Data Protection in Africa: A Look at OGP Member Progress

Tara Davis

August 2021

altadvisory question convention .africa

Open Government Partnership

Acknowledgements

OGP would like to thank the following stakeholders who generously gave their time to contribute to this report and whose input has been invaluable: Alison Tilley, Amrit Labhuram, Anri Van der Spuy, Chawki Gaddes, Fatou Jagne, Gabriella Razzano, 'Gbenga Sesan, Grace Bomu, Hlengiwe Dube, Mugambi Laibuta, Mustafa Mahmoud, Teki Akuetteh Falconer, and the four stakeholders who wished to remain anonymous.

For the drafting of this report, OGP is grateful to Tara Davis of ALT Advisory, supported by Avani Singh and Wendy Trott. For initial reviews of the preliminary draft of this report, OGP is thankful to Michael Power, Joseph Foti, Sandy Arce, and Jessica Hickle.

OGP would also like to thank Omidyar Network for their support and helpful feedback in the first phase of this research project.

Disclaimer

While OGP, including its directors, employees, consultants, partners, and affiliates, has made every attempt to ensure that the information contained in this analysis is up-to-date, is compliant with the applicable legislation and regulations, and has been obtained from relevant and reliable sources, OGP is not responsible for any errors or omissions, or for the results obtained from the use of this information.

All information contained in this analysis is provided "as is", with no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability, and fitness for a particular purpose.

In no event will OGP be liable to any natural or juristic person or entity for any decision made or action taken in reliance on the information contained in this analysis or for any consequential, special, or similar damages, even if advised of the possibility of such damages.

The information in this report is as of **1 July 2021**.

TABLE OF CONTENTS

ACRONYMS **3**
GLOSSARY **4**
EXECUTIVE SUMMARY **5**
INTRODUCTION **15**
THE RIGHT TO PRIVACY AND DATA PROTECTION **17**
OVERVIEW OF THE REGULATORY CONTEXT **24**
SCOPE OF APPLICATION **27**
Focus 1 | Legislative Exclusions 28
Focus 2 | Application of the Legislation to Foreign Entities 31
CONTEXTUAL AND LEGISLATIVE ANALYSIS **33**
TRANSPARENCY **33**
Focus 3 | The Right to Notification 35
Focus 4 | Breach Notification 36
Focus 5 | Data Processing Registers 39
Focus 6 | Terms of Service Icons 42
ACCOUNTABILITY **43**
Mechanisms for The Data Subject to Hold the Data Controller Accountable **44**
Focus 7 | Civil Liability 44
Mechanisms for the Regulatory Authority to Hold the Data Controller Accountable **46**
The Powers of the Regulatory Authority 47
Focus 8 | The Power to Investigate 48
Focus 9 | The Power to Sanction 48
The Structure of the Regulatory Authority 50
Focus 10 | Independence 50
Focus 10.1 | Collaboration and Reporting Requirements 53
Focus 10.2 | Budget 53
Focus 10.3 | Security of Tenure 54
The Capacity of the Regulatory Authority 61
Focus 11 | Resources 61
The Regulatory Ecosystem **62**
Mechanisms for the Public to Hold the Regulatory Authority Accountable **63**
Focus 12 | Regular Reporting 64
PARTICIPATION **66**
Data Subject Participation 66
Focus 13 | The Right to Access Personal Data 68
Focus 14 | The Rights to Request the Correction or Deletion of Personal Data 70
Focus 15 | Consent 71
The Regulatory Authority's Domestic Participation 73
Focus 16 | Stakeholder Engagement 73
Focus 17 | The Regulatory Authority's Mandate to Participate in Policy Formulation 74
The Regulatory Authority's Regional and International Participation 74
Focus 18 | Regulatory Authority Participation 75
AUTOMATED PROCESSING **77**
CONCLUSION **80**
REFERENCE LIST **81**

ACRONYMS

AFAPDP	the Association of Francophone Data Protection Authorities
CSO	civil society organisation
DPA	data protection authority
ECtHR	the European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation 2016/679
ICO	information commissioner's office
INPDP	Instance nationale de protection des données personnelles
OECD	the Organisation for Economic Co-operation and Development
OGP	Open Government Partnership
POPIA	Protection of Personal Information Act 4 of 2013 (South Africa)
RAPDP	Réseau Africain Des Autorités De Protection Des Données Personnelles (the African Network of Data Protection Authorities)
UK	United Kingdom
UK ICO	United Kingdom Information Commissioner's Office
US	United States of America

GLOSSARY

Data protection legislation in the members recognizes roles which are substantially similar in function but are named differently. To avoid ambiguity, we have compiled this glossary of terms which will be used throughout the report.

automated processing	The processing of personal data using digital means without human involvement.
data subject	The person to whom personal data relates. Domestic legislation generally defines this term to refer to a living person while some jurisdictions also provide for a data subject to be a company.
data controller	The body or organisation which determines the purpose of and means for processing personal data.
data processor	A person or entity that processes personal data for a data controller in terms of a contract or mandate, without coming under the direct authority of the data controller.
European Directive	European Directive 95/46/ EC.
member	An African country which is a member of the Open Government Partnership.
personal data	Information which relates to a data subject. This is also often referred to as personal information. Domestic legislation generally defines the term by noting the types of information which would constitute personal data, some of which may include race, identifying numbers, biometric information or contact information.
processing	Any operation or activity concerning personal data. Domestic legislation generally notes that such activities or operations may be conducted by manual or automatic means and includes a list of the type of conduct included. Some of the most common types of activity include collection, storage, use and modification.
regulatory authority	The body, often established in data protection legislation, that is responsible for the enforcement of the legislation.

