Vol. 2, Issue 2 | 2020

NEWSLETTER

GLOBAL PRIVACY ASSEMBLY

GPA
Global Privacy Assembly

Message from the Chair

Elizabeth Denham CBE, UK Information Commissioner and GPA Chair

I normally begin these introductions with a brief update on what has happened since the last newsletter, but it is difficult to know where to start in describing how all of our lives – professional and personal – have changed since January.

What is consistent across the membership is that we are as busy as ever. Data is a key plank of infrastructure in the fight against this pandemic. Our community is reflecting on location tracking, immunity testing, new government-backed apps, data sharing, the development of enormous data sets, and many more innovations besides.

We are being asked to answer some difficult questions, and I know many of us appreciate the support of our international colleagues as we look to find the best answers. I am pleased that the GPA is able to facilitate the sharing of best practice, through the COVID-19 Response Repository on our website, our convening of our joint workshop with the OECD, and the launch of our COVID-19 Taskforce.

What has shone through in the contributions from around the world is the need for regulators and authorities to be both enabler and protector: encouraging the innovative solutions we need to address this health crisis, while standing up for people's privacy rights.

The two statements issued by the Executive Committee on COVID-related matters have demonstrated that balance, reflecting the importance of pragmatism around the critical sharing of information to tackle the pandemic, and around privacy considerations in contact tracing design. Those statements showed the positive role the GPA can take in the current climate.

Our work has never been more vital, to advise and influence the design of data-centric solutions and to maintain public trust that oversight and safeguards are in place. It is crucial that we do not lose our momentum on how we are shaping the future of our community.

We have had to postpone our annual conference, in Mexico City, until 2021, but that does not mean postponing our important work, and I am pleased that we intend to bring privacy authorities together for the essential elements of our annual conference at a virtual closed session later this year. Further details will follow in due course.

You will also notice we are not standing still with this newsletter. This edition sees a fresh approach, and a focus on how privacy rights interact with other human rights and freedoms.

I hope it is a valuable read. Thank you for your continued support, and I hope you and your families are staying safe.

Inside this issue:

Horizon scanning

Balancing fundamental rights with crisis response measures to build trust

European Data Protection Board Chair, Dr. Andrea Jelinek

Dr. Andrea Jelinek, Chair of the EDPB, writes exclusively for our inaugural Horizon Scanning feature

As countries search for ways to exit the lockdown and to prevent a second wave of COVID-19, many governments are evaluating to what extent data and technology can help to mitigate the impact of this virus. The Coronavirus is an unprecedented challenge, not only to our health systems and our economy, but also to the values on which we have built our societies.

"The coronavirus is an unprecedented challenge...to the values on which we have built our societies"

Some suggest we should, for the time being, shelve these fundamental values, such as the right to data protection, to allow us to fight this pandemic more effectively. Others go even further and use the efforts to curb COVID-19 as a reason to push through far-reaching reforms to increase state power.

How we will react to this crisis and how we will safeguard fundamental values when national governments are in crisis mode, is being closely scrutinised. As Europeans, we have to remain vigilant that the fundamental rights, on which the European Union is built, are not eroded.

There is no justification for chipping away at these fundamental rights. The General Data Protection Regulation is designed to be flexible. It allows for an efficient response to the pandemic, while at the same time protecting fundamental human rights and freedoms. Data protection principles always allow for balancing the interests at stake.

As the European body which guarantees a consistent application of data protection rights across the European Economic Area, we are determined to uphold the principles of the GDPR. The European Data Protection Board published a statement in the early days of the EU-wide lockdown, firmly rejecting the notion that privacy rules stand in the way of public health responses.

We have taken it upon ourselves to continue to speak out on the data protection implications of the COVID-19 response and to contribute to a pan-European and coordinated approach with regard to all the different initiatives to combat COVID-19. The last thing we want to see is every Member State going in a separate, different direction.

To this end, we have developed guidance on the different aspects of data processing in the context of COVID-19, including geolocation and tracing tools, and the processing of health data for scientific purposes. In our guidance, we have pointed out that European data protection law enables the data processing operations that are necessary to contribute to the fight against a pandemic. Some of the obligations included in the GDPR, such as data quality and transparency, can actually reinforce measures by national governments in the fight against COVID-19. Data quality, or the fact that data must be adequate, relevant, limited to what is necessary, accurate and kept up to date, can ensure the effectiveness of the measures taken. Transparency can reassure the public that their governments

"Without trust, no technological solution will ever reach its full impact"

respect their fundamental rights and gain their trust and support for these measures. We also stated that the use of contact tracing applications should be voluntary, another element which is key to ensure public trust.

This brings us to the heart of the matter: without the guarantee that data protection rights are respected, there will be no trust in the technology. It is trust that makes any solution

socially acceptable, and thereby guarantees that the measures will be more effective. This was confirmed by a recent EU-wide survey by Euroconsumers: while respondents agreed that personal data can be used to fight the virus, 60 to 70 percent said they were concerned about privacy. It is clear: without trust, no technological solution will ever reach its full impact.

Therefore, now is not the time to suspend or bypass our data protection laws, but to use the flexibility provided by the legal provisions to balance fundamental rights with crisis response measures. Whoever introduces such measures should bear in mind that only actions that are transparent, necessary and proportionate in a democratic society can count on the broad support of citizens. Whenever personal data is processed in the context of fighting COVID-19, the respect of data protection rules is indispensable.

Data protection and the use of technology to mitigate the spread of COVID-19 can go hand in hand. We do not have to choose between protecting a fundamental right and our health.

Focus

Privacy, Electoral Propaganda, and Disinformation: Challenges and Opportunities for Data Protection Authorities

Professor Colin J. Bennett assesses the valuable impact of the data protection and privacy community in defending fundamental democratic rights

Before the global COVID-19 pandemic disrupted our lives and directed the attention of the international privacy community to questions of health surveillance, perhaps the most pressing data protection issue was the use, and abuse, of personal data in election campaigns. At the 2019 International Conference of Privacy and Data Protection Commissioners in Tirana, I had the privilege of addressing the assembly (virtually) on privacy and democratic engagement to

Professor Colin J. Bennett, Department of Political Science, University of Victoria, B.C. Canada

Ad transparency requirements can provide an important source of leverage for regulators and advocates

draw some larger lessons for data protection authorities in the aftermath of the Cambridge Analytica / Facebook scandal.

