

# Regulatory Strategies and Priorities of Data Protection Authorities in Latin America: 2024 and Beyond

Author: Maria Badillo and Momina Imran, FPF

Editor: Lee Matheson, FPF

May 2024

# Table of Contents

<b>1. Introduction</b>	<b>2</b>
<b>2. Regulatory Priorities</b>	<b>3</b>
<b>3. Enforcement Priorities</b>	<b>7</b>
<b>4. Advocacy &amp; Public Participation</b>	<b>10</b>
<b>5. Strengthening Institutional Capabilities</b>	<b>11</b>
<b>6. Conclusion</b>	<b>12</b>
<b>7. Annex 1: Overview of Strategic Topics per Jurisdiction</b>	<b>15</b>
<b>8. Annex 2: Overview of Strategies and Operational Plans per Jurisdiction</b>	<b>16</b>
Argentina	16
Brazil	19
Chile	25
Colombia	25
Mexico	26
Panama	28
Uruguay	29
Ibero-American Data Protection Network (RIPD)	29

---

# Regulatory Strategies and Priorities of Data Protection Authorities in Latin America: 2024 and Beyond

Author: Maria Badillo and Momina Imran, FPF, May 2024

## 1. Introduction

Privacy and personal data protection are widely recognized as fundamental rights in modern democracies. Most governments in Latin America have gradually recognized at least one of these rights in their constitutional and legal frameworks, with jurisdictions like Mexico and Brazil recognizing both of them as separate rights.<sup>1</sup> In parallel, some countries have also issued general data protection laws and created corresponding regulatory authorities.

The most active data protection authorities in the region are generally from the nations with the oldest data protection laws. Chile became the first Latin American country to enact a data protection law in 1999, followed by Argentina in 2000, Uruguay in 2008, Mexico in 2010, Peru in 2011, and Colombia in 2018, and all but Chile have created authorities that are active in the data protection regulatory space. This first set of data protection laws was largely inspired by the European Union's Directive 95/46, the predecessor of the General Data Protection Regulation (GDPR).

The 2016 passage of the EU's GDPR appears to have catalyzed a new wave of lawmaking in Latin America. In 2018, Brazil passed major legislation on data protection with the approval of the *Lei Geral de Proteção de Dados Pessoais* (LGPD), and in 2022 it recognized data protection as a fundamental right under the Brazilian Constitution.<sup>2</sup> Panama passed similar legislation in 2019, and other countries with "first generation" data protection laws such as Argentina and Colombia are actively looking to update their regulations to broaden the set of rights and include more stringent obligations.<sup>3</sup>

---

<sup>1</sup> The Mexican Constitution recognizes a right to privacy in Article 16, paragraph 1, and a right to data protection in paragraph 2. Similarly, the Brazilian Constitution recognizes the right to privacy and private life in Article 5, section X, and a right to data protection in section LXXIX.

<sup>2</sup> Amendment 11/2022, enacted in February 10, 2022, included the protection of personal data among the set of fundamental rights and guarantees in the Brazilian Constitution to establish exclusive competence of Congress to legislate on the protection and processing of personal data. See: <https://www2.camara.leg.br/legin/fed/emecon/2022/emendaconstitucional-115-10-fevereiro-2022-792285-publicacaooriginal-164624-pl.html>

<sup>3</sup> In June 2023, Argentina's Executive sent to Congress a proposal to update law 25.326 on the Protection of Personal Data and in August 2023, a data protection law proposal was introduced in the Chamber of Representatives in Colombia. See: <https://www.argentina.gob.ar/noticias/el-poder-ejecutivo-nacional-envio-al-congreso-el-proyecto-de-ley-de-proteccion-de-datos> and <https://www.camara.gov.co/proteccion-de-datos-personales>

Having updated frameworks for data protection and privacy is essential for modern democracies around the world. Data, including personal data, has become an invaluable asset for governments and private companies. In addition, the widespread adoption of technologies and the digitalization of services and products, including the increasing deployment of Artificial Intelligence (AI) across diverse services, demands more oversight of organizations' processing of personal information and more transparency and control of people over their personal data. Now more than ever, the role of data protection authorities is crucial to ensuring and safeguarding individuals' rights and interests concerning their personal information.

The objective of this Report is to provide an overview of the current and future work that data protection authorities in Latin America are focusing on, based on strategies, activity reports that look towards the future, and other announcements they made publicly available. It aims to identify trends and highlight commonalities regarding the issues and concerns prioritized by regulatory authorities in the region and showcase the diverse set of strategies they will deploy in coming years.

Although most countries in the region have at least a constitutional and legal framework for data protection, not all of them have a designated enforcement authority, and of the countries with authorities, not all have published a strategic plan. Therefore, the scope of this Report is limited to selected jurisdictions where there is (i) a designated data protection authority and (ii) such authority has issued a strategic or planning document.

The Report is divided into the following sections: **regulatory priorities, enforcement priorities, advocacy and public participation, strengthening institutional capabilities**, a **conclusion**, and two **annexes** containing a detailed **analysis of each jurisdiction's strategic plan**, and a **comparative table identifying the key topics and areas of focus for the covered DPAs**. This Report was produced via analysis of institutional planning documents issued by data protection authorities or other designated regulators, as well as other relevant guidance documents such as national strategies. With a few exceptions, the "strategic documents" cover 2024 and the following years.

The goal of this Report is to provide insight into the current and future expected activities of Latin American data privacy regulators. At the same time, the Report may be helpful in achieving other policy goals, such as increasing collaboration among authorities in the Latin American region, by showcasing shared strategic goals and commonalities of policymaking.

## 2. Regulatory Priorities

Updating existing data protection frameworks is a key concern for many regional authorities. In Argentina, Chile, and Colombia, proposals to update the data protection laws are already being considered by each

nation's respective legislature. Some DPAs, such as those from Argentina and Mexico, have also publicly prioritized the update of their data protection laws as an objective to actively work on in coming years.

In Argentina, the *Agencia de Acceso a la Información Pública* (AAIP) has been particularly active in the process: a proposed law was drafted by the AAIP and introduced in the national legislature after multiple consultations with the broader public and relevant stakeholders, and the AAIP continues to push for its adoption in national and international fora.<sup>4</sup> In Mexico, while the *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* (INAI) has not offered a specific proposal, the INAI has raised its concerns about the need to update the data protection framework.<sup>5</sup> Particularly, the INAI has mentioned that the data protection law applicable to the private sector, the Federal Law for the Protection of Personal Data in Possession of Private Parties (LFPDPPP), which dates back to 2010, must be revised and updated to maintain effective data protection.<sup>6</sup>

Some regulators have indicated that in coming years, they will focus more heavily on issuing secondary regulations, which necessarily supplement and expand primary laws. Secondary regulations are drafted under a legal mandate and are thus legally binding. For instance, Argentina's AAIP has indicated that, if the data protection bill is approved, the agency will contribute to drafting its secondary regulation (which must be issued by the Executive through a *Decreto Reglamentario*) that would complement the law.<sup>7</sup> Although the approval of the bill is uncertain for political reasons, the planning instrument of the AAIP envisions working on this secondary regulation around 2025.<sup>8</sup> In 2022, the AAIP approved a specific regulation updating the calculation and imposition of sanctions for violations of Argentina's existing data protection law, which

---

<sup>4</sup> In August 2022, the AAIP's President Beatriz Anchorena presented the data protection law proposal as a result of a months-long participatory process, which was later introduced in Congress in June 2023. See: <https://www.argentina.gob.ar/noticias/beatriz-anchorena-presento-la-actualizacion-de-la-ley-de-proteccion-de-datos-personales>

<sup>5</sup> On several occasions, INAI Commissioners have expressed at public events the need to update the data protection law in Mexico in order to tackle challenges brought by digitalization and the use of Artificial Intelligence. See: <https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-372-23.pdf> and <https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-054-24.pdf>

<sup>6</sup> As part of "Strategic Objective 3," on its strategic document the INAI plans to strengthen the right to data protection and its normative framework by "providing technical support and consulting in the process of updating the law" applicable to the private sector. See *INAI, Programa Institucional 2020-2024*, p. 91, available at: <https://micrositios.inai.org.mx/planeacion/images/pi/programainstitucional2021-2024.pdf>

<sup>7</sup> Although a Decreto Reglamentario is issued by the Executive, the AAIP considers working on the drafting of the proposal of this regulation; similarly as the AAIP did for the proposal of the data protection law.

