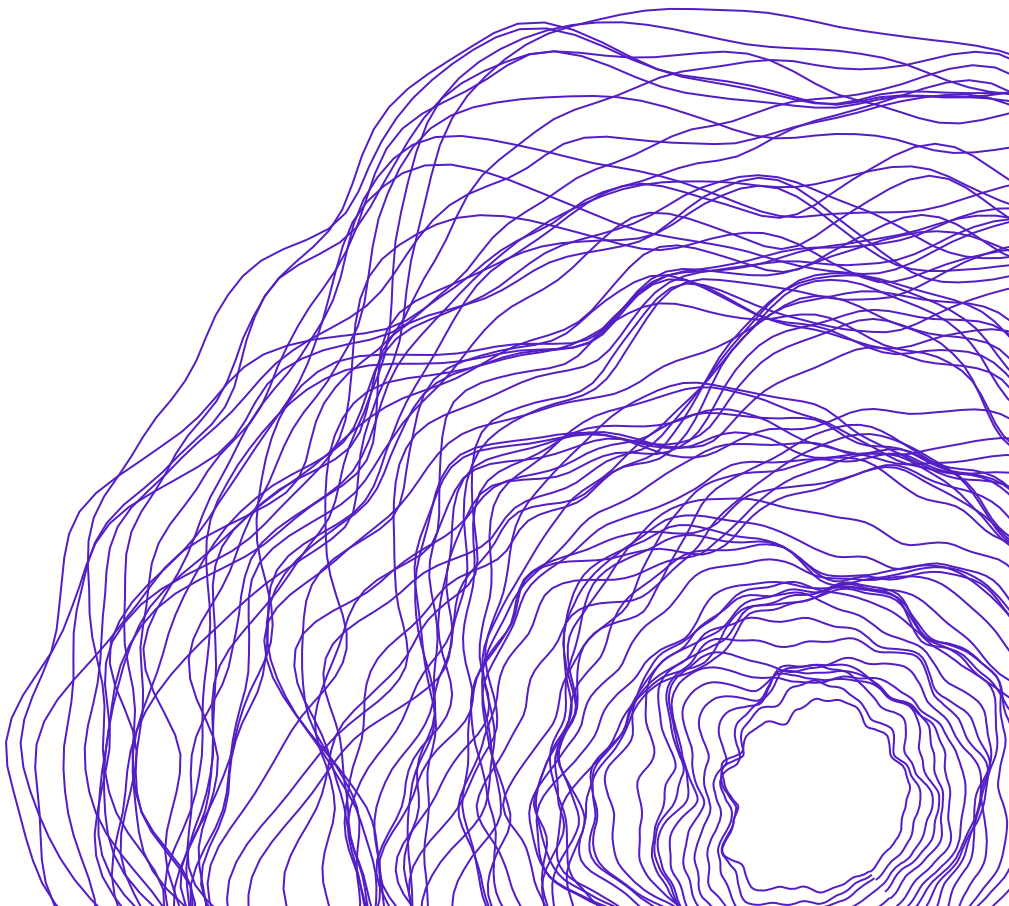
adapt

Understanding the Challenges Data Protection Regulators Face: A Global Struggle Towards Implementation, Independence, & Enforcement

Pawel Popiel & Laura Schwartz-Henderson

With Forward by Eduardo Bertoni



About This Report

Since 2018, over sixty countries around the world have enacted or proposed new data protection laws, with those numbers steadily increasing each year. Data protection regulatory bodies and agencies are entrusted with massive responsibilities to enforce these newly passed laws across all sectors of society- often while significantly under-resourced with small budgets and skeleton staff. Many countries continue to grapple with the issue of independence, as these bodies are frequently housed within, funded by, or connected to ministries and executive offices while also tasked to ensure government entities and political parties comply with the law.

In late 2021, Internews' ADAPT project brought together a group representing data protection regulatory authorities (DPAs) in 11 countries across Africa and Latin America for a roundtable to discuss the challenges that they face in setting up, implementing, and enforcing newly created data protection laws as well as to brainstorm best practices and opportunities for cross-border collaboration. Building on this conversation and drawing on additional interviews with regulators and key informants from civil society, this report seeks to outline the key challenges faced by DPAs and areas for support and information sharing.

The authors would like to thank all of the participants from the roundtable and interviews, and particularly highlight the feedback and contributions from Eduardo Bertoni, Rafael Zanatta, Luã Cruz, Khadijah El-Usman, Hlengiwe Dube, Benjamin Whitehead, and Skyler Sallick

Table of Contents

A BRIEF FORWARD FROM THE PERSPECTIVE OF A FORMER DPA 3

INTRODUCTION 7

CHALLENGES FACING DPAS 9

Establishing a Data Protection Authority 10

Implementing a data protection framework 11

Structuring a DPA 14

Balancing institutional growth and regulatory oversight 16

Adequate Funding and Capacity 17

Ensuring Independence 18

Compliance and Raising Awareness 21

Enforcement 23

Emerging Policy Issues 26

Collaboration with Other DPAs, Regulatory Agencies, & Civil Society 27

Collaboration with other DPAs 27

Collaboration with domestic regulatory agencies 31

Collaboration with civil society organizations 32

BEST PRACTICES AND RECOMMENDATIONS TO CONFRONT CHALLENCES FACING DPAS ... 34

1. *Advocating for DPA independence from the start bolsters independence in the future* 34
2. *Ensuring local values and needs are balanced with baseline data protection from the start is essential to DPA legitimacy and effectiveness* 34
3. *Collaboration with civil society is essential to basic DPA functions and legitimacy* 35
4. *Collaboration among DPAs can pool resources, build awareness, and strengthen enforcement* 35
5. *Strategic targeting and framing of messaging, and building relationships between DPAs and the media can help raise awareness* 36
6. *Collaboration with other regulatory agencies, adopting a risk-based approach, and strengthening the judicial system can bolster enforcement* 37
7. *Funding education programs to cultivate local expertise and public awareness* 37
8. *Cultivating domestic and regional civil society networks can strengthen enforcement investigations* ... 38
9. *Cultivating open civic spaces and building local networks of policy stakeholders can protect and bolster DPA independence and accountability* 38

ABOUT THE AUTHORS 39

A brief forward from the perspective of a former DPA

I am pleased to have been asked to write the introduction to this report on the challenges that data protection regulators face in Africa and Latin America. The report is based on conversations and debate we initiated during a multi-lingual workshop I was invited to facilitate with 11 regulators from Africa and Latin America. The resulting report seeks to distill some of the main takeaways from this conversation, with the authors building on the topics discussed during this event including follow-up interviews with expert stakeholders from both regions. While the following report excellently describes and catalogues a variety of issues DPAs must confront- such as independence, funding, technical capacity and expertise, and enforcement challenges-, I thought the best way to enter into a discussion on these challenges would be to tell a more personal story about what I have witnessed as an advocate and a regulator in Latin America, and more specifically in Argentina, where I headed the Data Protection Authority from 2016 to 2020.

As I mentioned in another work, [1] over the past twenty years, several countries in Latin America have enacted their own data protection laws and, in many cases, these laws have followed standards that were and still are being developed in the European Union. Despite that, only a few of those countries -namely, Uruguay, Argentina and Mexico- have acceded to the Convention 108. Moreover, fewer countries -only Uruguay and Argentina- have been granted by "adequacy decisions" which are regularly determined by the European Commission and approved by the European Union.

The benefits for those who obtain these decisions, are, among others, enabling free data flows between the EU and those countries in accordance with the Data Protection Directive 95/46/EC (hereinafter 'Directive'). It may not be a coincidence that two of the three countries that have ratified the treaty (Convention 108) have also been considered adequate by the European Union. In this sense, it might be important to mention that Convention 108 and the GDPR, are two pieces of the same puzzle that has been influencing many of the reforms.

Many of the new data protections laws were inspired both by the GDPR and the Convention 108. However, passing regulations that meet these international standards has not been an easy work. The standards are often mismatched with regulatory capacity, and the reforms needed are very important. Moreover, there are many challenges to confront before having laws that comply with the international standards. Many of those challenges are often, of course, politically, and economically motivated.

The history of the Argentine personal data protection law demonstrates two of the most important challenges facing data protection authorities in Latin América and in Africa.

[1] Eduardo Bertoni, "Convention 108 and the GDPR: Trends and Perspectives in Latin America," *Computer Law & Security Review* 40 (April 2021): 105516, https://doi.org/10.1016/j.clsr.2020.105516.

The first challenge relates to designing the office to be independent, both in practice and in regulation. The second challenge is linked to the "strength" that data protection authorities have to enforce the law.

Briefly, the story is as follows: Argentina reformed its Constitution in 1994. The reform introduced Article 43, which states:

Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired.

Shortly before the beginning of the 21st century, a strong debate had begun in Argentina to approve a law that would regulate concretely this article 43 of the Constitution. So, in 2000, the Congress approved a personal data protection bill that included two issues that I want to highlight.

The first issue refers to the fact that the project approved by Congress included the existence of a specific office in charge of controlling compliance with the law. But in addition, the law designated who was in charge of that office - a Director appointed by the President and approved by the Senate- to ensure independence and autonomy.

The second issue concerns fines. For many reasons that are not related to this conversation, Argentina at that time had a stable economy where the equivalence between the US dollar and the Argentine peso was 1u$s=1AR$. Politicians at the time were convinced that parity between the US dollar and the Argentine peso would last a long time. For that reason, many of the laws that were approved at that time - when they expressed the amounts of the fines - did not include ways to update them over time. The maximum fine that was included in the bill was AR$100,000.

In Argentina, once a project is approved in Congress, it is sent to the President of the Nation for his approval or his right to veto. The veto can be total or partial. At that time -in the year 2000- the President of Argentina partially vetoed the law and annulled the article defining the design of the data protection authority. According to the Decree Nº995/2000 signed by the President, the reason for the veto was related to budgetary issues.

Vetoing just that part of the article creates a problem: the law mentioned in general the existence of a body to oversee the new data protection law, but, because of the veto, the law did not provide details about that oversight body.

In other words, the result of the veto was clear: Argentina had a personal data protection law that said there was an office in charge of enforcing it, but it did not describe who was in charge of that office, how he or she might be appointed or dismissed, or where

that office would be situated. For this reason, the following year, the President, when regulating the law, created that office, but as a Directorate within the Ministry of Justice and Human Rights. The Director of the office could be appointed or dismissed by the Minister of Justice like any other employee.

For this reason, the independence and autonomy of the data protection authority was greatly affected, raising international concerns about the real independence of the newly created DPA. Despite this poor regulation, Argentina argued before the European Union and the Council of Europe that the office had been acting independently. Those arguments were successful at the time, and Argentina was considered a country with adequate legislation. Compounding this very acute issue with the structural independence of the DPA, inflation in Argentina over the last 20 years increased substantially. There is no longer that parity between the Argentine peso and the US dollar. Therefore, the maximum fine that can be imposed today by the data protection authority in Argentina is barely five hundred US dollars.

