

NEWSLETTER

GLOBAL PRIVACY ASSEMBLY

Chair's Message



As Chair of the Global Privacy Assembly and on behalf of the Commissioners of the National Institute for Transparency, Access to Information and Personal Data Protection of Mexico, I would like to share with you some remarks. Each new year represents an excellent opportunity to reflect on past times and the future ahead of us.


The year 2021 was marked by the flexibility and resilience that society showed to respond to the health, technological, economic, political, and social conditions present worldwide. Given this scenario, the Global Privacy Assembly managed to position itself as a cutting-edge forum and a world reference in the protection of privacy and personal data.

During the last few months, this organization has kept working, and has demonstrated its ability to face the challenges arising from the new paradigm of the digital age, which implies severe risks to privacy given the massive flow of data. Proof of this work was the

joint statements and resolutions issued, such as the *Joint Statement on the Use of Health Data for Domestic or International Travel Purposes*, published a few months ago, with the aim of encouraging organisations to minimize data collection to only that information that can contribute to the protection of public health.



Also, thanks to the establishment of the **Reference Panel** designated last March, our relationship with public and private organizations and other experts was strengthened. The participation of specialists with diverse normative and cultural backgrounds allow us to learn and exchange knowledge on these matters and enrich our actions within



GPA

Global Privacy Assembly

In this issue:

- > [Chair's Message P1](#)
- > [Highlights from the 43rd Closed Session GPA P2](#)
- > [Focus: Would you pay with your personal data? P3](#)
- > [Working Groups Highlights P4](#)
- > [Message from the SDSC Chair P6](#)
- > [Regional Perspectives P7](#)
- > [ExCo Collaboration: CNDP: Data protection, from files, data base to data behaviors P9](#)
- > [Get to Know your ExCo P11](#)
- > [Meet our Member P13](#)

the Working Groups of the Assembly and the Executive Committee.

Mexico held the Open Session of the 43rd Global Privacy Assembly last year, with a completely digital scheme for the first time in our history. Thanks to this, we fulfilled our duties even with the obstacles that the health emergency represented.

I take this opportunity to recognize the achievements and results obtained under the Presidency held by Information Commissioner's Office and led by Elizabeth Denham, whose term ended in 2021. Her effort, dedication, and perseverance made possible to construct a community capable of meeting

strategic objectives and promoting new insights regarding privacy in the world.

Now, the National Institute for Transparency, Access to Information, and Personal Data Protection in Mexico will take the Presidency of the Assembly for the next years. We will seek to promote the necessary actions to assertively comply with the strategic objectives enacted for the 2021-2023 period. Likewise, we will maintain an open-door policy, with the commitment to act as an impartial, objective, and open-to-dialogue facilitator, both inside and outside our forum.

The year 2022 represents a

time of hope and recovery. The storage and processing of data are advancing rapidly, bringing new challenges; so, through a joint effort and collective work, I am sure that, at our next meeting in Turkey, we will be able to develop and strengthen a governance structure capable of guaranteeing the right to privacy and the protection of personal data.

To conclude, I want to remind you that the Global Privacy Assembly is called to be a leading and constructive voice, capable of facilitating digital innovation in a changing and challenging environment while contributing to the guarantee of human rights. We are an active, vibrant, and

multicultural Assembly in which the exchange and learning among peers are the pillars that guide our actions.

Let us strengthen our work cohesively under a broad and united front that fulfills our purpose of acting as an ally of the people by answering their demands and needs. To achieve this, and for the benefit of our nations, we wish all of you a fruitful year 2022, full of work and good results.

Blanca Lilia Ibarra Cadena

President Commissioner at INAI
Mexico
GPA Chair

Highlights from the 43rd Closed Session of the Global Privacy Assembly 2021

INAI as host authority of the 2021 GPA edition

On October 20th and 21st, 2021, the National Institute for Transparency, Access to Information, and Personal Data Protection (INAI, Mexico) virtually hosted the Closed Session of the 43rd Global Privacy Assembly (GPA).

During two days of hard work, more than 150 Member Authorities of the GPA discussed relevant issues related to the human right of the protection of personal data. Among the topics addressed, the following stand out:

- Data-Driven Innovation for the Public Good
- Enforcement Cooperation
- Fostering Innovation through engagement

A group of Member Authorities presented the progress made in their respective jurisdictions to protect personal data, especially sensitive data, during the health crisis management. They also discussed the topic that has stressed the world, the learned lessons, and the importance of continuing to safeguard privacy in the Covid 19 pandemic. Thus,

the discussion focused on the key role of data protection authorities as enablers and protectors in this new phase of the pandemic: the importance of building trust using privacy by design, while improving impact assessments, reviewing the evidence and a rethink of existing models, and development of new models for the use of public data.



This space also allowed the presentation of the work carried out by the other international forums such as the International Working Group on Data Protection in Technology (IWGDPT, also known as "Berlin Group"); the UN Special Rapporteur on Privacy; the Council of Europe; the European Data Protection Supervisor, the

Global Privacy Enforcement Network; the Asia Pacific Privacy Authorities Forum; the African Network of Data Protection Authorities, among others.