<sup>8</sup> AAIP, *Plan Estratégico 2022-2026*, p. 23, available at: [https://www.argentina.gob.ar/sites/default/files/plan\\_estrategico\\_aaip\\_2022-2026.pdf](https://www.argentina.gob.ar/sites/default/files/plan_estrategico_aaip_2022-2026.pdf)

redefined the degree of severity for certain conducts (categorized from low to high severity).<sup>9</sup> Notably, another area where the AAIP intends to regulate in 2024 is on data protection and its relation with AI.<sup>10</sup>

Brazil has perhaps the most ambitious plan to adopt binding regulations in the near future. Its Regulatory Agenda,<sup>11</sup> which divides by phases the areas and activities that the *Autoridade Nacional de Proteção de Dados* (ANPD) will undertake in a year, contemplates that the agency will issue regulations for the application of sanctions, rights of personal data holders, incident reporting and notification periods,<sup>12</sup> international data transfers, personal data protection impact reports, and the role of personal data protection officers (DPOs) by early 2024.<sup>13</sup> Towards the end of 2025, the ANPD envisions issuing additional regulations on a broad range of topics related to the authority's terms for approving codes of conduct, standardizing technical, administrative, and security measures, and on the processing of sensitive and biometric data.

Another important element of a DPA's work is to provide clarity on legal concepts and provisions within existing law and regulation via the publication of regulatory guidance. This guidance, serving as a 'soft-law' tool, provides regulated entities with more certainty about the authority's interpretation of specific provisions and the application of the data protection framework in diverse contexts, and guides organizations on best practices. Some of the topics that DPAs have indicated that they will develop in upcoming guidance are the following:

- **Compliance and data subject rights (AR, BR, MX):** Argentina's AAIP indicates it will issue guidelines to support compliance with the current data protection law, and on data subject rights in particular.<sup>14</sup> Brazil's ANPD has also opened a public consultation on potential guidelines on the rights of data holders, with the aim to provide more certainty on the applicable LGPD provisions to controllers.<sup>15</sup>

---

<sup>9</sup> AAIP, Resolución 240/2022, Annex I and II, available at:

<https://www.boletinoficial.gob.ar/detalleAviso/primera/277165/20221205#:~:text=Resoluci%C3%B3n%20240%2F2022,-RESOL%2D2022%2D240&text=Que%2C%20asimismo%2C%20a%20trav%C3%A9s%20del,Registro%20Nacional%20%E2%80%9CNo%20llame%E2%80%9D>

<sup>10</sup> AAIP, *Plan Estratégico 2022-2026*, p. 23, available at:

[https://www.argentina.gob.ar/sites/default/files/plan\\_estrategico\\_aaip\\_2022-2026.pdf](https://www.argentina.gob.ar/sites/default/files/plan_estrategico_aaip_2022-2026.pdf)

<sup>11</sup> ANPD, *Agenda Regulatória 2023-2024*, available at:

<https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885>

<sup>12</sup> On April 26, 2024, the Board of Directors of the ANPD approved Resolution 15/2024 on the regulation of security incident reporting. Available in portuguese at:

<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>

<sup>13</sup> At the time of the publication of this Report, most of these guidance documents have not received final publication.

<sup>14</sup> AAIP, *Plan Estratégico 2022-2026*, p. 23, available at:

[https://www.argentina.gob.ar/sites/default/files/plan\\_estrategico\\_aaip\\_2022-2026.pdf](https://www.argentina.gob.ar/sites/default/files/plan_estrategico_aaip_2022-2026.pdf)

<sup>15</sup> The ANPD closed the period for contributions for this guidance on April 3, 2024. See:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/prorrogadas-consultas-sobre-guia-de-anonizacao-e-norma-de-direitos-dos-titulares>

Although Mexico's INAI has not specifically announced any plans to issue guidance on this topic, its planning document specifies that the Institute will seek to support the compliance and respect for data protection rights through the development of "strategic and civic education,"<sup>16</sup> which may ultimately result in guidance aimed at clarifying individual rights provisions. Finally, Colombia's action plan<sup>17</sup> does not make an explicit reference to data subject rights but it indicates that Colombia's SIC will issue guidance on personal data protection in general, which may include data subject rights.

- **Processing children and adolescents' personal data (AR, BR, CH):** Argentina recently issued a set of recommendations for the processing of personal data from children and adolescents under its 2022-2026 strategy.<sup>18</sup> Brazil is set to issue similar guidelines under the LGPD; the Brazilian authority has been active on this issue since 2022 when it prepared a preliminary study on the LGPD concept of "best interest of the child" and the legal hypotheses that would authorize the processing of children's personal data. Although Chile's SERNAC has not specifically committed to issuing guidance on the issue, it has identified e-commerce as an area of interest, placing a special focus on protecting the use of personal data of children and other vulnerable groups.
- **Marketing and dark patterns (CH):** Chile's SERNAC will prioritize marketing in the digital environment, pointing to dark patterns as a particular concern used to deceive consumers and affect the expression of their privacy preferences. Although the authority has not expressly committed to issuing guidance, SERNAC has issued interpretive documents after marking them as priorities in previous plans.<sup>19</sup>
- **Data protection officers (AR, BR, RIPD):** Both Argentina's AAIP and Brazil's ANPD have committed to providing guidance and training for data protection officers in both private and public sectors, including providing more clarity regarding when appointing a DPO is necessary. Notably, the Ibero-American Network also plans to prompt the development of the DPO figure as "an essential tool" to promote compliance, which may also be reflected in forthcoming guidance.

---

<sup>16</sup> INAI, *Programa Institucional 2020-2024*, p. 77-78, available at:

<https://micrositios.inai.org.mx/planeacion/images/pi/programainstitucional2021-2024.pdf>

<sup>17</sup> SIC, *Plan de Accion Institucional 2024*, available at:

<https://sedeelectronica.sic.gov.co/transparencia/planeacion/plan-de-accion-institucional/plan-de-accion-institucional-v3-0>

<sup>18</sup> AAIP, *Plan Estratégico 2022-2026*, available at:

[https://www.argentina.gob.ar/sites/default/files/plan\\_estrategico\\_aaip\\_2022-2026.pdf](https://www.argentina.gob.ar/sites/default/files/plan_estrategico_aaip_2022-2026.pdf)

<sup>19</sup> For instance, in 2022, the SERNAC published criteria regarding its interpretation of what constitutes abusive provisions in adhesion contracts in relation to personal data processing, and criteria for the protection of consumers in light of risks posed by the use of AI systems. See:

<https://www.sernac.cl/porta/618/w3-article-65388.html> and

<https://www.sernac.cl/porta/618/w3-article-64740.html>



- **Artificial Intelligence (AR, BR, CH, RIPD):** Under its current strategy, Argentina’s AAIP collaborated on a guidance document about the ethical uses of AI in the public sector, and issued guidance on the lawful processing of personal data through video surveillance and facial recognition systems.<sup>20</sup> Also, via a recently launched AI Program, the AAIP has committed to publish more guidelines and best practices on personal data protection in the context of AI. Relatedly, Brazil aims to clarify the ways in which data holders will be able to exercise their right to review automated decisions under Article 20 of the LGPD, provide more certainty on the applicability of the LGPD in the context of AI in general, and increase education levels of controllers and data holders related to AI. Chile’s SERNAC also released interpretive criteria for the protection of consumers and their data in the context of AI in 2022. Last but not least, the RIPD Plan calls for establishing common criteria in areas of special impact for data protection and privacy, such as AI.

### 3. Enforcement Priorities

Most strategic documents published by authorities in the region do not identify any specific priority area of policy for intended enforcement. However, many DPAs do signal an intent to implement their supervisory and inspection powers to ensure data controllers are complying with obligations under the data protection framework and handling data subjects' requests and complaints lawfully.