EXECUTIVE SUMMARY

The global adoption of data protection legislation has been slow. Only 66 per cent of countries in the world have legislation in force, while an additional 10 per cent have draft legislation. African countries are behind this global trend, with only 52 per cent having data protection legislation in force. Of OGP's fourteen African members, ten states have enacted data protection legislation,[1] two states have draft legislation,[2] and two have no law at all.[3]

Significantly, all fourteen African OGP members recognise the right to privacy domestically, and there is growing consensus that the right (as well as the right to be free of unlawful discrimination, bias, or any other denial of due process) must evolve to include considerations of data protection. Importantly, it was noted throughout the report that the regulation of data protection must strike an appropriate balance with important human rights, such as access to information and freedom of expression.

This report aims to understand and analyse the context and major barriers to effective data protection in the fourteen African OGP members and to make informed recommendations that strengthen data protection on the African continent. In doing so, this report focuses on three thematic areas that are of particular interest to OGP: transparency, accountability, and participation. Within these thematic areas, eighteen focus areas were analysed, consisting of common mechanisms included in data protection legislation that enable an effective framework and contribute to greater transparency, accountability, and participation.

A summary of the outcomes and findings of the contextual and legislative analysis in each thematic area are briefly detailed in this executive summary.

[1] These include Burkina Faso, Cabo Verde, Côte d'Ivoire, Ghana, Kenya, Liberia, Malawi, Morocco, Nigeria, Senegal, Seychelles, Sierra Leone, South Africa, and Tunisia.

[2] These include Malawi and Nigeria.

[3] These include Liberia and Sierra Leone.

Transparency

Transparency is an important tenet of data protection legislation: it builds trust between the data subject and the data controller, and it empowers the data subject to exercise control over their data and make informed decisions about which service providers to use. It further enables data subjects to seek redress if necessary and works to increase accountability. The legislation of all African OGP members included some commitment to transparency, with five members explicitly including it as a condition for lawful processing. Within this thematic area, four focus areas were analysed: the right to notification, notification in the event of a data breach, data processing registers, and terms of service icons.

Significantly, twelve members provide data subjects with the right to be notified that their personal data is being processed. Many correlative rights, such as the right to request the deletion or rectification of personal data, as well as accountability mechanisms—such as the right to lodge a complaint with a regulatory authority—are premised on the data subject being aware that a certain data controller is processing their personal data. The absence of notification makes it difficult for a data subject to be aware of non-compliance and undermines their ability to exercise additional rights or seek redress.

Notification in the event of a data breach is another important mechanism that increases transparency and enables data subjects to seek redress. The effectiveness of such an obligation is undermined in three ways: first, through the absence of a prescribed timeframe for notification; second, through the use of vague terms for the notification period; and third, through the inclusion of exceptions that allow for non-reporting. Legislative texts that include these concerns may be open to abuse and provide loopholes for non-compliance.

It was recognized by stakeholders that transparency, at a bare minimum, requires the publication of information, specifically relating to data controllers and data processors. This may be achieved through a data processing register which is required by eight of the members. Such a register allows a data subject to confirm which data controllers are bound by the obligations of the data protection legislation and determine which data controllers they may exercise their rights against. The effectiveness of the register depends on its accessibility—which should require manual and digital access. Significantly, all eight members require that the register be made publicly available.

Interestingly, terms of service icons were not provided for by the legislation of any members. These easily identifiable, standardized icons can be used to convey large quantities of information to a data subject, but they are not utilized by the OGP members. The reason for their exclusion is uncertain.

Accountability

Accountability in data protection is context-dependent, which makes it difficult to develop uniform rules or standards for an institutional framework for accountability. Despite this, common mechanisms are utilised in data protection legislation and were analysed in the context of the following accountability relationships: the ability of a data subject to hold a data controller accountable, the ability of the regulatory authority to hold a data controller accountable, and the ability of the public to hold the regulatory authority accountable.

Mechanisms for the Data Subject to Ensure Accountability

A data subject can hold a data controller accountable through civil liability which is provided for in the data protection legislation of six OGP members. The exclusion of such a provision does not necessarily preclude a data subject from bringing such an action as the domestic law may provide for it elsewhere. The effectiveness of civil liability relies on the judicial process and stakeholders noted that accountability is undermined by the court system. The technical and evolving nature of data protection issues has meant that judges are ill-equipped to preside over such matters. It was noted that these concerns extend to all actors in the accountability chain—members of the regulatory authority, members of the police service, lawyers, and judges—all of whom require a level of specialisation. It was accordingly recommended that education and training be provided to equip these actors to determine whether a violation has occurred and to understand and enforce appropriate remedies. In relation to the judiciary, it was recommended that specialised courts, or specialised units and registries within courts, be set up to adjudicate on these matters.