In addition, a variety of resolutions were discussed and adopted by consensus. These documents, while reflecting the concerns of Member Authorities, provide specific recommendations to improve the guarantee of the right of data protection in regional contexts, such as

- Resolution on Data Sharing for the Public Good
- Resolution on Children's Digital Rights
- Resolution on Government Access to Data, Privacy, and the Rule of Law: Principles of Governmental Access to Personal Data for National Security and Public Safety Purposes

Regarding the future work of the GPA, the Member Authorities decided firstly that the organization should focus on providing practical and

prompt advice to international organizations, policymakers, and other actors to remain relevant and have an impact on the world. And secondly, the importance of Data Protection Authorities role in keeping up to date with privacy enhancing technologies and delivering appropriate safeguards with necessary international law

and regulatory frameworks.

The strategic priorities of the GPA that will guide the future work were confirmed:

- To advance global privacy in an age of accelerated digitalization.
- Maximizing the GPA's voice and influence.
- Capacity building for GPA members.

Finally, it was announced that the Data Protection Authorities of Turkey and Bermuda will host the annual meetings in 2022 and 2023, respectively. INAI's President Commissioner, Blanca Lilia Ibarra Cadena, was elected as new Chair of the GPA, replacing Elizabeth Denham, the former UK Information Commissioner.

Focus

Would you pay with your personal data?

Elena Gil González

Legal advisor on Data Protection, PhD with honours and Awarded by the Spanish Data Protection Authority

A few years ago, technological development was synonymous with online services, e-commerce and social networks. Today, all of these are everyday things, and innovation is now seen in the development of the metaverse and augmented reality technologies.

On some occasions, these services are provided in exchange for a monetary payment to the service provider, but on many other occasions the services are provided in exchange for displaying advertising to users. To the extent that the operation of the advertising industry is based on the higher rate of "clicks" that a user makes on the advertisements shown to him, the personalization of advertising increases the provider's profit margins. As a result, data collection, tracking of online user behavior and creation of increasingly detailed profiles seek to understand the tastes of each user in order to personalize advertising and services so that the business of data monetization becomes more lucrative.

In other words, our personal data has now been commoditized. In the European Union, this is a reality that clashes with the fact that data protection is so important that it is declared a fundamental right.

In any case, the exchange of services for personal data should not mean that data subjects are deprived of their rights.

In addition to the profound debate about the validity of consent based on "take it or leave it" options, and even accepting the possibility that personal data can be used as a bargaining chip for digital services, other problems remain.

But really, what is the price?

This situation is intended to resemble that whereby a thing is exchanged in exchange for a price, which is the basis of the contract of sale regulated in most of the Civil Codes of European States.

In Civil Law, the contract is perfected by the consent of both parties once they have agreed on the object of the contract and the price. Taking the Spanish Civil Code as an example, the price must be determined in advance and not be left to the discretion of one of the contracting parties.

On many occasions, however, the price, in terms of giving consent for the collection and processing of personal data in exchange for the enjoyment of a service, is not specified and cannot be subject to negotiation by the data subject. For example, when consent is sought to collect or to access information stored or emitted by the device, the data subject does not know exactly what data he or she is providing in the exchange. Likewise, on many occasions, they also do not have the ability to decide



who will be able to access their data, beyond the ability to accept or deny third party cookies without much granularity. Even when the option exists, selecting one by one among the dozens or hundreds of third-party names that a notice displays does not give the user any control power either, insofar as the machineries of the data marketplace and the specific players are not transparent or known to the average user.

On the other hand, sometimes the request for consent is presented in terms of accepting or refusing to receive advertising or other functionalities in a personalized manner. However, is the refusal to provide this consent a refusal to have the data collected or a refusal to have it used for personalization functionalities?

Thus, even an economic conception of data as a price for a product or service would not meet the most basic legal requirements for price determination.

In connection with this, the debate also opens up as to whether, therefore, consent to the collection and processing of information as a price should be restricted to those services provided without economic consideration, such as access to the



content of a digital newspaper, or also to those other services for which the user already pays a price, such as making a purchase of clothing through the company's website.

All this debate is further fueled, if possible, by the fact that in the EU, as of January 1st, 2022, the Directive 2019/770 on contracts for the supply of digital content and services is in force. For the first time in the EU, this norm expressly regulates the possibility of paying for certain digital services with personal data.

On the one hand, this is a step forward in raising users' awareness, since it encourages them to stop considering that access to services via the Internet is "free", and rather call it "price".

Apart from opinions on the positive and negative aspects of trading with personal data, the fact is that this set of rules puts black in white what is a reality: services are currently offered without consideration in currency, but in data.

There are many practical doubts that this rule raises, in particular because it must be applied consistently with the GDPR, and in particular, what role do the legal grounds of the GDPR play, such as consent, contractual performance or legitimate interest. Undoubtedly the next few years will see some fine-tuning.

Working Group Highlights

The current work of the DEWG

Marie-Laure DENIS, Chair of the Digital Education Working Group (DEWG) highlights progress and future developments to implement the key objectives of the 2021 GPA Resolution on Children's Digital Rights.

The protection of children's privacy online is more than ever at the heart of the public debate in many countries and on the agenda of international organisations.

The new national and international legal landscape is emerging in search of a balance between autonomy and child protection as shown by the adoption the past year of the United Nations [General Comment No. 25 on the rights of the child in the digital environment](#), the [OECD Recommendation on children in the digital environment](#), or the [Council of Europe's Declaration on the Protection of Children's Right to Privacy in the Digital Environment](#).

The voice of the GPA was again made public on these priority issues of common interest when reporting on national and international pro-active initiatives of data protection authorities at the high-level launch conference of the OECD Recommendation on Children in the Digital Environment

(last November, panel attended by the CNIL, Garante, ICO and FTC as GPA members engaged on children's digital rights among others - see below).