Brazil, Mexico, and Panama intend to facilitate enforcement by implementing accessible portals and simplified processes for receiving data subject complaints. Brazil’s ANPD, in particular, recently announced that it would be adopting a “simpler and more efficient” procedure that divides data holders’ requests into complaints and petitions, reduces the steps to file each of them, and improves the information provided on the ANPD’s website.<sup>21</sup>

Argentina, Brazil, and Colombia have all indicated they plan to safeguard data subject rights and guarantee their protection through an increased number of inspection visits and formal investigations. Colombia’s SIC, in particular, intends to follow up with investigations based on previous monitoring reports and verify compliance in the context of decisions made in *habeas data*<sup>22</sup> processes. Although the SIC does not specify the matter of such reports, in previous years, the authority has carried out investigations related to security

<sup>20</sup> AAIP, *Plan Estratégico 2022-2026*, available at:

[https://www.argentina.gob.ar/sites/default/files/plan\\_estrategico\\_aaip\\_2022-2026.pdf](https://www.argentina.gob.ar/sites/default/files/plan_estrategico_aaip_2022-2026.pdf)

<sup>21</sup> See ANPD, Press Release, April 2024, available at:

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ministerio-da-gestao-redesenham-processo-de-tratamento-de-requerimentos-de-titulares>

<sup>22</sup> Under Colombian law, *habeas data* is the right of an individual to access, update, and rectify their information contained in public and private records and databases. It has constitutional protection and the Supreme Court has linked it to the separate rights to privacy and access to information. See SIC, *Habeas Data*, available at: <https://www.sic.gov.co/manejo-de-informacion-personal>



incidents and compliance with related obligations to diverse platforms, such as Zoom, Facebook, Uber, and Avianca.<sup>23</sup>

Brazil also published its “Map of Priorities,” a detailed document highlighting the areas where it plans to focus its investigative and supervisory powers during 2024 and 2025.<sup>24</sup> Some of these areas include the following:

- **Rights in the financial and telecommunications sectors.** Brazil’s ANPD intends to inspect the processing activities of public authorities, digital platforms, and controllers in the financial and telecommunications sectors. During the first half of 2024, the ANPD will evaluate how to best coordinate with the Central Bank, the National Telecommunications Agency, and the National Consumer Secretariat. During the second half of 2024, the ANPD has set a target to carry out at least ten inspection activities in these sectors.
- **Processing of children and adolescents data in the digital environment.** During the second half of 2024, the ANPD also intends to carry out other inspections to verify that the processing of personal data in digital platforms is in compliance with the LGPD. In the second half of 2025, the ANPD then intends to propose safeguards to enhance the protection of children and adolescents’ data in the digital environment, including techniques for obtaining consent and age verification.
- **AI for facial recognition systems and personal data.** During the first half of 2025, the ANPD will carry out inspections on facial recognition systems, particularly seeking to identify and evaluate those used in public areas, reaching a significant number of data holders, or targeting vulnerable groups, including children and adolescents.
- **Data scraping and data aggregation.** In the first half of 2025, the ANPD will carry out at least three inspections of the processing operations of data aggregators and data scrapers. In the second half of 2025, based on such inspections, the ANPD will consolidate guidelines for the processing of personal data in the context of data scraping, and issue additional measures to ensure the processing is LGPD-compliant.

---

<sup>23</sup> See SIC, Press Release, January 2019, available at:

<https://www.sic.gov.co/superindustria-exige-a-facebook-fortalecer-medidas-de-seguridad-para-proteger-datos-personales-de-mas-de-31-millones-de-colombianos>; SIC, Press Release, June 2020, available at:

<https://www.sic.gov.co/slider/superindustria-ordena-la-plataforma-zoom-reforzar-medidas-de-seguridad-para-proteger-los-datos-personales-de-los-colombianos>; SIC, Press Release, November 2021, available at:

<https://www.sic.gov.co/boletin/juridico/habeas-data/se-abre-investigacion-avianca-sa-por-la-presunta-violacion-al-regimen-de-proteccion-de-datos-personales>; SIC, Press Release, September 2020, available at:

<https://www.sic.gov.co/slider/superindustria-ratifica-orden-uber-para-garantizar-seguridad-de-los-datos-personales-de-los-colombianos>

<sup>24</sup> ANPD, Resolution 10/2023, “Map of Priority Themes,” December 2023, available at:

<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528>

Chile's SERNAC identified e-commerce, digital marketing, and dark patterns as areas of interest in its 2023 strategic plan,<sup>25</sup> and may maintain those priorities into 2024 and beyond. As a result, SERNAC may open inspections to verify the lawful processing of personal data in the context of digital transactions and marketing with a special focus on children and other vulnerable groups. Moreover, the SERNAC has indicated it will continue to monitor activities related to new trends and consumer-related problems associated with digital transformation and the use of personal data. For instance, two specific issues recently identified by the consumer watchdog are the unlawful recording of individuals at gymnasiums, and commercial practices offering economic compensation in exchange for biometric information.<sup>26</sup>

The Ibero-American Data Protection Network (RIPD) also plans to support DPAs enforcement activities and potential collaborations. Concretely, the RIPD intends to identify real cases affecting individuals in jurisdictions from Members of the Network and facilitate enforcement cooperation among them.<sup>27</sup> The Network will also disseminate cases related to the unlawful processing of personal data by transnational enterprises, with the goal of identifying potentially similar cases in the region.<sup>28</sup> The RIPD aims to collaborate with authorities and courts to generate additional precedents to guide future data protection enforcement.<sup>29</sup>

Relatedly, the RIPD intends to enhance the Permanent Group of National Data Protection Authorities (GPAN), created in the XVII Annual Meeting of the Network, by establishing it as a forum where authorities can establish common guidance and criteria. Among other issues, this forum will prioritize the release of guidance on large-scale processing of personal data, including that related to internet of things and AI technologies.<sup>30</sup> Select working groups within the GPAN will be charged with broadly investigating issues with a strong global and regional impact. In 2023, the RIPD specifically created working groups to investigate the rise of neurotechnologies, digital violence and digital health, ChatGPT, and WorldCoin.<sup>31</sup>

---

<sup>25</sup> SERNAC, *Directrices Plan Anual De Fiscalización 2023*, available at: [https://www.sernac.cl/portal/618/articles-55703\\_archivo\\_01.pdf](https://www.sernac.cl/portal/618/articles-55703_archivo_01.pdf)

<sup>26</sup> For instance, the SERNAC has recently served all gymnasiums operating in Chile and requested to set up protocols for the unlawful recording of customers that may occur in their premises, and also opened an investigation to Worldcoin for their processing of sensitive and biometric data. See: <https://www.sernac.cl/portal/604/w3-article-79352.html> and <https://www.sernac.cl/portal/604/w3-article-79115.html>

<sup>27</sup> RIPD, *Plan Estratégico 2021-2025, Red Iberoamerica de Proteccion de Datos*, 2020, pp. 4-6, available at: <https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf>

<sup>28</sup> *Idem*, p. 6.

<sup>29</sup> *Idem*, pp. 7-8.

<sup>30</sup> *Idem*, p. 4.

<sup>31</sup> RIPD, "Final Declaration of the Meeting of the Ibero-American Network," 2023, p. 1, available at: <https://www.redipd.org/sites/default/files/2023-10/declaracion-encuentro-xx-aniversario-ripd.pdf>

## 4. Advocacy & Public Participation

Raising awareness of data protection issues remains a shared priority of the region's DPAs. These activities include public statements and social campaigns, training, and issuing guidelines and infographics, and are intended to target individuals, regulated entities, and public authorities. In addition, most DPAs prioritize including a participatory approach in their decision-making processes.

Argentina's AAIP has an ambitious agenda for enhancing the country's data protection culture. Between 2021 and 2026 the AAIP plans to focus on providing training for the development of privacy policies for the public sector and on privacy in the context of AI.<sup>32</sup> It has also committed to providing assistance to data controllers on more technical aspects such as interoperability, algorithmic transparency, the Internet, and their intersection with data protection.<sup>33</sup> Moreover, it will amplify current channels of communication to increase public participation in its policymaking.<sup>34</sup> In 2023, the AAIP developed a Registry for civil society organizations dedicated to the promotion and advocacy for data protection.<sup>35</sup>

Colombia's SIC has also recently prioritized the promotion and awareness of data protection. Its 2023 planning document identifies the need for the SIC to continue to develop educational resources covering data protection and the agency's mission and objectives.<sup>36</sup> A similar need was identified by Mexico's INAI, as awareness and education regarding data protection supports the public's trust and its credibility, which in turn can positively impact the exercise of data subject rights in Mexico.<sup>37</sup>

The INAI has also indicated that it will provide assistance and consulting to controllers and processors to facilitate compliance and safeguard data subject rights. In addition, the INAI will focus on improving public participation and work with civil society organizations where possible.<sup>38</sup> A major component of this goal is to increase INAI's presence in national and international fora.

