantly accelerated – and accelerating – digitisation that affects the way we all live, work, travel, learn and socialise. We have seen an increased appetite to use personal data in both short-term and longer-term responses. And on a practical level we have all seen our domestic workload rise; we are all busier than ever before.

Against that backdrop, we have shown the pragmatic approach our community brings. We can build on the approach our members have taken across the past year, of both enabling and protecting.

The plan the Executive Committee has set out retains our three strategic priorities but adapts them for our changing world. And it is accompanied by a clear implementation plan, to ensure we continue to have a practical impact.

The draft GPA Strategic Plan 2021-2023 will be circulated to GPA members for consultation for final adoption at the GPA Closed Session 2021. It is an important part of our continued modernisation, and I urge all members to read and consider it.

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

Working Group on COVID-19 related privacy and data protection issues

Chair of the Working Group on COVID-19 related privacy and data protection issues, Commissioner Raymund E. Liboro, highlights the innovative approaches being applied by the working group to emerging global issues

In many parts of the world today, the pattern of COVID-19 infections is upward while revenues across many industries remain subdued. In an attempt to achieve normalcy in economic terms, the government and the private sector have been implementing more protocols while still strictly observing COVID-19 safety measures.

We at the GPA are in full support of all efforts to bring back livelihoods and catalyze economic recovery. But we remain steadfast in instilling our values for protecting personal data and deterring data privacy risks.

GPA COVID-19 Working Group

"We continue to work closely to ensure that the guidance the GPA provides to the global community is relevant, practical, and effective... We are also charting new strategies to create new points of contact to influence external stakeholders."

In the first formal joint statement of the GPA Executive Committee, we focus on guiding authorities and industries involved in domestic and international travel, which have been gradually re-opening to revitalise the sectors involved and arrest further losses.

The travel industry was among the sectors that suffered gravely. According to the World Travel and Tourism Council, the industry lost $4.5 trillion in 2020.

As in other industries, travel industry organisations see personal data processing as an excellent way to facilitate safe travel during the ongoing pandemic.

There are also considerations of so-called digital 'health passports' or 'health codes' intended to help personal information controllers identify a passenger's COVID-19 results and vaccination status.

Given the enormous involvement of sensitive health-related data in these developments, it is only prudent for all to adopt an exemplary attitude in implementing these new measures. Likewise, we must ensure that the use of personal data is regularly assessed for its effectiveness in the immediate goal of eliminating COVID-19, and for the long-term risks to personal privacy and data protection.

As all these are unchartered territories, the GPA's latest issuance helps the aviation and tourism industries gain travellers' trust, which is key to a successful contact-tracing campaign. In turn, effective contact tracing can jumpstart the recovery of both business and entire sectors amid the ongoing COVID-19 crisis while minimising risks to data subjects.

Our joint statement encouraged governments and organisations to minimise data collection to only that information that can contribute to the protection of public health while also factoring in reasonable retention periods and other privacy protection measures at the outset.

Governments and organisations must also ensure that technology solutions adopted and promoted comply with 'privacy by design and default' principles and have considered cybersecurity risks.

Consent for data collection and processing must also have a well-defined purpose and information provided as to the extent of the data processing is made accessible and clear to all users, regardless of their geography and the language spoken.

Likewise, we reminded everyone to put in place protection measures for vulnerable

individuals who may not be able to use or have access to electronic devices. Also needing protection are individuals who cannot be vaccinated due to their age, possible health risks, or other underlying conditions.

Ongoing work

As the GPA intensifies its campaign to ensure the implementation of privacy-protecting measures across sectors as we move toward mass immunisation, we look forward to our success in shaping COVID-19 strategies from national agencies down to organisational level.

In fact, since November last year, the COVID-19 Working Group has been making strides in this endeavour.

Among these is the adoption of the Working Group's Terms of Reference and the nine meaningful Working Group Meetings to date.

We have also adopted a COVID-19 Working Group Portfolio of work, which identified three strategic issues: alternative working arrangements; the use of e-learning and online schooling technologies; and, sharing of data between hospitals and health ministries and other relevant government bodies. In addition, two new emerging issues were included: personal data processing for vaccination programmes and the processing and sharing of health data concerning travel and passenger data.

We also continue to promote the adoption of the GPA's 2020 'Compendium of Best Practices' across jurisdictions. To recall, the Compendium was created last summer following a global collaboration to address emerging privacy issues in the wake of the COVID-19 outbreak.

> **"Our latest joint statement encouraged governments and organisations to minimise data collection to only that information that can contribute to the protection of public health while also factoring in reasonable retention periods and other privacy protection measures at the outset."**

The Compendium is a comprehensive guide for authorities and organisations from all sectors to transition to the new normal while equipping them with policies, measures, and solutions mindful of the data privacy principles of transparency, legitimate purpose, and proportionality.

Emerging issues survey

Moreover, as we continuously assess the privacy landscape, the GPA COVID-19 Working Group recently held a survey to identify the most pressing privacy issues at this point of the COVID-19 pandemic, requiring internationally coordinated action from the GPA.

The survey will serve the needs of non-privacy regulators, bodies, and organisations dealing with new, more detailed, or high-risk personal data processing due to COVID-19 protocols.

We hope to finalise the results of this survey and provide support to GPA members and the wider GPA community on these issues and succeed in the fight against the pandemic with adequate safeguards for the right to personal data privacy and protection.

At present, we continue to work closely to ensure that the guidance the GPA provides to the global community is relevant, practical, and effective. We are also charting new strategies to create new points of contact to influence external stakeholders.

We remain resolute that new technologies involving personal data must be secure and all risks eliminated, to avoid contact-tracing databases becoming a valuable treasure trove that risks falling into the wrong hands.