This complex conflict was, of course, about some huge threats to democracy and national sovereignty from widespread voter manipulation and the spread of electoral propaganda and misinformation. However, at the heart of this scandal were some familiar data protection questions about transparency, consent, proportionality, and security. Thus, international DPAs have found themselves at the center of a global conversation about the future of democracy.

Historically, most DPAs have been reluctant to enter this "political terrain" although there have been exceptions. Both the Information Commissioner's Office in the UK and the Commission Nationale de L'Informatique et Libertés (CNIL) in France have been issuing useful guidance on best practices for electoral communication for many years. However, the Cambridge Analytica

International DPAs found themselves at the center of a global conversation about the future of democracy

/ Facebook scandal shone a spotlight on the widespread risks of "data-driven elections" and the global reach of the "political influence industry." The use and abuse of personal data for purposes of political engagement is an issue for any democracy, and for every DPA. In this new climate, how might DPAs respond to these challenges and thereby contribute

to the international struggle against electoral manipulation and disinformation?

First, there is a pressing need to understand the complete network of organizations engaged in political campaigning, which is invariably complex, opaque, and involves a shifting ecosystem of actors and organizations. Voter analytics practices are often imported, typically from North America, and often with scant regard for local democratic institutions and cultures. An important lesson from the investigations of political campaign practices in the UK and elsewhere, is that DPAs should acquire a broader understanding of that network in their respective societies, and how parties and candidates are using these new digital campaigning tools.

They also need to understand the entire regulatory environment for elections. A diverse array of constitutional, statutory, and self-regulatory rules can affect the processing of personal data in the electoral context. National DPAs need to have a comprehensive grasp of the regulatory conditions that permit, or prohibit, the processing of personal data for purposes of democratic engagement, including the rules for campaign financing. Election practices are also influenced by more elusive cultural traditions. In some societies, for example, direct candidate to voter canvassing is considered common; in others, it is considered highly intrusive.

It is equally important to cooperate with other relevant regulators. Elections regulators, in particular, have the long-standing expertise in elections law and experience in administering the many facets of elections administration, including the distribution of voters' lists. However, the wider context of "data-driven" elections is not something the typical elections regulator has the resources, or competence, to regulate. Early experience in both Canada and the UK suggests that cooperation between DPAs and elections regulators is invaluable in producing informed and credible advice to political parties and their candidates.

Recent proposals designed to promote transparency and accountability for digital advertising also offer opportunities for DPAs better to understand the nature of political micro-targeting in their respective societies, the level of granularity, and the source(s) of payment. In the world of political campaigning, data protection infractions can also be elections financing infractions, and vice versa. Ad transparency requirements can provide an important source of leverage for regulators and advocates.

The risks to democratic practices from the unethical and/or illegal processing of personal data on voters cannot simply be understood in response to individual complaints to particular candidates and parties at the time of elections. DPAs can assist political parties more pro-actively. They have valuable experience in the detailed and practical work of data protection implementation and privacy management and can assist in the tailoring of data protection rules to the campaign context. Codes of practice, of the sort being developed in the UK, can provide the kind of nuanced and precisely tailored rules that strike the appropriate balance between the public interest in an informed electorate, and the privacy rights of voters or potential voters.

These are global questions requiring the highest level of international collaboration between DPAs. The political "influence industry" knows no geographic boundaries. Its impact nationally and internationally will require the most vigilant and constant cross-national attention from DPAs through their international and regional associations, as well as from the wider network of international privacy advocates and experts.

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 globalprivacyassembly.org

Follow us on Twitter

@PrivacyAssembly

A Case Study – The ICRC: Data Protection in Humanitarian Action

Peter Maurer, President of the International Committee of the Red Cross (ICRC), (Observer to the GPA) highlights the critical role of data protection in humanitarian action

Peter Maurer, President, International Committee of the Red Cross

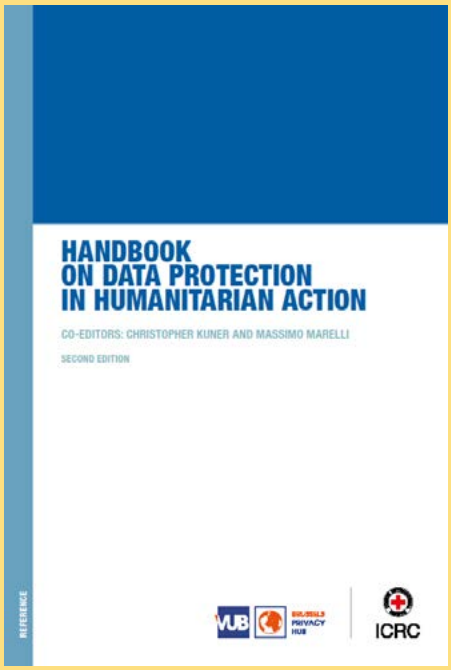
The protection of life and dignity in conflict is core to the mandate of the International Committee of the Red Cross (ICRC) and has been for more than 150 years. Over the decades, amid global shifts and the changing dynamics of conflict and violence, our work has adapted to address the protection risks for affected people and communities. Today, data protection and respect for privacy are integral operational issues.

The ICRC, at work in more than 80 contexts around the world, is often entrusted with sensitive personal information which must be handled with the utmost care to avoid putting people at risk. For example, our delegates visit people in detention who share confidential information about the way they have been treated, or about their relatives with whom they would like to remain in contact. Similarly, as we provide assistance and healthcare to populations at risk of further harm, we are privy to highly sensitive information about vulnerable people.

With enormous trust placed in our hands, it has been critical for ICRC to responsibly develop tools and mechanisms to protect people's data in a way that places the human dignity at the centre and ensures that our activities protect the populations we want to serve without exposing them to risk. Over many years we have developed a wide body of expertise grounded in the realities of our humanitarian operations.

With the rapidly increasing use of new technologies in the humanitarian sector, new challenges have emerged, from the use of biometrics and mobile-messaging apps to data-driven partnerships with the financial sector to target financial assistance where it is needed most. This has required us to devise new ways to ensure that humanitarian action can both benefit from the possibilities created by these technologies and ensure that we maintain the core humanitarian principle of "do no harm" in the digital age. To meet these challenges we have invested in building up our data protection expertise and expanded our knowledge by working with and learning from innovative practitioners.

