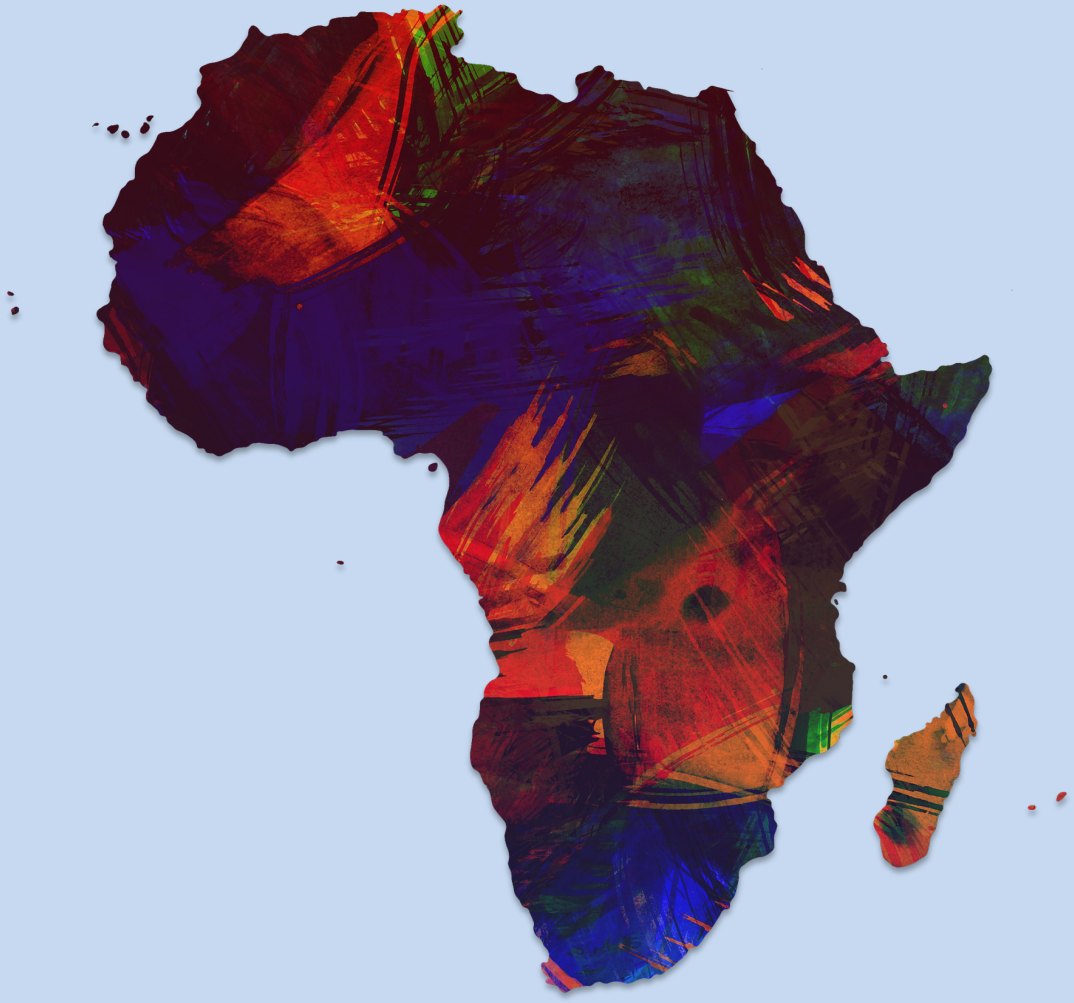
A Look into DPA Strategies in the African Continent



FUTURE OF PRIVACY FORUM

May 2022

Authored by:

Mercy King'ori and Hunter Dorwart
for the Future of Privacy Forum

The authors thank Katerina Demetzou, Sebastiao Barros Vale and Lee Matheson for contributing to this Report

.

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

Content

Summary

Since the enactment of the first data protection law in Africa in 2001 in Cape Verde, many other African countries have followed suit. Two decades later, 33 countries boast comprehensive data protection laws. This growth in legislation has received well-deserved attention as the continent continues to articulate its position on privacy and data protection matters.

Until now, most publications on the state of data protection in Africa have focused on the processes leading up to the creation of laws and their enactment. As a result, other important parts of the data protection environment including implementation and enforcement have received little attention. This has hampered efforts to obtain a comprehensive picture on the state of data protection in Africa. Particularly, despite their important role in shaping data protection discourse on the continent, the activities of the Data Protection Authorities (DPAs) entrusted with implementing the laws are not well known or documented.

It is worth noting that even with comprehensive data protection laws, not all countries have operational DPAs due to factors such as lack of political will, competing priorities and financial constraints. This report seeks to address this gap and shed light on notable activities and strategic plans of established DPAs in seven African countries in depth: Kenya, Nigeria, South Africa, Benin, Mauritius, Côte d'Ivoire, and Burkina Faso. At the same time, the Report draws on research including most African jurisdictions that passed data protection laws, also observing how some of those have not yet created a DPA, despite the law including obligations for them to do so.

The report analyzes various DPA strategy documents including their most recent annual reports and national data protection plans for 2022-2023 from these seven jurisdictions and includes a brief overview of the key developments and trends in administrative enforcement. These documents provide important insights into the priority areas of DPAs as well as their current operational conditions.

Most countries, by virtue of provisions under their national data protection laws, contain reporting requirements that mandate them to publish annual reports. Such reports reveal information about the status of enforcement and the numerous factors that affect the organizational and administrative goals of the regulatory bodies. A discussion of such factors is necessary as many countries are navigating the path of establishing and operationalizing new regulatory authorities.

The report structure includes the background of the DPA in question and key takeaways from each plan. There is significant variation between the seven countries' plans. Despite these varying structures, key findings include certain common themes:

Setting Up the DPA Structure, a Key Challenge

While most countries have made strides in enacting data protection laws, some of these countries have yet to establish the DPAs created under these laws. This is particularly seen in countries that have dual data protection regimes and separate the promulgation of legal authority into substantive and procedural tracks. For example, Angola first adopted its data protection law in 2011 (the Personal Data Protection Law of 2011) but only established its DPA through a 2016 Presidential Decree.