Over many years, myself as well as other experts and advocates continued to argue that a change in regulation was urgently needed and demanded. This finally happened in 2017. We were able to change the regulations necessary to include the DPA under the framework of the then newly created National Access to Information Agency, an independent office created by law with its own budget and with the specific clarification that the Director could not be fired by the President without having an agreement of the Congress.

The history of the Argentine law and the evolution of the DPA, one of the first in the region, leaves several lessons for all the countries that are designing or implementing new laws.

New data protection laws must be constructed through significant consultation and consensus among the different stakeholders (civil society, private sector, academia, and also some specific government offices, like Central Banks, Tax offices, etc.) so that the data protection authority is independent and autonomous and that this is stated in the law. When designing data protection laws, the importance of the independence of data protection authorities cannot be undervalued and there is a need for clear mechanisms for compliance with the law. Data protection laws must be strong but also flexible for future technological, political, and economic changes. Fines also must be dissuasive such that those who are tempted to break the law do not do so.

To be clear: the lessons learned from the Argentina case are much more than those mentioned above, but I cannot under-emphasize the importance of the independence of the DPA, particularly the following key points:

- Independence of the DPA is key for the success of any data protection regulation.
- Independence must be guaranteed by law.

- Independence must be accepted in practice by different stakeholders.
- Independence also means giving the DPAs enough resources to comply with their duties.
- Independence also means having a staff with enough expertise to conduct serious investigations.

But the work ahead does not stop with these many issues. The advances in technology are very fast now. In addition, in this era, possible violations of the personal data located in a country may occur outside the borders where the data protection authorities of those countries are located. It is therefore necessary to generate mechanisms that allow DPAs to carry out cross-border investigations, and even impose sanctions on companies not located in their territories. The following report seeks to aggregate the perspectives from several regulators, experts, and advocates to better understand how some of these challenges play out in different jurisdictions. At the end of the report, we have also distilled some of the suggested best practices for individual DPAs as well as for collaboration across regulatory agencies and civil societies within and across countries. We hope that this report can be used as a tool by advocates, policymakers, and regulators at all stages of the legislative and regulatory process.

Building laws and regulatory structures commensurate to the complex and ever-evolving task of protecting citizens' data is not an easy task. But it is well worth a try. The protection of personal data is closely related to the human right to privacy. Therefore, when we work to prevent violations of a human right, any effort and creativity is welcome.

adapt

Introduction

As a result of the growing diffusion of internet access in Global South regions and the rapid expansion and integration of global data economies,[2] regional data flows implicate more users across a growing range of daily activities. While participation in these economies can afford greater innovation and economic growth along with other potential benefits, it also introduces significant harms. For instance, the expansion of data infrastructures has increased the capacity for state surveillance projects, including the accumulation of individuals' personal data.[3] Similarly, the growing use of data by private and public sectors poses increased cybersecurity concerns and raises key questions about the accountability of data controllers and processors.[4] The attendant and expanding collection of data by a growing range of private entities—from social media companies to commercial banks and credit bureaus—compounds these security concerns, while intensifying risks of behavioral targeting and data inaccuracy, which may result in the discriminatory provision of key public and private services.[5]

Data protection frameworks and the regulatory agencies that enforce them are essential mechanisms for governing these data flows. However, despite considerable progress in the Global South to implement such frameworks, lags persist. Currently, 71 percent of the countries in the world have some data protection legislation, including 73 percent in Latin America, while in Africa and Asia 61 percent and 57 percent do, respectively.[6] Since the European Union's General Data Protection Regulation (GDPR) legislation has set the global standard for data protection regulation, failure to impose equally robust protections economically marginalizes Global South countries that lack them, while heightening local risks of surveillance, unconsented collection of data, and data misuse.[7] Moreover, in countries that have passed such legislation, as in the majority of Latin

[2] UNECLAC, "Data, Algorithms and Policies: Redefining the Digital World" (UN Economic Commission for Latin America and the Caribbean (ECLAC), April 2018), https://repositorio.cepal.org/bitstream/handle/11362/43515/7/S1800052_en.pdf; Héctor J Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean" (Santiago: UN Economic Commission for Latin America and the Caribbean (ECLAC), 2019), https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf.

[3] Lukman Adebisi Abdulrauf and Charles Manga Fombad, "Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms," *Liverpool Law Review* 38, no. 2 (2017): 105–34, https://doi.org/10.1007/s10991-016-9189-8.

[4] Ibid.

[5] Ibid.

[6] UNCTAD, "Data Protection and Privacy Legislation Worldwide," United Nations Conference on Trade and Development (UNCTAD), accessed April 30, 2022, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[7] Justin Bryant, "Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights," *Stanford Law Review* 24 (2021): 389–439; Cara Mannion, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets," *Vanderbilt Law Review* 53, no. 2 (2020): 685–711.

America, existing data protection frameworks vary in scope, implementation, and level of enforcement.[8]

The task of ensuring compliance with data protection laws, which often requires educating the public and the private sector about privacy rights and data obligations, falls to Data Protection Authorities (DPAs). These regulatory bodies—often, though not always, established with the passage of data protection legislation—face a series of challenges in the Global South that impact their operational capacity, enforcement capability, and regulatory independence. Many factors contribute to these challenges, including resource constraints, limited digital literacy among the public, inexperienced courts, and skeptical policymakers.

To illuminate and assess factors, this report examines the challenges facing DPAs in Africa and Latin America. The report's analysis draws on findings from research that involved two stages. The first stage consisted of desk research collating work by experts, including data regulators, data protection advocates, and academics on implementing and enforcing data protection frameworks in the Global South. For the second stage, as part of its ADAPT (Advocating for Data Accountability, Protection and Transparency) project, Internews convened a roundtable of data protection regulators from Argentina, Brazil, Burkina Faso, Chile, Mauritius, Morocco, Niger, Peru, South Africa, and Uganda in November 2021. This recorded discussion was translated, transcribed, and coded, and its themes serve as the basis for the topics and issues discussed in this report. The insights from the roundtable discussion were also supplemented with eight interviews with current and former DPA regulators, some of whom participated in the roundtable, as well as civil society representatives from both regions. The roundtable and interview participants' responses are anonymized in the report.

Both research stages involved identifying concrete challenges facing DPAs in implementing and enforcing data protection frameworks as well as best practices to address them. Although the report foregrounds shared challenges facing DPAs in Africa and Latin America, it also highlights meaningful differences both between and within these two regions. However, despite assessing understudied obstacles to data protection in a sample of African and Latin American countries, this report has geographical limitations. Future research should include perspectives from other regions to broaden the account of both unique and shared challenges by DPAs in the Global South.

Drawing on the desk research and qualitative roundtable and interview data, this report assesses challenges related to:

1) Establishing a DPA

[8] DLA Piper, "DLA Piper Global Data Protection Laws of the World - World Map," DATA PROTECTION LAWS OF THE WORLD, 2022, https://www.dlapiperdataprotection.com/index.html.

2) DPAs' funding and capacity
3) Independence in structure and decision-making
4) Compliance and raising awareness
5) Enforcement
6) Tackling emerging policy issues
7) Collaboration within and across regions with other DPAs and with civil society

Among these, two prominent factors emerged as key obstacles to effective data protection oversight in the two regions examined in this report: resource constraints and threats to independence. Resource constraints undermine DPAs' ability to raise awareness about data protection laws, recruit experts, conduct investigations, and pursue enforcement actions, particularly against big tech companies. Threats to independence often compound resource constraints, particularly when a DPA's parent organization or the executive branch of the government controls the budget. They also undermine effective enforcement, especially of the public sector, which increasingly engages in data collection and processing in many countries in the region.

The report also identifies essential best practices and recommendations aimed at tackling these challenges. In particular, the interviewees highlighted collaboration between regional DPAs and between DPAs and civil society as especially useful strategies for raising public and private sector awareness, pooling resources, sharing best practices, increasing expertise, and assisting with litigation and enforcement. Moreover, such policy networks can also foster mutual accountability, potentially offsetting or reducing threats to DPA independence. Interviewees also noted that a related priority involves bolstering regional education to facilitate the cultivation of local expertise and community-level awareness of data protection rights and laws. Such expertise and familiarity are essential to effective enforcement, high compliance with data protection regulations, and to making data protection issues as political and social priorities.

Challenges Facing DPAs

Data protection frameworks have proliferated in Africa and Latin America within the last decade. The adoption of these frameworks and the establishment of DPAs occurred partly in response to the pressures created by the passage of the GDPR and, especially in Latin America, the Council of Europe's (CoE) international data protection treaty Convention 108, ratified by countries like Argentina, Cabo Verde, and Uruguay.[9] These

[9] Eduardo Bertoni, "Convention 108 and the GDPR: Trends and Perspectives in Latin America," *Computer Law & Security Review* 40 (April 2021): 105516, https://doi.org/10.1016/j.clsr.2020.105516; Council of Europe, "Chart of Signatures and Ratifications of Treaty 108," Council of Europe, 2022, https://www.coe.int/en/web/conventions/full-list; Council of Europe, "Chart of Signatures and Ratifications

legal and regulatory processes have also been accelerated by the growing technological diffusion in the two regions. However, progress has been uneven and data protection frameworks range in scope and robustness. For instance, in Latin America, Brazil has led by passing the GDPR-inspired General Personal Data Protection Law (LGPD), while Argentina has not updated its pre-GDPR legislation.[10] In Africa, countries like Rwanda and Zambia passed their first data protection legislation in 2021, while Cabo Verde and Burkina Faso updated their existing laws, with the former exceeding certain GDPR requirements.[11] Similarly, countries with existing frameworks like Kenya and South Africa issued new regulations.[12] However, many laws in the region do not guarantee basic rights like privacy and new ones like data portability, or provide key accountability measures, like requirements for documenting data processing.[13]

While drafting robust legislation and establishing an effective DPA are the foundation of strong data protection, countries in Africa and Latin America face or have faced a range of challenges in these initial stages, from securing political support to ensuring regulatory independence. Once established, DPAs must traverse barriers to securing regulatory compliance, including significant resource constraints that hamper enforcement, limited sanction mechanisms, and judicial inexperience; lack of public awareness about privacy laws, and data protection rights and obligations; and occasional state interventions that undermine their regulatory independence and legitimacy. Such obstacles serve as a counterpoint to the promising expansion of data protection frameworks in Africa and Latin America. These barriers must be addressed to maximize the benefits of regional participation in global data economies on terms that reflect local values and needs, while minimizing associated harms.

Establishing a Data Protection Authority

Central challenges in establishing DPAs relate to building initial political support, drafting and passing strong data protection frameworks, and structuring the agency. First, policymakers must draft and pass legislation that establishes a data protection

of Treaty 223," Council of Europe, 2022, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223; Ceyhun Necati Pehlivan, "Editorial: Data Protection in Latin America: An Overview," *Global Privacy Law Review* 2, no. 2 (2021): 102–7.