For Mexico and Panama, another priority is the creation of digital repositories where practitioners, authorities, and individuals can access relevant information on data protection, such as guidance and relevant

---

<sup>32</sup> AAIP, *Plan Estratégico 2022-2026*, p. 19, available at:

[https://www.argentina.gob.ar/sites/default/files/plan\\_estrategico\\_aaip\\_2022-2026.pdf](https://www.argentina.gob.ar/sites/default/files/plan_estrategico_aaip_2022-2026.pdf)

<sup>33</sup> *Idem*, pp. 23-24.

<sup>34</sup> *Idem*, p. 12.

<sup>35</sup> *Idem*, p. 33

<sup>36</sup> SIC, "Institutional Action Plan - V3," 2024, available at:

<https://sedeelectronica.sic.gov.co/transparencia/planeacion/plan-de-accion-institucional/plan-de-accion-institucional-v3-0>

<sup>37</sup> INAI, *Programa Institucional 2020-2024*, p. 33, available at:

<https://micrositios.inai.org.mx/planeacion/images/pi/programainstitucional2021-2024.pdf>

<sup>38</sup> *Idem*, p. 33-34.

administrative and judicial precedents.<sup>39</sup> It is likely that other authorities in the region will work on similar projects, considering the RIPD plans to support the creation of national databases and repositories.

## 5. Strengthening Institutional Capabilities

A recurring priority in the agenda of regional DPAs is strengthening their institutional capabilities. Most authorities indicate they struggle with a shortage of resources to perform assigned duties. Thus, institutional and capacity building of DPAs is a priority for most authorities in the region.

Several data protection authorities in the region have a dual mandate to safeguard transparency and access to information and personal data protection. These agencies have to prioritize both mandates with a tight budget and limited personnel. Argentina's AAIP, Mexico's INAI, and Panama's ANTAI were all created as agencies with transparency mandates and later assigned the mandate to enforce data protection laws. Interference with a DPA's efforts in one area can impact the agency's credibility with the general public in the other areas of its operation. In this context, some authorities such as the INAI in Mexico seek to promote a data protection culture and inform individuals about the significance of the Institute as an independent body and how it safeguards their fundamental right to privacy and data protection.<sup>40</sup>

Both Argentina's AAIP and Mexico's INAI indicate that to achieve other goals, they must first strengthen their institutional reach and capacities. Under their current plans, both agencies prioritize the training of their personnel and signal an intention to review their management systems and technological infrastructure. In particular, the INAI intends to review its administrative processes to ensure resources are efficiently allocated as part of its 2021-2024 strategy.<sup>41</sup> Panama's ANTAI will prioritize the adoption of an institutional system based on results, and it will seek to amplify its territorial presence and influence in Panama.<sup>42</sup> Similarly, the RIPD has committed to the professionalization and training of public officials for member DPAs. The Network plans to provide assistance through online, specialized training and education programs for the management and capacity building of authorities.<sup>43</sup>

All DPAs covered in this Report acknowledge that an important element to achieving their goals is to increase their collaborative efforts with national and international authorities, especially when resources are

---

<sup>39</sup> ANTAI, *Plan Estratégico Institucional 2020-2024*, available at:

<https://www.antai.gob.pa/plan-estrategico-institucional-2020-2024/>

<sup>40</sup> INAI, *Programa Institucional 2020-2024*, p. 34, available at:

<https://micrositios.inai.org.mx/planeacion/images/pi/programainstitucional2021-2024.pdf>

<sup>41</sup> *Idem*, p. 97.

<sup>42</sup> ANTAI, *Plan Estratégico Institucional 2020-2024*, available at:

<https://www.antai.gob.pa/plan-estrategico-institucional-2020-2024/>

<sup>43</sup> RIPD, *Plan Estratégico 2021-2025*, *Red Iberoamerica de Protección de Datos*, 2020, pp. 5-6, available at:

<https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf>

limited. Brazil's ANPD has indicated it will collaborate with Brazil's Central Bank and the National Telecommunications Agency concerning its inspection activities in both sectors.<sup>44</sup> Argentina's AAIP also plans to collaborate with relevant stakeholders –including other public authorities – for the elaboration of guidance, particularly, to achieve the goals listed within its National AI Program. Mexico's INAI intends to continue to grow its presence in international fora as a way for the authority to learn from policies and best practices that might be applied to the Mexican data protection framework. In addition, the Colombian government intends to maximize the SIC's collaboration with other data protection agencies in Iberoamerica and Asia-Pacific.<sup>45</sup>

The Ibero-American Data Protection Network will prioritize strengthening its role in international fora such as the Global Privacy Assembly (GPA), promote the role of the Ibero-American representation in the Consultative Committee and in the Bureau of Convention 108 of the Council of Europe, and strengthen collaboration with other regional or international networks or organizations in which RIPD member authorities participate, such as the Ibero-American Transparency and Access to Information Network (RTA) and the Asia-Pacific Forum of Data Protection Authorities (APPA Forum).<sup>46</sup> The RIPD seeks to promote a specific action before the Inter-American Court of Human Rights to ensure that privacy and data protection are among its pronouncements and that issues of data processing are given greater presence in the judicial sphere.<sup>47</sup>

## 6. Conclusion

Most countries in Latin America recognize privacy and data protection as two separate rights deserving of constitutional and legal protection. While some of the data protection laws in the region are over two decades old, and not all provide for an independent data protection authority, these laws provide a general framework of principles, rights, and obligations concerning the processing of data of individuals.

Among countries with a supervisory authority in charge of enforcing the data protection laws and regulations, the levels of activity and enforcement differ. These differences can be explained by multiple factors, including the authority's legal composition and mandate, level of independence, resources, and maturity. However,

---

<sup>44</sup> ANPD, Resolution 10/2023, "Map of Priority Themes," December 2023, available at:

<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528>

<sup>45</sup> Colombia, *Ministerio de Comercio, Industria y Turismo, Plan Estratégico Sectorial 2023-2026*, pp. 21-22, available at:

[https://sedeelectronica.sic.gov.co/sites/default/files/planeacion/Plan\\_estrategico\\_sectorial\\_2023\\_2026.pdf](https://sedeelectronica.sic.gov.co/sites/default/files/planeacion/Plan_estrategico_sectorial_2023_2026.pdf)

<sup>46</sup> RIPD, *Plan Estratégico 2021-2025, Red Iberoamerica de Protección de Datos*, 2020, pp. 6-7, available at:

<https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf>

<sup>47</sup> RIPD, "Final Declaration of the Meeting of the Ibero-American Network," 2023, p. 2, available at:

<https://www.redipd.org/sites/default/files/2023-10/declaracion-encuentro-xx-aniversario-ripd.pdf>

DPA's across the region will undoubtedly have an active role in an increasingly digital society. This Report has sought to identify key topics and areas where DPAs will focus their resources in the coming years.

Analyzing the planning documents and agendas made available by the authorities of Argentina, Brazil, Chile, Colombia, Mexico, and Panama, and the multi-jurisdictional Ibero-American Data Protection Network, organizational priorities can be organized into the following categories: **regulatory priorities, enforcement priorities, institutional capacity building, and advocacy and public participation.**

For most jurisdictions examined, the most critical regulatory priority is to **update applicable data protection laws**. Argentina, Chile, and Colombia are all actively pursuing proposals to update their laws, and some of them have made progress in their respective legislatures. Argentina's DPA, the AAIP, has been particularly active in drafting new legislation that was recently introduced in Congress. Other DPAs, such as Mexico's INAI, have also voiced their support for an updated legislation that stays relevant to the challenges posed by the digital economy and AI. Another "strategic topic" in this category is the need for most DPAs to continue enacting guidance and other soft-law tools that help increase understanding and compliance with the data protection normative framework. Some areas subject to future guidance include **the processing of children's data** (AR, BR, CH, MX), **marketing and dark patterns** (CH), the role of **data protection officers** (AR, BR, RIPD), and **AI** (AR, BR, CH, RIPD).

Regarding enforcement, most DPAs reviewed agree on the need to increase their investigatory and sanctioning powers. Authorities acknowledge that the increasing reliance on personal data processing by multiple actors will continue to generate new risks and challenges in terms of data protection, making their mandate to protect privacy and data protection even more relevant. In that sense, some authorities indicate that they will focus on active monitoring and inspection where appropriate. Only Chile, Brazil, and the RIPD specify the areas in which they will focus this effort –including but not limited to, the financial and telecommunications sectors, AI systems in general, children and adolescent apps and platforms, and data scraping services.