While not unique to the African continent, the phenomenon of having data protection laws on the books for many years prior to creating an enforcement body applies to many countries in Africa. For instance, while Egypt has recently passed a data protection law (2020), it has yet to set up a DPA. There are numerous reasons for this delay across affected jurisdictions, including procedural and political barriers, inadequate funding and capacity-building, and lack of expertise and process.

Raising Data Protection Awareness and Ensuring Budgetary Means: Chief Common Goals among New DPAs

Because the majority of DPAs are novel bodies, priority areas for these entities include raising privacy and data protection awareness, ensuring the means to access funds, and improving institutional capacity to implement the new laws. Particularly, the issue of data protection awareness has been a key issue for many DPAs (e.g., Kenya, Nigeria and Mauritius) as it forms the foundation of the implementation of certain provisions of data protection laws such as the rights of data subjects.

As the privacy and data protection ecosystem in Africa continues to grow, DPAs will play a crucial role in protecting the rights of data subjects while ensuring data controllers and processors fulfill their duties and obligations. This is particularly important in an environment of growing data processing activities where privacy awareness is still a challenge. Stakeholders now recognize that the presence of independent, functional and transparent authorities as mandated in national and regional legal regimes such as the African Union's (AU) Convention on Cybersecurity and Personal Data Protection represent fundamental building blocks in creating awareness about the status of enforcement and for improving the operational status of the new regulators.

Significant barriers: Budget and funding

New DPAs often grapple with insufficient funds and budgets, which may cripple their functioning and enforcement capabilities. For example, the Office of the Data Protection Commissioner, Kenya's DPA, has recently highlighted it will experience a resource gap of 76%[1] if budgetary allocations remain as indicated in the larger governmental plan.

[1] https://www.odpc.go.ke/download/odpc-strategic-plan-2022-2023-2024-2025/, last accessed May 11, 2022.

Shortages in funding reduce the capacity of DPAs to effectively carry out their roles, especially those related to investigations. As some countries amend their data protection laws to align with modern requirements of data protection, DPAs with expanded roles require adequate funding for effective operations – see, for example, the Burkina Faso[2] DPA, which has increased regulatory expectations with respect to penalties, international cooperation, and mutual aid.

The majority of strategic documents analyzed point to **lack of funding as a major barrier to effective operationalization**. In addition to obtaining more funds from relevant national Treasuries, DPAs across Africa are searching for alternative and reliable sources of funding, such as registration and filing fees, enforcement penalties, forging partnerships or other costs associated with regulatory services. Without appropriate budgets and with DPAs relying on alternative sources to fund their activity, there are concerns about DPAs being able to carry out their mandates efficiently.

There is a Focus on Independence in most DPA Strategies Studied

The independence of a DPA is important for transparency and accountability purposes, and public perception of the regulator as an unbiased, neutral enforcement authority and it weighs as a relevant criterion for some lawful cross-border data transfers from key jurisdictions engaged in trade, like the European Union and its General Data Protection Regulation. Several jurisdictions surveyed recognize that as DPAs become functional, they need to ensure some degree of independence from other administrative and political structures.

In the African context, DPA strategies and reports devote entire sections exploring the concept of independence, its structure under relevant national legislation, and how the DPA prioritizes it. The question of whether a DPA is independent depends on factors including the manner in which appointments of its leadership are made, terms and removal from office, remuneration, and what reporting mechanisms are in place. It is important to note that those African countries that wish to eventually obtain adequacy decisions under EU's GDPR may recognize the need to create independent DPAs to implement the laws.

DPAs Expect to Focus more on Enforcement

In jurisdictions with older DPAs, authorities have used enforcement to compel compliance by data controllers and data processors. The power to issue penalties and even shut down services or restrict data processing serves as bedrock of data protection compliance in many jurisdictions around the world. Stakeholders expect that DPAs will enforce the law and take into consideration the probability of an administrative order into how they calculate compliance and legal risk.

The situation appears to be slightly different in Africa. While there are examples of noteworthy enforcement decisions by DPAs (such as Nigeria's NITDA which fined a digital

[2] https://www.jdsupra.com/legalnews/recent-developments-in-african-data-7141556/, last accessed May 11, 2022.

lending company[3] 10 million Naira), so far the majority of DPAs have focused on **providing authorizations for data transfers**. For example, since its establishment in 2015, the National Commission of Data Protection (CNPD) in Cape Verde has issued 1307 authorizations[4], but there are no fine or penalty decisions published. Other DPAs have similarly devoted resources to other administrative matters such as registering data controllers and processors with priority, with scarce enforcement actions. Recognizing that formal investigations and enforcement procedures are costly, this status quo may be linked to the budgetary concerns mentioned above.

The official documents issued by DPAs analyzed for this Report show that some DPAs are moving towards a more active and robust approach to enforcement. For example, the Instance Nationale de Protection des Données à Caractère Personnel (INPDP), Tunisia's DPA, has already acted upon the goal of robust enforcement. Active from the beginning of its creation, the INPDP has encouraged citizens to make complaints regarding data protection infringements, particularly around the time of Tunisia's 2019 presidential election. In 2020, the INPDP issued 117 fines.

As DPAs become more comfortable and effective as organizations, enforcement may become a top priority for regulators. Every strategy and report examined below has a section on enforcement and an acknowledgement of both the recent successes and the need to ensure consistency of legal application moving forward.

Providing Guidelines and Drafting Regulations is an Area of Priority

A final priority for many DPAs in Africa is to draft guidelines and regulations on key provisions of data protection law including registration of data controllers and processors[5]. Stakeholders rely on these guidelines to fill in gaps of interpretation and compliance expectations. Almost all strategies examined have highlighted regulatory activities in this space and drawn attention towards the key documents issued by the DPA over a specified period of time.

While the process of issuing guidelines and draft regulations is set to increase compliance rates, gaps still exist as some DPAs have yet to become fully operational. To accomplish this, DPAs are looking at capacity building through means such as improving human resource capacity, and strengthening operational processes to improve response to data protection processes including drafting regulations and guidelines.

Detailed country reports providing context and analysis for each of these outlined trends follow below, in this order: Kenya, Nigeria, South Africa, Benin, Mauritius, Côte d'Ivoire, Burkina Faso.