[10] Eduardo Bertoni's introduction to this report discusses the Argentinean framework in more detail. See also, Gilberto Martins de Almeida, "International: A Brief Perspective on Data Protection in Latin America," DataGuidance, January 2022, https://www.dataguidance.com/opinion/international-brief-perspective-data-protection; Katitza Rodriguez and Veridiana Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain," Electronic Frontier Foundation, September 21, 2020, https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain.

[11] Aissatou Sylla, "Recent Developments in African Data Protection Laws – Outlook for 2022," Hogan Logells Engage, February 1, 2022, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2022_1_1.

[12] Ibid.

[13] Idris Ademuyiwa and Adedeji Adeniran, "Assessing Digitalization and Data Governance Issues in Africa," CIGI Papers No. 244 (Waterloo, Canada: Centre for International Governance Innovation (CIGI), July 2020), https://www.cigionline.org/static/documents/documents/no244_0.pdf.

framework, and define the structure, mandate, and scope of the DPA that will implement and enforce this framework. The first step in this process requires convincing the government, the public, and the private sector that robust data protection should be a political priority, often amid other pressing goals. Cultivating this support represents a key challenge, particularly in Africa where fewer data protection laws have been passed than in other regions and where significant gaps in public awareness of data protection issues persist.

Drafting a data protection framework also requires input from local experts on international data protection regulation and on data-intensive technologies and markets to ensure such legislation is not only comprehensive, but also attuned to local contexts, needs, and values. This expertise is especially crucial for navigating the immense influence EU's regulatory frameworks exert on international data protection, and for establishing DPAs that represent local political, economic, and social interests. However, the scarcity of such experts, particularly prominent in Africa, represents another key challenge to establishing a DPA. Absent such expertise, legislation that defines DPAs' structure can lack clarity. This absence of organizational clarity may hamper building out a new DPA's institutional capacity, which regulators often must engage in while performing their daily regulatory work of fulfilling the data protection mandate. This dual work, in turn, can significantly strain already limited resources. Moreover, absent such clarity, DPAs may face threats to independence or lack sufficiently broad mandates to balance data protection with related regulatory domains, like access to information, undermining effective enforcement. These challenges emerged as a key theme in the interviews, reflecting concerns of both African and Latin American regulators.

Implementing a data protection framework

Although many countries in Africa and Latin America provide constitutionally guaranteed rights to privacy,[14] one of the major obstacles to establishing DPAs involves convincing political elites that data protection should be a national priority. This represents a significant challenge especially in Africa, where developmental issues and economic growth have historically taken precedence over other concerns.[15] Concurrently, governments view data protection bills with caution, especially if the activities they mandate could encroach on state surveillance activities or expand public data access rights.[16] Consequently, several African and Latin American data protection

[14] Ademola Adeyoju, "International: Data Privacy Harmonisation in Africa - Progress, Challenges, and Predictions," DataGuidance, December 9, 2020, https://www.dataguidance.com/opinion/international-data-privacy-harmonisation-africa; Rodriguez and Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain."

[15] Alex Boniface Makulilo, "Privacy and Data Protection in Africa: A State of the Art," *International Data Privacy Law* 2, no. 3 (2012): 163–78, https://doi.org/10.1093/idpl/ips014; Abdulrauf and Fombad, "Personal Data Protection in Nigeria."

[16] Abdulrauf and Fombad, "Personal Data Protection in Nigeria"; Bryant, "Africa in the Information Age."

frameworks have exemptions for often vague categories like national security, intelligence services, and the public sector more broadly.[17]

The challenge of prioritizing data protection amid other political goals can be compounded by policymakers' lack of expertise with privacy and data regulation. Key barriers to cultivating this expertise include the migration of skilled workers abroad or to the private sector, as well as the regional scarcity of higher education institutions that provide technology policy training, especially salient in Africa.[18] The lack of expertise inhibits drafting robust data protection frameworks, which often establish DPAs and define their regulatory scope. For example, efforts to draft legislation in Nigeria, which has no legal framework for data protection, lacked expert involvement resulting in cases of "cut and paste,"[19] namely contracting non-specialized lawyers who copied foreign privacy laws. This process produced weak or inconsistent draft bills, none of which has passed. Furthermore, policymakers issued no official reports and public statements on data protection, which are crucial to building support for such legislation.[20] South Africa's efforts to pass the Protection of Personal Information Act No. 4 of 2013 (POPIA), which updated the country's data protection framework, followed similar patterns: politicians showed little interest in advancing the legislation, whose content "was partly drawn from other countries, with limited customization"[21] and whose passage was very slow. Such cases stand in contrast with the seasoned and durable networks of regulatory experts that interviewees described in countries like Argentina, Brazil, Chile, and Colombia, suggesting expertise is unevenly distributed between and within Africa and Latin America.

As these African experiences suggest, absent local expertise, policymakers seeking to establish DPAs may end up emulating foreign, particularly European, data protection models. However, other factors contribute to such policy transfer. International data protection regulations often are influenced by Global North frameworks, specifically the EU's GDPR, which is considered the gold standard, and Convention 108, particularly in Latin America. In addition to the GDPR's reputational prominence, the draw of the EU's sizeable market means that tech companies are likely to comply with the law rather than to forgo doing business in Europe. Since the GDPR is stricter than most privacy laws and

[17] Tara Davis, "Data Protection in Africa: A Look at OGP Member Progress" (Open Government Partnership (OGP), Altadvisory.Africa, August 2021), https://www.opengovpartnership.org/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf; Rodriguez and Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain"; Abdulrauf and Fombad, "Personal Data Protection in Nigeria"; Mpho Ngoepe, "Balancing and Reconciling the Conflicting Values of Information Access and Personal Data Laws in South Africa," in *Information Knowledge and Technology for Development in Africa*, ed. D. N. Ocholloa, N. D. Evans, and J. Britz (Cape Town: AOSIS, 2021), 71–84, https://uir.unisa.ac.za/handle/10500/28429; Ewan Sutherland, "The Governance of Data Protection in South Africa," *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3922218.

[18] Makulilo, "Privacy and Data Protection in Africa"; Mannion, "Data Imperialism."

[19] Abdulrauf and Fombad, "Personal Data Protection in Nigeria," 124.

[20] Abdulrauf and Fombad, "Personal Data Protection in Nigeria."

[21] Sutherland, "The Governance of Data Protection in South Africa," 14.

since it applies to any company that processes the data of EU citizens, strong incentives exist not only for non-EU firms to comply with it, but also for national data protection frameworks to harmonize with it. This "Brussels Effect,"[22] namely Europe's international regulatory influence, inevitably shapes data protection frameworks in the Global South, especially since the costs of noncompliance, namely being shut out of European markets, will disproportionately impact poorer developing countries.[23]

Although countries in Africa and Latin America seek harmonization with the GDPR—especially adequacy decisions granted by the EU to compliant nations, which facilitate cross-border data transfers[24]—potential challenges arise here as well. First, notions of privacy differ across political and social contexts, raising the risk of incongruities and incompatibilities in policy translation of concepts like data rights. Simply copying the GDPR to facilitate cross-border data flows may subjugate regional and local values and needs to those embodied in EU's framework, which centers the interests of EU citizens.[25] Yet, technology practices vary. For instance, smartphone uses drastically differ across the Global South,[26] social privacy boundaries may be blurrier than in Europe, and key legal concepts like "personal data" and "digital identity" also have different local referents.[27] While the Western conceptualization reflected in the GDPR embraces an individualized right to privacy, Global South countries may prioritize communal and relational dimensions of privacy rights.[28] Moreover, they may balance privacy rights with other rights differently than Western countries, for instance prioritizing rights to water or healthcare that reflect local values and needs.[29] Failure to reconcile data protection goals with local needs can intensify the limited public awareness of and support for data protection that regulators observe and decry. For instance, one African data protection regulator stated: "you still hear people who wonder whether privacy and data protection are important." This regulator noted that limited awareness is especially prominent in rural areas and among the low-education, including illiterate, population. Another African regulator put it more bluntly: "Some people think that data protection is mainly

[22] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York, NY: Oxford University Press, 2020).
[23] Mannion, "Data Imperialism"; Adeyoju, "Data Privacy Harmonisation in Africa."
[24] Devika Kornbacher et al., "21. Demonstrating Compliance with Data Privacy Legislation," LatinLawyer, August 3, 2021, https://latinlawyer.com/guide/the-guide-corporate-compliance/second-edition/article/21-demonstrating-compliance-data-privacy-legislation.
[25] Bryant, "Africa in the Information Age."
[26] Daniel Miller et al., *The Global Smartphone: Beyond a Youth Technology* (UCL Press, 2021), https://doi.org/10.2307/j.ctv1b0fvh1; Seyram Avle, Emmanuel Quartey, and David Hutchful, "Research on Mobile Phone Data in the Global South: Opportunities and Challenges," in *The Oxford Handbook of Networked Communication*, by Seyram Avle, Emmanuel Quartey, and David Hutchful, ed. Brooke Foucault Welles and Sandra González-Bailón (Oxford University Press, 2020), 487–509, https://doi.org/10.1093/oxfordhb/9780190460518.013.33.
[27] Martins de Almeida, "Data Protection in Latin America."
[28] Davis, "Data Protection in Africa: A Look at OGP Member Progress"; Martins de Almeida, "Data Protection in Latin America"; Makulilo, "Privacy and Data Protection in Africa."
[29] Davis, "Data Protection in Africa: A Look at OGP Member Progress."

for the rich." Yet more than just limited public understanding, such attitudes likely also reflect the challenges of reconciling foreign data protection models with local contexts and needs. Second, the GDPR was built on 30 years of legal precedent, which many countries in these regions lack when they draft new data protection legislation. Relatedly, the EU wields immense resources to implement and enforce its framework, which is impractical for developing countries that face significant budgetary constraints.[30] Finally, some experts argue that imposing a stringent data protection framework like the GDPR too quickly may thwart local innovation key to regional economic growth and international competition.[31]

More problematically, data protection laws are sometimes funded or drafted by external actors with troubling consequences.[32] As one African policy actor recounted,

> [p]eople who are not living in country, write the laws and the government is then [pressured] to pass the law in order to access either aid or additional aid. Very often those things are linked, and it becomes a tick box exercise that the law is on the statute books. When you try and actually enforce it or have any kind of implementation mechanism, you'll find that no one's been given a budget for it.[33]

Furthermore, external imposition of data protection laws and simply copying them can contribute to a "transplant effect," namely low demand for laws foreign to a nation's residents, including because of perceived illegitimacy, resulting in poor implementation.[34] Thus, policymakers establishing local data protection frameworks face key tradeoffs between baseline harmonization with international standards—essential to regulatory predictability for businesses operating transnationally, for instance—and local expectations and priorities, which may outrank data protection issues.