Connecting with the wider data protection community has been a key asset. Since 2016, the ICRC has benefited immensely from its Observer status at the GPA and the collaborations and partnerships this has inspired. The 2015 ICDPPC Resolution on Privacy and International Humanitarian Action was particularly important for the ICRC: it allowed us to take forward initiatives with members of the Resolution Working Group and present the work of the ICRC Data Protection Office at side events at the International Conferences in Hong Kong and Brussels.



In response to the rapid pace of technological change and acute data protection challenges facing the sector, the new Handbook is now published

The "Handbook on Data Protection in Humanitarian Action", published by the ICRC and Brussels Privacy Hub in 2017, was a key outcome of this

collaboration. Developed with the support from other humanitarian organisations, data protection authorities, academia, civil society and the corporate sector, the Handbook provides guidance on the interpretation of core data protection principles in humanitarian action. It has played an instrumental role to support the sector in complying with data protection standards, particularly when new technologies are employed.

The Handbook has been widely used in the humanitarian sector as data protection has taken on greater importance for aid organisations, their donors and affected populations. The wide range of insights gained during the development of the Handbook has also shaped the ICRC's policy and practice, embedding a privacy-by-design approach to the use of information and communications technologies, and helping the organisation navigate the challenges of innovating while respecting data protection. The ICRC's Biometrics Policy, adopted in August 2019, which balances the growing demands for increased efficiency and accountability to donors with respect for the rights and dignity of the individuals affected is an example of the impact of the Handbook on our work.

With the rapidly increasing use of new technologies in the humanitarian sector, new challenges have emerged

In response to the rapid pace of technological change and the acute data protection challenges facing the sector, the ICRC and the Brussels Privacy Hub has now updated the Handbook. The new chapters of this 2nd edition address blockchain, digital identity, artificial intelligence, connectivity as aid and the use of social media in humanitarian crises. The Handbook will include, among other topics, guidance on how artificial intelligence can be used to improve the effectiveness and efficiency of humanitarian work: for example, monitoring displacement patterns for prompt provision of essential humanitarian services, or locating people separated from their families during conflicts, while at the same time ensuring respect for their rights and dignity. The new Handbook was released on the 3 June, and we rely on the support of the GPA in disseminating it far and wide.

Another important area in which the global privacy community could support the humanitarian sector is in striving to ensure that the personal data in its possession is used for exclusively humanitarian purposes. This was a key theme that States discussed with national and international components of the Red Cross and Red Crescent Movement during the 33rd International Conference of the Red Cross and Red Crescent which took place in December 2019.

Reuniting families separated by conflict and disaster is a core activity of the International Red Cross and Red Crescent Movement globally. Data related to these activities has become increasingly attractive for those engaged in security and border control, and other actors, who may wish to use them for example to address movement of populations or security concerns. To safeguard the independence, neutrality and trust in humanitarian organisations, the Conference adopted a landmark Resolution on "Restoring Family Links while respecting privacy". Founded on the principle of purpose limitation, the Resolution "urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement". Support is needed for these important commitments to be realised.

Finally, like many organisations with a public interest mandate, the ICRC has rapidly shifted gears to protect communities in conflict zones from the effects of COVID-19. This pandemic comes on top of an already difficult humanitarian situation in conflict zones, where health systems are struggling to cope, and economies are being shaken. The ICRC has been working to protect the most vulnerable by providing medicine and equipment, working to improve sanitation in displacement camps and detention facilities, or advising authorities on planning for mass causalities to ensure that those who die are treated with dignity.

We have also been following closely the opportunities and the risks involved in using technology to support the response to the pandemic, for example with the use of contact tracing applications. It is important that the rights and the dignity of individuals are upheld, even when emergency measures are enacted. Here again we look forward to continued partnership with the GPA and its membership to develop workable and innovative data protection solutions: this public health emergency is revealing new data protection challenges, requiring the very best expertise and a collaborative approach from across the humanitarian, health and digital communities.

If you would like to become an Observer to the GPA, contact the Secretariat at secretariat@globalprivacyassembly.org.

IN CONVERSATION WITH

Mr. Omar Seghrouchni, President of the National Commission for the Control and the Protection of Personal Data (CNDP), Morocco

To live digital, we have to breathe data protection

Tell us about the origins of the National Commission for the Control and the Protection of Personal Data, (CNDP), Morocco, and your role in driving forward data protection in your jurisdiction?

The CNDP was established in 2010, on the basis of Law 09-08 of 18 February 2009, and its Implementing Decree No 2-09-155 of 21 May 2009. The Act provides for a Board of six members, in addition to its chairman.

> "We are working to make privacy a reflex, a natural part of everyday life"

Like many DPAs around the world, the CNDP is working on several axes. The first one is educational, to explain, reassure and disseminate the principles of personal data protection. The second axis focuses on the industrialisation of our processes and the development of more efficient means of communication with companies, administrations and citizens. The third one is to contribute to societal debates on the values underlying the respect and protection of privacy: taking the current COVID-19 crisis as an example, what proportionality can be established between health risk management, the maintenance of economic activity and respect for privacy? Finally, a fourth area, but not the least, concerns keeping a permanent watch on the dizzying evolution of technologies and their emerging new uses.

Please could you highlight the role of the CNDP in the international arena?

It is our conviction that personal data protection legislation is being built internationally. We must share and learn together from each other's experiences to build a universal response.

Also, we believe that our contributions to various organizations, such as AFAPDP (the French-speaking network) or RAPDP (the African network), are strategic. We provide the permanent secretariat of the African Network, and we lead a working group on identity management. We consider that the latter provides structure for the protection of personal data in our countries. We need to find the right compromise between economic efficiency and privacy. Our Commission is also participating in a recently established working group within the PRIDA project, a joint initiative between the European Union and the African Union. The CNDP, with the support of experts from the African Union, is chairing the working group on data protection and localization. Nigeria holds the vice-chair.

What in your view are the key regional level priorities to further the unity and relevance of our international community?

We believe that harmonization work is essential at regional level. Projections, such as the one offered by Convention 108-Council of Europe should be deployed in Africa, Asia, and the Americas. We need to coordinate our laws and regulations and strengthen data protection rules when data crosses borders.

> "COVID-19 ... what proportionality can be established between health risk management, the maintenance of economic activity and respect for privacy?

Please explain the initiatives introduced by the CNDP to tackle the impact of COVID-19 on data protection, privacy, and the fundamental rights of the individual.