At the European level, the European Data Protection Board (EDPS) has initiated the drafting of guidelines on children's data protection and the European Commission adopted its [New 2021-2024 EU Strategy on the Rights of the Child](#).

The UK ICO developed an ["Age-appropriate design Code"](#), the Irish DPC published ["14 Fundamentals for a child-oriented approach to data processing"](#) for public consultation in 2021, the French CNIL published [8 recommendations to enhance the protection of children online](#), the Dutch government commissioned the ["Code for Children's Rights"](#) while in the United States, two [pieces of legislation](#) emerged in the US Congress in June 2021 to develop so-called "COPPA 2.0".

All these initiatives reveal a



positive dynamic of awareness of the issues related to the digital practices of children, which must be pursued and encouraged, particularly as regards the promotion of children's digital rights.

We recall that the issue of children's rights online has been made as a focus of priority in the GPA's 2021-2023 Strategic Plan, which will seek to strengthen the actions already undertaken and performed by the Digital Education Working Group in this area. The GPA will continue to support and provide input to such initiatives and invites all working groups to consider in their work plans how

their mandate and work intersect with children's privacy.

The Resolution on children's digital rights

In line with this, the GPA members adopted a very consensual Resolution on children's digital rights on 21 October 2021 tabled by the French CNIL and the Italian Garante on behalf of the DEWG, and co-sponsored by 21 DPAs.

The **2021-2022 DEWG Action Plan** focuses on the implementation of the key objectives of the Resolution in a phased approach within the GPA's Strategic plan:

- **Better educating children on digital environment and developing child-friendly digital tools**

At present, the DEWG continues to jointly facilitate access to adequate digital literacy and education for all children from an early age, in order to allow them to use digital tools autonomously, to acquire skills to explore, create and interact online safely, and with an understanding of the digital environment, its prospects and its risks.

Key highlights include:

Priority Action I - Undertaking support initiatives to facilitate the exercise of the rights of children and of their parents/ legal guardians in a manner appropriate to their maturity in the digital environment:

- Encouraging DPAs to update the [CIRCABC online library](#) with appropriate educational tools, guides, and other FAQs to help children understand their rights on personal data, how to exercise these rights, including by parents for data concerning their children, how to report or complain to DPAs or other agencies in relay.
- Designing a flow chart and/or an infographic of the ways in which children exercise their rights on the main social networks to inform and guide young people and/or parents. We will carry out this exercise collaboratively.

The resolution provides for support of the fundamental role of parents and educators within the digital environment, through educational programmes, actions and awareness campaigns.

Priority Action II addresses:

- Strengthening cooperation between DPAs to support parents and educators in acquiring digital literacy and awareness of the risks to children in order to help assist their children in the realization of their rights *while respecting their best interests*, and protect regarding risks in relation to the digital environment.
- Exchanging on digital parenting and focusing on parental control systems by compiling existing studies and research publications on data protection evaluation of such systems.

Protecting children effectively against online threats

In support of the resolution, the GPA aims to commit governments and online service providers to:

- provide concrete responses to the major societal challenge related to the widespread and poorly supervised presence of children online
- safeguard greater protection for children against the commercial exploitation of their data, and
- prohibit practices that aim to manipulate children or influence their behavior, and
- foster the implementation of industry codes and terms and conditions of service that meet the highest standards of ethics, privacy and child safety in all stages of the value chain, including design.

Among the strategic issues adopted in the work programme:

Priority Action III includes over this year at least:

- Reviewing interfaces and design prototypes that emphasise children's rights and address them in a child-friendly manner

on the basis of works carried out by DPAs or other IT partners and legal design firms.

- For online service providers, publishing guidance (and other tools) from sites used by children to help organisations comply with their obligations to provide children with online services and redress mechanisms in a clear, comprehensible and child-friendly manner.

The DEWG is also conducting monitoring activities on other important related topics such as the age verification of children and their further related-development on both national and international levels.

More information to join the DEWG, email the Coordinator at pserrier@cnil.fr



Message from the SDSC Chair

Over recent years, the Global Privacy Assembly has achieved significant outcomes, having developed into a forum which is active across the year to deliver pragmatic outcomes for global citizens.

When we first adopted the Strategic Plan in Tirana, Albania, we could not have envisaged the challenges that lay ahead of us, and yet I cannot think of a time where the Vision of the Strategic Plan has been more important or relevant to our community.

The new Strategic Plan 2021-23 builds on the successful foundations provided by the 2019-21 Plan. It continues to set out the GPA's roadmap to achieving our Vision. Our Vision is to create an environment in which privacy and data protection authorities worldwide can practically fulfil their mandates, both individually and in concert, to ensure high standards of data protection globally and promote and facilitate effective regulatory cooperation.

As Chair of the Strategic Direction Sub-Committee (SDSC), I have the privilege of assisting with the practical implementation of the Strategic Plan.

This year, the SDSC will welcome its newest two members – Morocco and Mexico – at its first meeting for 2022, to join Germany and Australia, as we farewelled the UK and Albania. I look forward to the new perspectives and experience these incoming members will bring to SDSC.

Strategic Plan 2021-23

The GPA's Mission under the new Strategic Plan includes being a highly effective global forum for data protection authorities and providing regulatory and policy leadership at the international level in data protection and privacy. Accordingly, the Strategic Plan recognises that the GPA must continue to strive to be an active

platform which is able to influence and engage on issues to ensure the GPA voice remains relevant on evolving issues.