Structuring a DPA

Passing robust, legitimate data protection laws sets the foundation for effective DPAs, but it remains only the first step. In fact, although such laws often establish DPAs,[35] this is not always the case; for example, some African countries do not have DPAs despite

[30] Michael Pisa and Ugonma Nwankwo, "Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development" (Center for Global Development (CGD), August 2021), https://www.cgdev.org/sites/default/files/are-current-models-data-protection-fit-purpose-understanding-consequences-economic.pdf; Mannion, "Data Imperialism."
[31] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[32] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[33] Ibid., 62.
[34] Bryant, "Africa in the Information Age."
[35] Davis, "Data Protection in Africa: A Look at OGP Member Progress"; Kornbacher et al., "21. Demonstrating Compliance with Data Privacy Legislation"; Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean."

having data protection legislation.[36] Moreover, national legislation does not always specify a DPA's structure or its funding mechanism, as in the case of Côte d'Ivoire, Ghana, and Malawi.[37] Consequently, DPAs vary in age, organizational structure, and mandate, among other dimensions.

The absence of legislative clarity on such key factors—particularly structure and budget—can serve as a significant obstacle to the agency's subsequent function. For instance, several roundtable participants noted the consequences of legislation that establishes DPAs within or under another regulatory body as opposed to as a standalone agency, including competition for resources, the lack of a clear mandate, and constraints on independence,[38] as explored in more detail in subsequent sections of this report. A related structural issue highlighted by participants concerned whether legislation established DPAs with a single mandate or a dual one, which combines data protection oversight with related regulatory areas like information access and free speech. Single mandate DPAs, as one Latin American regulator argued, can create challenges in harmonizing laws governing information flows:

> We are also facing a very hard challenge [...] trying to harmonize the [...] general data protection law with [...] access to public information laws [...] [I]f you could concentrate the enforcement powers in a single entity, maybe this harmonization would be easier.

Conversely, a dual mandate DPA, as one African regulator argued, "works for us because the right to privacy has to be always balanced against freedom of expression and access to information." DPAs with dual mandates, like in Argentina and South Africa, have a dedicated regulator with authority over data protection, transparency, and information access. In some cases, a transparency regulator is charged with data protection or vice versa, and the order of expanding the mandate influences how the DPA reconciles the often conflicting goals between data protection and transparency.[39] As one policy expert described drafting data protection legislation in Africa, "you start with secrecy—that's exactly the wrong starting point [since] many countries who now have these lovely model laws on privacy and data protection, have shocking laws on media freedom, freedom of expression, access to the internet."[40] Since data protection can encroach on information flows, striking the right balance in a way that reflects local contexts is essential to effective frameworks.

[36] Pam Dixon, "ROUNDTABLE OF AFRICAN DATA PROTECTION AUTHORITIES: Status and Response to Privacy Risks in Identity Systems," in *ID4AFRICA 5TH ANNUAL CONFERENCE* (Johannesburg, South Africa: The Round Table of African Data Protection Authorities (RADPA, 2019), 13, https://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf.
[37] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[38] see also Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[39] Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean."
[40] Davis, "Data Protection in Africa: A Look at OGP Member Progress," 23.

Balancing institutional growth and regulatory oversight

Once a DPA is legally established, regulators may face challenges in balancing the organizational work of establishing the regulatory institution with the legally required work of data protection oversight. As one civil society actor working closely on data protection in Latin America noted, DPA regulators "don't really have time to set up their own their own institution [...] and to keep up [with] their work [that] they're legally obligated to do, which is to investigate these issues, investigate problems, release recommendations." An African academic and civil society activist echoed these concerns about her country's DPA:

> They are recruiting personnel and building a structure, and this is happening at the same time when they are expected to hit the ground running. There is no time to process or to say, 'We're building ourselves as an institution.' [...] Data protection requires them to be applying or to be performing the mandate which has been granted to them by the law, but the institution is still very immature, and the subject of data protection is developing, it's evolving.

For new DPAs, the work of building institutional capacity and starting to enforce the law often occurs concurrently. One African data regulator described their approach to setting up a DPA while confronting lack of legislative clarity on organizational structure and insufficient capacity:

> We appointed just the five of us with nothing, just budget of about $3.5 million, no staff. We started literally from scratch [...] The data protection part was quite difficult. We started by doing what we call 'study visits' to similar organizations. We went to Canada, and we went to the UK and to Germany. After that, the five of us sat and said, 'How do we then fashion this organization?' We were lawyers. [...] Because we did not have money, we could not even engage consultants. [...] We came up with the organizational structure. [...] We interviewed people. We started with the top layer being the CEO and the executive members. [...] We had to do a lot of slogging. We now have an organization which has 80 staff members. We now have an organization which has a budget.

For new DPAs, the practical work of defining the organizational structure, hiring staff, obtaining a budget, and expanding capacity happens alongside data protection oversight. Consequently, recently established commissions often face significant constraints in enforcing regulations and ensuring compliance. As one civil society actor from Africa pointed out, "coming up with laws and decorating our legal frameworks with very nice laws in not enough. There is need to take the step further and actually put the data protection principles into practice. And that is where we lack quite a lot." The next sections examine these challenges in more detail.

Adequate Funding and Capacity

Funding constraints are a major obstacle for DPAs in the Global South.[41] As an example, in 2018 the median DPA budget per African country was $500,000 with 14 staff and per Latin American country it was $400,000 with 13 staff, compared to $58 million and 647 staff per country in North America.[42] As Teki Akuetteh Falconer, founder and executive director of Africa Digital Rights' Hub and former Ghanaian data regulator, noted, "The key issue is not whether countries have the 'right' laws or the 'right' institutions in place [but] whether they have the resources needed to effectively implement existing laws."[43] Although governments in the Global South increasingly prioritize data protection oversight, DPAs must compete for funding with other state priorities, like national security and infrastructure development. As one interviewee representing an African DPA stated, government "resource provision is put more on either health because of COVID or those many other priorities, like infrastructure development." Among these, as the roundtable participants stressed, the COVID-19 pandemic precipitated significant DPA budget constraints as governments reallocated funds to health ministries.

A DPA's structure and mandate also impact funding. For instance, despite their enforcement and harmonization benefits, dual mandates can strain operational resources, as one roundtable participant noted. Another interviewee from an African DPA argued that because their data protection office was structured within another agency, "the budget is very limited because [government officials] look at our budget as a whole. […] They will segregate it and say this is for the office. But because of so many competing priorities, we will not have enough resources." However, another respondent said that being nested within a parent organization shielded their DPA from significant funding cuts, particularly in its early stages and during the global pandemic. In many jurisdictions, funding concerns are also aggravated by DPAs' inability to levy sizeable fines and, sometimes, the means to collect them. Additionally, legal provisions sometimes prohibit DPAs from collecting fines and using them for their budget, directing them to the treasury instead. Relatedly, some DPAs only have the power to levy criminal sanctions rather than administrative fines because, as one regulator from Africa stated, "the government is worried that this power may be abused."

Funding challenges inevitably curtail DPAs' activities. Inadequate budgets constrain staff recruitment efforts, impacting agencies' capacity and investigative capabilities. One regulator from Africa facing resource constraints explained that

[41] Bryant, "Africa in the Information Age"; Mannion, "Data Imperialism"; Makulilo, "Privacy and Data Protection in Africa."
[42] Müge Fazlioglu, "How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population" (International Association of Privacy Professionals (IAPP), January 2018), https://iapp.org/media/pdf/resource_center/DPA-Budget-Staffing-Whitepaper-FINAL.pdf.
[43] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?," 2.

> in terms of human resources, you're very limited. We have a structure of about 35 [staff and], in terms of people with fairly longish-term contracts, we have about three. We've now been able to get some temporary staff to help [...] but their contracts are also very short. So, in terms of the human resources, in terms of the tools, in terms of the capacity to ensure compliance that is a challenge when you have limited resources.

Often, as in regulatory agencies in Europe and North America, DPAs compete with the much better-resourced private sector for data protection experts, putting the agencies at a disadvantage.[44] The "brain drain" phenomenon, namely the migration of experts to more lucrative, often non-regional markets,[45] intensifies this disadvantage. In addition to restricting DPAs' staffing capacity, resource constraints affect agencies' ability to carry out basic functions. For instance, several regulators stated that establishing a registry for data controllers and processors—key to maintaining transparency and accountability—overwhelmed under-resourced DPAs and redirected attention from the crucial task of enforcement and compliance monitoring. Likewise, newly established and underfunded DPAs struggle with raising public awareness about data protection laws, which is essential not only to establishing compliance, but also to enforcement via civil litigation. As one regulator stressed, such campaigns can be costly since public messages not only must be created, but also launched repeatedly through multiple channels to ensure they reach the public and the private sector.

Ensuring Independence

A DPA's regulatory independence is essential to its legitimacy, accountability, and effectiveness.[46] Several interrelated factors shape this independence. Structural factors relate to how a DPA is designed, including whether it is situated within and responsible to another agency. Reporting factors relate to DPA governance, particularly which entity oversees the agency and whether it can override the DPA's decisions. Budgetary or economic considerations involve who controls a DPA's budget, including concerns over the weaponization of this control by threatening funding to weaken enforcement.[47] Together, these factors can undermine a DPA's institutional and adjudicatory independence, with the former relating to operational concerns like funding, and the latter denoting independence in decision-making.[48]

[44] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[45] Mannion, "Data Imperialism."
[46] Davis, "Data Protection in Africa: A Look at OGP Member Progress"; Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean"; Internet Society, "Personal Data Protection Guidelines for Africa" (Internet Society and the Commission of the African Union, May 9, 2018), https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/.
[47] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[48] Ibid., 50.

Many DPAs in the Africa and Latin America struggle with achieving independence from both public and private actors, which undermines their enforcement capability. They are especially vulnerable to threats to independence from the governments that create and fund them. The official reasons for building budgetary and decision-making dependencies into a DPA's structure vary. For instance, one former Latin American data protection regulator noted that the official rationale for initially structuring the country's DPA under the aegis of the Ministry of Justice rather than as an independent agency was that "a new body with an independent budget [...] will create more problems for the national budget [since the country] was not in a very good economic and financial situation." This structure significantly undermined the DPA's independence, and the agency was not reformed until years later. Similarly, a civil society representative offered an illustrative example of the structural and financial threats to an African DPA:

> Our regulatory authority is kind of merged into a ministry, and that ministry is under the presidency. So, it hasn't allowed [the DPA] any sort of independence. They do not have structural independence or financial independence. No matter how good-intentioned the regulation or legislation might be, their hands are constantly tied. Those on the board are also part of the government. The head of the organization is [...] appointed by the President, so there's really no wiggle room for [the regulators] to put their foot down in terms of enforcement, which is a big problem, because the biggest processors of data [in the country] are the government.