[3] https://techcabal.com/2021/08/24/nitda-fines-soko-loan/, last accessed May 12, 2022.
[4] https://www.cnpd.cv/autorizacoes.php?page=1, last accessed May 12, 2022.
[5] https://www.odpc.go.ke/regulations/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021/, last accessed May 12, 2022.

1. KENYA

Background

Established under the Data Protection Act 2019, the Office of the Data Protection Commissioner (ODPC) serves as Kenya's primary regulator for the processing of personal data. As part of the larger government initiatives like Kenya Vision 2030, the Third Medium Term Plan (2018-2022), and the "Big Four" Agenda, the ODPC released its Strategic Plan (Plan) covering the 2022-2025 period to guide its mandate, set priorities, assess performance, and communicate its efforts to national and international stakeholders.

Key Takeaways

The Plan lays out key priorities for the next few years with the ODPC's mission and vision, administrative relationships, and its structure and culture in mind. Three focus areas are stipulated: (i) institutional capacity development to enhance data protection and partnerships throughout Kenya, (ii) regulatory services to establish a policy framework that safeguards private data, and (iii) awareness creation to equip stakeholders with adequate capacity on data protection. The plan attempts to provide mechanisms for stakeholders to collaborate with the ODPC to achieve these key objectives and operationalize data protection law in practice, as well as sets forth the budgetary and personnel requirements needed to accomplish its priorities. The key sections of the plan include: an overview of data protection in Kenya, situation analysis, strategic model, implementation and coordination framework, monitoring and reporting, and annexes.

Overview of Data Protection in Kenya - The plan outlines the background and context of the Data Protection Act of 2019, including its relationship to the right to privacy in the Constitution of Kenya, and the role and function of the ODPC in Kenya's larger administrative system and its independence. In particular, the plan provides information about the mandate, the development challenges, and the development role of the ODPC.

- **Mandate** - The Plan first outlines the ODPC's mandate under the Data Protection Act, which includes regulating personal data processing in line with data protection principles, upholding privacy, establishing institutional mechanisms to protect data, and providing data subjects with rights and remedies to protect their information.
- **Development Challenges** - The ODPC recognizes the global, regional, and national development challenges facing its goals including: addressing gaps in coverage, new technologies, cross-border transfers, balancing surveillance and data protection, and strengthening enforcement, institutional capacity, and compliance burdens. The Plan highlights how global trends in data protection have further complicated the ODPC's mandate and acknowledges the need to understand and reconcile different legal frameworks.
- **ODPC's Development Role** - The ODPC states that it primarily wants to encourage self-regulation by all entities involved in data protection while instituting enforcement mechanisms to ensure compliance only when necessary. According to the plan, building human capacities and strengthening operational processes is key to both realize the goals of data protection and appreciate the centrality of data

in the growth of the digital economy. Privacy and data protection are seen as necessary pillars, not trade-offs, to economic development, market competition, and innovation of business models.

Situation Analysis - The plan highlights the context in which the ODPC operates, recognizes that lack of human resource capacity has hindered the growth of its operations, and identifies opportunities for the ODPC to strengthen its current role. The ODPC's situational analysis consists of key achievements, environmental analysis, stakeholder analysis, and strategic issues.

- Key Achievements - The Plan lists a number of key achievements since 2019 including facilitating the roll out and DPIA of Huduma Namba[6], issuing three draft regulations including those related to registering data controllers and processors and complaints, staffing key personnel and leaders, setting up a functional office, developing guidance notes, creating a training curriculum and standard operating procedures, participating in consultation forums, establishing a framework for handling complaints, issuing advisories, and establishing international cooperation partnerships.
- Environmental Analysis - The ODPC assesses environmental constraints through Critical Success Factor Analysis techniques and identifies a series of factors and implications for the office, which range from structural and financial constraints, to enforcement context, economic factors, and digital skills. Each identified issue has a corresponding impact factor.
- Stakeholders Analysis - The Plan also sets forth an analysis of the various stakeholders involved in the data protection landscape in Kenya. For each stakeholder, the analysis focuses on the corresponding expectations of the ODPC and their degrees of influence and interest. The Plan identifies both public and private stakeholders including relevant government departments and ministries that process personal data, media, private companies, civil society and religious organizations, development partners, global networks, and data subjects.
- Strategic Issues - The following strategic issues are prioritized:
    - Standard operating procedures
    - Multi-skilled team building
    - Budgetary gaps
    - Data protection infrastructure and systems
    - Decision-making structures and reporting
    - Policies and procedures for setting up registers
    - Coordinating with multinational corporations
    - Compliance and enforcement mechanisms
    - Frameworks for reporting and complaints management
    - Public awareness and communication
    - Culture and value systems
    - Self-regulation

[6] Huduma Namba refers to Kenya's central population database under the National Integrated Identity Management System (NIIMS) to verify and collate population identities.

Strategic Model - The Plan sets forth a strategic model for the ODPC to aid the formulation and implementation of the ODPC's decisions in the next three years including:

- **Vision, Mission Statement and Core Values** - The Plan identifies the ODPC's vision and mission to protect personal data in Kenya, build trust and transparency, and promote the core values of collaboration, ethical organizational practices, transparency and accountability, inclusivity and accessibility, and effectiveness.
- **Functions** - The ODPC highlights its function of enforcing the Data Protection Act, establishing a register of data controllers and processors, receiving complaints from data subjects, carrying out inspections, promoting interssors, exercising oversight, promoting self regulation, conducting its own assessment, national cooperation, and undertaking research on the development of data processing.
- **Key Result Areas, Enablers, and Foundation** - Three key result areas are identified: i) institutional capacity development, regulatory services, and awareness creation. For each of these, the plan highlights strategic enablers to guide the development of these result areas such as formulating a legal and policy framework, fostering partnerships and collaborations, and engaging in research. Finally, the Plan lists governance and leadership as foundations to enable these key result areas.
- **Strategic Objectives and Strategies** - The Plan lists its objectives and strategies for each key result area specified above. For each result area, a list of focus areas, strategies and objectives to measure impact are offered. These focus areas range from internal accountability mechanisms such as risk management, financing, and audits to larger regulatory and training initiatives such as compliance, enforcement, public outreach, internal training, and communication. Lastly, the Plan synthesizes its focus areas to identify enablers of an effective data protection regime, which involve all three result areas.