Underpinning the new Strategic Plan are three Strategic Priorities.

- **Strategic Priority 1** focuses on advancing global privacy in an age of accelerated digitisation. The GPA will work towards a global regulatory environment with clear and consistently high standards of data protection, as digitisation continues at pace.
- **Strategic Priority 2** considers ways to maximise the GPA's voice and influence. This aims to enhance the GPA's role and voice in broader digital policy and strengthen relationships with other international bodies and networks advancing data protection and privacy issues, including through observer arrangements.
- **Strategic Priority 3** addresses capacity building, with the objective of supporting Members' shared learning from experiences, strategies and best practices, including cooperation and capacity building tools. This strategic priority works to recognise and strengthen the importance of working together to ensure a coordinated response to data protection and privacy issues.

These three Strategic Priorities have been identified by the GPA as we face new digital challenges and common global societal risks.

The global pandemic has significantly accelerated digitalisation in both the public and private sectors, making significant changes to the way people live, work, travel, learn and socialise, and how services are delivered.

It was recognised by GPA members that in this environment it is more important than ever that the GPA and its members collaborate to enable innovative changes to take place in a way that



benefits society and protects our citizens from data protection and privacy risks.

The year ahead for the SDSC

The SDSC's first important priority of the year will be to commence the development of a new work plan which will align with the newly adopted Strategic Plan. This is to ensure that the SDSC can support the GPA and the Executive Committee in achieving its Vision. The key aims of the SDSC will continue to be:

- advancing our strategic direction,
- promoting strategic messaging by the GPA, and
- strengthening our engagement with key stakeholders.

Advancing strategic direction through the Working Groups

Advancing strategic direction is not possible without the work of the GPA Working Groups - the GPA Working Groups bring to life the actions set out in the GPA Strategic Plan. The GPA Working Groups undertake an impressive amount of work to share their work with the wider world, to bring data protection and privacy considerations into other fora.

At the 2021 GPA conference in Mexico, we heard from GPA Working Groups on the important work they have undertaken to advance high standards of data protection and privacy globally.

Overall, the Working Groups achieved the objectives set out in the previous Strategic Plan, producing pragmatic and tangible outcomes against the Plan. This is something to be truly proud of.

Under the 2021-23 Strategic Plan, the Working Groups committed to an impressive amount of work, some of which includes:

- working towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards,
- building capacity in relation to enforcement strategies,
- identifying areas for cross regulatory cooperation,
- delivering a compendium on best practices for data sharing and the public good,
- continuing work on facial recognition technology, and
- taking initiatives to facilitate the effective exercise of children's rights.

We have no doubt that going forward the Working Groups will achieve the objectives in the new Strategic Plan. The SDSC is committed to supporting Working Groups to successfully deliver on the Strategic Plan and to collaborate to enable innovative changes to take place in a way that benefits society and protects our citizens from data protection and privacy risks.

Promoting Strategic Messaging

A significant achievement of the GPA over the past few years was to adopt the Joint Statement mechanism. This mechanism ensures that members can meet global issues that demand swift and immediate responses. I welcome initiatives from members in using the Joint Statement mechanism, and invite them to reach out to the SDSC for support and guidance.

Strengthening engagement with key stakeholders

In 2021, the SDSC undertook preliminary work to map current regional and linguistic networks. Looking ahead, the SDSC will aim to continue to adopt strategies to increase cross-communication and engagement between the GPA and other important networks.

As we take forward the important work of the SDSC, I welcome the expertise from our new members, Morocco and Mexico, as well as the continued involvement from Germany.

If your agency has or is undertaking work that relates to the Strategic Plan, including the work of the working groups, please reach out to the SDSC.

I look forward to working with you all in the year ahead.
Regards,

Angelene Falk

Australian Information Commissioner
and Privacy Commissioner

Regional Perspectives

National Data Protection Authority of Brazil: Structuring and Initiatives

Public and legislative discussions over data protection and privacy in Brazil began in 2010, with the opening of a public consultation on the subject which later resulted in a Law proposal.

After almost 8 years of processing in the National Congress (House and Senate), many public hearings, more than 2500 contributions from national and international actors, from all sectors, countless events, the Brazilian General Data Protection Law (LGPD), Law no. 13.709, was approved in August, 2018, with an adaptation period of 18 months.

LGPD, in force since September 2020, provided new rules for use, protection and personal data transfer, by both public and private sectors. The law requires explicit consent, among other legal basis, for data collection and use, and

establishes that the data subjects shall have an array of rights, such as the option of viewing, correcting and deleting their data.

Before LGPD, data protection and privacy were handled by a variety of laws in Brazil, such as Article 5 of the Constitution, the Civil Rights Framework for the Internet, provisions from the Consumer Protection Code, the Law on Access to Information and some specific sector regulations. LGPD came exactly to provide a more comprehensive and harmonic approach to personal data and privacy protection.

At the same time, the creation



of LGPD left Brazilian society amid questions on how this new regulation would take place: the corporate world questioned how they should act to adapt to the required practices; on the other hand, consumers showed doubt about how their data would be processed and if the new regulation would be effective or would it only

create more bureaucracy?

In order to manage these uncertainties, in July 2019, Law 13.853 created the National Data Protection Authority (ANPD), the supervisory authority in charge of supervising, implementing and inspecting compliance with LGPD. The creation of ANPD was fundamental for the LGPD enforcement, once the full implementation of the law depends on the Authority's decisions, interpretation and regulations.