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

globalprivacyassembly.org/covid19

GPA
Global Privacy Assembly

Working Group Highlights

Leveraging the intersection of regulatory spheres to forge new partnerships and enhance the protection of privacy rights

An update from the Co-Chairs of the GPA's Digital Citizen and Consumer Working Group: The Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner

Australian Government
Office of the Australian Information Commissioner

Office of the Privacy Commissioner of Canada

Established in 2017, The Digital Citizen and Consumer Working Group (DCCWG) 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. This Working Group seeks to explore and better understand these intersections, foster greater collaboration across regulatory spheres, and holistically realise superior privacy and consumer outcomes for individuals across the globe.

Cross-regulatory collaboration

By all measures, the start of the second year of our current mandate has proven an overwhelming success. Our membership has grown to 18 agencies with the addition of four new working group members.

Following the GPA's first ever Virtual Annual Conference in October 2020, we also hosted our first DCCWG webinar welcoming approximately 50 participants from 22 GPA members and observers. In addition to outlining the DCCWG's progress, participants heard from working group guest speakers including the:

- **Information Commissioner's Office of the UK**, who discussed their Digital Regulation Co-operation Forum with the Competition and Markets Authority and the Office of Communications (Ofcom);
- **Norwegian Datatilsynet**, who discussed their joint guidance with the Norwegian Consumer Authority on Consumer Data and Digital Services;
- **Office of the Australian Information Commissioner (OAIC)**, who presented a case study in co-regulation with respect to Australia's Consumer Data Right;
- **Competition and Consumer Commission of Singapore**, who discussed how their Competition Guidelines were amended to specifically identify privacy as an aspect of competition on quality that may be taken into consideration; and
- **Colombian Superintendencia de Industria y Comercio (Colombian SIC)**, who discussed how they incorporated privacy considerations into a competition remedy reached with a joint venture between Colombia's three largest banks.

DCCWG members have also been in heavy demand promoting cross-regulatory collaboration with presentations, panels and keynotes at various conferences and webinars. This includes presentations at the Digital Clearinghouse (DCH), the Canadian Bar Association's Privacy Division, an Advertising and Marketing Conference, the IAPP Australia and New Zealand Summit and an expert panel at the Computers, Privacy and Data Protection (CPDP) 2021 Conference entitled: 'When Regulatory Worlds Collide – the Intersection of Privacy, Competition and Consumer Protection'.

The DCCWG is in the process of completing its 'Deep Dive' into the complements and tensions created by the intersection of the privacy and competition regulatory spheres.

A cross-regulatory event of note was the first ever joint Global Privacy Enforcement Network (GPEN) / International Consumer

Protection Enforcement Network (ICPEN) Best Practices workshop in February 2021. This joint event brought together 175 privacy and consumer protection enforcement professionals to discuss the intersection and potential cooperation strategies between the regulatory spheres. Given the DCCWG's experience with cross-regulatory work, we were invited to design and oversee sessions.

DCCWG members have also been in heavy demand promoting cross-regulatory collaboration with presentations, panels and keynotes at various conferences and webinars

The webinar itself was the last in a series of four ICPEN best practices workshops and focused on the enforcement of consumer data privacy. Chaired by Working Group members the Office of the Privacy Commissioner of Canada (OPC, Canada) and the Federal Trade Commission of the United States of America (FTC, US), the webinar consisted of two brief introductory presentations as well as breakout sessions to work through a practical exercise.

The introductory presentations saw the OPC, Canada present highlights of the GPA's Enforcement Collaboration Handbook, while the Netherlands Authority of Consumer Markets gave a brief overview of the digital advertising ecosystem, including the various entities and actors that collect and use personal data and the ways in which the information is used.

Assisted by DCCWG moderators from the Colombian SIC, the OPC, Canada, the OAIC, as well as the FTC, US, the breakout sessions explored the consumer protection and privacy issues raised by digital advertising. The sessions also went on to explore the substantive legal intersection between these regulatory spheres, as well as how the various forms of cross-regulatory enforcement cooperation can lead to greater compliance.

The ICPEN/GPEN webinar itself represented a pragmatic example of cross-regulatory collaboration, which is a key objective of the DCCWG: to promote greater cooperation across regulatory spheres.

Another recent example of cross-regulatory collaboration includes a pair of opinions published by the European Data Protection Supervisor (EDPS) related to the European Commission's Digital Markets Act and the Digital Services Act.

On the Opinions, Supervisor Wojciech Wiewiórowski, pronounced that:

"Competition, consumer protection and data protection law are three inextricably linked policy areas in the context of the online platform economy. Therefore, the relationship between these three areas should be one of complementarity, not friction."

To guarantee the successful implementation of the European Commission's Digital Services Act package, the EDPS called for a clear legal basis and structure for closer cooperation between the relevant oversight authorities, including data protection authorities, consumer protection authorities and competition authorities.

Looking to the future

The DCCWG is in the process of completing its 'Deep Dive' into the complements and tensions created by the intersection of the privacy and competition regulatory spheres. To date, we have completed 11 competition regulator interviews and we are starting to analyse those responses. As a 'sneak peek', certain of the preliminary findings or comments from those interviews include:

- **The intersection phenomenon is not new**, but it is certainly more pronounced than ever in today's exponentially expanding digital economy;
- **We are speaking different languages** across regulatory spheres – privacy authorities tend to talk about data as 'personal information' while competition authorities tend to conceptualize how data can represent 'the relevant product' for anti-trust analyses;
- **Measuring privacy can pose challenges for competition analyses** – Privacy is a less tangible, qualitative concept. There's greater difficulty in seeing a 'privacy protection' increase or degradation than a quantifiable price increase or fall;
- **Competition remedies can raise privacy concerns**, as with a merger remedy that contemplates data-sharing with other market participants. The challenge lies in finding a balance between the two without sacrificing either – and we have heard it can be done!