Most authorities also recognize the need for **more awareness of data protection** in their respective jurisdictions. Most DPAs include this element as a primary, key goal that will help them achieve other objectives. For that purpose, DPAs will continue to organize **social awareness** campaigns, and issue **guidance** and other types of **educational materials** intended to inform individuals about their rights as data subjects. Relatedly, some authorities (including those in Panama and Mexico) intend to prioritize the **simplification of processes**, particularly for the presentation of data subject complaints, and decrease the time it takes to process them internally.

Lastly, a common priority is continuing to build **institutional capacity** while facing limited resources and time constraints. Similar to education and awareness-raising campaigns, the strengthening of institutional

capabilities is a crucial factor for achieving other objectives. In that sense, all but Brazil and Chile expressly indicate that they will continue to train personnel (not only from the DPA but also from other areas of government) and review the allocation of resources, to achieve efficiency. Importantly, for most DPAs an important goal is to continue to increase their **collaboration** with other sectoral agencies in their jurisdiction and other DPAs in the region.

---



## 7. Annex 1: Overview of Strategic Topics per Jurisdiction

	ARG	BR	CH	COL	MX	PAN	Ibero-American Data Protection Network (RIPD)
Data Subject Rights	✓	✓	✓		✓	✓	✓
Institutional Capacity Building	✓			✓	✓	✓	✓
Public Participation	✓	✓				✓	
National and International Cooperation	✓			✓	✓	✓	✓
Update Regulations	✓	✓		✓	✓	✓	✓
Training & Awareness	✓			✓	✓	✓	✓
Inspections & Sanctions		✓	✓	✓			
Incident Reporting	✓	✓			✓		✓
International Data Transfers	✓	✓		✓			✓
DPIAs		✓			✓		
Data processing by public entities		✓			✓		
Sensitive & Children's Data	✓	✓	✓				
Certification/Codes of Conduct		✓					✓
AI	✓	✓	✓				✓

## 8. Annex 2: Overview of Strategies and Operational Plans per Jurisdiction

### I. ARGENTINA

- **Materials:** AAIP's Strategic Plan 2022-2026 (Plan); National Program on Transparency and Data Protection in the Use of AI (National AI Program); Argentina's Digital Agenda; Decree 996/2018 (Digital Agenda)
- **Summary:**
  - **Plan:** The AAIP's Plan is based on several commitments made during Director Beatriz Anchorena's designation as General Director of the AAIP in 2022, and focuses on institutional strengthening; updating the data protection law through a participatory approach; increasing transparency goals, and creating open data mechanisms; and consolidating the Federal Transparency Council. These commitments are reflected in the Plan through four strategic objectives that will guide the agency's work during the covered period, such as:
    1. **Promoting and strengthening the exercise of data subject rights.** The AAIP intends to direct efforts to visualize and promote data subject rights and, secondly, to guarantee that regulated entities respect such rights. This includes increasing its investigatory powers through a greater number of inspection visits to regulated entities and official investigations, as well as providing technical assistance to entities and citizens. The authority also intends to issue guidance based on best practices that will support compliance with the Argentinean data protection framework and respect for data subject rights.

The Plan covers 2022-2026, and the AAIP has already achieved some of its stated goals. For instance, in 2022, the agency focused on a proposal to apply administrative sanctions for the violation of data protection regulations and to update the mechanisms for the imposition of sanctions. During 2023, it also updated Guidance regarding the National "Do-Not-Call" Registry and the National Registry of Challenged Identity Documents; defined a classification regulated entities under the Personal Data Protection Law, and provided technical assistance and consulting according to that classification — which it will continue through 2026.

For the following years, the AAIP plans to focus on the following actions:

- a. The design and implementation of the National Data Protection Plan for the public sector; (2023-2026)
- b. Providing greater education to parents, children, and educators about the relevance of data protection (2024)
- c. Providing training programs to Data Protection Officers and support for the development of privacy policies in the public sector (2024)
- d. Providing training programs for the protection of personal data in the context of AI (2025)

## **2. Widening the regulatory capabilities of the AAIP on a national and federal level.**

The agency intends to design and propose new tools for the government to exercise more autonomy and capacity to influence a global digital economy. This will include the consolidation of federal public policies to build a harmonized normative framework that respects the autonomy and jurisdiction of Argentinean provinces.

In particular, the AAIP considers an update of the Data Protection Law in Argentina an essential step towards achieving this goal, and the development of secondary regulations and guidance to complement the law of similar importance. It will also prioritize collaboration with other responsible stakeholders in data protection for the public sector. The agency will also maintain its commitment to participation in international fora.

In particular, the Plan indicates that the agency intends to invest in creating a collaborative document with the help of other agencies, academia, and civil society, regarding the ethical use of AI in the public sector and provide assistance and consulting in technical areas such as data governance, interoperability, internet, algorithmic transparency to other regulated entities.

In 2022, the AAIP presented Argentina's Congress a proposal to update the Data Protection Law (elaborated on through 2023 by the AAIP through a participatory process), supported the ratification of the additional protocol of Convention 108; and adopted a Resolution to update the model contractual clauses for international data transfers. In addition, the AAIP issued the guidance on several issues:

- a. Resolution about the security measures and incident reporting
- b. Guidance on the basic principles for the appropriate use of personal data in video surveillance and facial recognition systems

- c. Recommendations on the conditions that must be met to process children's data

In 2024, the AAIP intends to focus on reviewing and updating the list of countries that meet an adequate level of protection for international data transfers; issue a normative digest on data protection regulations, and issue new guidance concerning the protection of personal data in the context of AI.

In 2025, the AAIP envisions the issuance of the regulation complementing the new Data Protection Law, following its approval, and its continued participation in international fora, such as the work it has been leading since 2023 at the Sub-Committee of Strategic Direction of the Global Privacy Assembly.

**3. Promoting public participation.** The AAIP is committed to creating mechanisms to increase public participation in the creation of data protection policies. The AAIP has indicated it will focus efforts on assisting citizens and promoting the amplification and strengthening of channels of communication and mechanisms for public participation. In 2023, the AAIP developed a Registry for civil society organizations dedicated to the promotion and advocacy for data protection, which will be helpful for continued collaboration with civil society in the coming years.

**4. Strengthening institutional capacity.** Under the Plan, increasing the AAIP's capacity is essential for the completion of the other objectives, as the AAIP's operational and functional capacity, including its management systems and technological infrastructure, will need to be improved to meet its current and future goals.

- **National AI Program:** In September 2023, the AAIP created the National Program on Transparency and Data Protection in the Use of AI through Resolution 161/2013, which also outlines some of the actions and objectives that the agency will work on related to AI. The National AI Program will be a central component for guiding the development and use of AI in the country, both for the public and private sectors and it is composed of the following segments:

- **AI Observatory:** the AAIP will map the key actors in the development of AI from the public and private sectors, monitor the regional and global initiatives on AI regulation, and elaborate statistics and periodic reports on the matter.
- **Social participation and governance:** the data protection authority will also institutionalize a Multidisciplinary Council, composed of experts from diverse sectors,

for better consensus for policymaking. The AAIP will also continue to interact with other National agencies on this matter and create participatory spaces to discuss the potential negative impact of AI, from a human-rights perspective.

- **Capacity building:** the AAIP will issue guidelines on best practices for regulated entities for personal data protection in the context of AI, provide technical assistance and consulting, create awareness campaigns and educational resources for society, and document automated decision-making systems in Argentina.
- **Agenda:** The Argentine Republic, in adherence to the Declaration of the OECD Digital Economy Ministerial Meeting, signed in 2016, pledged to work together to preserve the internet's openness, reduce digital divides, promote digital skills, and deepen the potential of the digital economy. The Argentina Digital Agenda, decreed by the Executive, sets out the following objectives including, implementing adequate treatment of public and private information, developing cybersecurity capabilities to build trust in digital environments, and boosting the country's economic growth through digital development.