Even countries with strong data protection records face such structural constraints. For example, Brazil's DPA has limited independence from the president, who has control over its budget. Moreover, three of the DPA's four board members are military officials. Such structural obstacles handicap DPAs' daily functions and enforcement capacities, particularly when the government or another agency controls the DPA budget. Respondents also stressed the role of limited term limits for regulators and non-transparent reappointment procedures in undermining DPAs' legitimacy and independence. One Latin American regulator emphasized structural factors like a DPA's inability to modify public policy amid new data protection developments as undermining adjudicatory independence.

Given the significant resource constraints facing many DPAs, several roundtable participants emphasized the importance of budgetary or "economic independence," namely financial stability and consistency. As one African regulator stated, "if we are not provided adequate budget then it also becomes very difficult for us to really show our independence." Yet, many participants saw their DPA funding reallocated or cut by governments during the COVID-19 pandemic, as remote work proliferated, raising the likelihood of data protection abuses. Similarly, while some participants noted that being embedded within another regulatory body can shield a DPA against threats to its budget,

others observed the opposite, including funding constraints imposed by the parent agency.

Constraints on DPA independence in Africa and Latin America stem not just from resource scarcity, but also because data protection regulation can encroach on public sector activity. As Kuda Hove of Privacy International noted about certain governments in Africa:

> There's this general distrust in having independent institutions [...] There is that distrust [that] if we grant them true autonomy, if we give them true independence, they might turn against us in future, that's sort of the feeling that governments have. So, to manage that fear, governments will then undermine the independence.[49]

For example, one researcher observed that in South Africa creating "independent agencies has never proved attractive to ANC [majority party] ministers, who prefer to keep control,"[50] resulting in slow implementation of data protection legislation and its evaluation. Furthermore, data protection legislation often gives ministers power to create legal exemptions, revise regulations, and intervene in enforcement activities, rendering DPAs vulnerable to regulatory capture.[51] For example, Nigeria's NDPR (Nigeria Data Protection Regulation) can be repealed by any act of Parliament, and the country's regulatory agency, NITDA (National Information Technology Development Agency) has a significantly limited mandate, including the lack of discretionary enforcement power.[52] Likewise, most Latin American countries' data protection laws exempt law enforcement and state intelligence agencies, like Brazil, Peru, and Panama.[53]

Yet public sector actors are among the prolific abusers of personal data protections.[54] For example, Kenyan election officials allegedly collected and misused biometric data during the 2017 elections.[55] Similarly, various Nigerian agencies collected vast amounts of public data as a condition for issuing key state documents, like drivers' licenses and passports. Similar cases of deliberate or accidental governmental privacy violations have arisen in countries like Ghana and South Africa.[56] In Latin America, one data regulator reported that "the federal government [is] using the [country's] general data protection law to deny access to the information." Meanwhile, other governments in the region have exempted themselves from data protection laws in their data processing and

[49] Ibid.
[50] Sutherland, "The Governance of Data Protection in South Africa," 14.
[51] Ademuyiwa and Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[52] Bryant, "Africa in the Information Age."
[53] Rodriguez and Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain."
[54] Bryant, "Africa in the Information Age."
[55] Ibid.
[56] Ibid.

handling activities, including notably contact tracing apps.[57] As one civil society representative recounted:

> We know that everything that occurs in the public sector, specifically related to the executive branch, it will become even harder to investigate, or there's going to be a soft investigation. [...] For instance, the executive branch and the federal police are trying to buy biometric systems. And we in our coalition of other organizations denounced that, and [...] the authorities said, 'No it's everything okay, you can count on us.'

Another Latin American representative argued that this lack of independence often entails non-transparent regulatory proceedings. The interviewee noted that, because of the proximity of the government in question to the private sector, DPA officials will sometimes meet with a company under investigation but not invite members of civil society and keep the proceedings hidden from the public. Civil society representatives stated they often could not get a response from regulators, schedule meetings with them, or access legal documents pertinent to investigations. Such procedural opacity, in turn, makes it difficult to identify whether a DPA fails to pursue a particular investigation because of resource constraints or because of conflicting political interests and alliances. Consequently, even if they often originate from the government itself, threats to DPAs' independence also can impact investigations in the private sector.

Compliance and Raising Awareness

The implementation and enforcement of data protection laws presupposes a degree of public digital literacy, for instance for obtaining informed consent from users prior to data collection.[58] Similarly, private sector compliance with the law requires companies' familiarity with existing laws and regulations. Both conditions present challenges for DPAs, particularly in countries with low digital literacy and technological diffusion. Although awareness about privacy issues has increased in the last several years—for example as evidenced by a 20-30 percent increase in privacy complaints filed with African DPAs[59]—the problem persists among the general population. For instance, surveys in Ghana found that internet users were unfamiliar with privacy and data protection issues, and often unaware of their privacy rights or what to do if these rights were violated.[60] Research also found that for many people, privacy was not a priority.[61] As one roundtable participant said, one of the major challenges is "the lack of awareness [both] in terms of

[57] Javier Pallero, "Collective Challenges and Opportunities in Data Protection: A Latin American Perspective," Luminate, May 26, 2021, https://luminategroup.com/posts/blog/collective-challenges-and-opportunities-in-data-protection-a-latin-american-perspective.
[58] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[59] Dixon, "ROUNDTABLE OF AFRICAN DATA PROTECTION AUTHORITIES: Status and Response to Privacy Risks in Identity Systems."
[60] Bryant, "Africa in the Information Age."
[61] Ibid.

the data subjects knowing their rights and even the data controllers knowing their obligations." Several other participants argued that raising awareness is a significant priority for DPAs in Africa and Latin America.

Informing the public about privacy and data protection is essential to DPAs' ability to effectively fulfill their mandates. Public unfamiliarity with privacy laws undermines not only potential civil liability enforcement, but also citizens' exercise of basic rights, such as rights to access, correct, or delete one's data.[62] Moreover, low digital literacy combined with limited privacy awareness may undermine DPAs' efforts to increase transparency around data protection issues (e.g., by developing a public data registry), and the agencies' public legitimacy. Often, as one interviewee from Africa noted, data protection laws must be translated from English to the local language and simplified "so that the population is able to understand 'What is in it for me? What are the benefits of having my personal data protected?'" The interviewee stressed that building public awareness is a long-term, often resource-intensive process:

> [R]esources for filling the human resource gaps and then resources for creating awareness are very important. Because my view is that for you to be able to reach this population [that lacks awareness of data protection laws], you have to send out this message several times, almost every week, or frequently. And this media space takes time. You need people to develop that content. You need to pay for your message to be broadcast.

Consequently, resource constraints can undermine efforts to raise public awareness of data protection laws, which in turn can intensify challenges related to DPA enforcement and compliance.

Likewise, both private and public sector data processors' and controllers' unfamiliarity with local data protection laws can depress compliance and overwhelm enforcement efforts. As an example, despite South Africa's passage of data protection legislation in 2013, many domestic and foreign businesses remain noncompliant and data breaches are likely underreported.[63] This noncompliance rate has grown with the diffusion of data-intensive technologies, like smartphones.[64] Additionally, despite years to comply with the new law, research reveals that only 25 percent of the country's most popular websites ask users for consent to collect their data.[65] Similarly, researchers found that certain Rwandan e-government websites failed to comply with basic data protection principles, such as having a privacy policy.[66] One website operator erroneously believed that data

[62] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[63] Sutherland, "The Governance of Data Protection in South Africa."
[64] Ibid.
[65] Bryant, "Africa in the Information Age."
[66] Chantal Mutimukwe, Ella Kolkowska, and Åke Grönlund, "Information Privacy Practices in E-Government in an African Least Developing Country, Rwanda," *The Electronic Journal of Information Systems in Developing Countries* 85, no. 2 (2019): 1–21, https://doi.org/10.1002/isd2.12074.

protection is rooted in tax law, while another stated that "[t]here is no policy to follow; I [handle personal information] following my common sense."[67] The public sector is not immune from low compliance and, in some cases, is an even worse offender than the private sector. After requiring that data controllers register in a newly established public registry, one African data protection regulator observed:

> We've noticed that, for instance, the financial sector, they are very compliant. The insurance sectors are very compliant. We are seeing hospitals and clinics starting to register. So that is improving, but where we've noticed low compliance rates is within government. And this may be because they are not aware of the laws.

As a result, public sector data controllers and processors may present the largest challenges to compliance and a key priority for DPAs' awareness campaigns around data protection laws.

Enforcement

Although it is one of their most fundamental responsibilities, many DPAs in Africa and Latin America face significant challenges in effectively enforcing data protection laws. These stem partly from unclear and unduly narrow enforcement mandates and ambiguous legal exemptions.[68] For example, Nigeria's DPA, NITDA, lacks clear enforcement power.[69] Another pressing obstacle, and a key theme in the roundtable, is the absence of expert staff and funding to pursue cases and investigate abuses. Concurrently, assessing DPAs' enforcement activities is difficult given inconsistent data on investigations across jurisdictions. For example, many African DPAs do not publicize their enforcement actions, though countries like South Africa and Ghana have actively pursued noncompliant companies, and the latter instituted a fast-track court to prosecute violators.[70]

Three related enforcement challenges involve punitive measures. First, many African courts lack judicial experience with data protection matters, compounded by insufficient privacy jurisprudence in the region.[71] Inexperienced courts can undermine enforcement, particularly civil liability actions.[72] Conversely, as has been documented in Nigeria, when the public is unfamiliar with local privacy rights, individuals rarely pursue legal action against violators, giving courts few opportunities to develop expertise and data

[67] Ibid., 8.
[68] Davis, "Data Protection in Africa: A Look at OGP Member Progress"; Rodriguez and Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain"; Ngoepe, "Balancing and Reconciling the Conflicting Values of Information Access and Personal Data Laws in South Africa"; Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"; Sutherland, "The Governance of Data Protection in South Africa."
[69] Bryant, "Africa in the Information Age."
[70] Ademuyiwa and Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[71] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[72] Ibid.

protection jurisprudence.[73] Relatedly, many African courts suffer from significant delays and public distrust, which contributes to individuals' reticence about seeking legal remedies.[74] For DPAs that can impose only criminal rather than financial sanctions, an overwhelmed judicial system can frustrate enforcement. As one African regulator pointed out, while governments may be reluctant to allow DPAs to issue administrative fines out of concern over abuse of power, the alternative is often delayed or under-enforcement.

Second, for DPAs that can pursue them, administrative sanctions for violators vary widely across jurisdictions. For example, under Brazil's LGPD law, fines can range up to ten percent of a company's annual gross,[75] while in Ghana the highest fine is approximately $10,500.[76] As a deterrence mechanism, many sanctions are considered not strong enough.[77] Limited enforcement actions coupled with ineffective sanctions risk cultivating a culture of impunity.[78] Such small fines are especially unsuccessful in punishing large, foreign offending companies.