Mechanisms for the Regulatory Authority to Ensure Accountability

Significantly, the legislation of twelve members designates a regulatory authority that is empowered to monitor and enforce compliance with the data protection law. Its ability to effectively execute this mandate depends on three overlapping factors: its powers, its structure, and its capacity.

Concerning the regulatory authority's powers, two focus areas were analysed: the power to investigate and the power to sanction. The legislation of the members provides significant powers of investigation—eleven members empower the regulatory authority to investigate instances of non-compliance and nine provide powers of access and seizure. It was noted, however, that the effectiveness of any investigation requires high levels of expertise, necessitating the regulatory authority to be appropriately resourced. The power to sanction was considered by stakeholders as vital for accountability, with several noting the need to ensure that non-compliant data controllers are punished to avoid creating a culture of impunity. It was further noted that the sanction of a fine is only prohibitive if the monetary amount is sufficiently high enough to act as a deterrent.

The structure of the regulatory authority significantly impacts its ability to bring about accountability. It was found that three institutional or operational concerns—budget, structural and reporting requirements, and security of tenure—may undermine a regulatory authority's institutional independence, which in turn may undermine adjudicatory independence.

The independence of the regulatory authority was noted by stakeholders as an imperative for effective data protection. However, such independence may be undermined by a lack of financial independence: a reliance on government bodies for funding creates an opportunity for the allocation of the budget to be weaponised, either as a punishment or to secure allegiance. This may ultimately influence the regulatory authority's decisions, particularly in response to processing conducted by government bodies.

Independence was also found to be undermined by legislative collaboration and reporting requirements. Such a legislative obligation was noted to create a chain of authority, with the regulatory authority in a subsidiary position, which may result in the government having undue influence over the regulatory authority.

Lastly, stakeholders consider the security of the regulatory authority's tenure to be a critical component of institutional independence. It allows regulatory authorities to make difficult or unpopular decisions. Without security of tenure, a regulator may, out of fear of losing their job, respond to a government department differently than they would otherwise, for example, by choosing to ignore evidence of non-compliance with the law. The ability to remove the members of the regulatory authority gives certain government departments or individuals significant power over the members of the regulatory authority, which may result in undue influence over their adjudicatory independence.

The regulatory authority's capacity was the final factor analysed under its ability to monitor and enforce compliance with data protection legislation. This focus area concerned the regulatory authority's resources. Stakeholders noted the enormous expense required for the regulator to operate and the need to draw appropriately skilled personnel. Stakeholders suggested that regulatory authorities may be deliberately underfunded and staffed with employees who have little experience in order to undermine their ability to function.

Mechanisms for the Public to Ensure Accountability

This focus area concerned the regulatory authority's reporting obligations. The public has an interest in ensuring that the regulatory authority executes its mandate effectively, and to do so requires access to information concerning its functions. Stakeholders noted that the most important thing for a regulatory authority to release is the information that allows other parties to monitor them—particularly in a context where institutional accountability might be lacking. The dissemination of such information will allow civil society organisations to monitor the enforcement of the law and play an oversight role. To effectively do so, regulatory authorities are encouraged to submit publicly available quarterly reports.

Participation

This thematic area concerns participation in three instances: first, the data subjects' participation in, and control over, the processing of their personal data; second, the participation of the regulatory authority domestically through its engagement with stakeholders and its ability to participate in legislative and policy developments; and third, the participation of the regulatory authority regionally through its cooperation in regional associations, networks, and organizations. Within this thematic area, six focus areas were analyzed: the right to access personal data, the right to request the correction or deletion of personal data, consent, stakeholder engagement, policy formulation, and regulatory authority participation.

Data Subject Participation

Data subject participation is enabled through the provision of three rights—the right to access personal data; the right to request the correction of personal data, and the right to request the deletion of their personal data. Significantly, twelve OGP members provide data subjects with the right to access their personal data, which enables the exercise of additional rights. Stakeholders noted that there is a gap between the information that a data subject has access to and the type of information that is required to lay a complaint, undermining their right to an effective remedy. It was further noted that the right to access personal data is undermined by inaccessible processes that are uncertain, are complicated, or provide complex language and literacy hurdles.

Twelve OGP members provide data subjects with the right to request the correction or deletion of their personal data. It was noted that the exercise of this right implicates other important rights such as access to information and freedom of expression. It was further noted that this right relies on the data subject's awareness that a data controller is processing their personal data and is accordingly enabled through their right to request access and their right to notification. The undermining of their access and notification rights accordingly diminishes their capacity to exercise the right to request the correction or deletion of their personal data.

Consent was an additional mechanism analyzed as it enables participation by allowing a data subject to control the ways in which their personal data is used. The legislation of eight OGP members provides requirements for valid consent. Notably, Kenya is the only member that expressly requires opt-in consent.

It was further noted that as awareness regarding data protection increased in one OGP member, the number of complaints received by the regulatory authority increased, providing some evidence that increased awareness correlates with increased participation by data subjects.