---

## II. BRAZIL

- **Materials:** Regulatory Agenda for the 2023-2024 Biennium (Agenda); Map of Priority Themes for the 2024-2025 Biennium (Map); Brazilian Digital Transformation Strategy (E-Digital) 2022-2026 Cycle (Digital Strategy)
- **Summary:**
  - **Agenda:** In November 2022, the ANPD's Board of Directors approved the Agenda, which is a planning instrument that brings together the actions that will be prioritized and studied by the agency during its validity period. The Agenda classifies the areas of priority into four phases, determined by their start date. Projects in Phase 1 (P1) are those that must be completed or finished under the 2021-2022 Regulatory Agenda; while Phase 2 (P2) projects will begin within a year of approval of the 2023-2024 Agenda, Phase 3 (P3) within a year and six months after, and Phase 4 (P4) within the next two years.

The ANPD will undertake the activities in the Agenda through several activities such as the issuance of regulations and standardization complementing the LGPD and other non-binding frameworks in the form of guidance, technical studies, and recommendations. The priority areas or topics addressed in the Agenda can be classified depending on the normative tool used by the ANPD, as follows:

### 1. Binding regulation and standards:

(P1)

- a. **Application of administrative sanctions.** The ANPD will define the methodologies for calculating the base value of fines and define the forms and parameters for the imposition of economic sanctions for violations of the LGPD.
- b. **Rights of personal data holders.** The agency acknowledges that while the LGPD provides for several rights for personal data holders through articles 9, 18, 20, and 23 LGPD, there are several points that deserve further clarification. In relation to this, the ANPD opened a public consultation in February 2024 on a proposed regulation on the rights of personal data holders and it mentioned that it is still considering whether this will be enforced through regulation or as non-binding guidance.<sup>48</sup>
- c. **Reporting incidents and notification period.** The ANPD indicates it will regulate Article 48 LGPD and related provisions that establish the obligation of the data controller to notify security incidents to the authority and data holders, by specifying the form, deadline, and minimum criteria when reporting these incidents. Accordingly, in December 2023, the ANPD issued a new form that seeks to simplify the process of communicating security incidents to the ANPD and data holders.<sup>49</sup> In April 2024, the ANPD approved the Regulation on Security Incident Reporting.<sup>50</sup>
- d. **International data transfers.** The authority will continue to work on complementary regulation of LGPD provisions related to international data transfers, in particular, but not limited to articles 33, 34, and 35 of the LGPD.
- e. **Personal data protection impact report.** Following the mandate under Article 55 LGPD, the ANPD will issue regulations on the elaboration of personal data protection reports in cases where the processing poses a high risk.
- f. **Personal data protection officers.** The ANPD will establish complementary rules on the definition and responsibilities of the data protection officer, including the hypotheses for waiving the need to appoint one.

(P2)

- g. **Criteria for ANPD's recognition of good practices and governance rules.** The ANPD will regulate the terms under which controllers are able to

---

<sup>48</sup> Available at: <https://www.gov.br/participamaibrasil/consulta-a-sociedade-sobre-os-direitos-dos-titulares>

<sup>49</sup> Available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/coordenacao-geral-de-fiscalizacao-da-anpd-divulga-novo-formulario-para-envio-de-comunicados-de-incidentes-de-seguranca>

<sup>50</sup> ANPD, "Resolution 15/2024, on Security Incident Reporting," available at: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>

formulate good practice and governance rules in relation to their processing activities. According to article 50 LGPD, controllers can, individually or through associations, formulate codes of good practice and governance rules for their organization and operations in relation to data processing activities, complaint handling mechanisms, security and technical standards, internal supervision, and risk management, among others. Such codes must be reviewed and recognized by the ANPD, according to its regulation.

**(P3)**

- h. Sensitive data and biometric data.** The Agenda indicates that the ANPD will focus on “necessary intervention,” whether through guidance or regulation, to clarify the context and situations in which the processing of sensitive personal data would be legitimate. Relatedly, the ANPD will provide further guidance, particularly for religious organizations, with the purpose of disseminating the basic measures that they can take to comply with the LGPD.
- i. Security, technical, and administrative measures.** Following article 46 LGPD, the ANPD will work on providing “minimum technical standards” that processing agents can adopt to prevent unauthorized access, loss, destruction, alteration to data, or any other form of inappropriate or unlawful processing. The standards will take into consideration the amount and type of information processed, the specific characteristics of the processing, and the current state of technology.

**(P4)**

- j. Conduct adjustment terms for sanctioning processes.** According to article 55-J, section XVII, of the LGPD, operators subject to an administrative process by the ANPD are able to enter into a commitment to eliminate the irregularity. In that context, the ANPD will issue further regulations to provide more information about how interested parties can enter into this commitment in the context of a sanctioning process.

**2. Guidelines and recommendations:**

**(P1)**

- a. Legal hypotheses for processing personal data.** The Agenda generally indicates that the ANPD will continue to guide the public on the legal basis for the processing of personal data described in Article 7 LGPD. Notably, the ANPD published in February 2024 its Guidance on legitimate interest, which



clarifies the applicability of this hypothesis as a lawful basis for the processing of personal data and provides more clarity on the agency's interpretation.<sup>51</sup>

- b. **Definition of “high risk” and “large scale.”** The ANPD will provide additional criteria for the definition of high-risk and large-scale concepts in the context of its Regulation for the applicability of the LGPD for small processing agents.<sup>52</sup>
- c. **Processing personal data for academic and research purposes.** The ANPD will work on a guiding document with recommendations and best practices supporting the processing of personal data for academic and research purposes, in a way that is compatible with the LGPD.
- d. **Anonymization and pseudonymization.** The agency plans on issuing guidance and clarifying the use of these techniques, in accordance with the LGPD.<sup>53</sup> In relation to this, the ANPD opened a public consultation on its draft guidance on anonymization and pseudonymization in January 2024, specifying that the guidance will take a risk-based approach and explore a variety of computational approaches for anonymization.<sup>54</sup>

**(P2)**

- e. **Data sharing by public authorities.** The LGPD determines that the ANPD will determine the form to publicize processing operations by public authorities, as well as contracts and agreements entered into with private entities. Therefore, the ANPD will seek to operationalize articles 26 and 27 of the LGPD, which regulate the procedures to be followed in public-private personal data sharing.
- f. **Processing children and adolescents' personal data.** Following previous work, the authority seeks to issue guidelines on the processing of personal

---

<sup>51</sup> ANPD, *Hipóteses legais de tratamento de dados pessoais: legítimo interesse*, available at: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia\\_legitimo\\_interesse.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf)

<sup>52</sup> As part of the process, on April 17, the ANPD opened a public consultation on its preliminary study on risk and large-scale processing for contributions from multistakeholders. See: <https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-a-sociedade-de-a-respeito-de-estudo-preliminar-sobre-alto-risco-e-larga-escala>

<sup>53</sup> The ANPD opened a public consultation period on its preliminary study on anonymization under the LGPD. The study is available at (in portuguese): [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo\\_tecnico\\_sobre\\_anonimizacao\\_de\\_dados\\_na\\_lgpd\\_uma\\_visao\\_de\\_processo\\_baseado\\_em\\_risco\\_e\\_tecnicas\\_computacionais.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais.pdf)

<sup>54</sup> The contribution period for the guidance on anonymization closed on March 14, 2024, after being extended. See: <https://www.gov.br/anpd/pt-br/assuntos/noticias/prorrogadas-consultas-sobre-guia-de-anonimizacao-e-norma-de-direitos-dos-titulares>

data from children and adolescents in accordance with the LGPD. Notably, the ANPD prepared a preliminary study and submitted it to public consultation in October 2022. The Guidance will particularly provide more clarity about the ANPD's interpretation of what can be considered as the "best interest of the children and adolescents" and the legal hypothesis that authorizes the processing of personal data of children.

- g. National Policy for the Protection of Personal Data.** Article 55-J, section III, authorizes the ANPD to issue guidelines for the implementation of a "National Policy of Personal Data Protection and Privacy." The National Policy intends to coordinate and direct the actions of all actors involved in the data protection ecosystem, including the ANPD. Thus, the guidelines will provide orientation on how the ANPD and other actors will coordinate and consider other public policies, such as the Brazilian Digital Strategy and the National Internet of Things Plan.