Implementation and Coordination Framework - The Plan presents strategies for implementation including an organizational model, structure, staff establishment, accountability model, and budget and risk plan.

- **Organizational Model** - The OPDC hosts a primary Data Commissioner followed by Deputy Data Commissioners that oversee four separate directorates respectively: (i) Corporate Services Directorate, (ii) Data Protection Compliance Directorate, (iii) Complaints, Investigations and Enforcement Directorate, and (iv) Research, Policy, & Strategy Directorate. Assistant Data Protection Commissioners head divisions and are responsible for project execution. The organizational structure is further broken down into heads of units and other technical and corporate affairs offices.
- **Staff Establishment** - As of 2021, the OPDC has 10 staff members, both in technical and support services. The Public Service Commission approved an establishment of 92 staff members of 57 officers for technical services for the 2022-2024 period. An updated organizational chart and accountability framework has been developed.
- **Strategies for Implementation** - The Plan recognizes the following strategies to implement the plan: a phasing and sequencing strategy to prioritize items of most importance, a results-based management strategy, institutional strengthening, human resources development strategy, financial resources management, and resource mobilization. In particular, generating and ensuring stable and consistent sources of financing is crucial for the success of the DPA.

- **Risk Analysis and Mitigation** - The Plan outlines a strategy to minimize risk to ensure internal processes focus on key outputs. A comparative table identifying risk categories (e.g., strategic risk, cyber risk, legal and compliance risk, operation risk, financial risk) is offered. For each risk category, the plan determines key risks, their relative likelihood and severity, and concrete mitigation strategies that the OPDC can employ.

Monitoring, Evaluation, and Reporting - The Plan presents a framework for monitoring, evaluation, and reporting the implementation of the strategic plan to provide an evidence-driven approach for decision-making. Monitoring will involve the systematic collection of data and analyzing information based on targets, outputs, outcomes, and feedback reports from the senior staff. The OPDC will conduct annual, mid-term, and end-term evaluations of the plan tied to employee performance targets, annual budget and reporting obligations, and recommendations for implementation. Reporting of these evaluations will follow a quarterly, bi-annual, and annual structure.

Annexes - Lastly, the plan includes an annex compiling charts of its strategic model (including result areas and corresponding strategies), its implementation and coordination framework, and its monitoring, evaluation, and reporting system.

2. NIGERIA

Background

In Nigeria, the National Information Technology Development Agency (NITDA) implements and enforces the Nigeria Data Protection Regulation (NDPR). However, this might change with the creation of a new data protection body, Nigeria Data Protection Bureau[7]. Housed within the Federal Ministry of Communications and Digital Economy, which was rebranded after the launch of the National Digital Economic Policy and Strategy (NDEPS 2020-2030) in 2019, the NITDA has implemented the NDPR with the overall policy objectives of the NDEPS in mind. Pursuant to its strategy, the organization released an NDPR Performance Report (Report) covering the period of 2019-2020. NITDA launched the 2020-2021 report during the annual International Data Privacy Day but is yet to circulate the digital version. The latest version is expected to be published in the future.

Key Takeaways

The Report highlights key initiatives, successes, and challenges of implementing the NDPR. Noting that the regulation was designed to match the foundational principles of Convention 108+ and the EU General Data Protection Regulation, the Report states that the implementation of the NDPR in Nigeria may serve as a learning curve for Nigeria to effectively implement global laws in the context of local peculiarities, opportunities, and

[7] https://ndpb.gov.ng, last accessed May 12, 2022.

structures. The report identifies 17 key takeaways that address a particular issue for the NITDA but many of them touch upon similar issues and draw from similar data.

State of Play - The report highlights the state of data protection in Nigeria including the recent history of the passage of the NDPR, the interplay between data protection and the growth of digital technologies, and the status of compliance expectations in the country. According to the report, in the 2019-2020 period Nigeria has recorded impressive growth in data protection compliance, has instituted a verifiable database of statutory audits by 635 entities, and has transformed the landscape for DPOs and other stakeholders. The introduction of Data Protection Compliance Organizations (DPCOs), entities licensed to provide data protection compliance services, is a feature highlighted as unique to the Nigerian market. The report notes the NITDA is monitoring the status of DPCOs and intends to issue a DPCO Code of Practice in the future.

Enforcement Statistics and Achievements - The report catalogs a number of notable statistics on data protection compliance such as audit filings received (635), amount of revenue generated by filing services, sectors represented, jobs created through NDPR implementation, the value of the NDPR audit market, number of events, enforcement actions (7), investigations on data breaches, and fines collected. Additionally, the report highlighted notable achievements of the NITDA, which include engagement with international organizations, successful investigations held, revenue generation, licenses issued, guidelines released, issues resolved, and the launch of a NDPR Portal for filing audit reports and breaches.

Capacity Building Awareness and Challenges - The report indicates that NITDA officials participated in 93 public and private sector organized events with other governmental bodies in Nigeria. Additionally, attention is raised to NITDA events hosted by the organization for the purposes of spreading awareness and building capacity. Despite this, the report notes that the NITDA faces numerous challenges in the years ahead including lack of funding, human resources and capacity to fully execute its mandate. The Report also identifies seven court cases involving the NITDA and numerous parties from various tech sectors, but does stipulate the matter or substance of the issue.

Cooperation and Partnerships - The report identifies several cooperation and partnerships the NITDA has embarked on with other organizations, including:

- African Union PRIDA Project
- Participation at the Africa Forum
- Participation at the American Business Council Workshop on Data Protection
- NITDA-Central Bank of Nigeria (CBN) Cooperation on Data Protection
- NITDA-Securities and Exchange Commission (SEC) Cooperation on Data Protection
- NITDA-MDA's Cooperation on Data Protection
- DPOs under the Digital Transformation Technical Working Group of MDAs.

Guidelines and Reforms - The report highlights the key reforms and guidelines issued by the NITDA in the 2019-2020 time period. First, the Guidelines on the Use of Personal Data by Public Institutions 2020 mandated that every public institution appoint a DPO and conduct DPIAs for major data processing projects. Second, the NDPR Implementation

Framework which provides clarification on various provisions of the NDPR and a template audit question, a sample privacy policy, and a whitelist of countries with adequate data protection laws. Last, instituting a license mechanism for data protection compliance organizations.