Thus, a third related enforcement challenge involves pursuing cases against foreign, often big tech companies. While European and North American privacy frameworks frequently offer protections for cross-border data flows implicating their citizens, big tech companies from countries like the US and China collect and process data from many Global South countries, often with impunity.[79] One study found that subsidiaries of European telecom companies operating in Senegal and Kenya failed to offer the same data rights to Africans that their parent companies grant to Europeans.[80] As one roundtable participant put it, "when we are going against big companies that are not based in our countries, it's difficult to do the investigation, and at the end of the day, it is difficult to enforce the decision." Another interviewee from Latin America highlighted how the lack of compliance with local laws combined with insufficient sanction mechanisms undermined enforcement actions against big tech companies:

[73] Abdulrauf and Fombad, "Personal Data Protection in Nigeria."
[74] Mannion, "Data Imperialism."
[75] Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean," 39.
[76] Ademuyiwa and Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[77] Ibid.; Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[78] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[79] Huw Roberts, Kirra Evans, and Charlotte Lenz, "Data Extraction by Chinese Phone Applications in Africa: An Analysis of Risks and Regulatory Protection," Oxford China International Consultancy, May 6, 2021, https://ocicoxford.com/wp-content/uploads/2021/05/Apps-Report-Final-6-May-2.pdf; Sutherland, "The Governance of Data Protection in South Africa"; Reuters, "South African Regulator Seeking Legal Advice on WhatsApp's New Privacy Policy," *Reuters*, May 13, 2021, sec. Africa, https://www.reuters.com/world/africa/south-african-regulator-seeking-legal-advice-whatsapps-new-privacy-policy-2021-05-13/.
[80] Bryant, "Africa in the Information Age," 424; Internet Without Borders, "Digital Rights in Sub Saharan Africa: Analysis of the Practices of Orange in Senegal and Safaricom in Kenya" (Internet Without Borders, January 2018), https://www.accessnow.org/cms/assets/uploads/2018/02/RDR-Africa_Final-version-5_January-2018.pdf.

> If I decided a case against Google, for example, the usual answer of Google is, "Your laws do not apply to me." [...] And even when the court said, "Yes, this law applies to you, you have to pay the fine," or whatever, sometimes it's complicated to enforce the decisions. [...] The other problem is [...] the amount of the fines is very low when you translate into dollars right now [...] It's cheaper to pay the fine if they want to pay than to, you know, do the structural changes that they have to do to respect the law.

The challenge of enforcing local data protection laws against foreign violations raises concerns about DPAs' international legitimacy. Moreover, since such enforcement actions often fail, DPAs often focus on domestic companies,[81] which can thwart local innovation and undermine the international competitiveness of local tech companies.

In addition to sanction-related obstacles, a pressing concern is the regional lack of expert technical consultants. The challenge affects both Africa and Latin America and can complicate enforcement actions. As one former Latin American regulator put it:

> If you really want to investigate seriously [a] data breach you need good computer scientists or engineers that can go to the records and see exactly if they were respecting basic, you know, safeguards to protect personal data or not. This is something that if you're a lawyer, it is very difficult to understand or to do. So, you need a specific department, a specific group of people, investigators, that are technicians. And this is a problem because in Latin America, and also in Europe as far as I know, it is very complicated to hire good people because of the salary of technicians, of people working in computer science, in safety of networks. In these kind of things, usually [...] people are very well paid, and they don't want to move to a Data Protection Authority. [...] Of course, if your budget is low, the problem is much worse. Of course, if you don't have your own budget, the problem is much worse. But even when you have a budget, it is a problem.

The lack of resources and lower public sector salaries impede recruiting local experts and, when coupled with inexperienced courts, can hinder thorough investigations and deterrent enforcement sanctions.

Finally, threats to DPA independence also can undermine enforcement. One African civil society advocate pointed out that the country's government does not want the DPA to pursue cases against the public sector. As a result,

> so far, all of [the enforcement] efforts have been turned towards businesses. Even then, I wouldn't call it very effective. [Since the authority's inception a few years earlier] there have been two or three prosecutions and there's no way that is an accurate [amount] of how many people are breaching data protection laws.

[81] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"

Ultimately, such patchwork data protection oversight erodes a DPA's legitimacy and, by extension, its ability to cultivate public and private familiarity with data rights and responsibilities.

Emerging Policy Issues

Established, but proliferating technological systems like the Internet of Things (IoT), the growing adoption of blockchain technologies and decentralized computing, and advances in Artificial Intelligence (AI) all carry implications for data protection and privacy regulation.[82] For instance, deletion requirements modeled after the GDPR predate and cannot easily apply to the immutable ledgers that characterize blockchains.[83] AI systems remain virtually unregulated in several African countries,[84] and policymaker efforts to evaluate regulatory approaches to emerging technologies have been slow.[85]

The proliferation of smartphones, IoT, and cloud processing significantly complicates cross-border data flows, raising key legal questions about obtaining consent and about how to achieve regulatory harmonization amid varying national data protection rules these data flows implicate.[86] Few African countries have clear rules on these flows,[87] the definition of which will become increasingly pressing. However, policy discourses that simply assume the social utility and economic benefits of emerging technologies serve as one obstacle to developing such rules. As one African civil society advocate emphasized:

> We seem to have a tendency of embracing technologies [...] because of the convenience that that they bring. And in most cases, the message about the convenience of the technology kind of overrides privacy-related concerns. Right now, there is a conversation around the Fourth Industrial Revolution, you know, 'We need to be part of the developed world,' 'You need to embrace this technology.' But the conversation around privacy data protection, you find that it's lost along the way. [...] And [our country] is moving towards adopting a more advanced and more centralized biometric identification system. And it is going to be very easy to access information on an individual and all that, but where is the conversation around protection of that information, that very sensitive information?

Moreover, as several interviewees pointed out, many DPAs in the region necessarily prioritize capacity building, taking up most of the data protection regulators' focus and

[82] UNECLAC, "Data, Algorithms, and Policies."
[83] Bryant, "Africa in the Information Age."
[84] Ibid.
[85] Sutherland, "The Governance of Data Protection in South Africa."
[86] Ibid.; Lehuedé, "Corporate Governance and Data Protection in Latin America and the Caribbean."
[87] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"

time. However, as one regulator noted, some African DPAs are taking proactive approaches and developing new policy frameworks, such as for AI-driven technologies and for fintech.

In Latin America, the development of regulations for emerging technologies is also uneven. Some countries have focused on developing frameworks for emerging policy issues. For instance, Barbados and El Salvador have embraced technologies like cryptocurrencies as part of their national development plan.[88] However, new policy concerns continue to materialize, including around regulating digital identity systems[89] and the digitalization of individuals' DNA data.[90] DPAs will need to define oversight of these data-intensive activities. Additionally, as civil society actors from the region argued, existing enforcement has yet to curb familiar problems like data breaches, banking fraud, related cybersecurity concerns around credit card systems, as well as insufficient oversight of new AI technologies. As one civil society representative argued, "the tendency is just [these problems will] get bigger since nothing is really being done systematically to deal with this." The uncertain political reality that faces several countries in the region, as several interviewees argued, only compounds DPAs' capacity challenges in overseeing new technologies and attendant data protection concerns.

Collaboration with Other DPAs, Regulatory Agencies, & Civil Society

Collaboration between regional DPAs, with other domestic regulatory institutions, and with civil society can increase the capacity and effectiveness of DPAs' daily activities—from raising awareness to conducting efficient and thorough investigations. Greater regional collaboration and coordination between DPAs, especially useful for newly established agencies, can enable sharing best practices and bolster enforcement actions against companies operating transnationally.[91] Partnering with other domestic regulatory bodies, like consumer protection agencies and sectoral regulators, can improve enforcement investigations and increase compliance. Working with civil society can cultivate public awareness about data protection issues, increase DPAs' accountability and legitimacy, and aid in identifying violations. Despite immense benefits, such alliances also face challenges, most often related to divergent goals and mandates, and occasional cultural differences.

Collaboration with other DPAs

Regional collaboration among DPAs has been instrumental to setting up new agencies and building out their capacities. For instance, one roundtable participant from Africa recounted how she and her team visited data protection agencies in several Global North countries to develop a blueprint for the DPA in their home country. However, another

[88] Martins de Almeida, "Data Protection in Latin America."
[89] Ibid.
[90] Sutherland, "The Governance of Data Protection in South Africa."
[91] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"

interviewee stated that partnerships with Global North DPAs are very rare. Instead, collaboration is more frequent at the regional level, where sharing best practices is equally, if not more useful. One African regulator related several ways in which such collaborations bolster domestic data protection:

> When I talk to my counterpart in South Africa, yes, it has taken them time to get where they are, but now they are fully funded. Their compliance levels increasing. So, we'll be discussing, how did they do it? Can we get certain tips that they can give us? We share frameworks like their strategic documents. We are currently doing our strategic plan, but we've gotten strategic plans from South Africa, from Kenya, from Ghana, so we share those documents. […] We also share some of those [regulatory] documentations, which help, especially for us who may not be able to immediately procure consultants to do this work for us [of drafting them]. […] Collaboration is very key. It's already taking place within the data protection commissioners. And I think we can only improve on it, but it's something that we all recognize it's necessary for us.

Aside from sharing best practices and regulatory documents, certain interviewees building out their DPA capacity also reported benchmarking their progress with other agencies in the region.

Partnering with regional DPAs also can strengthen the collective ability to influence foreign big tech companies. As SmartAfrica's Thelma Quaye stated, "If African countries present a united front on data policy, like EU Member States, they would have greater power to influence and change the behavior of these companies."[92] For instance, Meta's March 2021 privacy policy update for WhatsApp, which announced the messaging service would share user data across the parent company's services including Facebook, violated POPIA (Protection of Personal Information Act), the South African data protection law.[93] The country's DPA escalated the issue to the Global Privacy Assembly, of which it is a member, to put pressure on Meta to comply with its law.[94] As one interviewee put it,

> We're so small, so we thought that as the Global Privacy Assembly, if we take on this matter, we're bound to go somewhere. We are still in conversation with the assembly about the approach that we should take, but I think those are some of the issues that if we're dealing with a big player such as WhatsApp or Facebook, it will be important for us as Data Protection Authorities in the world, to come together in an attempt to force big players like that to comply.

[92] Ibid., 2.
[93] Reuters, "South African Regulator Seeking Legal Advice on WhatsApp's New Privacy Policy."
[94] Duncan McLeod, "South Africa Threatens Litigation over New WhatsApp Privacy Policy," TechCentral, May 14, 2021, https://techcentral.co.za/south-africa-threatens-litigation-over-new-whatsapp-privacy-policy/170079/.

Aside from increasing enforcement capacity against big tech companies, regional collaboration is also often a prerequisite for effective investigations, particularly given the increasingly international nature of data flows. As one former Latin American regulator stated:

> Today, when you want to investigate some [...] infringement of the law in terms of data protection, it is highly possible that you need to investigate something that [also] takes place in another country. So, you need to have cooperation of the other agencies that are in another country as well. [...] If you see what's going on in Europe, under the GDPR I mean, the different DPAs collaborate. The problem in Latin America is that we want to collaborate, but collaboration is not something that is happening, is taking place right now. So, it's very difficult to investigate the personal data protection violations when you don't have the possibility to investigate or to get some evidence that it is abroad.