The Regulatory Authority's Domestic Participation

In this section, two focus areas were analysed: stakeholder engagement and the regulatory authority's mandate for policy formulation. Stakeholders noted that effective engagement requires the regulatory authority to have a cross-cutting mandate to facilitate engagements with multiple stakeholders, and it requires that individuals have direct access to the regulatory authority. It was further emphasized that data protection should be a participatory process that requires that regulatory authorities consult with stakeholders on the development of legislative instruments. The regulatory authorities of eight OGP members are empowered to participate in domestic policy. It was further noted that the regulatory authority will have the relevant expertise to guide data protection policy and their inclusion in the process provides an opportunity to strengthen weaknesses that exist in the regulatory system.

The Regulatory Authority's Regional and International Participation

It was noted that effective data protection requires the regulatory authority to be integrated into regional associations to assist with coordination and the development of jurisprudence and resources. Regional cooperation was noted as being particularly important for regional concerns such as cross-border data transfers. Although such bodies do exist, they are not at a stage where they are providing technical support to each other. Greater regional cooperation was posed as a possible solution to the lack of legitimacy which stems from laws being drafted by external actors or funders. It was further noted that some concerns could be mitigated if the process was African-led, and if jurisprudence could be developed regionally. Increased regional cooperation was also recommended to harmonise legislative standards and to facilitate and enable technical aspects such as cross-border data transfers.

Important Components of Data Protection Regimes in Africa

The findings of the legislative and contextual analyses of the eighteen Focus Areas are briefly detailed in the tables below.

Focus Areas	Findings
Focus 1 | Legislative Exclusions	The effectiveness of data protection legislation is undermined if a significant number of entities are excluded from complying with its requirements. All members—except Malawi—include legislative exclusions, the most common of which are processing for domestic purposes, national security, and processing for journalistic, literary, or artistic purposes. Exclusions that are drafted in vague or broad terms may be open to abuse.
Focus 2 | Application to Foreign Entities	The legislation of most members exclude application to foreign entities that only forward personal data through the territory.

Transparency

Focus Areas	Findings
Focus 3 | The Right to Notification	Twelve OGP members provide data subjects with the right to be notified that their personal data is being processed. In the absence of notification from a data controller that a data subject's personal data is being processed a data subject may be unaware of non-compliance, which undermines their ability to exercise additional rights.
Focus 4 | Breach Notification	Only four members require notification in the event of a data breach. It was noted that the obligation to notify a data subject in the event of a data breach contributes to increased transparency and enables a data subject to control their personal data. The purpose of such an obligation may be undermined by the legal text in three ways: (1) through the absence of a prescribed timeframe for notification; (2) through the use of vague terms for the notification period; and (3) through the inclusion of exceptions which allow for non-reporting.
Focus 5 | Data Processing Registers	Eight OGP members require the development of a data processing register, which is a consolidated bundle of information that the regulatory authority develops and maintains. To be effective, and to contribute to transparency and enable the exercise of data subject rights, the register must be accessible which requires digital access.
Focus 6 | Terms of Service Icons	None of the members require the use of terms of service icons.

Accountability

Focus Area	Findings
Focus 7 | Civil Liability	The effectiveness of civil liability is undermined by the lack of expertise in the judiciary, the police service, and the legal profession.
Focus 8 | The Power to Investigate	This power significantly impacts on a regulatory authority's ability to sanction non-compliant parties and requires it to have the necessary resources and capacity, as investigations into non-compliance entail a high level of technical expertise. This in turn requires that the regulatory authority be appropriately resourced with such technical expertise.
Focus 9 | The Power to Sanction	It was noted by stakeholders that a sanction will only be effective if it is prohibitive, which requires that the fine must be sufficiently high to act as a deterrent. Legislatively low amounts weaken the role of the regulatory authority.
Focus 10 | Independence	Institutional independence is undermined by concerns relating to budget, collaboration and reporting requirements, and security of tenure which in turn may undermine adjudicatory independence.
Focus 11 | Resources	In order for the regulatory authority to function effectively, it requires sufficient financial resources to hire appropriately skilled staff members.
Focus 12 | Reporting	The regulatory authority should provide publicly available reports that allow external actors to hold it accountable.

Participation

Focus Area	Findings
Focus 13 | The Right to Access Personal Data	This right is undermined in two ways: (1) there is gap between the type of information required to lay a complaint and the type of information that a data subject has access to, which in turn undermines a data subject's right to an effective remedy; and (2) it is made inaccessible by processes that are uncertain, are complicated, or provide complex language and literacy hurdles.
Focus 14 | The Right to Request the Correction or Deletion of Personal Data	These rights rely on the data subject's awareness that a data controller is processing their personal data and is accordingly enabled through this right to request access and their right to notification. The undermining of these rights diminish their capacity to exercise the right to request the correction or deletion of their personal data.
Focus 15 | Consent	Opt-in consent is not generally required in OGP members.
Focus 16 | Stakeholder Engagement	Effective engagement requires the regulatory authority to have a cross-cutting mandate to facilitate engagements with multiple stakeholders, and it requires stakeholders have direct access to the regulatory authority.
Focus 17 | The Regulatory Authority's Mandate to Participate in Policy Formulation	The regulatory authority will have the relevant expertise to guide data protection policy and their inclusion in the process provides an opportunity to strengthen weaknesses that exist in the regulatory system.
Focus 18 | Regulatory Authority Participation in Regional Bodies	Effective data protection requires the regulatory authority to be integrated into regional associations in order to assist with coordination and the development of jurisprudence and resources.