Future of Data Protection in Nigeria - Finally, the report outlines future trends in data protection in Nigeria, including the passage of a Data Protection Bill in 2020, the creation of a Data Protection Commission, and the amount of money compliance will generate for the Nigerian economy.

3. SOUTH AFRICA

Background

The Information Regulator is South Africa's primary enforcement body for data protection. Established under Section 39 of the Protection of Personal Information Act (POPIA), the Regulator is responsible for the promotion and protection of the right to privacy as well as promotion of access to information and exercises its powers in accordance with POPIA and the Promotion of Access to Information Act 2 (PAIA). Appointed by the President for a period of five years, five members comprise the agency, three of which (including the Chairperson) are full-time, with one of those full-time members responsible for POPIA while the other is responsible for PAIA.

The Regulator announced its first batch of members in 2016 and has taken a phased approach in recruiting staff for its offices due to budgetary constraints. Despite these limitations, the Regulator has accelerated its staffing in multiple divisions, begun enforcing POPIA, and issued Codes of Conduct to facilitate compliance. In 2020, the Regulator released its Strategic Plan[8] outlining key priorities and areas of focus for the 2020-2025 period.

Key Takeaways

The Strategic Plan identifies key goals including (i) implementing privacy education and awareness programs nationwide, (ii) facilitating a complaint mechanism for data subjects, (iii) embarking on privacy litigation, (iv) researching proposed legislation or policies that may affect personal data protection, (v) monitoring developments of information processing in the market, (vi) and issuing Codes of Conduct. Notably, the Plan also identifies organizational hurdles for building administrative capacity, including staffing and budgetary challenges. Below are the main sections of the strategy.

[8] https://www.justice.gov.za/inforeg/docs/pptr/InfoRegSA-2020-2025-StrategicPlan.pdf, last accessed May 12, 2022.

Mandate - The Plan first identifies the mandate of the Regulator, including constitutional, legislative, policy, and judicial sources of authority. Notably, the POPIA outlines the Regulator's core functions and responsibilities for enforcing data protection compliance and information privacy in South Africa, while policy mandates authorize the agency to conduct research and issues Codes of Conduct.

Strategic Focus - The Plan outlines the strategic focus of the Regulator including its vision, mission, values, and situational analysis.

- **Vision, Mission, and Values** - The Regulator aims to be a world-class institution for data protection while retaining sufficient independence to protect the rights of ordinary consumers. Its core values, which mimic those seen in other DPA strategies, include transparency, accountability, integrity, excellence, impartiality, and responsiveness.
- **Situational Analysis** - The Plan identifies external and internal environmental considerations for the Regulator.
    - External Environment - The Plan recognizes the opportunity of the Regulator to address the processing of personal information in the digital ecosystem and its relationship with other governmental bodies. Notably, the Regulator has a dual mandate to protect personal information while promoting its access by members of the public. External threats such as delay or lack of resources could inhibit the protection of personal data and leave data subjects vulnerable and without recourse.
    - Internal Environment - Strengths of the Regulator include independence and functionality, while its primary weakness is lack of resources to oversee the scope of its mandate.

Performance Information - The Plan identifies the following metrics for evaluating performance: institutional performance and key risks.

- **Institutional Performance** - The Plan specifies a range of institutional factors to measure the impact of the Regulator and offers a quantitative analysis of key enforcement actions with expectation goals for the next five years. These include number of complaints received (roughly 271 for 2020 to 700 for 2025), awareness, and improvements in PAIA compliance. Additionally, the Plan specifies the rationale for Outcome Indicators in relation to specific goals such as protecting personal information and access to information.
- **Key Risks** - The Plan outlines key risks for its success. These include delay in operationalization of POPIA, delay in the establishment of the Regulator, and inadequate funding. Additionally, the Plan offers mitigation measures for each of these risks such as submitting requests for more funding or information to other bodies, developing a financing plan to prioritize key goals, and developing alternative sources of funding from the National Treasury.

Technical Indicator Description - Finally, the Plan sets forth a list of outcomes and corresponding technical indicators and reporting mechanisms such as tracking the number of received complaints, percentage of stakeholders who know of the regulator, and percentage of increased compliance with relevant provisions of POPIA and PAIA.

4. BENIN

Background

In the Republic of Benin, the Autorité de Protection des Données à Caractère Personnel (APDP) serves as the primary regulator that ensures and enforces the application of the Digital Code and the right to privacy. The APDP is composed of 11 members from different professional sectors and divided into a core bureau, a group of advisors, a secretary-general, and a government commissioner. Under the Law No. 2017-20 on the Digital Code, the APDP must report each year on the execution of its mission, actions, and objectives. The latest publicly available report is for the year 2019.

Key Takeaways

The report is divided into four parts, each covering a unique area of the APDP's core functions and responsibilities. For each part, the report identifies the actions and objectives of the organization as well as notable challenges in executing its mission. The four parts are as follows: (i) activities for the year of 2019, (ii) new legal environments, (iii) problems of video surveillance, and (iv) an annex containing unique deliberations.

Activities for 2019 - The report highlights various activities in 2019 including its regulatory activities, international collaborations, actions to raise awareness and visibility, and the function of the APDP.

- **Regulatory Activities** - The APDP undertook a series of regulatory actions in 2019 pursuant to its obligations under the Law No. 2017-20 on the Digital Code and the Data Protection Law of 2019. In particular, its authorizations, declarations, complaints and opinions warrant attention. In total, the APDP issued 91 decisions relative to authorizations and declarations, and received four complaints.
    - Authorizations - The report highlights numerous APDP authorizations including for government entities to process biometric data when issuing passports, enable health application processing, issue biometric identity cards for census purposes, financial data sharing, government services, and anti-corruption.
    - Declarations - The APDP received 72 declarations from other government bodies indicating the processing of personal information for government services. The APDP followed up on each of these declarations.
    - Complaints - The APDP received several complaints against foreign technology firms and against users of such services for improper data processing. At the end of the examination, the complaints indicating cybercriminal behavior were transferred to the Central Office for the Repression of Cybercrime. Some complaints led to amicable settlement.
    - Opinions - The APDP issued a number of opinions on topics such as credit information platforms and law enforcement processing of biometric data.