In August, 2020, Decree no. 10.474 created the Regimental Structure of ANPD and turned light to the release of the organ's internal regiment (released on March 2021). Also, right after its creation, ANPD published its Strategic Planning for 2021-2023 and its Regulatory Agenda, both norms have illustrated the Authority's work and priorities at this early stage of legal enforcement. Those documents demonstrate the Authority's intent to devote itself to the educative aspects of law enforcement, in view of the country's incipient knowledge on the topic.

Since its creation, ANPD has been developing standards, fomenting data protection and privacy culture and enforcing procedures to ensure that the subject's rights are being respected. ANPD has produced guiding content materials aimed at different target audiences in various formats, constantly updating its website with news that end up allowing access to information and, at the same time, demonstrating the transparency of its work. Since then, ANPD has already released content related to Information Security for Small Treatment Agents; Instructional Guide for Personal Data Protection; Guide on the Definition of Personal Data Processing Agents; Educational Booklets on Leakage and Data Protection; Guide on the LGPD enforcement in the electoral context.

Regarding ANPD's sanctioning

competence, effective as of August 1, 2021, the application of sanctions includes the possibility of using warnings, fines, suspensions and partial or total prohibition of the exercise of data processing activities carried out by agents. It also includes the possibility of carrying out audits both in the public and private spheres, as well as other measures depending on the specific situation.

The criteria for applying sanctions by the LGPD take into account: the impact of the incident and what data it affects; whether there is good faith on the part of the company in the processing of data; what motivated the company to process the data; the company's economic power; whether or not the company is a repeat offender; what damage is generated; cooperation with ANPD and users; the development and application of technological and organizational measures that help to prevent damage; good practice and governance policies; the adoption of corrective measures; and the proportionality between the seriousness of the offense and the intensity of the sanction.

Another legal competence of ANPD is provided by the article 55-J, paragraph forth, in which it is inserted the maintenance, by ANPD, of a permanent communication forum, including by technical cooperation, with bodies and entities of the public administration responsible for the regulation of specific sectors of governmental and economic activity, in order to facilitate ANPD's regulatory, monitoring and punitive duties. In the context of institutional relations, ANPD has developed some cooperation agreements in order to always keep the communication channel open in both direction between the interested parties.

Within the scope of international interactions, ANPD has been increasing its active participation and also achieving international acknowledgement, remaining as observer of the

Global Privacy Assembly – GPA -, as well as member of the Red Iberoamericana de Protección de Datos – RIPD.

ANPD, in close cooperation with the Ministry of Foreign Affairs, also, has already achieved participation in relevant international fora and bodies through the nomination of a representative group. This group may follow the discussions within, for example, OECD and G20 working groups and can give its contributions on Recommendations' reviews and Questionnaires. ANPD's representative group had the privilege of participating as an observer at the 41st Plenary Meeting of the Convention 108+ in the framework of The Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

ANPD recognizes the multifaceted role it has, as an educator, a law enforcer and a regulatory authority, so it is pursuing and learning from partner's best practices to tutor Brazilians and its companies into the culture of Data and Privacy Protection. In this sense, 2021 was a structuring year, ANPD reached significant goals to ensure the application of LGPD and to foster discussions on privacy and protection of personal data in Brazil.

For the near future, ANPD intends to expand its activities with a greater number of public consultations, in addition to inspections and the effective regulation of LGPD, thus ensuring legislation effectiveness. Above all ANPD foresees participation in as many educative initiatives as possible as the Authority understands that at this stage its main role is to elevate Data and Privacy Protection dialogue in Brazil. Specially after Brazilian Senate approved an Amendment to the Constitution turning the protection of personal data a fundamental right. Even though, the novelty needs to wait for a National Congress approval before



it is added to the Constitution, it serves as proof of how data protection has gained legitimacy and relevance in Brazilian society.

In light of all the recent development in the area, ANPD is pushing for the fulfillment of art. 55-A, §1, which calls for the revision of the Authority's legal status to special independent government entity two years after

the implementation of LGDP. Once that is settled, the Authority will have total budgetary autonomy to hire and train its personnel and to direct its work as it were established in LGDP.

Despite Brazil being at its early stages on the topic, it is evolving fast and steady towards a society that can give its citizens more control over how

their personal data is handled. ANPD will continue on working to fulfil its mission of ensuring the protection of personal data and privacy. In this sense, ANPD believes that clear, transparent and comprehensive rules for the proper use of personal data encourage technological development, innovation and economic stability.

ExCo Collaboration: CNDP: Data protection, from files, data base to data behaviors

About the CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel)

The CNDP was established in 2009. The institution is responsible for verifying that the processing of personal data is lawful, legal and does not infringe on privacy, freedoms and fundamental human rights. The Commission is made up of personalities known for their impartiality, their moral probity and their competence in the legal, judicial and computer fields. Since November 17, 2018, the CNDP is chaired by Mr. Omar SEGHRUCHNI who is appointed by His Majesty the King Mohammed VI.

Hosting of the 38th edition of the International Conference of Data Protection and Privacy Commissioners (ICDPPC)

Morocco hosted the 38th edition of the Global Privacy Assembly (Ex-International conference of data protection and privacy commissioners (ICDPPC)) from October 17 to 20, 2016. Several experts and world-class personalities took part in this Conference and 500 participants

from 70 countries were present. The event was a great success

Ratification of Convention 108 and validation process of Convention 108+

In order to align itself with international standards and norms in the area of personal data protection, Morocco ratified, in 2019, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its additional protocol. Thus, Morocco became the 55th State Party to the Convention and the sixth country in the African region to join. CNDP participates in the work of the Council of Europe on the modernization of Convention 108 (Convention 108+) with a view to its adoption.