Recommendations to Strengthen Transparency

- Proactive audits of data controllers should be conducted in order to confirm their compliance with data protection legislation. Such audits are useful to ensure that data subjects have been notified that their personal data is being processed, which will enable the exercise of additional rights. It is envisaged that members will be the implementing actors, although private sector actors may also consider conducting such audits.
- The obligation to notify the regulatory authority and data subjects in the event of a breach must prescribe specific and certain time frames. The use of vague time-frames is open to abuse and may lead to non-compliance. It is envisaged that members will be the implementing actors.
- Data processing registers should be made available to the public. Any prescribed fee must not limit access to certain members of the public. The mechanism that provides access to the register must be accessible, and is recommended to include digital access. It is envisaged that members will be the implementing actors.
- The mechanisms or processes that enable the exercise of the right to access information must be accessible. It is envisaged that data controllers will be the implementing actors.

Recommendations to Strengthen Accountability

- All key-players in the accountability ecosystem should have the requisite technical capacity and knowledge to handle data protection matters. This includes members of the regulatory authority, members of the police service, lawyers, and judges. All of these actors must be appropriately trained with the skills to determine whether a data protection violation has occurred and to understand and enforce the appropriate remedies. It is envisaged that members, regulatory authorities, and professional bodies will be the implementing actors.
- Specialised courts, or units and registries within courts, should be designated to adjudicate on data protection issues. It is envisaged that members will be the implementing actors.
- Sanctions in terms of monetary fines must be sufficiently high to act as a deterrent. It is envisaged that members will be the implementing actors.
- The institutional independence of the regulatory authority must be secured in order to ensure adjudicatory independence; this requires a sustainable financial model that secures the regulatory authority's financial independence. It is envisaged that members will be the implementing actors.
- The regulatory authority must be appropriately capacitated. This requires sufficient funding to employ technically skilled staff. Members of the regulatory authority should consider alternative ways to draw in technical skills, such as public-private partnerships, the development of networks, and internships. It is envisaged that members and regulatory authorities will be the implementing actors.
- The regulatory authority should publicly report on its activities and functions to enable external actors to hold it accountable. It is recommended that such reports be released quarterly and should include disaggregated statistics and information. It is envisaged that regulatory authorities will be the implementing actors.

Recommendations to Strengthen Participation

- Audits should be conducted to determine what information a data subject has access to and what information is required in order to lay a complaint. The two must align to enable a data subject to exercise their right to an effective remedy. It is envisaged that data controllers will be the implementing actors.
- Data controllers must ensure that the process they implement to realize a data subject's right to request access to their personal data is clear, is certain, and considers contextual language and literacy barriers. The law should provide for minimum requirements that notes a timeframe for a response, it should not entail a cost, and the information should be provided in an intelligible format. It is envisaged that data controllers and members will be the implementing actors.
- Data subject participation is undermined by a lack of awareness of data subject rights. Awareness campaigns should be undertaken to facilitate data subject participation. It is recommended that linking data protection concerns to real-life harms makes the content more accessible. It is envisaged that the regulatory authorities, members, and civil society organizations will be the implementing actors.
- The regulatory authority should have a cross-cutting mandate and the capacity to facilitate multi-stakeholder conversations. It is envisaged that members and the regulatory authorities will be the implementing actors.
- Data protection should be a participatory process: to enable this, regulatory authorities should consult with stakeholders before releasing regulatory documents such as guidance notes. It is envisaged that regulatory authorities will be the implementing actors.
- A body or mechanism should be established to enable greater regional cooperation. It is recommended that such coordination take place at the African Union level and an office similar to the European Data Protection Board should be established. Such a body could provide regional guidance to states on data protection issues. It is envisaged that members and the African Union will be the implementing actors.

INTRODUCTION

The information age has placed new emphasis on data protection and the right to privacy. In 2020, it was estimated that people created an average of 2.5 quintillion bytes of data a day.[4] This proliferation of data creation, coupled with the technological capacity to store and analyse unprecedented amounts of data, has caused concerns around its misuse.[5] Small amounts of information concerning an individual may be collated to create a profile that is used to inform decisions, such as the type of content or advertisements to make available to a person. Sometimes it is used to inform consequential decisions, like whether to grant someone a loan. The mass creation and collection of personal data has also increased concerns regarding identity theft and fraud. As noted by the United Nations High Commissioner for Human Rights:[6]

> "Digital technologies that continually exploit data linked to people's lives, are progressively penetrating the social, cultural, economic and political fabric of modern societies. Increasingly powerful data-intensive technologies, such as big data and artificial intelligence, threaten to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree. While there is no denying that data-driven technologies can be put to highly beneficial uses, these technological developments carry very significant risks for human dignity, autonomy and privacy and the exercise of human rights in general if not managed with great care."