In addition to the regulatory interviews, the Deep Dive also involves an academic review assessing how privacy and competition regulators have historically approached/discussed this intersection as well as its growing implications in the digital economy. To this end, Professor Erika Douglas of Temple University in Philadelphia is conducting the academic review. Professor Douglas has been studying this intersection for some time and has written numerous papers and given multiple talks on the subject.

Ultimately, the Deep Dive will be comprised of two complementary reports setting out a baseline of what this intersection looks like and how competition regulators have approached it. We look forward to sharing the results of the Deep Dive with our DCCWG annual Working Group Report later this year.

New Chair for the Berlin Group – International Working Group on Data Protection in Technology (IWGDPT)

Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information, Germany, talks about the important work undertaken by the Berlin Group – IWGDPT, and his new role as Chair

Maya Smoltczyk, Berlin Commissioner for Data Protection and Freedom of Information hands over the chairmanship to Ulrich Kelber

Background

The Global Privacy Assembly (GPA) is proud to host a broad variety of expert-level permanent Working Groups – from Digital Education to International Enforcement Cooperation and many others. But what the GPA does not feature, is a dedicated Working Group for technology issues. The GPA addresses this gap by continuing its strong relationship with the independent 'International Working Group on Data Protection in Technology (IWGDPT), which, a few years ago, changed its scope and name from 'Telecommunication' to 'Technology'.

The IWGDPT dates back to 1983, when it was founded on the initiative of the Data Protection Commissioner of the federal state of Berlin in Germany and when the GPA (or, as it was known then, the 'International Conference of Data Protection and Privacy Commissioners') was still in its infancy, having held only its fifth annual meeting. Due to these circumstances, the group became better known under its nick-name: the 'Berlin-Group'.

In 1983, at a time when for example, personal computers emerged for the mass market, the Berlin Data Protection Commissioner felt the need to keep a close eye on technological progress and to provide data protection friendly solutions for new products and services, which for many years centered around telephones and other telecommunication-related devices.

> **"I believe there would be value in exploring ways and means whereby both the GPA and the Berlin Group might be enabled to further inform and liaise with each other on current topics and issues for future review."**

With the rapid advancement of technology, most notably the creation of the Internet or World Wide Web, together with the long-term and overarching trend towards the digitisation of society, the group felt the need to widen the Berlin Group's focus and to shift its scope from telecommunication to technology in the wider sense.

Future path

For almost 40 years now, the Berlin Group has worked successfully. This has always been supported by the specific composition of the Berlin Group, comprising technical, legal and regulatory experts from data protection and privacy supervisory authorities, as well as from non-governmental organisations (NGOs) and academia. In effect, this enabled the Group to elaborate tailor-made and practical solutions or suggestions that are applicable, scalable and feasible for all relevant stakeholders.

Having said this, and taking into account the long history and high reputation of the Berlin Group, I feel very honored that I was asked by my colleague, the Berlin Commissioner for Data Protection and Freedom of Information, Ms. Maja Smoltczyk, whether I would be willing to accept, with the consent of the Group, a transfer of the chair function from her authority to my office. Now I am very pleased to announce that this transfer has taken place on the occasion of the latest meeting of the Berlin Group on 24 March 2021.

My sincere thanks go to my Berlin colleague, Ms. Smoltczyk, for her dedication and commitment to the Berlin Group during the

past years. Of course, I will strive to maintain and continue the extraordinary significance and value of the Group to the global data protection community.

As to the unique nature and independence of the Berlin Group, I am not intending to change this; however, I believe there would be value in exploring ways and means whereby both the GPA and the Berlin Group might be enabled to further inform and liaise with each other on current topics and issues for future review. Coincidentally, I was elected as a member of the GPA Executive Committee in October 2020, and this may help smooth the way in this regard. In any case, I will be happy to report to the GPA Chair and Executive Committee as well as to the GPA membership on the activities and results of the Berlin Group.

The Berlin Group will continue to work on specific, topic-related recommendations. A paper on sensor networks – or 'digital dust' – will soon be tabled for adoption, and the Group decided at its recent 24 March 2021 meeting to further work on voice-controlled devices, as well as to prepare papers on smart cities and on facial recognition technology (FRT).

With regards to future meetings, I am hopeful and confident that we may meet in person again in the not-so-distant future. For a lively and debate-driven group, such as the Berlin Group, I believe it is vital to engage in face-to-face discussions and to have a direct and in-depth exchange of views. Therefore, I am very grateful to my colleagues at the Privacy Protection Authority of Israel and at the UK Information Commissioner's Office that – after another virtual meeting in September 2021 – they are volunteering to host in-person meetings of the Berlin Group in spring 2022 in Israel and in autumn 2022 in the UK.

Regional Perspectives

A Viewpoint from the Middle East – The Dubai International Financial Centre (DIFC) – Lori Baker, Vice President Legal and Director of Data Protection

The establishment of the DIFC

The Dubai International Financial Centre (DIFC) is home to the region's largest financial ecosystem of more than 25,000 professionals working across nearly 3,000 active registered companies, making up the largest and most diverse pool of industry talent in the region.

DIFC was established in accordance with the United Arab Emirates (UAE) Federal Decree No. 35 of 2004, as a part of Dubai's strategic vision to diversify its economic resources and attract capital and investments in the region. It is a financial free zone defined in Federal Law No. 8 of 2004. An independent jurisdiction within the UAE, the DIFC is empowered to create its own legal and regulatory framework for all civil and commercial matters.

DIFC is unique in that it has a legislative system consistent with English Common Law. Given its construct, the DIFC has its own set of civil and commercial laws and regulations and has developed a complete code of law governing financial services regulation. As part of its autonomy, the DIFC has created an independent judicial system within the jurisdiction as well.