CNDP and GAFAM

In April 2019, the CNDP hosted a meeting with representatives of Facebook and presented its demands, among which is the establishment of mechanisms allowing Facebook to deal effectively with complaints addressed to the CNDP and linked to, inter alia, profiling by the

social networks of the Facebook company. Facebook has offered to set up a "Data Protection Authority Casework" for the purpose of providing specialized and specific assistance to data protection authorities, such as CNDP.

The CNDP in the era of the Covid-19 crisis

The CNDP was one of the institutions that anticipated its actions from the very beginning of the crisis by : (1) Delivering on several topics related to the current situation like teleworking, temperature measurement, facial recognition for remote management of bank accounts; (2) Studying the implementation of the application WIQAYTNA (the national "antiCOVID-19 application") on the basis of clearly identified hypotheses and evaluation process; (3) The CNDP has also set up a crisis cell in order to meet the needs of the health emergency period, in terms of personal data protection.

Position on facial recognition

Facial recognition technology is governed by three deliberations, namely: (1) Deliberation n°D-97-2020 of 26/03/2020 concerning

the extension of a moratorium on facial recognition ; (2) Deliberation No. D-108-EUS/2020 of April 23, 2020 on the definition of the use of facial recognition technologies in the context of the remote account system by banks and payment institutions ; (3) Deliberation No. D-126-EUS/2020 of July 29, 2020 on the definition of the use of facial recognition technologies by pension funds institutions for the proof of life of retirees.

These deliberations emphasize the need for a trusted third party in the use of this technology.

Position on a credential architecture and on the trusted third party for authentication

The FATF guidance for governments « Digital Identity », issued in 2020, was motivated by the rapid growth of digital payments and the need to control the risk relating to the level of security of key system components. In this sense, the CNDP supports the fact that digitalization must be conceived beyond a technical implementation project and that one of the pillars of this digitalization is the architecture of identifiers. Thus, the Commission recommends: (1) An architecture of identifiers that considers constitutional, economic, societal and technical requirements; (2) That data usage and data authentication **should not** be stored within the same architecture and under the responsibility of the same entity; (3) That the use of sector-specific identifiers, at a granularity to be defined according to the requirements of each sector of activity. The use of a unique identifier is then a technical mechanism secured by “tokenization” policies, ensuring that this unique identifier is not public but under the imperative protection of the regalian authorities, which encourages the use of sectoral identifiers.

DATA-TIKA programs (the term « Tika » means “trust” in Arabic)
The CNDP works for the

development of digital trust with its DATA-TIKA programs which aims to protect the citizen within the digital ecosystem. Joining a DATA-TIKA program will reverse the paradigm, that means that instead of simply understanding the actions to be taken to comply with the law, the member will be able to proactively feed the CNDP's field approaches. The DATA-TIKA programs are declined in 3 formulas: (1) DATA-TIKA private Companies; (2) DATA-TIKA Public Institutions; (3) DATA-TIKA Associations & NGOs.

Risk Analysis and Impact Assessment

In December 2020, CNDP delivered a deliberation on Risk analysis and Impact assessment (Deliberation n° D-188-2020) which highlights the importance of the principle of proportionality and the use of risk analysis techniques to assess situations related to new uses induced by technological progress. The Commission wants to promote the principle of risk assessment in the field of privacy protection. Therefore, during its support mission and after examining requests submitted by data controllers, the Commission recommends the application of convenient measures that deem sufficient to ensure an adequate level of protection of personal data.

Experimentation and Sandboxing

The CNDP applies a “test & see” approach and sandboxing in order to develop its capacity for experimentation, which eventually allows it to absorb the new uses induced by the various technological trends.

Membership at AFAPDP

CNDP is a member of the Association of Francophone Data Protection Authorities (AFAPDP), which brings together the personal data protection authorities of French-speaking countries. CNDP had co-chaired with the Belgian authority the working group set up within the AFAPDP to define a reference framework governing the

transfer of personal data within the French-speaking world.

Permanent Secretariat of NADPA/RAPDP

CNDP acts as the Permanent Secretariat of NADPA-RAPDP (The Network of African Data Protection Authorities) since its General Assembly held in Morocco in February 2018. This Network was established in Burkina Faso in September 2016 and currently comprises several African privacy and data protection authorities (19 members and 2 observers), with the aim of setting up a platform for exchanges and co-operation between its members and making Africa's voice heard in its dealings with partners around the world.

Membership at the Executive Committee of the GPA

CNDP was elected as a member of the Executive Committee of the GPA (Global Privacy Assembly) during its General Assembly held in October 2021, in Mexico.

National Consultation with the Institution of the Ombudsman of the Kingdom

In July 2020, the Institution of the Ombudsman of the Kingdom and the CNDP initiated a joint consultation in order to understand the expectations and constraints of the various actors in society regarding the necessary digitization and the expected, acceptable and possible positioning of international platforms. This consultation aims to: (1) Identify the elements of a responsible digital for the benefit of citizens, the economy, and society; (2) Analyze the advantages and disadvantages of the use of commercial digital platforms; (3) Determine the appropriate regulatory framework to make the most of the innovative contributions of these commercial platforms and their ecosystems; (4) Collect relevant ideas and proposals capable of reinforcing digital trust in essential digital services (public or private) provided to citizens as well as the coherence



of the state's prerogatives in this area; (5) Identify the emerging international approaches aiming at making digital a universal right; (6) Develop an action plan to ensure the protection of citizens within the digital ecosystem.