**(P3)**

- h. Artificial Intelligence.** The ANPD aims to provide more guidance in the context of personal data protection and AI. On one side, the ANPD intends to clarify the ways in which data holders will be able to exercise their right to review automated decisions under Article 20 LGPD. On the other side, the agency will also address the topic of AI and data protection to provide more certainty on the applicability of the LGPD in the context of AI, and increase the education and awareness levels on AI of both controllers and data holders. The studies and monitoring of the ANPD on the issue could develop more specific guidance related to AI in the future. Moreover, in 2023, the ANPD launched its "Sandbox on Data Protection and AI" with the intention of testing AI projects in a regulatory-controlled environment.
- **Map:** In December 2023, the Board of Directors approved the Map, with the aim of defining four (4) "priority themes" that will guide the agency's technical areas work during 2024-2025 and, in particular, the areas that will be more prone to inspection.
    - **Theme 1: Rights of data holders.** The ANPD will inspect the processing activities of public authorities, digital platforms, and controllers in the financial and telecommunications sectors, in particular. The Map indicates that, during the first half of 2024, the ANPD should evaluate the possibility of coordinating with other authorities, such as the Central Bank, the National Telecommunications Agency, and the National Consumer Secretariat, for the elaboration of guidance and other related activities in relation to the promotion and safeguard of data holders rights. Such guidance must be consolidated or decided within the second semester of 2025. In

addition, within the second half of 2024, the ANPD will also carry out at least ten inspection activities for the actors and sectors previously identified.

- **Theme 2: Processing of children and adolescents' data in the digital environment.** Within the second semester of 2024, the ANPD intends to carry out inspections to verify that the processing of personal data in digital platforms is in compliance with the LGPD. For the second half of 2025, the ANPD intends to propose safeguards directed to enhance the protection of children and adolescents' data in the digital environment, for example, with regard to techniques for obtaining consent and age verification.
  - **Theme 3: AI, facial recognition systems, and personal data.** During the first half of 2025, the ANPD will carry out inspections on facial recognition systems, particularly those used in public areas, reaching a significant number of data holders or targeting vulnerable groups, including children and adolescents.
  - **Theme 4: Data scraping and data aggregation.** In the first half of 2025, the ANPD will carry out at least three inspections of the processing operations of data aggregators and data scrapers. In the second half of 2025, based on such inspections, the ANPD will consolidate guidelines for the processing of personal data in the context of data scraping, and issue additional measures to ensure the processing is LGPD-compliant.
- **Digital Strategy:**
    - **Digital transformation of the economy:** The Ministry of Science, Technology and Innovations (MCTI), in collaboration with the Center for Strategic Studies and Management (CGEE), published the Digital Strategy. This strategy reflects that Brazil has adopted the conditional transfers model which seeks to strike a balance between the imperatives of personal data protection and the need for openness of data transfers. A few of the strategies planned to achieve this transformation include encouraging open innovation, data portability, and open data as tools for access to technologies, aiming at increasing the competitiveness of companies, and creating a national interoperability policy. It also includes improving mechanisms to protect rights in the digital environment, including aspects related to privacy and personal data protection.
-

### III. CHILE

- **Materials:** 2023 Inspection Program of the National Consumer Service Authority (SERNAC)
- **Summary:** Since 2021, the SERNAC has the competence to supervise the lawful processing of personal data in the context of consumer relations.<sup>55</sup>

The SERNAC published the “2023 Inspection Program” which sets out the criteria that the authority followed for conducting inspections that year. Although the SERNAC has not published the inspection program for 2024 or the following years, the 2023 program sheds light on some of the authority’s priorities during that year, which will probably follow in 2024 and the following years. In 2023, the SERNAC identified e-commerce as an area of interest where the agency sought to promote the rights of individuals, with a special focus on children and other vulnerable groups. In relation to this, the SERNAC indicated it would continue to monitor activities related to new trends and consumer-related problems associated with digital transformation and the use of personal data. Another theme prioritized by the SERNAC was publicity and marketing in the digital environment, where a particular concern was the increased use of dark patterns to deceive consumers and affect the expression of their privacy preferences.

Although the SERNAC has not published a specific plan or strategy for data protection, it issued two interpretative guidelines in 2022 related to the protection of consumers and their personal data in the context of AI, and criteria on fairness and personal data protection in adherence contracts.

---

### IV. COLOMBIA

- **Materials:** Sectoral Strategic Plan 2023-2026 of the Ministry of Commerce, Industry and Tourism (MINTIC); Institutional Action Plan 2024 of the Superintendent of Industry and Commerce (SIC)
- **Summary:**
  - **SIC’s Action Plan:** The 2024 Action Plan indicates the general objectives that the areas of the SIC will focus on during the year. Among these objectives are the promotion of the capabilities and powers of the Superintendent; strengthening its institutional capacity and improving its information management; optimizing the use of technological resources; generating synergies with other national and international agents to maximize institutional capabilities; and improving the SIC’s attention to procedures and services.

---

<sup>55</sup> Under Consumer Law (21.398) that came into effect in December 2021, the SERNAC has competence to protect consumers in relation to their personal data. This means the SERNAC can inspections, set criteria, and pursue compensation in collective cases where there has been a violation to the rights of data holders. See: <https://www.sernac.cl/portal/604/w3-propertyvalue-66795.html>

The activities that the SIC will prioritize during 2024, include:

1. **Harmonize data protection framework.** The SIC will direct efforts to harmonize the national data protection framework with other global and regional laws with the purpose of increasing and facilitating trade.
  2. **Interoperability and data portability.** The SIC will deploy a strategy to facilitate interoperability and data portability in the context of technology transfers for trade while ensuring the protection of personal data. individuals.
  3. **Data protection awareness and promotion.** The authority will organize events dedicated to promoting a culture of data protection and raising awareness and education about the SIC's mission and objectives.
  4. **Issuing guidance on personal data protection.** The SIC's Action Plan does not specify the topics or issues to be addressed in its forthcoming guidance.
  5. **Inspection activities.** The SIC intends to initiate investigations based on previous monitoring reports and verify compliance with respect to decision issues on habeas data procedures.
- **MINTIC's Strategic Plan:** Relevant for guiding the work of the SIC is the strategy defined by the MINTIC, to which the Superintendence is adhered to. According to MINTIC's strategy, the government needs to focus on the "internationalization" of Colombia as a main objective during 2023-2026. The strategy indicates that in order to improve the exportation levels of Colombia it is necessary to strengthen relationships on a jurisdictional and institutional level. For that matter, among other activities, the Plan mandates regulatory convergence of the SIC, particularly with data protection authorities from the Asia-Pacific and Iberoamerican regions. At least two (2) collaborations in favor of the application of data protection regulations must be achieved during the Plan's implementation period.

---

## V. MEXICO

- **Materials:** INAI Institutional Program 2021-2024
- **Summary:** The Institutional Program is the principal planning tool that will guide the regulatory and institutional activities of the Institute throughout a specific period. During 2021-2024, the INAI committed to focus on reaching the following objectives:

1. **Ensure compliance with the right to personal data protection.** The INAI will focus on providing assistance and consulting to regulated entities to ensure they comply with their legal obligations and respect the rights of personal data subjects. Relatedly, the authority intends to manage its processes more efficiently, through the improvement of the time it takes to process complaints and procedures.
2. **Promote the exercise of data subject rights.** The INAI intends to strengthen the exercise of data subject rights through the promotion of its policies throughout the population. For that purpose, the agency will work on consolidating actions to improve public participation and collaboration forums with civil society organizations. Relatedly, the INAI intends to contribute to the design and development of a “strategic and civic education” in relation to personal data protection on a national level.

The INAI also intends to achieve this goal by increasing its presence and leadership in international forums, as a way to learn from the experience of its counterparts in other countries. In particular, the INAI intends to identify potential policies in data protection that can be similarly implemented in Mexico, propose collaboration agreements with other jurisdictions and international organizations, and prepare the necessary components for the adoption of the additional protocol of Convention 108 by Mexico and postulate for a declaration of adequacy by the European Union.

3. **Strengthen procedures and mechanisms for data protection in the public and private sectors.** For this purpose, the INAI plans to make the processing of procedures more transparent and efficient. In addition, it seeks to create sensibilization in the private sector with the purpose of promoting the protection, safeguarding, and access to the personal data of individuals.

The INAI also intends to update the technological capacity of the Institute in order to facilitate the exercise of rights by individuals and diminish waiting times for the processing of complaints. Relatedly, the Institute indicates it will work on tools that help with the elaboration of personal data protection impact reports, including the use of formats and documents that facilitate the presentation of such reports, while providing assistance to those reporting.