The CNDP is proactive in this crisis. From the very first hours of lockdown, we announced that we were ready to both help identify and support, in a pragmatic way, the right compromise between managing health risks, protecting privacy and maintaining economic life. We have deliberated on several topics, for example, teleworking, temperature measurement, facial recognition for remote management of bank accounts, the importance of sector identifiers, and tracking applications.

We have also publicly warned about the rules to be respected regarding a COVID-19 application, and we are currently working with the authorities to carry out a DPIA (Data Protection Impact Assessment) on this. We propose to be the digital trusted third party in support of the deployment of this application.

Concerning the application, WIQAYTNA (the national "anti-COVID-19 application"), CNDP decided, based on clearly identified hypotheses, to approve the application. In addition, CNDP has set up a mechanism to both verify and re-evaluate this, to ensure that the initial assumptions are respected.

WIQAYTNA is intended to be deployed according to the following assumptions:

- Volunteer basis use only.
- Health system support, in particular to rationalize the attribution of resources, to strengthen the screening policy and public information dissemination.
- Health authorities control of alert calculation algorithm parameters.
- Use of " tracing" without a tracking mechanism.
- Appropriate User information.
- Data access restricted to authorised persons only.
- Commitment not to use data for purposes other than those authorised.
- Commitment to destroy collected and generated data at the end of health emergency state, except those that can be used, in an anonymized and regulatory manner, for scientific research purposes.
- Declaration of non-use of black box (non-transparent code).
- Commitment to make the code accessible for audit and verification purposes.

What is your vision for the data protection and privacy agenda in Morocco and that of our global community in making a real difference to people's lives?

We are currently working on an overhaul of the law in Morocco to clarify the terms and conditions for protecting privacy. Beyond the matter of personal data, the aim is to protect the citizen within the digital ecosystem, while also promoting exchanges within the global digital economy.

We are working to make privacy a reflex, a natural part of everyday life. We have many ideas that we would like to share with other DPAs for coordinated international implementation. We believe that the GPA is a significant achievement that we can all be proud of.

Working Group highlights

Implementation of the Digital Education Working Group Resolution on E-Learning

GPA Digital Education Working Group (DEWG) reviews progress in the implementation of the Resolution on E-Learning

In the wake of the COVID-19 pandemic, countries around the globe have been called upon to redefine the way they operate in an effort to protect against the spread of the virus. Many governments have put in place voluntary and/or mandatory orders for citizens to isolate themselves to slow the spread of COVID-19. Now more than ever, digital services and technologies are being relied upon to assist those who cannot leave their homes. Many schools have closed their doors and have shifted from in-person to online learning in order to maintain physical distancing. While this shift is necessary to continue to educate students, it is important that the privacy rights of students, teachers and parents continue to be upheld.

Remit of the Working Group

The work of the Global Privacy Assembly's Digital Education Working Group (DEWG) can

provide valuable guidance as educators and schools begin to consider integration of e-learning at this time. Specifically, the Resolution on e-learning platforms, adopted at the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels on October 2018, provides broad direction in this area. The Resolution called upon all relevant parties in the field of e-learning to fully respect students', parents' and educators' ("individuals") rights to: i) protect their personal data and privacy; and ii) guarantee that the data collected is solely used for educational purposes in compliance with data protection law. The Resolution addresses key privacy and security considerations relating to computer software, mobile applications, and web-based tools specifically provided to schools that students, parents and educators access via the Internet and use as part of an educational activity.

One year later, at the 2019 ICDPPC Conference in Tirana, the Office of the Privacy Commissioner of Canada (OPC Canada) produced a first Report regarding the Implementation of the Resolution on E-Learning Platforms. It highlighted initial progress by data protection authorities on their engagement with government and school authorities, development of useful resources, and outreach activities. The report reiterated several of the recommended actions contained in the E-Learning Resolution's Implementation Guide for DPA's and suggested follow up activities.

Current progress

The DEWG is continuing to track activities to monitor progress in this key area, as well as the success and impact in advancing and disseminating this key Resolution. The ultimate goal is to establish a directory of Guidelines and Codes of practice developed by relevant actors in relation to e-learning platforms. This work aligns with the GPA's 2019-2021 Strategic Plan and its first strategic priority, 'Advance Global Privacy in a Digital Age'. The sharing of information and experiences from national initiatives focused on children's privacy online and the mapping of data protection issues related to digital education supports broader work under Pillar 3, Action Item III of the Policy Strategy which directs the GPA to: "Share information and experiences from national initiatives focused on children's privacy online and map the related data protection issues".

Ms. Marie-Laure Denis, Chair of the GPA Digital Education Working Group (DEWG), President of the CNIL

> **"The current period of online educational continuity poses technology and privacy-related challenges"**

As part of the Working Group's ongoing monitoring, a follow-up questionnaire was distributed to its DPA members in February 2020, and would benefit from updated feedback from all the GPA data protection community who adopted this resolution. The current period of online educational continuity poses technology and privacy-related challenges, and has reinvigorated a need to collect information related to:

- Current media coverage and dissemination of the e-learning Resolution that brings more prevalence to our privacy message in the field of online education;
- Contact made with relevant government or education authorities and feedback received from school authorities and other educational partners who are concerned about using secured online tools;
- Adaptation of resources and informational sessions to raise awareness of the data protection risks and mitigation measures identified in the Resolution; and
- Development of any guidelines, emerging codes of conduct or consultation initiatives that have proven useful in ensuring that the private sector develops e-learning services in a privacy protective manner.

The original deadline of the questionnaire has been extended and the DEWG encourages all members to submit their questionnaire responses by July 1, 2020 to Melissa Goncalves (Senior Policy and Research Analyst, OPC Canada) at melissa.goncalves@priv.gc.ca. Any question related to this survey can be addressed to Melissa Goncalves and/or Pascale Raulin-Serrier at pserrier@cnil.fr at the DEWG Secretariat.

Working Group highlights

Ethics and Data Protection in Artificial Intelligence Working Group

The Chairs of the Working Group highlight progress in promoting implementation of the Declaration on Ethics and Data Protection in Artificial Intelligence

This permanent Working Group was established after the adoption of the Declaration on Ethics and Data Protection in Artificial Intelligence in October 2018, at the 40th ICDPPC. The aim of the Working Group is to promote the understanding of, and respect for, the guiding principles of the Declaration by all relevant parties involved in the development of AI systems, including; governments and public authorities; standardisation bodies; AI system designers; providers and researchers; companies; citizens and end-users of AI systems. The guiding principles of the Declaration include fairness, privacy by design and by default as part of ethics by design, reducing biases and discrimination, individual empowerment, continued attention and vigilance, system transparency and intelligibility.