At the end of the consultation, operational recommendations will be established by the closure of the first quarter of 2022.

Ongoing work on IoB (Internet of Behaviors) and behavioral data:

The CNDP has developed a doctrine around data protection and privacy in the form of deliberations. Its content has been developed in consultation with various actors (administrations, public bodies and professional federations) while taking into account international best practices in connection with the subject of each deliberation. The doctrinal deliberations of the

CNDP aim, inter alia, at supervising certain processing operations which may infringe the privacy and protection of the personal data of the persons concerned, such as those related to IoB (Internet of Behaviors) and behavioral data. In the event of consultations, CNDP meets with relevant stakeholders to examine the means in place to ensure the protection of personal data in Morocco, including of its foreign residents.

Get to know your ExCo

Turkish Personal Data Protection Authority has participated GPA activities as a member since 2017, and will be hosting 44th Conference this year.

Turkish Personal Data Protection Authority (KVKK) has participated GPA activities as a member since 2017 and our Authority will be hosting 44th Conference this year. In this sense, I would like to express my pleasure to be able to contribute to GPA as ExCo member.

We meticulously follow the works provided by the working groups established within GPA, which offer pioneering reports/guidelines in the field of personal data protection. Working groups that we are part of are as follows:

- Working Group on Global Standards and Framework,
- Working Group on Digital Economy,
- International Enforcement Working Group (IEWG),
- COVID-19 Related Privacy and Data Protection Issues

KVKK also undertook the responsibility of updating the Repository under IEWG, and duly

performed this duty in 2021.

Since being appointed as a member of the Personal Data Protection Board on 15 December 2016 by the President of Republic of Türkiye and elected as Chair of the Personal Data Protection Authority on 30 January 2017, I have always expressed that it is important to see the protection of personal data as a means and the protection of the person as a goal. Within this framework, we aim to promote public awareness and ensure the best practices by maintaining communication with the sectors through "Wednesday Seminars" held in our Authority, "Awareness Meetings" held in different provinces of Türkiye and "A Little Awareness is Enough" Podcast series, which started broadcasting on December, 2021. Aiming to create a new platform that enables sharing of relevant regulation and practices in the international arena, we organized



the "1st International Congress on Personal Data Protection" in November 2021 with the valuable contributions of the Chairs of foreign DPAs. Our Authority conducts promotional activities to develop data protection culture specifically for the youth and children such as the "Project to Raise Personal Data Protection Volunteers among University Youth" and a cartoon series called "Data Crew".

The Background of the Personal Data Protection Law No. 6698 and the Organizational Structure

Türkiye is one of the first signatories of the Convention No. 108 for the Protection of Individuals with regard to Automatic



Processing of Personal Data.

With the Turkish Criminal Code that came into force in 2005, types of crimes related to personal data have been regulated, and although there are tools in our legislation to ensure the protection of personal data, with the Constitutional amendment in 2010, protection of personal data has been recognized as a constitutional right and enshrined in the Constitution. Following the works on the Law

Everyone has the right to request the protection of his/her personal data (Article 20 of the Constitution of the Republic of Türkiye)

on the Personal Data Protection Law No. 6698, prepared by taking the Directive No 95/46/EC as a basis within the scope of the harmonization process with EU, was published in the Official Gazette on 7 April 2016. Our Authority also carries out works for the compliance with GDPR.

KVKK is a regulatory and supervisory authority, established to ensure the protection of personal data in Türkiye. Pursuant to Law No. 6698, KVKK, being established in Ankara, is a public legal entity with administrative and financial autonomy. Authority is composed of the Personal Data Protection Board and the Presidency. The Board, the decision making body, performs and exercises its duties and powers conferred on it under the Law independently. The Board consists of 9 members, including the Chair. The primary duties of the Board are; to carry out regulatory acts on the matters concerning the Board's field of duty and to examine whether the personal data is processed in compliance with the laws, upon complaint, or ex officio and impose sanctions in case of breach. Also, the Board adopts

resolutions and publishes them in cases where it is determined that the breach is widespread.

The Personal Data Protection Law observes the balance between freedom and security, technology and privacy, the interests of data controllers and the fundamental rights of data subjects. The Authority has issued numerous guidelines in order to ensure the implementation of the Law in an effective way. Some of the guidelines have been published so far can be listed as: Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence, Guide to the Right to Be Forgotten, Guidelines on Implementation of the Obligation to Inform, Guidelines on the Points to be Considered in the Processing of Biometric Data, Guideline on Personal Data Security (Technical and Organizational Measures). In addition, our Authority has also published the documents "False Facts I" and "False Facts II" to raise public awareness and clarify the issues that are determined to be frequently misapplied by the data controllers.

What matters most in the digital age is the use of advancement in technology for the benefit of humanity. In order to achieve this goal, cooperation among members becomes inevitable in a data-driven world.

KVKK in the International Area

KVKK, in addition to its role in GPA, actively contributes to various international platforms such as Global Privacy Enforcement Network (GPEN) and Spring Conference. Our Authority was also accepted to APPA with the observer status in 2021 and within this scope, it participated

in the 56th Forum hosted by The Office of the Information and Privacy Commissioner for British Columbia, Canada. The activities that our Authority is part of in the other international organizations are; G20 Digital Economy Task Force, OECD Working Party on Measurement and Analysis of the Digital Economy, OECD Working Party on Data Governance and Privacy in the Digital Economy, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108) Bureau Meetings, Digital Economy and Society Index of EU.