4. **Strengthen the data protection normative framework.** The authority intends to elaborate studies and regulation proposals on data protection that are in line with current needs in the digital environment to provide enhanced protection to individuals. The INAI announced it will also work on a digital repository containing relevant information regarding privacy and data protection, and related matters. Finally, the Institute remains committed to providing support

for the update of the data protection framework, especially the law applicable to the private sector, which dates to 2010; and help with the analysis of regional and state frameworks to ensure they are aligned with the Mexican Constitution and international treaties.

- 5. Boost organizational performance and promote public service with a human rights and gender perspective.** With this strategic objective, the Institute aims to ensure that all the administrative processes are using resources efficiently. The Institute aims to increase its organizational performance through training of its public officials and improving its management systems.

---

## VI. PANAMA

- **Materials:** ANTAI Strategic Institutional Plan 2020-2024
- **Summary:** From ANTAI's Strategic Plan we can highlight the following pillars, that has guided the agency's work since 2020 and will continue to 2024:
  - **Guaranteeing and promoting rights and a culture of data protection.** The ANTAI aims to promote the right to data protection through a set of actions with the purpose of sensitizing and raising awareness about the matter in the general public, providing training and assistance to public officials to increase their knowledge and expertise in the area, and improving social communication campaigns. To safeguard the right to data protection, the authority also intends to establish mechanisms for the exercise of the rights of data holders; for instance, the ANTAI plans to implement a unified portal where individuals can present requests and complaints in an easy and effective manner. Moreover, the ANTAI aims to work on a repository where individuals and regulated entities can consult interpretative precedent from the ANTAI and judicial decisions on data protection. Lastly, the authority contributed to this objective through the formulation of the secondary regulation of Law 81 on Personal Data Protection, issued in 2019, and in force since 2021.
  - **Strengthening institutional capabilities.** To reach this goal, the ANTAI aims to improve on its structural organization, adopt a management system based on results, and amplify the territorial presence of the agency throughout the country.



## VII. URUGUAY

- **Materials:** Uruguay Digital Agenda 2025 (Agenda)
- **Summary:** The Uruguay Presidency published its Agenda which sets out the direction of the strategic priorities which will promote a digital society and inclusion of digital technologies in all sectors of public policy.
  - **Digital Citizenship:** The agenda aims to ensure that all people can acquire competency and skills in the digital environment and that such skills are incorporated into formal education.
  - **Community Integration:** To allow citizens to use digital technologies as tools for social integration, promote access to knowledge, achieve digital accessibility of services, and design a digital inclusion strategy for rural populations.
  - **New Strategies for Employment:** To enable working conditions that are adapted to the digital era, by providing vocational guidance and training, expanding educational offers in technological careers, etc.
  - **A Simpler State to Interact with:** For the state to collaborate with economic development, transform services, coordinate and incorporate the internet of things in the provision of public services such as water, energy, communications, etc.
  - **Digital Transformation in Productive Sectors:** To achieve sustainable development of strategic productive sectors, to promote competitiveness.
  - **Transparency, Efficiency, and Stewardship of the Public Sector:** Optimize the use of data as a key factor for effective decision-making and efficient public management, taking into account aspects of ethics, privacy, etc.
  - **Universal Quality Connectivity:** To guarantee quality physical and mobile connectivity throughout the national territory, minimizing geographic inequalities in the access and use of telecommunications by individuals and companies.

---

## VIII. IBERO-AMERICAN DATA PROTECTION NETWORK (RIPD)

- **Materials:**
  - Strategic Plan 2021-2025 Ibero-American Data Protection Network (“RIPD Plan”)
  - Final Declaration of the Meeting of the Ibero-American Network on the Occasion of the 20th Anniversary of RIPD (“Declaration”)
  - Implementation Guide on Model Contractual Clauses for International Personal Data Transfers (“MCC Guide”)
- **Summary:**

○ **RIPD Plan:**

- Following the approval of the RIPD 2020 strategic document, which was approved at Montevideo in November 2016 and has met its main objectives, the RIPD Plan for the years 2021-2025 is designed to be oriented towards the expansion of the scope of the influence of the RIPD, continue to strengthen its institutionality as well as its international projection.
- To continue promoting a regulatory framework for regional convergence. This includes giving special priority to the Personal Data Protection Standards for Ibero-American States approved by the RIPD in 2017. Additionally, it seeks to promote supranational or regional regulatory frameworks that contribute to the objective of regional integration, while giving special consideration to the cooperation framework of Convention 108 of the Council of Europe.
- The RIPD Plan calls for enhancing the role of the Permanent Group of National Data Protection Authorities (GPAN) created by way of the XVII Ibero-American Data Protection Meeting as a specific forum for Ibero-American Authorities to establish common criteria in areas of special impact for privacy, especially new technologies for massive processing of personal data such as Big Data, Internet of Things, and Artificial Intelligence. It also seeks the development of innovation units or divisions for Authorities to stay informed of the latest technological developments.
- **Institutionalization and Professionalization of the Authorities** – To promote collaboration or "networked" work between the Authorities and their employees, especially for training activities and for the creation of databases or common repositories as tools for their day-to-day management. Additionally, this involves the development of online (specialized) training and education programs for the management and employees of the Authorities.
- **Investigations into Cases that Impact Data Subjects** – To identify real cases affecting citizens of countries in the network so that the Authorities in all or most countries can respond ex officio and from their countries to such situations, and to disseminate resolution of cases related to unlawful access of personal data in order to create precedents in such areas.
- **Leadership in the International Scenario** – To strengthen the role of the RIPD in the Global Privacy Assembly (GPA), promote the role of the Ibero-American representation in the Consultative Committee and in the Bureau of Convention 108 of the Council of Europe, and strengthen collaboration with other regional or international networks or organizations in which RIPD member authorities participate, such as the Ibero-American Transparency and Access to Information Network (RTA) and the Asia-Pacific Forum of Data Protection Authorities (APPA Forum).

- **Innovation, Data Protection, and Social Responsibility (Sustainability)** – To promote the initiatives of the Control Authorities to combat “digital violence” against women and minors, as well as in the workplace. This also includes the development of digital education in school curricula and reinforcement of the principle of “privacy by design.”
  - **Greater Presence of Data Protection in the Judicial Sphere** – The RIPD Plan seeks to promote a specific action before the Inter-American Court of Human Rights to ensure that privacy and data protection are among its pronouncements and that issues of data processing are given greater presence in the judicial sphere.
  - **Certification Schemes** - The RIPD Plan also aims to establish a network for collaboration with privacy professionals at the regional level and to explore the possibility of a Certification Scheme within the framework of objectives of the RIPD.
  - **Compliance** - To promote compliance in the public figure, it seeks to strengthen collaboration between the RIPD and the Ibero-American Transparency and Access to Information Network (RTA).
  - **Data Protection Delegate** - It also prompts the development of the figure of the Data Protection Delegate as an essential tool to promote legal compliance with the obligations of companies in the area of data protection.
- **Declaration:**
- The Final Declaration of the Meeting of the Ibero-American Network on the 20th Anniversary of RIPD was made in Guatemala on September 20, 2023. It agreed to formulate changes to the internal rules.
  - Creates an exclusive collaboration space for national and regional DPAs to share criteria and practices for decision-making on specific issues, specific working groups on issues with a strong global impact such as Neurodata, Digital Violence and Digital Health, ChatGPT, and WorldCoin have been approved, and strengthens the institutional framework of the RIPD.
  - The Executive Committee’s presidency will continue to be held by INAI (Mexico), and four members: Argentina, Uruguay, Peru, and Colombia. It also welcomes new state-level members and observers including the San Luis Potosi Authority (Mexico), the Nuevo Leon Authority (Mexico), and the Ombudsman of Buenos Aires (Argentina) as members, and the UN Rapporteurship on Privacy as an observer.
  - The Declaration also promotes initiatives such as defining harmonized model clauses between the RIPD and the European Commission, for international data transfers to favor the exchange of information. This also includes collaboration with the Inter-American Executive Committee of the Organization of American States, to promote the right to data protection among its members.

- Lastly, the Declaration approved a declaration on neuro-rights by which the RIPD adheres to two declarations of the Inter-American Juridical Committee of the OAS including the Declaration on “Neuroscience, Neurotechnologies and Human Rights: New Legal Challenges for the Americas” of August 2021 and The “Declaration of Inter-American Principles on Neurosciences, Neurotechnologies and Human Rights” of March 2023.
-



Washington, DC | Brussels | Singapore | Tel Aviv

[info@fpf.org](mailto:info@fpf.org)

[FPF.org](http://FPF.org)