> It will not be long before the guiding principles of the Declaration create a flow-on effect on the general GPA community

After the adoption of the Declaration, the Executive Committee Secretariat launched a public consultation, which received a number of responses from different social and economic stakeholders. We have published a report on the responses to this public consultation, including the principles which might require more specific guidance.

While all respondents generally supported the six principles and the broad values presented in the Declaration, some respondents (mainly private enterprises) were of the opinion that ethical considerations should be flexible enough to cater for different types of AI use. One-size-fits-all approaches are not recommended by respondents. Feedback will be reflected in the future practical guidance. During the consultation period and after it, Working Group members also had direct exchanges with stakeholders, e.g., at the RightsCon in Tunis in 2019.

Current priorities

The Working Group currently has a 10-item work programme, which includes, but is not limited to, the following significant and far-reaching projects, on which the members and observers are currently working:

- Statement on the relationship between ethics, human rights, and data protection in AI;
- Statement on the need for demonstrable accountability for AI systems;
- Planned resolution on how data protection and privacy is essential to sustainable digital growth and AI innovation; and
- Member survey on the capacity and expertise of authorities in addressing ethical and data protection issues in AI systems – a starting point towards a gap analysis.

The Working Group invites all members and observers of the GPA to contribute to two repositories, which it has set up. One includes policy documents and legal instruments, adopted by privacy and data protection authorities or relevant legislative bodies at national, supranational, or subnational level. The other repository collects real life cases of applications of AI, in particular where GPA members or observers have observed or assessed their impacts. The Working Group welcomes submissions to its Secretariat and will make the collected material available to the GPA membership.

Adapting to new considerations

In light of the "White Paper on Artificial Intelligence – A European approach to excellence and trust" (the White Paper) released by the European Commission in February 2020, members of the Working Group are discussing the issues raised in the White Paper and plan to submit a collective and well-balanced response to the European Commission.

The thrust of the White Paper is the importance of human-centric development for trustworthy and transparent AI, which fits well with the principles that the Working Group is aiming for. The Working Group will carefully consider the suggestions in the White Paper to further promote the Working Group's main objectives and proactively support an active public debate on digital ethics

to build a strong ethical culture and raise awareness. With the concerted efforts by members of the Working Group in promoting data governance and data ethics, it will not be long before the guiding principles of the Declaration create a flow-on effect on the general GPA community.

Recently, the globe has almost come to a standstill amidst the pandemic of COVID-19. It is widely acknowledged that there needs to be the right balance between data protection and privacy rights, and other fundamental rights, such as physical and mental health freedoms – the right to free movement and assembly – as we address the pandemic. Data protection rules do not hinder responses to the pandemic and the fundamental rights they protect should not be discarded.

Data protection and privacy authorities are prepared to help their governments in finding sound legal grounds for personal data processing that will allow the necessary research and pandemic control, while being respectful to the spirit of the data protection and privacy regulations.

All this does not necessarily result in a trade-off between privacy and public health. Data ethics and accountability provide us with a viable way of enjoying both and using the technologies to the fullest, especially when different interests, freedoms and rights require a careful balancing exercise. While some consider that the pandemic will change the world and reshape the future of data privacy, what will remain unchanged is that data protection and privacy authorities are committed to help all stakeholders in finding data protection and privacy-respectful ways to fight the pandemic.

The Chairs of the Working Group, PCPD, Hong Kong, EDPS and the CNIL, France, can be contacted via the Secretariat email address: secretariat@globalprivacyassembly.org.

Regional Perspectives

British, Irish and Islands' Data Protection Authorities, BIIDPA

The members of the BIIDPA explain the origins and role of this unique network

BIIDPA is a platform that connects data protection authorities. In doing so, although BIIDPA is not a formal observer to GPA, BIIDPA members contribute to the GPA's objectives by connecting the efforts of the participating data protection authorities (DPAs). Its members include both EU and non-EU jurisdictions, serving as an example of global international cooperation, which has been in place for more than 30 years.

The Formation of BIIDPA

The organisation of meetings for the platform began in the late 1980s. Initially, they were bi-annual meetings between the UK, Isle of Man, Jersey and Guernsey. In the early 1990s, recognising common issues and shared data flows, an invitation was extended to the Republic of Ireland.

In 2004, invitations were extended to Malta and Cyprus. The UK ICO was assisting both Cyprus and Malta with data protection at that time and it was felt that as both were relatively small jurisdictions with common law backgrounds, the issues discussed could be of benefit to all.

Similarly, invitations were extended to Gibraltar in 2006, which had received assistance from Ireland in relation to its data protection legislation, and Bermuda in 2008, which implemented its Personal Information Protection Act.

BIIDPA meetings tend to focus on practical matters and have resulted in a common approach being taken with regard to certain business sectors, for example, subject access requests by the beneficiary of a Trust was an issue which led to a common advice note being issued by BIIDPA members.

There have always been particularly close links between the Isle of Man, Jersey, and Guernsey, who regularly seek each other's views and usually find common interpretations. This benefits both the DPAs and businesses, particularly in the finance sector, who have commented that the common interpretation is of benefit to them.

For the smaller jurisdictions, BIIDPA has always provided a key opportunity to discuss both the thinking and decisions of the Article 29 Working Party (pre-GDPR) and now the EDPB.

It also facilitates a free and frank discussion on matters which may be particular to one jurisdiction. When Bermuda joined BIIDPA, existing members provided advice on the new privacy law which the country was drafting, as well as on the setting up of its privacy authority.

Given the similarities in our jurisdictions and backgrounds, and the close working relationships established, BIIDPA membership is of mutual benefit for all concerned.

Current priorities

Current BIIDPA priorities include dealing with Brexit and its impact for DPAs, with analysis of/support for development of guidance by individual BIIDPA members over the past 12 months.

Members are also sharing experiences related to the EU adequacy process. Both the UK and Gibraltar are currently seeking GDPR and Law Enforcement Directive adequacy rulings from the EU Commission. Guernsey, Isle of Man and Jersey have existing adequacy findings from the EU which are due for renewal under the GDPR this year; adequacy findings for each island with regard to the Law Enforcement Directive are also due for consideration.