- **International Activities** - The report highlights the various international activities the APDP participated in over the course of 2019, including joint conferences, workshops with other regional regulators, and regional and international events.
- **Awareness and Visibility Actions** - The APDP also conducted numerous awareness-raising events and workshops it hosted to boost the visibility of its mandate. Many of these include training sessions, public and private events, coordination with other government and non-government entities, and outreach events.
- **Function** - The report also highlights the function of the APDP and discusses topics such as plenary sessions, the adoption of regulations, how private firms can acquire services, budgetary limitations and information, challenges, and perspectives.

New Legal Environments - The report highlights the evolving nature of information processing in the market and provides a brief history of data protection in Benin. Notably, the report indicates that the adoption of the EU GDPR had a profound impact on the approach to data protection regulation in Benin, particularly around the surfacing of DPOs in the country and the novel international juridical environment. The Digital Code in Benin implemented the requirement to appoint a DPO, changed the functions of the controller/processor arrangement, expanded the mission of data protection in Benin, and how the APDP trains its delegates within other government bodies.

Video Surveillance - The report dedicates many pages to discussing the problem of video surveillance for data protection in Benin. It identifies three types of video surveillance (deterrent, observation, and invasion) and discusses the complexities each type poses for the enforcement of the Digital Code. After listing the utility of video surveillance, the report highlights obligations for controllers or users of the video surveillance technologies, including the obligation to make a declaration to the APDP, the rights of persons being filmed, how to handle DSARs, and retention periods.

Annex - Finally, the report lists an annex of the four deliberations the APDP conducted over the course of 2019. The report documents the parties, the nature of the processing, the technology involved, reasons and rationales used to apply the law, obligations of parties, and the outcome of the deliberation.

5. MAURITIUS

Background

The Data Protection Office (DPO) is the primary data protection enforcement agency in Mauritius. Housed within the Ministry of Technology, Communication and Innovation, the Office has operated since 2009 and must submit an annual report to the National Assembly of Mauritius under Section 55 of the Data Protection Act. The most recent report was submitted in 2020 with the next edition expected sometime later in 2022. This provides an opportunity to compare reports and track the progress of the DPO in the past two years. The DPO has not released a long-term strategy document.

Key Takeaways

The report identifies the background and organizational structure of the DPO as well as budget expenditures for the 2020-2021 period before delving into key highlights, priorities, and activities in 2020. These highlights cover a range of issues facing the DPO as well as general data protection developments in Mauritius in recent years.

Highlights - The report identifies four primary highlights: (i) ratification of Convention 108+, (ii) passage of the Data Protection (Fees) Regulations, (iii) holding a conference on data protection, and (iv) research and publications.

- **Ratification of Convention 108+** - In September 2020, Mauritius ratified the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+), becoming the first country in Africa to follow this course.
- **Data Protection (Fees) Regulations 2020** - The report highlights that the new regulation came into force in August 2020 to assist in the effective implementation of the DPA. In particular, the regulation empowers the DPO to charge fees to controllers and processors for certification services and other activities as well as streamlines the process to submit applications for registration.
- **Data Protection Conference** - The DPO organized a conference to promote awareness of the GDPR and the implementation of the Mauritius' data protection act. The conference drew around 500 participants, including DPOs, lawyers, IT professionals, and compliance offices from the public and private sectors.
- **Research and Publications** - The DPO launched four codes of practice in 2020 to help organizations understand and apply data protection law in their practice. The four guidelines are:
    - Guide on Data Protection for Health Data and Artificial Intelligence Solutions in the Context of the Covid-19 Pandemic.
    - Information Sheet on Privacy and Virtual Currency
    - Code of Practice for the Operation of the Safe City System(s) Operated by the Mauritius Police Force (MPF)
    - Guide on National Security and Privacy

The Covid-19 Pandemic - The report highlights implications of the Covid-19 pandemic for data protection in Mauritius and notes that the DPO maintained continuity of service despite being in lockdown, including registration of controllers and processors, responses to queries on the application of data protection, and reviewing data breach notification assessments and DPIAs. The report provides additional information on the kinds of activities the DPO undertook to ensure continuity of service during Covid-19 including a list of online meetings held by its officers.

Activities - The DPO engaged in nine categories of activities, including its financial status, international collaboration, national engagement, enforcement actions, improvement of legal protection, registration and requests for legal advice, advisory roles and data breach responses, data transfers, and miscellaneous achievements.

- Financial Status - The report highlights the amount of revenue collected in 2019-2020, audit observations, and an application from the DPO to its parent ministry regarding the pay and grading structure of officers at the organization.
- International Cooperation - The report compiles a list of events and organizations the DPO collaborated with in the relevant period.
    - These organizations span continents and sectors and include notable entities like the African Union (AU), the Association Francophone des Autorites de Protection des Donnees Personnelles (AFAPDP), the Commission Nationale de l'Informatique et des Libertes (CNIL), the Council of Europe, the Global Privacy Assembly (GPA), and Global Privacy Enforcement Network (GPEN), and the World Bank.
    - Additionally, the report documents all of the virtual meetings it held with international organizations and participants.
- National Engagement - The report highlights its efforts to spread awareness of data protection to the public, including by launching informational videos, distributing training toolkits, hosting press interviews, participating in data privacy day, launching joint platforms with other public bodies in Mauritius, and hosting in-house training for the public and private sectors.
- Enforcement Actions - During the period covered in the report, the DPO received 60 complaints regarding investigations into various data protection areas such as unauthorized use of CCTV cameras, DSARs, and unlawful disclosure of personal data. The report documents its trend of receiving more complaints each year as well as notes seven important decisions of the DPOs.
- Improving Legal Protection - The report highlights the participation of the DPO in judicial proceedings including important cases before the Supreme Court and the ICT Appeal Tribunal.
- Registration and Requests for Legal Advice - The report documents the number of applications (12,809) for registration as controller and (744) for processor, as well as the number of certificates issued (2,365). Additionally, the DPO received a total of 455 written requests for legal advice.
- Advisory Roles and Data Breach Notification - The report notes the activities of the DPO in providing input to government projects that involve the processing of personal data. Notable projects include national SIM card registration, Covid-19

management systems, and a domestic violence report database. Additionally, the report documents the number of personal data breaches reported to the DPO as well as the number of DPIAs it analyzed on behalf of organizations.