Finally, DIFC has its own privacy law, Data Protection Law, DIFC Law No. 5 of 2020 (DIFC DP Law 2020), which is an update of the 2007 law that preceded it. The main objective of updating the 2007 law and regulations was to reinforce compatibility with international standards while addressing globally developing data protection and security issues, thereby building a flexible yet robust law that could cope with emerging technology and inspire ethical data management. Like the Directive and the GDPR, they provide for principles, such as accountability, transparency, fairness and adequacy.

Since DIFC Data Protection Law 2020's enactment in May of last year, coupled with earning Observer status from the GPA in 2019, and Member status in 2020, the DIFC Commissioner's Office has taken advantage of the opportunity to expand its reach in the region.

The goal for 2021

The goal this year for the Commissioner's Office is adequacy in all directions – issuing adequacy decisions of its own, receiving adequacy decisions from other jurisdictions, and really exploring what adequacy means in practice. The main questions we are addressing in this exercise include: Will personal data, once it arrives in an adequate jurisdiction, be treated in the way it would be treated at home? And how do we assure ourselves of that?

Adequacy recognition between governments or data protection authorities is key, as many hours of analysis, discussions and agreements go into an adequacy decision at this level. But it is also important for us to understand, what will the processors and controllers in that jurisdiction actually do if the culture and processing environment is not supportive of privacy practices? Consequently, the DIFC Commissioner's Office is evaluating risk, and mitigation measures at multiple levels, to expand and add depth to the current, more popular practice of merely adding standard contractual clauses to a contract or binding corporate rules. As such, we have developed a tool for assessing such risk, which is being vetted and further developed at the moment.

Regional collaboration

The Commissioner's Office has also been very successful in bringing together privacy professionals from around the Gulf Cooperation Council (GCC), Middle East and Central Asia regions to participate in an information sharing forum. In addition to discussing topics of all sorts regarding regional developments, often, presentations by privacy experts in prominent law firms, privacy activists and even other regulators foster the growth and understanding of data protection practices and knowledge.

This group is a safe place to bring together those who see the high value of privacy and security practices implemented, giving them feedback and the room to engage in thought leadership through the several white papers coming out of collaboration between group members, some of which may be shared upon request. One such paper was published in the GPA COVID-19 resources library of regulator's guidance on COVID-19 and privacy practices, and another discussed the CLOUD Act and the optimal regulatory model of addressing the issues, political and technical, that the Act presents.

Similarly, in March 2021, for the first time, privacy regulators from across the Middle East, including previously blocked countries, met to discuss forming a significant, supportive forum. The DIFC's efforts in bringing this group together is focused on consistent messaging and communal assistance, as well as sending its message to the rest of the world that privacy and security in the Middle East are growing in interest and influence in the world.

> **In March 2021, for the first time, privacy regulators from across the Middle East... met to discuss forming a significant, supportive forum.**

As many of the regulators in the group oversee the development of advanced technology that will have a global if not regional impact, getting this forum established will equip us with the necessary information to produce helpful guidance and get involved in vital 'privacy by design' efforts undertaken by entities operating in each other's jurisdictions. The group will seek to prevent regulatory barriers and hard stops in the evolution of technology, especially for example life-saving technology, such as contact tracing apps and other means of personal data collection that supports public well-being.

DIFC and the GPA

Finally, the Commissioner's Office is an active participant in GPA working groups, such as International Enforcement, and primarily, the Working Group on COVID-19 related privacy and data protection issues where DIFC is leading sub-group 2 on regulatory capacity building. While it can be tricky bringing everyone in the sub-group together, as it spans from Mexico to South Korea, and schedules are busy for everyone in privacy these days, the benefits of this sub-group's work not only to the GPA but to DIFC and the other members will prove to be many.

One activity of the sub-group was to survey non-privacy regulators and organisations to obtain feedback on personal data, security and privacy-related guidance provided during this last year of major change and upheaval around COVID-19 restrictions and requirements for protecting the public at large. It also collected information about how to improve, what details were missing, how to develop COVID-19 prevention technology while honouring the privacy of individuals, and overall, what the next steps should be as we continue to live in the post-COVID-19 world.

The survey was one activity amongst others planned for 2021. Leading this gave DIFC insights and tips about very basic things, such as crafting an information gathering tool like the survey, as well as connecting with well-established regulators that have shared experiences and positive (and even negative) examples of privacy governance. The takeaway for DIFC as a Member of the GPA and as a sub-group leader continues to provide us with a much richer view of how to improve as a supportive, flexible, yet consistent regulator in a jurisdiction where privacy and security are still very new concepts to some of its constituents.

The DIFC Commissioner's Office aims to work with processors and controllers in our jurisdiction, giving them the tools and guidance they need to build a business environment conducive to protecting individuals' rights while fostering innovation and inclusion. Being Members of the GPA and all the opportunities it affords us has been immeasurably beneficial to DIFC in achieving these goals.

In conversation with...

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

Marie-Laure Denis talks exclusively to the GPA about the role and work of the CNIL both domestically and globally

As President of the Commission Nationale de l'Informatique et des Libertés, (CNIL), France, tell us about your background and the role of the CNIL in France.

I am a State Counsellor at the Conseil d'Etat, the highest administrative jurisdiction in France and I was appointed President of the CNIL in February 2019. Prior to this appointment, I was already involved in regulatory activities related to the digital environment, as an official member of the French regulatory bodies for the telecom sector and for the audio-visual sector.

> **"'A trusted ally of the digital daily life' is the CNIL's motto for its strategic roadmap until 2021... it is in this spirit that I believe our community can also make a difference at the global level!"**

The CNIL is one of the oldest national data protection authorities, established in 1978, as a follow up to an intense public and political debate regarding a project the government had at the time to create a centralised database allowing French citizens to be personally identified by different government services.