Guidance on data protection during the COVID-19 crisis has been issued by each member of BIIDPA. Due to this crisis, unfortunately, the next BIIDPA meeting scheduled for June 2020 in Ireland has been postponed and will be rescheduled.

BIIDPA and the GPA

The aim of the Global Privacy Assembly is to "provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe."

As outlined above, BIIDPA members contribute to the GPA's objectives by providing a platform that connects the efforts of the participating data protection authorities. As a small group, BIIDPA's members work closely together and frequently engage to assist each other, sharing guidance, views on any particular subject that may arise, sharing experience and/or internal procedures that may be useful to others, for example, on secondments (e.g. Gibraltar secondment with Irish DPA). If attendees so choose, this may include projects aligned with, and which may contribute to, the work of the GPA, for example, the working groups dedicated to International Enforcement or Digital Education.

In the context of international investigations, aside from the legal mechanisms used, e.g. Article 60 of the GDPR for EU members, the close relationships also facilitate cooperation in a practical sense that helps to accelerate cases.

BIIDPA's members include EU and non-EU jurisdictions, which may serve as an example of global international cooperation

BIIDPA's members, including both EU and non-EU jurisdictions, may serve as an example of global international cooperation.

Report from the UN Special Rapporteur on the Right to Privacy

Joe Cannataci, UNSRP, highlights his current priorities regarding COVID-19, and guidance available on the management of health-related data and gender equality

At present, much of my attention is directed to the privacy impacts arising from implementation of COVID-19 strategies around the world. These strategies are using all forms of digital technology, such as AI, facial recognition technology, geo location tracking amongst others, teamed with Big Data. Collaboration between States and the technology sector is a feature of many responses.

Concerns have been raised regarding whether these strategies meet accepted requirements of proportionality, necessity and lawfulness. Other issues concern data governance particularly for health-related data, transparency, and accountability for the erosion of freedoms. I am preparing a Recommendation on privacy appropriate responses to the COVID-19 pandemic for presentation to the UN General Assembly later this year. Your input is welcomed.

To assist Data Protection Authorities and civil society, I draw your attention to guidance

material released in late 2019, on the management of health-related data. The 'Recommendation on the Protection and Use of Health-related Data' and the accompanying Explanatory Memorandum are relevant to responses to the pandemic, as are my preceding recommendations for Big Data – Open Data and the oversight of Government led surveillance.

In March 2020, I called for

> **"I urge all DPAs ...to do more to achieve gender equity in privacy rights."**

gender equality in privacy practices around the world following the identification of deeply disturbing infringements of privacy arising from individuals' gender. These infringements frequently led to discrimination, and some to violence. Privacy infringements based on gender, disproportionately affect women, intersex and non-binary gender individuals. Infringements, for example, have 'outed' people and safety has been jeopardised in cases of intimate partner violence or homophobia. Consultations emphasised the need for international leadership on gender equality in the right to privacy as this issue is typically overlooked in privacy and data protection.

The Recommendations cover the responsibilities of State and non-State parties across matters such as gender identity and legal recognition; civic, recreational and cultural activities; housing and education; physical autonomy, reproductive rights, well-being and health care; data analytics; online violence; digital technologies and online digital platforms; work and employment; social security protection; security and surveillance; detention and asylum-seeking. Particular concerns for Indigenous peoples; people living with disabilities, and children and young people, are addressed also.

The 'Recommendations for Protecting Against Gender Based Privacy Infringements' are a starting point for Member States to realise their obligations to protect the privacy rights of all of their citizens without discrimination. It follows my preliminary report to the UN Human Rights Council in March 2019 and the General Assembly in October, 2019, and is available at ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

I urge all DPAs not to neglect this area of privacy and data protection and offer the mandate's assistance to those who wish to do more to achieve gender equity in privacy rights.

Work continues in the areas of children and privacy; encryption, and work is commencing on privacy and prisoners. Any queries about the Recommendations mentioned in this update and in relation to the 'Privacy: A Childhood Perspective' work should be sent to Dr Elizabeth Coombs at ecoom02@sec.research.um.edu.mt cc.ed, or to myself jcannataci@sec.research.um.edu.mt.

Observer on the Road

Latest update from the GPA observer at the Council of Europe

The EDPS provides an update on the Council of Europe activities as the representative of the General Privacy Assembly

The Global Privacy Assembly (GPA) enjoys observer status before the Consultative Committee (T-PD) of the Council of Europe Convention 108 and since June 2019, the European Data Protection Supervisor (EDPS) has had the honour to represent the GPA at the meetings of the T-PD.

The Council of Europe is an international organisation of 47 member States. Twenty-five years ago, it adopted the first international binding instrument on data protection, the Convention of the Council of Europe, for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). To date, 55 States, including eight non-members of the Council of Europe (Uruguay, Senegal, Mauritius, Tunisia, Cape Verde, Mexico, Argentina and Morocco), are parties to the Convention.

The Consultative Committee (T-PD) established by Convention 108 is composed of representatives of the States Parties to the Convention and observers (from 15 States non-parties to the Convention, as well as from international organisations and non-governmental organisations, such as the European Union, the OECD, the Hague Conference, the AFAPDP, EDRI or Privacy International).

The Committee is responsible for interpreting the provisions of the Convention, facilitating and improving its implementation.

For the past few years, the T-PD's work was mainly focussed on the modernisation of Convention 108. A Protocol amending the Convention (Convention 108 +) was adopted by the Committee of ministers on 18 May 2018,

To date, 35 countries have signed the Convention 108+

and opened for signature on 20 October 2018. To date, 35 countries have signed the modernised Convention 108+ and three have ratified it.

The T-PD Bureau meets several times a year, in general for two to three days, in Paris or Strasbourg, to prepare for the plenary session of the Committee, which takes place twice a year in Strasbourg.

The T-PD works on a wide number of topics of interest for the members of the GPA. Last year, it adopted:

- A recommendation on the protection of health related data, guidelines on artificial intelligence and data protection;
- The T-PD(2019)09 opinion on the draft recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems, and;
- The T-PD(2019)8FIN Opinion on the provisional text and explanatory report of the draft Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data.

Currently, the T-PD is preparing guidelines on facial recognition, on data protection and education systems, and is updating its Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling. A report on digital identity is also under preparation and preparatory work has recently been launched on personal data in the context of political activities and elections.

After each meeting, a report is produced by the EDPS. Member authorities who are interested in receiving the reports can contact the GPA Secretariat at secretariat@globalprivacyassembly.org.