These observations also extend to Africa, where many regional economies are fragmented and have small markets. Consequently, regional tech firms have incentives to expand operations beyond national borders.[95] However, data protection regulations across the region are inconsistent, stipulating different rules for user information access, deletion, and data breach notifications, and requiring varying protections for sensitive data.[96]

The patchwork regulatory landscape can increase compliance costs for companies operating transnationally, which creates incentives for African regulators to harmonize their data protection laws.[97] Collaboration between DPAs is fundamental to this endeavor. During the last decade, African countries have articulated several regional data protection frameworks, including the prominent African Union Convention on Cybersecurity and Personal Data Protection 2014, known as the Malabo Convention.[98] Additional incentives for harmonization came from the Africana Continental Free Trade Agreement (AfCFTA), which promotes regional market integration, interoperability, and safeguarding regional data flows.[99] As one African regulator pointed out, establishing a common regional framework can increase compliance and aid in pursuing enforcement actions against big tech companies: "If we were to agree, 'These are the principles that you must comply with,' and we ensure that [big tech companies] do it across the African region, that collaboration also enables us to get to that leverage that [our DPA] may not be able to take on." Yet, neither the Malabo Convention nor the other frameworks have

[95] Ademuyiwa and Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[96] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[97] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"; Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[98] Adeyoju, "Data Privacy Harmonisation in Africa"; Bryant, "Africa in the Information Age."
[99] Adeyoju, "Data Privacy Harmonisation in Africa."

been ratified, and African data protection remains predominantly the domain of national laws and regulations.[100]

Such harmonization efforts are undermined by the absence of a comprehensive legal infrastructure, like that in the EU, which could support the implementation and enforcement of regional integration.[101] Moreover, collaboration is also frustrated by inconsistent technical and regulatory expertise across the region and sometimes contradictory political and regulatory goals. Some regulators may prefer stronger or different data protection frameworks than their regional collaborators, contributing to frictions or disagreements.[102] Despite the desire to collaborate and to share experiences, interviewees also mentioned cultural and language barriers as occasional obstacles to effective partnerships, both across and within regions. For instance, one African regulator noted:

> I think the English-speaking behave differently from French-speaking. Sometimes that can hinder that collaboration because, I think, sometimes we don't quite understand each other. [...] Some are very bureaucratic. The Anglophone prefer to set the principles and allow people to work. The French, they set the principles, then they want to go through a period of coaching for them to make a decision [on the principles]. So there are some differences.

Additionally, on a practical level, work with regional DPAs may be time-consuming and require significant coordination. Such collaboration requires structure: meetings must be set and attended, and their goals must be defined and tracked. As one former Latin American regulator pointed out, collaborative networks are only as strong as the nodes that constitute them, and they require significant trust to operate effectively. Building this trust may be challenging since regulators running DPAs change. Regional coordinating bodies, like the Red Iberoamericana de Protección de Datos (RIPD) in Latin America, can address some of these challenges. However, as one African civil society advocate put it, "meeting is one thing and actually making changes is another." While DPA regulators meet and exchange best practices, implementing them depends on resources, willpower, and other factors that may undermine more cohesive regional enforcement.

Finally, participation in international forums for regulatory collaboration inevitably can reflect historic global inequalities. For instance, one African regulator reflected on recent experiences with global regulatory networks on privacy and information access:

> When I look at the Global Privacy Network, I think the voices of African countries are a little bit muted, not by design. But I mean everywhere. [...] There is a conference coming in Mexico: the Annual General Conference of the ICIC

[100] Ibid.; Bryant, "Africa in the Information Age."
[101] Adeyoju, "Data Privacy Harmonisation in Africa."
[102] Ibid.

> [International Conference of Information Commissioners] which is [on public information] access. I looked at the program. There is no African in that program. And then, I have to say, but how come there is no African in the program? [...] So all the time you have to fight for space. Otherwise, if you don't fight, we get forgotten.

Thus, while Global South DPAs may significantly benefit from participating in regional networks, they may experience marginalization in international forums.

Collaboration with domestic regulatory agencies

DPAs also collaborate with regulators from local regulatory agencies, such as those that oversee competition policy, consumer protection, and financial regulation. As digitization expands, data regulation intersects with a growing number of policy domains, and collaboration between various regulators is increasingly required. As one African regulator described it,

> We collaborate with institutions that might have an overlapping, so to speak, mandate or areas that are similar like the Competition Commission, for instance, like the National Consumer Commission. We signed memoranda of understanding. Not only that. We also collaborated with the Electoral Commission that manages elections. [...] They have to process data in their voters lists, you know. So, we do have collaboration with similar organizations that are regulatory in nature.

Yet, such collaboration is uneven. For instance, Latin American civil society representatives argued that inter-regulatory communication often occurs informally, rather than at a formal administrative level that results in binding actions and is open to public scrutiny. Also, new DPAs may be less experienced and slower than other agencies, disrupting potential harmonization. For instance, in March 2021, the Brazilian DPA investigated Meta's planned privacy policy update, which sought to integrate data flows between the WhatsApp messaging service, used by more than half of the country's population,[103] and other Meta services. According to interviewees, the DPA was slow in analyzing the case, which in turn slowed down other agencies.

Sometimes, the DPAs' lack of independence can also create collaborative friction; they may be less willing to tackle investigations in the public sector than other, more independent agencies, which are freer to do so. On the other hand, potential for collaboration may be strained when the DPA must sanction another regulatory agency for noncompliant data practices. As one African regulator recounted:

[103] Joen Coronel, "Whatsapp Upcoming Privacy Update Sparks Uproar in Brazil; Data Protection and Privacy Rights Among Concerns," Tech Times, April 16, 2021, https://www.techtimes.com/articles/259192/20210416/whatsapp-upcoming-privacy-update-sparks-uproar-brazil-data-protection-rights.htm.

> During the management of COVID, the National Department of Health became a custodian of a lot of data of people who tested positively [to conduct contact tracing.] The regulations which we adopted under the National State of Disaster Act say: six weeks after the end of the national state of disaster the National Department of Health must delete that information or de-identify it if they want to use it for such purposes. And as soon as the national state of disaster came to an end [...] they came back and said, "Well, give us a month." They still have not done it. So it means that they will then force us to then use our powers to compel them to do that.

Consequently, while collaboration with other domestic regulatory institutions is increasingly essential, these agencies themselves may become targets of enforcement actions.

Collaboration with civil society organizations

Civil society organizations serve as instrumental partners to DPAs. As one African civil society actor noted, "the biggest role of CSOs [civil society organizations] would be in oversight and ensuring accountability in whatever form might be needed in the stage that the country is in." Another referred to both parties as "natural allies." For instance, interviewees from African DPAs listed civil society campaigns to raise public awareness about data protection and trainings for various private sectors actors, including in health, insurance, and the media, as especially helpful. The trainings especially helped increase regulatory compliance. As one interviewee pointed out, civil society organizations sometimes have a bigger public reach than DPAs, giving them an advantage in crafting effective awareness campaigns. More generally, civil society organizations in the Global South play a vital role as watchdogs: one African regulator noted that a civil society report in the country resulted in the DPA's first investigation. Likewise, as a Latin American civil society representative recounted, often "after we coach the media and make a complaint, a public complaint, the authorities start to investigate" the offending party.

Moreover, civil society organizations assist with investigations and enforcement. One interviewee from a prominent Latin American civil society organization argued that the organization's main goal is to strengthen and support the DPA by drumming up awareness around data protection and assisting with litigation. Such assistance can involve making amici curiae submissions to courts and supplying DPAs with legal and technical arguments to win data protection cases. For instance, civil society organizations played a key role in assisting the Brazilian DPA in pushing back against Meta's 2021 privacy policy update for WhatsApp. They not only created a sense of urgency around the case, drawing public attention to the foreign company's problematic privacy change, but also advised regulators in their investigation.

Despite the seemingly natural relationship between civil society and DPAs, several factors can thwart effective collaborations. Civil society organizations rely on donor support and, like DPAs, they can face resource constraints, which can undermine their ability to raise public awareness, monitor the data protection space, and assist in investigations and enforcement proceedings. Furthermore, the ability of civil society organizations to engage in these activities and to develop relationships with regulators depends on the health of the civic space. As one African civil society advocate noted,

> If the civic space is closing [...] it can present very difficult challenges for work such as advocacy or capacity building and all that. And if also there's a lack of trust or the relationship between the civil society and the executive is very constrained, sometimes when you try and bring into the room, the executive, you find there's that animosity. And we also face the challenge of just the general lack of interest from the executive.

Civil society representatives from several African and Latin American countries reported challenges related to gaining access to regulators and regulatory proceedings. Another challenge, as one advocate emphasized, is "a skills gap within civil society itself, which makes the [technical] expertise concentrated among very few people," making it difficult to recruit local experts. Others noted that the goals between civil society and regulators may diverge. For instance, one advocate from Africa argued that civil society organizations come at data protection "from a human rights perspective [while] governments never really do that." Conversely, one regulator observed that civil society organizations sometimes can be single-minded in focus (e.g., exclusively championing stronger privacy protections), while regulators must often balance multiple goals, such as privacy rights and information access. Additionally, one African regulator said that civil society can lack a "balanced" approach to data protection advocacy that acknowledges that

> many of our companies cannot innovate if they do not utilize data. We know that data is useful in terms of making informed decisions, in terms of improved service delivery, and the like. But you find that civil society, their interpretation is really very extreme: 'It's my data you cannot utilize it.' [...] In many cases, it will not even appreciate what government has done [such as passing laws]. [...] [This] creates a lot of friction with government, which ultimately then affects how we do some of our work.

Striking the balance between safeguarding data rights and concurrently not stifling emerging digital economies can cause friction between civil society and DPAs.

Best Practices and Recommendations to Confront Challenges Facing DPAs

The challenges identified above often interrelate and overlap. For example, public unfamiliarity and politicians' sidelining of data protection issues not only thwart efforts to establish DPAs, but also to secure funding for them, recruit experts, ensure compliance, and effectively enforce privacy laws. Likewise, effective enforcement requires sufficient funding, robust independence, significant public and private sector awareness of privacy rights and data protection laws, and a large degree of compliance. Consequently, DPAs' problems are often linked and therefore require multi-pronged solutions. At the same time, individual solutions can tackle more than one problem. Several best practices and recommendations have emerged from the experiences of DPAs and civil society actors working on data protection in Africa and Latin America, discussed below.