Since its creation, our authority and regulatory landscape has significantly evolved and we now play a significant role as a 'data regulator', with a dual mission of supporting and supervising all public and private actors of the digital ecosystem. Our activity and missions are now deeply rooted in European and international cooperation, in particular as a member of the European Data Protection Board since the entry into force of the GDPR.

What do you consider are the main achievements of the CNIL to date?

Looking back at the past year and months, which have been particularly challenging for all of us, I would say that our main achievement has been to be able to react and adapt to an unprecedented situation, while fulfilling our duties and tasks as a data protection authority to protect individuals' personal data.

When it comes to personal data processing in the context of the fight against the COVID-19 pandemic, our expertise has been extremely sought after, both at national and European level, to provide guidance and recommendations on various issues, such as the setting up of new health information systems, contact tracing applications, public health research, remote teleworking tools and health at work, or the more recent issue of health certificates. These were also extremely demanding times for our staff and Commissioners. But we knew we had to provide timely answers to ensure the development of consistent, compliant and effective solutions.

Our guiding principle in this endeavour has been the following: data protection and privacy are not an obstacle to the development of digital solutions to address the COVID-19 crisis but an enabler to design tools that respond to the societal demand of trust in public policy and action. We also clearly highlighted that, to be effective, new technologies and personal data processing must not be seen in isolation but must be fully integrated within an overall public health strategy.

During this difficult period, we have also maintained a clear focus on our role and priorities in protecting the fundamental rights to data protection within the

digital economy. We have adopted landmark decisions and sanctions regarding the main actors, such as Google and Amazon, and we have completed the process of the review of our recommendation on cookies, which is now fully applicable. These are major steps which we consider as milestones for the development of a digital ecosystem which responds to a growing consumer demand of trust and respect for their privacy, as well as of more control on the way their personal data is handled when using tools which are now part of their daily lives.

> **"We are seeing that privacy and data protection are becoming a growing consumer and societal demand, which need to be answered, to build trust."**

In your view, what are the significant future challenges for both the CNIL and the data protection and privacy community?

Challenges ahead – at national, regional or international level – will certainly lie in our capacity to collectively demonstrate the effectiveness of our actions and the ability for individuals to gain trust in an environment which is in constant evolution.

Some of the solution towards a 'recovery' from the COVID-19 crisis will probably need to build upon a more sustainable innovation strategy, also when it comes to the processing of personal data. We need to enshrine data sharing and innovation in a more comprehensive way, calling for greater regulatory cooperation. Numerous rising challenges are now addressing an array of combined issues going beyond data protection and privacy, such as competition, consumer protection, cybersecurity, content moderation, ethics, etc... We have here an important role to play in ensuring our values and principles are fully integrated in new technologies and innovation going forward.

That's a challenge, but also an opportunity, so that privacy and data protection are fully integrated into the new governance models that are to be set up and deliver outcomes for people's daily lives.

Are there any significant lessons learnt or other important elements to consider that can be shared with the GPA community?

It might be too early to draw lessons from the current crisis but one thing we can already highlight is that we have been able to adapt to unprecedented challenges and that we need to keep up with a strategy of ambition and resilience.

Over the past year, we have extended our connections and interactions with our environment and stakeholders, as a necessity in order to gain expertise in fields, such as public health, research, new technology and innovation. We also further developed our effective cooperation with other regulators and this is certainly a trend that will increase in the coming years.

I consider that the impact of COVID-19 is not to be seen as a 'game changer' but rather as an accelerator of trends and developments which were already here and which we will have to address collectively in the future.

The GPA has all the tools for this and has already demonstrated its capacity to anticipate these changes, for example by setting up a relevant working group, the Working Group on COVID-19 related privacy and data protection issues, or establishing the Reference Panel. The ongoing discussion on the future of our organisation shall also take these elements into account in order to ensure our means are fit for the challenges ahead.

What are the important opportunities that lie ahead for the CNIL, domestically, regionally and on the international arena?

Though most of our borders have been closed and our travel is still significantly restricted, the current crisis has also led to a more connected world, relying increasingly on digital solutions. In parallel, we are also seeing that privacy and data protection are becoming a growing consumer and societal demand, which need to be answered, in order to build trust.

We have seen for example that a change of privacy policy terms from a messaging services application can lead to a real 'migration' of consumers to competitors and more privacy-friendly solutions. Cybersecurity incidents and data leaks are also highlighting the need to further protect our infrastructure, our tools and our personal data. The demands and the expectations are here. Policy makers are also progressively apprehending these issues in their decisions and strategies.

That's a real opportunity for the CNIL and for the Global Privacy Assembly. From the daily use of mobile applications to the broader issue of international data flow, we need to articulate our actions and discourse in order to provide for a trusted digital environment. This will only be possible if we have the means to act, and if we are able to make our voice heard, strategically and collectively.

My view is that we need to remain proactive, to anticipate and lay down clear recommendations, so that we can feed into discussions at national, regional and global levels. If we follow the right approach and are provided with the sufficient means to act, I sincerely believe that we can make a difference in people's lives, and I hope we will continue advancing in this direction with the Global Privacy Assembly.

"A trusted ally of the digital daily life" is the CNIL's motto for its strategic roadmap until 2021. And it is in this spirit that I believe our community can also make a difference at the global level!

Get to Know your ExCo...

John Edwards, Privacy Commissioner, Office of the Privacy Commissioner, New Zealand

Privacy commissioners and data protection authorities are often seen as 'getting in the way' of data sharing, of stifling innovation, and valuing legacy inefficiencies over contemporary solutions to policy problems and business initiatives.

Much of my tenure as Commissioner has involved pushing back on this narrative. The New Zealand Privacy Act, almost certainly like yours, is a handbook for information sharing. Every privacy or data protection law in the world exists only with reference to the need and importance of sharing information. Rather than arbitrarily restricting the movement of personal data, privacy laws seek to answer the question, "how can we have the innovation, the efficient solution, the ***benefits*** of the digital economy, in ways that foster and maintain trust, and that value and preserve individual autonomy?".