Retrospective report coming soon on the GPA 41st event in Tirana

IDP Albania, the GPA's 2019 Host Authority gives an update on the follow-up to their successful and historic event of last autumn

A lot has happened since October's 41st GPA (or our last gathering under the ICDPPC acronym) around the world, no less in our community. From telecommuting to sharing articles online, following webinars and exchanging GPA members' guidance in the context of Covid-19, our community has managed to keep the pace amid a strict global lockdown due to the coronavirus outbreak.

While our data protection enforcement activities have continued, the pandemic has nevertheless succeeded in calling off all the international events requiring international travel, including the GPA's annual event in Mexico City planned for October 2020 (an online Closed Session will take place in October instead, run by the GPA Executive Committee, and Secretariat). As the lockdown is being slowly lifted worldwide, we are resuming our normal activities, hence we have now an opportunity to complete some unfinished work and concentrate more on what's to come.

We, at the Information and Data Protection Commissioner of Albania, have used this time to work on preparing a **final report of the 41st Global Privacy Assembly**, held in Tirana, to keep up with the remarkable practice established by previous ICDPPC conferences, and compile our own minutes of the event. The report is being finalized, thanks to the dedicated assistance of the GPA Secretariat, and we expect to circulate it by the end of June 2020.

You should expect a step-by-step guide through all the event segments on the conference theme: 'Convergence And Connectivity: Raising Global Data Protection Standards In The Digital Age'. This brings together the Open and Closed Session outputs in one single document: from reporting on the expert discussion on AI and GPA conference community resolutions in the Closed Session, to exploring the learnings from the Open Session, including quotes from panellists, thought-provoking statements recorded from keynote speakers, information on all the events held during the conference week and tons of pictures.

Your GPA News Highlights

For each edition of the GPA Newsletter, this section features your GPA News Highlights

Since our GPA January Newsletter, the world has been gripped by the COVID-19 pandemic. This has brought into focus the importance of our data protection and privacy community as both enablers and protectors of the interdependence of data protection and privacy as a fundamental human right and other democratic rights at this critical time.

The GPA community has responded to the issues raised by this pandemic, with initiatives highlighted below:

Statement by the GPA Executive Committee on the Coronavirus (COVID-19) Pandemic

On 27 March 2020, the GPA Executive Committee issued a statement to set out our support for public bodies and health practitioners to be able to communicate directly with the public, and scientific and government bodies in order to coordinate nationally and globally to tackle the COVID-19 pandemic. The Statement observes that GPA members and authorities operate under data protection and privacy laws that enable the use of data to protect public health, while also protecting the public's personal data in a way that the public expects: globalprivacyassembly.org/gpaexco-covid19

GPA COVID-19 Response Repository

In line with the Executive Committee's recent statement, we launched the GPA COVID-19 Response Repository, providing one-stop shop access to the latest guidance, statements and information from GPA members and observers for GPA members and observers: globalprivacyassembly.org/covid19/covid19-resources

Achieving Privacy by Design in Contact Tracing Measures

More recently on 21 May, the GPA Executive Committee issued a new Statement about contact tracing measures being implemented around the globe, recognising that public trust and confidence in the way personal information is handled and protected is a necessary precondition for a measure's success. It highlights the value in achieving privacy by design when developing new technologies in the interests of protecting public health: globalprivacyassembly.org/contact-tracing-statement

Launch of the GPA COVID-19 Taskforce

The GPA COVID-19 Taskforce led by Raymund Liboro, Privacy Commissioner of the Philippines National Privacy Commission and Taskforce members held its first meeting on 26 May 2020. The Taskforce was primarily established with the aim of driving the GPA's practical responses to the privacy challenges emerging from the COVID-19 pandemic. The Taskforce aims to also provide capacity building activities for the GPA community to assist our membership with insight and best practices. The Taskforce will regularly communicate progress and information on initiatives to the GPA membership community and wider audience, formally reporting to the 2020 GPA Closed Session: globalprivacyassembly.org/global-privacy-assembly-launches-covid-19-taskforce

Members are invited to share their events on the COVID-19 and data protection/privacy theme on our new event calendar: globalprivacyassembly.org/covid19/covid19-events. The next Taskforce meeting will be on **10 June 2020**.

The Strategic Direction Sub-Committee

The GPA's Strategic Direction Sub-Committee (SDSC) led by Angelene Falk, Information Commissioner for the Office of the Australian Information Commissioner and GPA's Executive Committee member, continues its important role in driving the GPA's current priorities, monitoring progress made in the delivery of our Policy Strategy and guiding the GPA's Working Groups: please refer to our Strategic Plan (2019 – 2020) and Policy Strategy. The next meeting will be on **18 June 2020.**

Proposal for Joint Statements on Emerging Global Issues

A membership consultation is now launched on the GPA Executive Committee's proposal for a new mechanism to enable the GPA as a whole to make its voice heard outside of the Closed Session on emerging issues with significant privacy implications. The proposal includes a suite of options to cater for different scenarios that might arise outside of the Closed Session. The deadline for member responses is **22 June 2020**.

GPA Reference Panel

Work continues to establish the GPA Reference Panel, which will provide expert knowledge and practical expertise on data protection and privacy, as well as on data protection-related issues and developments in information technology. In recognition of the GPA principle of cultural, geographic and legal diversity, membership will include international representatives of: civil society; academic institutions; think tanks; non-privacy supervisory authorities; representatives of public authorities, such as law enforcement authorities; and representatives of the private sector who have an interest in the vision and mission of the GPA.

Save the date

We would like to inform all GPA members and Observers that the GPA Closed Session 2020 will take place online during the week of 12 October – 16 October. More news to follow.

Have you thought about contributing to the GPA Newsletter? We are now planning content for the September Edition. Please contact the GPA Secretariat if you would like to contribute, and for more information on any of the issues highlighted above: secretariat@globalprivacyassembly.org.

GPA key upcoming dates

10 June	**GPA COVID-19 Taskforce Meeting**	**Mid-July**	**59th GPA Executive Committee Meeting**
18 June	**SDSC Meeting**	**31st July**	**GPA Resolutions Deadline**
22 June	**Complex/Technical Resolutions Deadline**	**11 September**	**Consultation on new Members/Observers Deadline**
22 June	**Comments on the Joint Statements proposal Deadline**	**12-16 October**	**GPA Closed Session 2020 (online)**

Watch our website for more information: globalprivacyassembly.org

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

globalprivacyassembly.org/covid19

GPA Global Privacy Assembly

COVID-19 TASKFORCE

Get to Know Your ExCo...