- **Data Transfers and EU Adequacy** - The report indicates that 48 companies received approval to transfer personal data outside of Mauritius and that the DPO aims to achieve EU adequacy in the coming period. The DPO has drafted and submitted the Terms of Reference (ToR) to its parent Ministry to invite proposals for outside expert consultancy to complete an assessment of Mauritius' existing data protection law for this end.
- **Miscellaneous Achievements** - Finally, the report lists other achievements for 2020 including the launch of a new DPO website, delays in international standards setting projects, and new projects in the pipeline such as creating a helpdesk, an interactive forum, and a new computerized system.

6. CÔTE D'IVOIRE

Background

The Telecom regulator of Côte d'Ivoire (Autorité de Regulation des Telecommunications/TIC de Côte d'Ivoire) is responsible for supervising the postal sector, electronic transactions, information network and systems security, and compliance with the country's data protection rules. In respect of the latter, the ARTCI focuses on checking stakeholders' compliance with the Côte d'Ivoire Data Protection Law from June 2013. This includes informing data subjects and controllers about their rights and obligations, addressing individuals' complaints, granting authorisations to controllers for data processing activities and exercising its corrective powers (including to impose financial penalties). It has rulemaking power to regulate specific elements of the law. Its 2019 Annual Report of activities provides an overview of its organization and functioning, cooperation with other regulators, recent regulatory acts and opinions, and supervisory activities in the field of data protection.

Key Takeaways

Staffing and governance

On December 31, 2019, the ARTCI had 225 employees, of which 48% were women and 52% men.

Within the ARTCI, there are dedicated Directorates for Data Protection and International Cooperation, as well as an advisory Committee for Data Protection. The latter examines the technical, legal and ethical aspects related to data protection, and counts on two sub-committees: a technical one, charged with checking compliance with data protection law,

and an ethical & moral one, charged with supervising personal data processing for commercial purposes, safeguarding privacy, human dignity and minor protection.

International context

The ARTCI participates in the activities of several international organizations, notably:

- The International Telecommunications Union (ITU), notably in its Telecommunications Development Advisory Group;
- The African Telecommunications Union (UAT);
- The French-speaking network of telecommunications regulators (FRATEL);
- The Francophone Association of Data Protection Authorities (AFAPDP); and
- The African Network of Data Protection Authorities (RAPDP).

In the context of the latter, the ARTCI helped approve the Network's 2019-2020 Action Plan, which included increasing cooperation and affiliation of the RAPDP in African institutions (African Union and ECOWAS), and the promotion of privacy and data protection in African countries which intended to legislate in these matters.

Opinions, decisions and audits

In 2019, the ARTCI issued 39 opinions and decisions (including sanctions) in the exercise of its powers and competences. None of them focused on personal data protection, but rather on telecommunications and postal activities.

In the context of its cybersecurity supervision activities, the ARTCI implemented action to tackle cyber criminality, processing a total of 4505 complaints (a 57.52% increase from 2018) and addressing 97 potential criminals. The top 3 infringments reported by the ARTCI relate to electronic transaction fraud, identity theft and the publication of sexually explicit images.

The ARTCI also conducted 6 organizational, physical and vulnerability audits on different public authorities' information systems, including the Social Security (CNPS), the Ministry of Transportation and the National Press Authority (ANP). The regulator also audited 6 companies for compliance with the Data Protection Law: CNPS, STANDARD CHARTERED BANK, LONACI, OLAM, CAAT, KPMG.

Personal data protection

In Côte d'Ivoire, personal data processing by organizations is subject to one of two regimes, depending on the nature of the processing at stake: one of prior notification to the ARTCI, or one of prior authorization from the ARTCI. The latter is the case of processing involving:

- Genetic, health and scientific research data;
- Criminal convictions and offenses data;
- National identification numbers and other unique identifiers (such as telephone numbers);
- Biometric data;

- Public interest purposes, including historic, statistic and scientific research; and
- Data transfers to third countries.

Data processing in the context of public services is subject to a prior opinion from the ARTCI, if it pursues one the following objectives:

- National security and defense;
- The prevention, investigation, prosecution and execution of criminal offenses and penalties;
- Population census;
- Salary, pension, tax, duty, levy and other types of financial processing.

The ARTCI issued its opinion in the context of the Côte d'Ivoire Data Protection Law's approval, and has proposed to the competent Ministry (MENUP) two ordinance drafts, including one on the processing of personal data in the national legal persons register.

During the course of 2019, more than 150 organizations contacted the ARTCI to obtain information about the steps they needed to take to comply with the country's data protection rules.

In 2019, the ARTCI processed 46 complaints, 45 of which were submitted by natural persons, and 1 from a legal person. The Annual Report's examples mention two controls which the ARTCI carried out as a result of such complaints: one against the use of a biometric system to monitor attendance at a school, and another related to the unauthorized publication of hotel guests' personal data on Facebook. It is also noteworthy that the ARTCI addressed complaints under the Côte d'Ivoire consumer law framework that closely relate to data protection, notably related to the unauthorized use of telephone numbers and of biometric data.

Future priorities

Although the ARTCI's 2021-2025 Strategic Plan has apparently not been published in the regulator's website yet, Part 5 of the 2019 Annual Report previews some of the ARTCI's regulatory priorities in the field of data protection. Those include:

- Increasing the ARTCI's visibility in the field, notably by setting up a dedicated website and improving its communication with the public about data protection rights and principles;
- Automating formal procedures, notably by using decision and audit generators;
- Publishing a guide on data retention and deletion for data controllers.