For many years as a practitioner, my mantra when asked "can we do [x] under the Privacy Act?" was "you're asking the wrong question" – ask, "how can we do [x]?".

New Zealand has had a Privacy Commissioner since 1991. The position was established to authorise and regulate automated information matching across government departments, primarily to detect social welfare fraud. The Office was and is an "Independent Crown Entity", funded by the state but free from government and ministerial control.

In 1993, the Act was expanded to become the first national information privacy law outside of Europe to apply universally across the economy to both the public and private sectors and not-for-profit sectors. The Act created a clear avenue for New Zealanders to make privacy complaints, but otherwise had no provision for fines or enforcement.

> **"We rely on the GPA to bring us together and provide a forum. By working together and harnessing collective knowledge, each of us can be far more effective at delivering beneficial privacy outcomes for our communities."**

In 2020, a new Privacy Act passed and came into force, substantially updating the original Act and granting my office new powers.

In addition to receiving and investigating individual complaints, the Privacy Commissioner is empowered to make public statements, to provide advice on the operation of the Privacy Act, to examine and report on proposed legislation and policies that affect privacy, and to undertake inquiries. We issue codes of practice that can relax or strengthen the information privacy principles, and can give one-off authorities for agencies to make an unexpected use or disclosure of personal information.

Unlike some jurisdictions, the Act is not founded on 'informed consent' for the use or disclosure of personal information. Rather, the primary authority for using data is the *purpose* for which it was collected.

So between structuring business processes to achieve clarity and transparency about those purposes, judicious use of the exceptions to privacy principles (such as, in the Covid-19 era, the need to protect from serious public health risks), specific statutory overrides, and codes of practice, you'd think there'd be little to stop business and government from reaching their legitimate objectives?

You'd be wrong. Uncertainty and risk aversion can create an echo chamber of misinformation about the obstacles that data protection laws impose. And the risk of these is that they are taken as fact, with politicians responding to the perceived need to act, and to solve a perceived problem, by unnecessarily stripping away citizens' rights.

In New Zealand, this narrative led to the addition of further instruments to facilitate information sharing in government. Approved Information Sharing Agreements (AISAs) were added to the Privacy Act in 2013.

AISAs have not completely curtailed the perception of privacy as an impediment to data sharing. A significant part of my role continues to be educating, even senior public sector leaders and politicians. I emphasise the importance of working within the system, rather than engaging in

perpetual law reform which may deliver death by a thousand cuts to data protection.

I've had the pleasure and good fortune of working with many highly dedicated and able team members. They have helped maximise the influence of our small office and, understood the genuine needs and concerns of stakeholders, helping them realise their objectives in ways which promote and enhance privacy.

"The (Privacy Act 2020) reforms gave the Commissioner, for the first time, powers to actually enforce the law, by issuing compliance notices, and access determinations."

One of my proudest moments was when we successfully argued that our intelligence and security agencies (the New Zealand Security and Intelligence Service and Government Security Communications Bureau) should be made more fully subject to the Privacy Act. We argued this was necessary to give the public confidence that those important activities of the State were being undertaken in accountable, lawful and transparent ways, especially following the controversy unleashed by the Snowden revelations. In my view, this reform made the New Zealand intelligence infrastructure one of the most regulated and transparent in the world.

While I can't claim credit for the passage of the law, I am also very proud of the work we have done to leverage what were essentially relatively modest reforms in the Privacy Act 2020, which came into force on 1 December last year.

While the Act stopped short of the benchmark for data protection set by the GDPR, it gave us an opportunity to modernise our approach to regulating for privacy in a data hungry digital economy.

The reforms gave the Commissioner, for the first time, powers to actually enforce the law, by issuing compliance notices, and access determinations. We've finally caught up on many of you, with mandatory breach notification. Our law will apply to agencies doing business here, regardless of where their servers, or lawyers are based. The fines are not at GDPR levels (NZD$10,000 for failure to comply with a notice, or failure to report a notifiable breach), but the reforms have given us an opportunity to reconsider our operating model, and approach to enforcement and compliance. We've borrowed from the best of you to develop our Compliance and Regulatory Action Framework. It will guide our decision making to direct our scarce resources to areas of greatest impact for New Zealanders.

My office, like data protection authorities around the world, continually faces complex privacy issues associated with increasingly pervasive digital technologies. Putting to one side the role played by big tech companies, gobbling up ever more personal information, this past year in New Zealand, some of the issues my office has dealt with are:

- Private and public sector COVID-19-related technology including testing and vaccine registers, and contact-tracing apps.
- Public privacy concerns associated with the disclosure of people's COVID-19 statuses.
- A probe into the collection, retention, and disclosure of personal information by landlords and property managers in the rental accommodation sector.
- A joint inquiry into Police's unwarranted photography of members of the public, particularly young Māori.

Internationally, privacy will continue to face challenges and need to adapt to developments in technology.

Biometrics and artificial intelligence are among the most urgently presenting challenges. They require us to think in new ways. For example, we used to think in a kind of binary way about being in public spaces. If you are out there in the street, capable of being observed, you don't have an expectation of privacy. But that approach is too blunt when we think of the potential harms from ubiquitous CCTV coverage, combined with facial recognition technology. Do we have a right to go about our business unobserved? Without being collected, collated, and curated? No authority can tackle these issues alone. We rely on our international colleagues to lead and inform our approach to emerging privacy issues that we share. We rely on the GPA to bring us together and provide a forum. By working together and harnessing collective knowledge, each of us can be far more effective at delivering beneficial privacy outcomes for our communities.

"Privacy laws seek to answer the question, 'how can we have the innovation, the efficient solution, the benefits of the digital economy, in ways that foster and maintain trust, and that value and preserve individual autonomy?'"