The "new normal". What's next? Reflections on the future of privacy

President Commissioner, Francisco Javier Acuña Llamas (left) and Jonathan Mendoza Iserte (right), Secretary for Personal Data Protection of the National Institute for Transparency, Access to Information and Personal Data Protection, INAI

The INAI is a young institution with nearly two decades of history. In 2020, it will be ten years since the Federal Law on Protection of Personal Data Held by Private Parties was published, the first secondary legislation in Mexico regulating the protection of personal data in the private sector. Seven years later, on 26 January 2017, the General Law on Protection of Personal Data Held by Obligated Parties was published in order to regulate the three levels of government and the public sector. We should not forget that, in the interim, in February 2014, there was a constitutional amendment that gave autonomy to the National Institute for Transparency, Access to Information and Personal Data Protection (INAI).

After a decade of work, INAI's Plenary is focusing on a strategic agenda of current projects on personal data protection, such as: the Mexican legislation's adjustment to the latest international instruments (for example, Treaty 223 of the Council of Europe – C108+); the accession of Mexico to Convention 108 of the Council of Europe in 2018; the analysis of possible adequacy in accordance with the EU's General Data Protection Regulation (GDPR), and the strengthening of the culture of personal data protection in view of the new technological trends in the framework of the digital economy.

Looking to the future and in line with the central theme proposed for the 42nd Global Privacy Assembly (GPA) to be held in 2021, the INAI will seek to promote an ethical approach to the processing of personal data

by data controllers: we will seek to draw conclusions on key tenets of the human factor in automated decision-making; and we will encourage proactive responsibility and compliance with legal requirements through effective self-regulatory mechanisms.

At the regional level, a cultural context prevails that has not allowed Latin American countries to take advantage of the benefits granted by the protection of personal data and privacy, intensified by the prevailing gaps in the take-up of digital technologies and economic inequalities. The great challenge of the region's Data Protection Authorities (DPAs) is to contribute to the actions aimed at diminishing these inequalities and to implement measures to increase the accessibility and inclusion of people to enable them to exercise their rights.

During the current global crisis, the measures adopted by Mexican States have highlighted the discussion on the use and processing of personal data in emergency situations, opening a critical debate on the future of societies. This forces us remember the following lessons:

- The importance of a permanent collaboration and the opening of communication channels with all the actors involved;
- The role of DPAs is fundamental in guaranteeing the exercise of people's freedoms and rights. Therefore, its role should not be limited to preventive actions, but will require constant monitoring and follow-up;
- The role of DPAs is not only to protect the use of personal data, but also to promote its proportionate and appropriate use through tools developed with privacy by design and default.

In addition, the solutions recently implemented to combat the health crisis will make us reconsider some of the following significant issues:

- Remote working and virtual platforms;
- Home delivery and consumer profiling;
- Digital commerce and cybersecurity;
- Geolocation and contact tracing applications;
- Convergence of personal data regulations in global emergency situations.

We conclude by emphasising that the postponement of the Mexican hosting of the First Global Privacy Assembly (compared with past events under the ICDPPC banner) will offer a new opportunity to (i) identify the new challenges facing our institutions, (ii) adapt to the "new normal" in relation to COVID-19, and (iii) reflect on the constant threats that the technological future holds for us.

Meet our Member

President Joël Dominique Ledaga of the National Commission for Data Privacy Protection in Gabon

The GPA is welcoming a number of new members, including Gabon (new member in 2019) one of a number of authorities on the African continent proactively cooperating with international counterparts

The National Commission for Data Privacy Protection in Gabon, created by Law No. 001/2011 on the protection of personal data, of 25 September 2011, is an independent administrative authority.

The Commission is led by the President whose role is to ensure the application of this law, to apportion the budget, to convene and chair plenary sessions, as well as to represent and manage the Commission.

Since its establishment in November 2012, and in accordance with Article 39 of this Law, the Commission has adopted internal rules governing its organisation, operation and procedures that have been declared in conformity with the Constitution by Constitutional Court decision Number 255 bis/CC of 13 December 2018.

Since then, the Commission has issued 17 Opinions on technology projects initiated by the Government, authorised 39 automated processing operations and issued 34 receipts for the declaration of automated processing operations, all implemented by legal entities under private law. The Commission has also published three simplified standards regulating aspects of personal data processing in telecommunications, video surveillance and geolocation.

Recent examples of the Commission's successful regulatory action include a financial penalty on a company misusing GPS, without prior authorisation and without notifying its employees. In another case, a victim of identity theft was able, after an investigation, to take action against Facebook to close a false account, in accordance with the deletion right stated in Article 14 of aforementioned law.

"The Commission aims to promote its role through educational campaigns on personal data protection issues, including ... the use of social networks."

In light of the above, the Commission aims to promote its role through educational campaigns on personal data protection issues, including in relation to the use of social networks. To this end, information and awareness-raising seminars were organised in Libreville (the political capital) and Port Gentil (the economic capital). Similarly, in collaboration with the National Education and Higher Education Ministries, the Commission conducted campaigns in both schools and universities to support young people, drawn towards technological innovation, to adopt a responsible attitude towards the use of social networks. Open days were also organised to mark International Data Privacy Day on 28 January. The Commission used the occasion to call on commercial operators who process and collect personal data to comply with the law.

Furthermore, in order to align itself with international standards, the Commission has joined the Global Privacy Assembly (GPA), the AFAPDP, the African Network of Data Protection Authorities (RAPDP) and is an observer member of the Council of Europe's Convention 108 Committee. The Commission regularly takes part in international conferences and other meetings organised by these bodies.

In terms of constraints, the lack of financial resources impacts on the implementation of the Commission's programmes, notably the establishment of a technology watch unit. To remedy this, a proposal was recently initiated to amend certain provisions of our Law including the introduction of an annual fee, which is in the process of being ratified by Parliament.

Finally, the impact of the COVID-19 pandemic in Gabon with respect to the protection of privacy can be seen in the abundance of personal information shared through social networks. This has led the Commission to emphasise that the universal principles of protection of sensitive personal data set out in the Law, must be applied in the context of the higher national interest. Consequently, health data may be published online while abiding by the rules of anonymisation in accordance with articles 49 and 81 of the current Law.