In a time where the cross-border data flows accelerate, it is of great importance to ensure cooperation among data protection authorities with the perspective of protecting personal data in a common understanding. Acting with this awareness, our Authority will continue to take an active part within the GPA and will be open to offers for cooperation.

KVKK as the Host of the 44th Conference

I hope that the 44th Conference, which we conduct the preparation process with great enthusiasm, will have wide participation and result in pioneering works in this field. Regards,

Prof. Dr. Faruk BİLİR

President Commissioner of KVKK



Meet our Member

Sami Mohammed, Commissioner of Data Protection, Abu Dhabi Global Market

Sami Mohammed, the first Emirati Commissioner to represent as a member of the GPA gives us an insight into his office and its role in shaping data protection in the United Arab Emirates.

Background

Abu Dhabi Global Market ("ADGM") is an international financial centre and financial free zone jurisdiction in the United Arab Emirates ("UAE"). The jurisdiction of the ADGM extends across the entire island of Al Maryah in Abu Dhabi.

Being a financial free zone means that UAE federal civil and commercial laws do not apply. Therefore, ADGM is able to create its own legal and regulatory framework for all civil and commercial matters on the Island. ADGM consists of four key public authorities. The Registration Authority, the Financial Services Regulatory Authority, the ADGM Authority and the ADGM Courts. Each Authority has specific mandates and together are responsible for regulating the jurisdiction. To date, there are over 4,000 entities established and licenced in ADGM with a total workforce of over 17,000.

Legal framework

Whilst UAE follows a hybrid system of Islamic and civil law, ADGM is a common law jurisdiction. The ADGM Courts headed by Chief

"Whilst UAE follows a hybrid system of Islamic and civil law, ADGM is a common law jurisdiction." "ADGM is unique in the region in that it directly applies English common law."

Justice the Rt. Hon Lord Hope of Craighead KT is responsible for the administration of justice in all civil and commercial matters on the Island.

ADGM Data Protection Regulations 2021

On the 11th February 2021, ADGM enacted the Data Protection Regulations 2021 ("DPR 2021"). The Office of Data Protection was formally established as the independent data protection supervisory authority following the enactment of DPR 2021. I was appointed Commissioner for a four-year term.

The DPR 2021 was benchmarked with international frameworks including the Council of Europe's Convention 108+, the EU GDPR and UK's Data Protection Act 2018.

The DPR 2021 provides my office with a range of enforcement powers which include the ability to levy fines of up to 28 million USD.

"The DPR 2021 equipped my office was the highest fines regime in the Middle East."

This demonstrates the importance ADGM places on the protection of personal data and individual rights.

My office will take a pragmatic approach but will not shy away from taking enforcement action where there has been a breach of the Law or the privacy rights and freedoms of data subjects are infringed.

My office recognises the importance of its role and obligations



as ADGM is home to many companies that undertake high risk processing activities in the areas of finance, technology, artificial intelligence and data analytics.

International Collaboration

Over the years I have been active in promoting data protection in the GCC and raising our profile internationally. I personally attended various in-person GPA Annual Assembly events in Hong Kong 2017, Brussels in 2018 and Tirana in 2019.

It is also important to note that ADGM has been an observer to the Council of Europe's Convention 108 since 2019. We were also the first in the Gulf to join the GPA's International Enforcement Cooperation Working Group (IECWG).

International cooperation is a key area for my Office. The processing and misuse of personal data is a global issue. In addition, many of us rely on technological solutions and services on a daily basis. Therefore, the cross border nature of information and data in key sectors and industries requires all of us to converge and build mechanisms for effective cooperation as authorities.



As Commissioner, I wish to reiterate my commitment to working closely with members and international partners for the interest of safeguarding individual rights.

Privacy in the Gulf

The right to privacy is not a new concept in the region. Privacy has been imbedded in Arab culture and traditions for centuries.

In many GCC countries including the UAE, the right to respect ones' privacy is treated seriously. For instance, capturing and using of photo of individuals without their consent is administered by law enforcement under the criminal provisions of the penal code in the UAE.

Following substantial economic growth in the Gulf and in light of the pandemic which has spurred digital transformation initiatives, Governments have been reviewing their laws to ensure privacy rights

are considered and addressed in the new working environments.

Within the GCC, Bahrain, Qatar, Saudi Arabia and most recently, the UAE has enacted a Federal Data Protection Law.

Due to our unique position within the landscape of the UAE, I alongside my counterpart in Dubai have been able to provide advice, support and guidance to relevant ministries on the development of laws and rules governing the processing of personal data.

We continue to shape data protection in the region through our meetings, cooperation and discussions with regional regulators and Governments across the GCC. We will continue to advance data protection in the region, and we look forward to working with other member authorities, international and multilateral bodies on privacy, data protection and individual rights.

DID YOU KNOW

Did you know that the majority of businesses regulated by the Office of Data Protection ADGM are non-financial?

Al Maryah Island is home to the Galleria Mall which consists of +300 retailers, luxury restaurants, hotels and tourism establishments. Also, the Island is home to the largest hospital in Abu Dhabi.



globalprivacyassembly.org



[PrivacyAssembly](#)



GPA

Global Privacy Assembly