Observer on the Road

Update from the GPA Observer at the Organisation for Economic Co-operation and Development (OECD)

Marie-Laure Denis, President, Commission Nationale de l'Informatique et des Libertés (CNIL), France, reports as the GPA representative at the OECD

Work of the OECD Working Party on Data Governance and Privacy

The Global Privacy Assembly (GPA), as part of its work with international fora, is an observer at the Organisation for Economic Co-operation and Development (OECD) Working Party on Data Governance and Privacy (WP DGP). The OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. The GPA's presence in OECD meetings is therefore essential and is strengthened with its key objective of reinforcing relationships with international bodies and networks advancing data protection and privacy issues as a key priority and as part of its 2019-2021 Strategic Plan.

The WP DGP is a platform where policy makers monitor trends, share experience, and analyse the impact of technology on information security and privacy policy making. It develops and monitors the implementation of several non-binding legal instruments (soft law) adopted by the OECD Council and maintains an active network of experts from government, business, civil society and the Internet technical community.

This group serves as a foundation for developing national co-ordinated policies and benefits for the broader international community through OECD's co-operation with non-members and other international and regional organisations (such as the GPA, the Council of Europe and APEC). It meets twice a year in Paris and organises workshops and conferences.

> **"The WP DGP is a platform where policy makers monitor trends, share experience, and analyse the impact of technology on information security and privacy policy making."**

WP DGP delegates come from various government bodies with an interest in the economic and social aspects of information security and privacy. Non-governmental stakeholders participate actively in the dialogue through the Business and Industry Advisory Committee to the OECD (BIAC), the Civil Society Information Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC). The working party has also established relationships with other international and regional organisations, such as Council of Europe, Asia-Pacific Economic Co-operation (APEC TEL and APEC ECSG), ENISA, the GPA and the Global Privacy Enforcement Network (GPEN).

Current work of the WP DGP and the GPA

The WP DGP currently works on several topics with a focus on:

- government access to personal data held by the private sector;
- the review of the implementation of the OECD Privacy Guidelines;
- the promotion of comparability in personal data breach notification;
- reporting data governance and privacy implications of the COVID-19 pandemic; as well as
- data ethics.

As part of its Strategic Direction Plan 2020-2021, the GPA has also initiated work on the question of government access to personal data held by the private sector with the preparation of a questionnaire circulated among members as a first step.

On data breach notifications, the GPA has also gathered important information on the matter and is actively cooperating with the OECD to share this information.

Finally, regarding the COVID-19 pandemic, the GPA and the OECD have been in close collaboration to provide a response to this important and urgent matter.

The GPA has set up a temporary working group on COVID-19 related privacy and data protection issues and the OECD as a GPA observer is collaborating in the activities of the working group. This Working Group put forward a proposal which resulted in the publication of the recent GPA Executive Committee Joint Statement on 31 March 2021, on the use of health data for domestic or international travel purposes, in particular the importance of privacy by design in the sharing of this data during the COVID-19 pandemic.

Meet Our Member

Alexander White, Privacy Commissioner, Office of the Privacy Commissioner, Bermuda

Alexander White explains the Bermudian approach to data protection 'Quo Data Ferunt' – following wherever the data may lead and persevering in the protection of individuals' rights and freedoms

Background

The Office of the Privacy Commissioner for Bermuda was established as an independent public office in accordance with the Personal Information Protection Act 2016 (PIPA), the first comprehensive data protection law for the jurisdiction.

The office holds the mandate to regulate the use of personal information by organisations in a manner which recognises both the need to protect the rights of individuals and the need for organisations to use personal information for legitimate purposes. The law currently stands in a transitional phase of being partially in effect, with the country's first Privacy Commissioner appointed in January 2020.

Setting a course as a new data protection regulator

It would be remiss not to take this opportunity to express a deep gratitude to the many GPA members who – in our office's early days – reached out, took the time for an introductory chat, or even supplied templates for policies, procedures, job descriptions, and more. Building a new office from scratch meant that there was quite a bit of blank slate to fill in!

Such a blank slate could be viewed in different ways: with a sense of joy for the endless possibilities that could take shape or with the heavy burden of infinite possible roads to go down...

Bermuda sits at a physical, cultural, and economic crossroads. We are, legally speaking, a European jurisdiction, with strong North American business ties, and cultural links to those places along with the Caribbean and Africa. This interconnectedness has long been to the island's benefit, claiming the best of multiple worlds to create a prosperous and successful community. Fitting, then, to speak about our work in this issue of the GPA newsletter that focuses on the balancing of interests.

We hold privacy as a fundamental right, yet must find a way to promote its use by businesses that may not have a strong tradition of incorporating these ideas. Instead of seeing this dichotomy as in conflict, we follow the Bermuda tradition of finding a middle way. We believe that the best strategy to encourage businesses to adopt data protection practices is by showing that they make sense, not only morally, but also for society and even, yes, for the business's interests.

We aim to help organisations navigate towards finding win-win scenarios, towards developing privacy practices to protect rights and enable business operations, and towards embracing challenges in order to find ways to innovate while protecting privacy.

> "We aim to help organisations navigate towards finding win-win scenarios, towards developing privacy practices to protect rights and enable business operations, and towards embracing challenges in order to find ways to innovate while protecting privacy."

Here, again, we see the power and the peril of the blank slate. Our jurisdiction is, in some ways, new to data protection and in need of education regarding rights and responsibilities that must take shape. By the same token, that lack of fixed legal precedent allows us to approach our strategy with fewer paths closed off.