In response, countries have incrementally enacted legislation that aims to regulate how personal data is processed and to give effect to the right to privacy. The right to privacy is an internationally recognised human right that is fundamentally important in and of itself, but it also enables other rights, such as the right to freedom of expression, the right to freedom of religion, belief and opinion, the right to freedom of association, the right to protest and right to freedom of movement.

Despite concerns about data protection being raised decades ago,[7] the adoption of relevant legislation has been slow. Currently, only 66 per cent of countries in the world have legislation in force, while an additional 10 per cent have draft legislation.[8] African countries are behind this global trend, with only 52 per cent having data protection legislation in force.[9] Such slow development has been attributed to assumptions that African countries prioritise collective rights over rights that are primarily concerned with the individual, such as the right to privacy.[10]

---

[4] Jacquelyn Bulao, 'How Much Data is Created Every Day in 2021?' *Techjury*, accessed on 19 May 2021, available here.
[5] David Banisar, 'The Right to Information and Privacy: Balancing Rights and Managing Conflicts,' *World Bank Institute Governance Working Paper Series*, 6, available here.
[6] United Nations Human Right Council, 'The Right to Privacy in the Digital Age,' *Report of the United Nations High Commissioner for Human Rights*, 3 August 2018, A/HRC/39/20, available here.
[7] The OECD issued guidelines on data protection as early as 1980, see for example: International Network of Privacy Law Professionals, 'A Brief History of Data Protection: How Did it All Start?' 22 May 2021, available here.
[8] United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide,' accessed on 19 May 2021, available here.
[9] *Id*.
[10] Alex Boniface Makulilo, 'Privacy and Data Protection in Africa: A State of the Art 2012,' *International Data Privacy Law* vol. 2. no. 3, 163, available here.

The omission of the right to privacy in the African Charter on Human and Peoples' Rights is regarded by some as indicative of this de-prioritisation. Such assumptions are spurred on by narratives that individuals on the continent are not concerned about data protection and that it is conceptualised as an elitist concern. Although some stakeholders agree with this view, others have debunked this rhetoric by noting harms and concerns relating to privacy rights infringements on the continent. Teki Akuetteh Falconer, the Founder and Executive Director of Africa Digital Rights' Hub and a previous member of the regulatory authority in Ghana, remarked on these narratives and noted that "we get carried away with the concept and notion of data protection itself, and the fact that it has a European origin. But it doesn't take away from the fact that it is something that is very real to us. To say there are no implications cannot be true."

Purpose of the Research

In order to unpack and understand the contextual nuance of data protection in Africa, the Open Government Partnership (OGP) commissioned research on data protection in its fourteen members.[11] Out of the fourteen members, ten[12] have enacted data protection legislation, two have draft legislation,[13] and two have no law at all.[14]

The purpose of this report is to understand and analyse the context and major barriers to effective data protection in the fourteen African OGP member states and to make informed recommendations that strengthen data protection on the African continent. In doing so, the report analyses eighteen focus areas—legislative mechanisms which contribute to an effective data protection framework. Sixteen of the focus areas aim to increase transparency, accountability, and participation—the three thematic areas that this report is primarily concerned with.

Research Methodology

The research was conducted in three phases. The first phase entailed a legislative review of the data protection law in each member. Despite the contextual differences in languages, legal systems, traditions, and values that exist across countries, commentators and academics have noted that there is consensus regarding the basic rules and content to be included in data protection legislation.[15] The review focused on the legislative mechanisms that contribute to transparency, accountability, and participation. The second phase involved engagements with various content experts, both on the continent and abroad, to gain an understanding of the contextual barriers to the effective implementation of data protection. The third phase culminated in desktop research and a synthesis of the findings. Throughout the research, the aim was to understand the particularities that emerged in the members in order to make meaningful and responsive recommendations.

---

[11] These include Burkina Faso, Cabo Verde, Côte d'Ivoire, Ghana, Kenya, Liberia, Malawi, Morocco, Nigeria, Senegal, Seychelles, Sierra Leone, South Africa, and Tunisia.
[12] These include Burkina Faso, Cabo Verde, Côte d'Ivoire, Ghana, Kenya, Morocco, Senegal, Seychelles, South Africa, and Tunisia. It must be noted that although Seychelles has enacted legislation, it is not in force.
[13] These include Malawi and Nigeria.
[14] These include Liberia and Sierra Leone.
[15] Anneliese Roos, 'Core Principles of Data Protection Law,' The Comparative and International Law Journal of Southern Africa vol. 39, no. 1, 107, available here.

THE RIGHT TO PRIVACY AND DATA PROTECTION

The right to privacy is broad, evolving, and an enabler of other rights such as freedom of expression, freedom of association, and freedom of movement. As noted by the United Nations High Commissioner for Human Rights:[16]

> "The right to privacy is central to the enjoyment and exercise of human rights online and offline. It serves as one of the foundations of a democratic society and plays a key role for the realization of a broad spectrum of human rights, ranging from freedom of expression and freedom of association and assembly to the prohibition of discrimination and more. Interference with the right to privacy can have a disproportionate impact on certain individuals and/or groups, thus exacerbating inequality and discrimination." (References omitted.)