1. Advocating for DPA independence from the start bolsters independence in the future

Since independence is essential to an effective DPA, regulators seeking to establish DPAs should make it a priority. As one roundtable participant emphasized: "if you don't assert your independence at the beginning, it's actually very difficult to regain it." Several countries offer possible structural approaches to maximize DPA independence. For instance, Mauritius and South Africa have legal, economic, and administrative autonomy, reporting only to Parliament, while Algeria's DPA is governed by a board with representatives from all branches of the government, diluting their individual influence.[104] Interviewees stressed the importance of separating DPA budgets from the executive as another key factor. For existing DPAs that face threats to independence, civil society can play a significant role by conducting and publicizing independent research and public reports, particularly at the local community level, to foster a demand for and culture of independence.[105]

2. Ensuring local values and needs are balanced with baseline data protection from the start is essential to DPA legitimacy and effectiveness

While European data protection frameworks serve as an international gold standard, they do not automatically translate to other regions, especially absent an equivalent regulatory and legal infrastructure. Regulatory harmonization can provide significant

[104] Ademuyiwa and Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[105] Internet Society, "Personal Data Protection Guidelines for Africa."

benefits, including with respect to cross-border data transfers that facilitate participation in global data economies. However, designing and implementing local data protection frameworks requires consideration of local, often unique legal and regulatory cultures and capacities, as well as economic realities. Concretely, design may involve series of consultations with various publics and private sector representatives. Such public engagement should be supplemented with research examining how data exploitation and attendant harms unfold in and impact different local contexts and sectors. Likewise, implementation of data protection frameworks may involve rolling out compliance and enforcement in benchmarked phases to ensure sufficient space for public and private sector feedback and compliance. Without such public engagement and feedback and careful evaluation of local needs and concerns, a DPA's public legitimacy may suffer. Moreover, data protection issues may fail to resonate with the very populations who are most at risk of having their data misused, perpetuating stereotypes about privacy concerns being the domain of politicians and wealthy elites.

3. Collaboration with civil society is essential to basic DPA functions and legitimacy

As several roundtable participants stressed, despite sometimes divergent goals, collaboration with civil society is essential to cultivating local awareness of privacy rights and obligations. As one regulator noted, "we've seen a lot of activity within the civil society. I think that is an opportunity because they're able to raise our voice where we are not. … [W]e collaborate a lot with them, especially in creating awareness in calling out organizations that are not complying." They remain crucial partners in educating the public, which may increase DPAs' legitimacy, but also in raising awareness in the private sector. Particularly, naming and shaming violators can assist with enforcement and improve compliance. For example, in Latin America, NGOs have filled a key enforcement gap by advocating for transparency on government data requests from Internet Service Providers; a task which is outside the mandate of many regional DPAs due to legal exemptions for public entities.[106]

4. Collaboration among DPAs can pool resources, build awareness, and strengthen enforcement

Despite certain challenges associated with collaboration among DPAs, the overwhelming consensus among data regulators is that the practice is immensely beneficial to raising awareness, strengthening enforcement, and sharing best practices. As one roundtable participant said, "international cooperation [and] developing cooperation between network members [can] improve visibility on world scene, create a network sharing with Africa bodies, develop tools and capacity building of members."

[106] Rodriguez and Alimonti, "A Look-Back and Ahead on Data Protection in Latin America and Spain."

Another regulator visited DPAs in Europe and North America to learn about best practices as one of the preliminary steps in launching an African commission. There is also opportunity for collaboration across regions in the Global South, but while at least one African data protection framework drew inspiration from a Latin American one, interviewees were not aware of any explicit collaboration.

Such collaboration and consultation need not overwhelm local goals, values, or needs, especially since there are many important cultural, economic, and other differences both within regions and even with individual countries.[107] Rather, since DPAs in Africa and Latin America often face similar problems (e.g., funding constraints, limited awareness), collaboration can prioritize addressing common issues. Also, coordinated enforcement can increase the likelihood of successfully sanctioning big tech noncompliance.[108] Finally, although harmonization remains elusive, efforts to harmonize frameworks can provide crucial predictability to firms operating across borders and, consequently, increase overall compliance.

5. Strategic targeting and framing of messaging, and building relationships between DPAs and the media can help raise awareness

Certain efforts to raise awareness are especially effective. One concrete approach to communicating the stakes of privacy violations to the public is to link data protection concerns to concrete, real-life harms.[109] Since the desire to participate in global data economies serves as a strong incentive to develop data protection laws and bolster enforcement,[110] stressing the economic benefits of strong data regulation and compliance can resonate with both the private sector and policymakers. Such framing can increase policymaker support of DPAs and potentially help with lagging compliance by linking good private sector data practices to economic success. Along these lines, one African regulator emphasized the usefulness of digital tools to reach the tech-savvy working class and raise awareness about data protection rights and responsibilities: "We have monthly webinars where we talk about topical issues, and our attendance has been good [...] And these have cost us very little. [...] Without putting in advertising space at all we've been able to reach very far." Another opportunity to increase awareness, as the former regulator argued, is to develop stronger relationships between DPAs and the media. These relationships may not only increase public awareness of data protection issues—potentially improving compliance and enforcement—but also increase transparency around DPA proceedings.

[107] e.g., Sutherland, "The Governance of Data Protection in South Africa."
[108] Davis, "Data Protection in Africa: A Look at OGP Member Progress."
[109] Ibid.
[110] Bryant, "Africa in the Information Age."

6. Collaboration with other regulatory agencies, adopting a risk-based approach, and strengthening the judicial system can bolster enforcement

To address enforcement challenges, which are often exacerbated by limited funding and capacity, experts advocate for creative solutions. For example, Carnegie India's Suyash Rai argues that since a "DPA's capacity will be limited early in its tenure, the institution should use a risk-based approach to direct resources to areas where the risks are highest to prevent overload.[111] Additionally, using RegTech (regulatory technology) to automate complaint processing can help address capacity challenges. Likewise, prioritizing existing resources to create a public registry of violators as a reputational sanction can also increase compliance and reduce enforcement burdens.[112] One interviewee also stressed that collaboration with other regulatory agencies in a country can improve enforcement and compliance. The interviewee, a regulator in Africa, noted improved compliance rates in financial, insurance, and telecom sectors, arguing that "working with regulators has really helped and it's something that we want to continue and ensure that we bring more people on board." Generally, DPAs that have cross-cutting mandates are especially well-positioned to engage multiple stakeholders, including civil society and other regulators.[113] Given that several interviewees recounted challenges related to judicial inexperience in adjudicating data protection cases, strengthening and technical capacity building for courts is also a key factor in more effective enforcement.[114]

7. Funding education programs can cultivate local expertise and public awareness

As South Africa's leadership in African data protection indicates, advocating for including data and privacy issues as part of university curricula can increase local expertise and digital literacy.[115] Similarly, a former Latin American regulator stressed the importance of cultivating local expertise through education. Such an effort would require not just expanding curricula at law schools and computer science departments, but also digital literacy education across universities. Funding academic programs that engage data protection and data flows can build a pipeline for future enforcers as well as cultivate public awareness and dialogue around data protection issues.

[111] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?," 4.
[112] Pisa and Nwankwo, "Are Current Models of Data Protection Fit for Purpose?"
[113] Ademuyiwa and Adeniran, "Assessing Digitalization and Data Governance Issues in Africa."
[114] see also Abdulrauf and Fombad, "Personal Data Protection in Nigeria."
[115] Makulilo, "Privacy and Data Protection in Africa."

8. Supporting domestic and regional civil society networks can strengthen enforcement investigations

Interviewees from civil society stressed that building regional networks between civil society organizations within and across countries can support enforcement investigations. Such networks can result in mutual aid, particularly around big legal cases. One interviewee described these as "network effects": with a substantial number of organizations collaborating, advocates became more effective at obtaining regulatory documents, crafting expert legal filings, and other supportive functions. Additionally, such collaborative networks served as a crucial source of social support and motivation for civil litigators involved in challenging and resource and time-intensive proceedings, like the WhatsApp case in Brazil.

9. Cultivating open civic spaces and building local networks of policy stakeholders can protect and bolster DPA independence and accountability

Although DPAs implement and enforce data protection frameworks, data protection is ultimately a collaborative effort that requires strong networks and healthy civic spaces. Civil society can help cultivate civic opportunities and spaces to build such networks where various policy stakeholders can engage in open discussion about data protection issues. One Latin American civil society representative offered an example of such meetings that occurred in his country:

> [I think it's important to] set up technical seminars in which people can freely talk about what they think about what should be the best regulatory approach for data protection. […] In the past ten years, we had [such] seminars organized. […] People, they felt in a safe space, […] people from the government, federal prosecutors, lawyers […] civil society, activists, and so on. […] It was a space for conversations, and to go deep into some policy issues, and even to disagree in the end. But I think this was really important to build trust. […] I think this was also key to build relationships with the members of the DPA.

Creating structures that cultivate robust civic spaces of free exchange are essential to building durable policy stakeholder networks invested in developing strong data protection frameworks and oversight. Even when the national civic space is curtailed or closed, such meetings can serve as the building blocks of networks of mutual accountability that provide crucial checks on threats to regulatory independence.

About the Authors

Pawel (Paul) Popiel is the George Gerbner Postdoctoral Fellow at the Annenberg School for Communication, University of Pennsylvania. His research examines how politics shapes the governance of digital media and emergent technologies. His research has been published in journals like *Policy & Internet*, *Critical Studies in Media Communication*, *Journal of Digital Media & Policy*, *Journal of Broadcasting & Electronic Media*, and others, and has been presented at major conferences. He obtained his Ph.D. at the Annenberg School for Communication, University of Pennsylvania. He also holds a B.A. in Political Science from McGill University and an M.A. in Media Studies from the University of Texas at Austin.

Laura Schwartz-Henderson is the Research & Advocacy Advisor on Internews' Global Technology team, where she develops strategic advocacy tools, programs and research on technology policy, media ecosystems, and social movements. Laura was previously a Fellow and Policy Manager for the German Marshall Fund's Digital Democracy program and the Research Project Manager at the Internet Policy Observatory at the University of Pennsylvania's Annenberg School for Communications. She has extensive experience conducting research on digital rights issues, managing programs, and working with activists and journalists in diverse political contexts. Laura received a Master's in Public Administration from the University of Pennsylvania. Her research focuses on the mechanisms through which technology mediates civic engagement and the institutional architectures and cultures of social justice and philanthropic organizations. She is the founder of the Creative Digital Rights Advocacy Collab Network and the Executive Producer of the Privacy is Global podcast.

Professor Eduardo Bertoni (PhD, Buenos Aires University) is currently the Representative of the Regional Office for South America of the Inter American Institute of Human Rights. He was the first Director of the Access to Public Information Agency (AAIP) which is the Argentine Data Protection and Access to Information Authority. He was the founder and the first director of the Center for Studies on Freedom of Expression and Access to Information (CELE) at Palermo University School of Law, Argentina. He was the Executive Director of the Due Process of Law Foundation (DPLF) until May 2006. Previously, he was the Special Rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights at the Organization of American States (2002–2005).