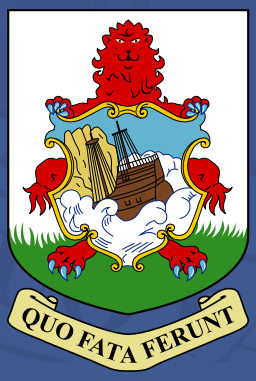
We started filling in our slate with the sorts of ideas that might guide a contemporary regulatory strategy, like the need to shift

business interests to focus more on the community good, or the importance of interoperability of law and technology, or how we may use incentives to proactively shift behaviour. You can read more than you might ever want to about these strategies in our office's Mid-Atlantic Privacy Compass. After all, what better tool for setting our course than a Privacy Compass?

The first permanent residents came to Bermuda in the early 1600s, around the same time that John Donne wrote, "No man is an island". It is often said that Bermuda's founding shipwreck inspired William Shakespeare's The Tempest, and I like to think that Bermuda also inspired Donne. In our workshops and discussion sessions with the public or aspiring privacy officers, we have taken to adapting the phrase with an ironic bent to say that, paradoxically, "Bermuda is not an island".

As true as this philosophy was at the birth of the modern world, thanks to our technological advances the idea has never been more relevant. We are all interconnected, and we may only solve the problems that arise from that fact by using interconnected solutions and fora, like the GPA.

We consider the role of the GPA to be critical in navigating these new issues and developing consensus solutions to our universal problems. As a small jurisdiction, we will always focus on the ways we may work with our colleagues to enhance our voice and present a united front to businesses or organisations that may be exponentially better resourced. Please know that our office stands ready to assist and support our colleagues at any time in our common, vital work.



Did you know?

Bermuda's national motto, Quo Fata Ferunt, comes from the Aeneid. Like the first Bermudians, Virgil's Trojans found themselves shipwrecked. Considering what to do next, they decided that wherever the Fates may take them, they will follow and persevere. With a cheeky, one-letter adjustment to "Quo Data Ferunt" the Office of the Privacy Commissioner commits to following wherever the data may lead and to persevering in the protection of individuals' rights and freedoms.

GPA key upcoming dates 2021

- **10 May** Launch of GPA Global Privacy and Data Protection Awards 2021
- **31 May** Deadline: Inform GPA Secretariat of intention to table Resolutions
- **14 Jun** Deadline: Submissions for GPA Global Privacy and Data Protection Awards 2021
- **21 Jun** Deadline: To table draft complex/technical Resolutions with the GPA Secretariat
- **18 Jul** Accreditation: Membership application deadline
- **30 Jul** Deadline: Submission of Working Group Reports
- **30 Jul** Deadline: To table all draft Resolutions
- **22 Aug** Accreditation: Observers application deadline
- **18-21 Oct** GPA 2021 Mexico

Check our website for more information: globalprivacyassembly.org

Your GPA News Highlights

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

Welcome to our May 2021 edition of the GPA Newsletter. We recently reached the half-way point in the run-up to the next Global Privacy Assembly in October 2021, and the GPA community has been intensively working together to help shape and influence the global data protection and privacy agenda. The level of collaboration has been impressive as the world continues to attempt to emerge from the COVID-19 pandemic, grappling with new ways of working. The GPA Secretariat has outlined recent GPA initiatives below for your information, which report on GPA members' valuable contribution to delivering the Conference's Strategic Plan priorities.

Publication of the first GPA Executive Committee Joint Statement in 2021

On 31 March 2021, the GPA Executive Committee issued a Joint Statement on the use of health data for domestic or international travel purposes, urging governments, public bodies and commercial enterprises to pay due regard to common global data protection and privacy principles, such as privacy by design and default, when considering these proposals.

This Statement provides practical guidelines that will be essential to building trust and confidence in the way health data is processed for travel purposes, building on the principles of effectiveness, necessity and proportionality, long-established in data protection laws worldwide.

This is the first Joint Statement to be published under the new Joint Statement on Emerging Issues mechanism as adopted at the 42nd Global Privacy Assembly Closed Session in October 2020.

The GPA Reference Panel Launched

The GPA Reference Panel is now launched following the successful completion of the work of a wide cross-section of GPA members around the globe as part of the Assessment Group. Under the chairmanship of Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information, Germany, the panel held its inaugural meeting on 29 April 2021.

Details of the Reference Panel and its 16 members can be found on the GPA website.

The GPA Reference Panel is a contact group involving a variety of external stakeholders to provide expert knowledge and practical expertise on the basis of ad hoc requests by the GPA on specific data protection and privacy related issues and developments in information technology.

Please contact the Secretariat for further information at secretariat@globalprivacyassembly.org.

GPA Strategic Direction Development Workshop 2021-2023

On 17 March, the GPA Executive Committee held its Strategic Direction Development Workshop 2021-23, with the aim to shape the next chapter of the Global Privacy Assembly over the next two years, agreeing the overall approach and policy priorities.

The subsequent draft GPA Strategic Plan 2021-2023 will be circulated to GPA members for consultation in May and submitted for final adoption in the Closed Session, October 2021.

Accreditation 2021

The Global Privacy Assembly's (GPA) application process for new members and observers remains **open** for the 2021 cycle**.**

Since its foundation in 1979, the GPA has been continually growing and now includes more than 130 authorities from across the globe. The GPA now welcomes new applications from authorities who wish to become members and from public entities/ international organisations that wish to participate in the GPA as observers.

- Applications for membership will remain open until **end of day, Sunday, 18 July 2021**
- Applications for those public entities or international organisations who wish to join as GPA observers will remain open until **end of day, Sunday, 22 August 2021**

All information including application forms can be found on the GPA website.

The GPA Global Privacy and Data Protection Awards launched

We are pleased to announce the launch of the GPA Global Privacy and Data Protection Awards 2021 on **10 May 2021**. We invite GPA members to submit their award entries by **end of the day 14 June 2021**.

All information including entry forms can be found on the GPA website, if you have any queries, please contact secretariat@globalprivacyassembly.org.