According to Privacy International,

> Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places, and things, as well as our communications and our information.
>
> The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances.
>
> As a result, privacy is an essential way we seek to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control.

Although domestic conceptions of the right to privacy differ, there is a growing consensus that the right must evolve to include the protection of personal data to enable a data subject to determine what information about themselves is made public and to control how that information is collected and used. This section unpacks the link between the right to privacy and data protection, notes conceptions of the right in African countries, and discusses the importance of balancing the right against other rights such as access to information and freedom of expression.

The right to privacy is well established in international law and is gaining prominence in domestic frameworks on the continent.[17] The right is recognised in Article 17 of the International Covenant on Civil and Political Rights, to which fifty-four African countries have signed or acceded to.[18] The Council of Europe Convention 108 on personal data was one of the earliest—and now one of the most widely influential—international treaties that recognised the need to protect individuals' rights in the use of personal data. Six African states have acceded to the treaty[19] since 1981, when it opened for accession by non-members states, and several others have used it as a model for the development of domestic or regional frameworks on data protection.

---

[16] Above n 6.
[17] Above n 10 at page 163.
[18] United Nations, 'International Covenant on Civil and Political Rights,' status as at 24 May 2021, United Nations Treaty Collection, available here.
[19] Council of Europe, 'Chart of signatures and ratifications of Treaty 108,' (2021), available here.

The African Union Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention) sets the standard for the management of the Information Society in Africa but has disappointingly received only fourteen signatures from countries on the continent.[20] Nevertheless, all of the OGP members in Africa have enshrined the right to privacy in their constitutions, and at least twenty-eight African countries have some form of a data protection law in place—though the degree of enforcement varies widely across the continent.[21]

Table 1: Domestic Recognition of the Right to Privacy

Country	Constitutional Provision on Privacy[22]
Burkina Faso	Yes, article 6 of the Constitution of Burkina Faso, 1991, provides for the right to privacy and confidentiality of correspondence.[23]
Cabo Verde	Yes, major provisions in data protection laws are effectively reproduced in the Constitution in article 41, and the constitutional right of ***habeas data*** in article 46 grants the right to a citizen to request, update, or destroy personal data.
Côte d'Ivoire	Yes, article 8 of the Constitution of Côte d'Ivoire notes that 'the home is inviolable'.
Ghana	Yes, article 18(2) of the 1992 Constitution recognizes the right to privacy.
Kenya	Yes, article 31 of the Constitution of Kenya protects the rights to privacy.[24]
Liberia	Yes, article 16 protects the right to privacy of person, family, home, and correspondence.[25]
Malawi	Yes, article 21 protects the right to privacy.[26]
Morocco	Yes, article 24 of the 2011 Constitution of Morocco guarantees the right to privacy.[27]
Nigeria	Yes, article 21 of the Constitution recognises the right to privacy.
Senegal	Yes, article 13 provides that "the secrecy of correspondence [and] of postal, telegraphic, telephonic and electronic communications" is inviolable, and article 16 provides the same for the domicile.[28]
Seychelles	Yes, article 20 of the Constitution protects the right to privacy.[29]
Sierra Leone	Yes, article 22 provides for the protection of the right to privacy of the person, home, property, and correspondence.[30]
South Africa	Yes, article 14 provides for the right to privacy.
Tunisia	Yes, article 24 provides for the right to privacy.

[20] 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection,' African Union, (2020), available here.
[21] ALT Advisory, 'Data Protection Africa,' (2020), available here.
[22] *Id*.
[23] 'Burkina Faso's Constitution of 1991 with Amendments through 2012,' Constitute Project, (2021), available here.
[24] Privacy International and the National Coalition of Human Rights Defenders in Kenya, 'The Right to Privacy in Kenya: Universal Periodic Review Stakeholder Report: 21st Session, Kenya,' (2017) available here.
[25] 'Liberia's Constitution of 1986,' Constitute Project, (2021) available here.
[26] 'Malawi's Constitution of 1994 with Amendments through 2017,' Constitute Project, (2021) available here.
[27] Privacy International, 'The Right to Privacy in Morocco,' (2016), available here.
[28] 'Senegal's Constitution of 2001 with Amendments through 2016,' Constitute Project, (2021) available here.
[29] Constitution of the Republic of Seychelles, Seychelles Government (1993), available here.
[30] Constitution of the Republic of Sierra Leone, CommonLII, (1991) available here.

The Link Between Privacy and Data Protection

The terms ***data protection*** and ***privacy*** are often used interchangeably. Some recognize ***data protection*** as a term used predominantly in Europe, and ***privacy*** as the American equivalent, but in practice they frequently overlap in meaning.[31] In Africa, data protection has traditionally been recognized in its relation to the right to privacy, which is dominant in the discourse. Some academics argue that data protection should instead be "'reconstructed' in order to operate as a fully-fledged fundamental right next to the right to privacy" so that data protection infringements can be evaluated "without the need to recourse to the right to privacy."[32]

Several notable distinctions should be made between the two terms. First, the right to privacy offers an individual protection from intrusion in their private sphere, while data protection is not limited to the private sphere of the individual.[33] Second, though protecting privacy is a central goal of data protection, it serves a variety of additional purposes beyond privacy,[34] including, for example, safeguarding personal data against misuse such as identity theft or fraud.