7. BURKINA FASO

Background

The Commission for Information Technology and Freedoms of Burkina Faso (la Commission de l'Informatique et des Libertés (CIL)) is the national body responsible for the protection of individuals in light of the processing of their personal data and responsible for the enforcement of the country's data protection Law 010-2004/AN of 20 avril 2004. The CIL published its Annual Activity Report for 2020. Despite obstacles such as terrorist attacks and Covid-19, CIL managed to take multiple national and international initiatives, during 2020, in order to raise awareness on issues relating to data protection and to assist policy makers, public and private actors in respecting data protection principles when deploying new technologies. In light of the widespread use of digital tools (eg. biometric electoral card, teleworking, MHealth applications for the management of Covid19), CIL is responsible for the protection of fundamental rights and individual and collective freedoms. In the African region, in the year of 2020, CIL had the presidency of the Network of African Data Protection Authorities (NADPA).

Key Takeaways

In its Annual Report, CIL focuses on the six most important actions taken in 2020.

Action 1: Information and raising awareness

The following activities have taken place:

1. Education of people, especially of the younger generation (students in schools), with regard to the digital world. CIL has focused on informing young people on the dangers of social networks and on their responsible use. CIL also promotes its role in protecting fundamental rights.
2. Organization of seminars in order to raise awareness for various actors (eg. politicians, members of cultural organizations, university students etc). There were 7 activities that took place in 2020 which reached approximately 29760 people in total.
3. Provision of support to other structures (Associations, schools, public and private actors) in the form of advice, opinions, lectures etc when asked on topics of data protection (eg. raise awareness for the National Identification Office agents, participation in the second edition of the Open Source National Forum, participation in meetings with actors responsible for administrative information systems, meetings with the Young Women Leader Club *-Club des Jeunes Femmes Leader-* etc). The Report enumerates 19 actions.
4. Public relations (11 in a total) and activities that will enhance CIL' s visibility. Media coverage of the various activities of CIL - approximately more than 30 interviews and reportages took place.

Action 2: Supervision of personal data processing operations

CIL is responsible for supervising controllers whether they comply with the data protection law requirements. This is done both upstream and downstream. During 2020, the CIL received 6 requests to issue an Opinion on projects that involved processing of personal data by both public and private actors. In addition, CIL received multiple declarations of processing operations (45 structures declared 79 files containing personal data) as well as requests to authorize the processing of personal data or the transfer of personal data abroad (CIL received 13 requests to authorize transfer abroad). CIL also examines compliance on the ground, either on its own initiative or on the basis of complaints. In total, CIL performed 123 inspections in 2020.

Action 3: Handling of claims, petitions and complaints

Complaints are handled either by the College of Commissioners (Collège des Commissaires) or by the technical services of CIL. In 2020 CIL received and handled 855 complaints. The majority of complaints related to data theft, the excessive collection of information, the putting in place of video surveillance systems without informing data subjects, the disclosure of personal data, identity theft, webcam blackmailing, hacking of accounts and telephone spying.

Action 4: Legal and technological monitoring

CIL has the **right to advise the government on legislative and regulatory measures** that need to be taken for the protection of fundamental rights in light of the ongoing technological developments (eg. deliberation on the use of pictograms). Most notably, in 2020, CIL initiated the revision of the data protection law. Some of the suggested points were: the reinforcement of the role of CIL (eg. in terms of enforcing the law), extension of data subject rights and especially the addition of the right to be forgotten, international cooperation with other data protection authorities, strengthening of the framework for data transfers etc. This revision was not adopted in 2020 due to the national elections that took place.

CIL's **technological monitoring** consists of identifying the impact of the use of new technologies on fundamental rights. For example, the impact of applications relating to the management of Covid19 (eg. Corona-Detect, Corona-Contact etc). For that purpose, CIL held meetings with the Ministry of Health. Additionally, CIL developed a charter for the responsible use of social networks.

Action 5: National and international cooperation

Cooperation with multiple actors which form part of the digital ecosystem is a necessity. On a national level, the CIL signed the following agreements: Convention with the National Commission for Human Rights (la Commission Nationale des Droits Humains (CNDH)), Convention with the Central Brigade for Cybercrime (Brigade centrale de lutte contre la cybercriminalité (BCLCC)) on a common front against cybercrime, Convention with the Nazi Boni University (UNB) which aims to:

- The regular training of UNB' s students and personnel on data protection issues,
- Advising the UNB on new projects that involve automated processing and

- The organization of common activities.

CIL has participated in joint activities, campaigns and seminars to raise awareness on the responsible use of social media and on cybercrime. On an international level, CIL participated in the annual meeting of the Global Privacy Assembly (GPA), in workshops and international conferences (eg. CPDP).

Action 6: Leadership and support

CIL consists of two bodies: a deliberative body called the College of Commissioners (Collège des Commissaires) and an executive body, the President, assisted by the General Secretary. The College of Commissioners meets regularly once per month to deal with complaints received, to issue opinions and to decide on authorizations requested. There are also exceptional meetings that might be arranged in case of urgent matters.

Management of Human and financial resources

With regard to human resources, by the end of the year 2020, 38 employees were occupied in various posts. Reinforcing the personnel is one of CIL's fundamental concerns. Most importantly, there is a need for specialized personnel. However, specialized training of the staff is a costly activity. The initial plan for 2020 was to arrange 7 training activities. Unfortunately, due to Covid19 and the high costs, only 1 training took place. This training educated the employees on techniques and practical methods that would allow them to excel their professional skills.

With regard to financial resources, they come exclusively from the State budget and public funds. Covid19 had a negative financial impact on CIL given that its budget was reduced by 20%. As to the execution of its budget, CIL used it 100% for 2020 to cover the above mentioned 6 activities, ie. (1) information and raising awareness, (2) supervision and monitoring, (3) handling of claims, (4) petitions and complaints, (5) legal and technological monitoring, (6) national and international cooperation, (7) leadership and support. The CIL has the intention to acquire land in order to build its headquarters.

Difficulties & Recommendations

Most difficulties experienced during 2020 relate to the low budget reserved for CIL. In addition to that, difficulties have been stemming from Covid 19, problematic Internet connectivity in the country and from the slow rhythm of adopting the revised law. CIL recommends that the budget is raised in order to perform its activities in a meaningful way and in order to have specialized staff as well as better infrastructure. Aside the budget, CIL suggests the following:

- Reinforcement of its powers
- Ratification of the African Union Convention on Cybersecurity and Personal Data Protection.
- Adherence to Convention 108 of the Council of Europe.
- Better life and working conditions for its staff.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005
FPF.ORG | info@fpf.org