Some have attempted to bridge this gap by using the terms ***data privacy*** or ***information privacy***.[35] The European Court of Human Rights (ECtHR) has likewise made the connection between the two concepts in its case law. Karanja notes that the ECtHR has "boldly manifested data protection principles in its decisions" but that the Council of Europe human rights framework still lacks "a positive statement . . . that human rights protects personal data" and that the EU has "cured the anomaly by enacting a data protection provision in its Charter of Fundamental Rights and the EU Constitution."[36]

In Africa, many countries' constitutions provide only for a very general right to privacy, though there are a few that include protections for the privacy of an individual's communications or correspondence. Interestingly, Kenya recently attempted to amend its constitutional right to privacy[37] to incorporate the right to the protection of personal data of citizens to "provide a constitutional underpinning for privacy of personal data of citizens as an emerging area in human rights owing to technological advancement."[38] However, the proposed amendment was struck down by the High Court in May 2021, for procedural reasons.[39]

---

[31] Above n 10 at page 164.
[32] Maria Tzanou, 'Data protection as a fundamental right next to privacy? Reconstructing' a not so new right,' *International Data Privacy Law*, vol. 3 no.2 (May 2013) available here.
[33] Colette Cuijpers, 'A Private Law Approach to Privacy: Mandatory Law Obliged?' (2007) 4/4 SCRIPTed 304–18, 312.
[34] Paul De Hert, and Steve Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action,' in Steve Gutwirth, et al. (eds), Reinventing Data Protection? (New York: Springer, 2009) 3–44, 10.
[35] Above n 10, 165.
[36] Karanja, SK., 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation,' PhD Thesis, Faculty of Law, University of Oslo, (2006), at page 123.
[37] Article 31 of the Constitution of Kenya.
[38] The Constitution of Kenya (Amendment) Bill, 2020, Republic of Kenya, at page 30. available here.
[39] Roger Andagalu, 'Kenya High Court rules constitutional amendment bill unconstitutional,' Jurist, 16 May 2021, available here.

The African Conception of the Right to Privacy and Data Protection

Some academics argue that the development of data protection legislation in African countries was spurred on by the implementation of the European Directive 95/46/EC.[40] The European Directive, which was replaced by the General Data Protection Regulation 2016/679 (GDPR), required that foreign countries that process personal data concerning a European citizen must provide an adequate level of protection for such data. African countries were subject to such a clause because some processed information concerning European citizens and they accordingly had to comply with the law; such compliance required the development of appropriate legislation. An additional cause for the development of data protection was the rapid increase in information and communications technology in recent decades.[41]

Commentators note, however, that literature and jurisprudence concerning the right to privacy and data protection has been slow to develop on the continent.[42] Some literature suggests that the concept of privacy is undeveloped in African countries due to a dominant culture of collectivism, in contrast to the Western culture of individualism.[43] This notion was supported by several stakeholders on the continent interviewed in this research who pointed out that the right to privacy was not a priority for many countries, with the focus falling primarily on collective or communal rights, such as the right to healthcare and the right to water.[44] The omission of the right to privacy in the African Charter on Human and Peoples' Rights is regarded by some as indicative of this de-prioritization of the right to privacy due to its association with the individual as opposed to the collective.[45]

In contrast, Gabriella Razzano argues that "individualised privacy self-management strategies are problematic as the sole (or chief) model for data protection" because "when one person either sacrifices, or is forced to surrender, their privacy, the potential consequence of that is the exposure of collective (and not just individual) identity."[46] She notes:

> "It may be more instructive instead to begin outlining the collective and relational aspects of the right to privacy. The value of protecting privacy goes beyond the protection of the dignity of the individual. The notion of ubuntu (the African concept 'that we are human through others'), which informs much contemporary African human rights theory on collective rights, also helps demonstrate how it is the relational aspect of our personhood that normatively underpins its value."[47]

[40] Above n 10 at page 163.
[41] *Id.*
[42] *Id.*
[43] *Id* at page 171.
[44] Gabriella Razzano, 'Understanding the Theory of Collective Rights: Redefining the Privacy Paradox,' Research ICT Africa, 5, accessed on 10 May 2021, available here.
[45] *Id* and Patricia Boshe, 'Data Protection Legal Reform in Africa,' Passau University (2017).
[46] Above n 45 at pages 1 and 5.
[47] Above n 45 at page 6.

The fact that users of services frequently exchange privacy for 'low rewards,' such as access to social media platforms has also been used by commentators as evidence that the right to privacy is deprioritised relative to other rights, particularly in the digital realm. [48] However, this view has been debunked. Daniel Solove and Gabrielle Razzano point out that "a single decision taken by a user on a discrete piece of data [cannot] be extrapolated to reflect on their attitude to privacy in its entirety," and that "many privacy protections nevertheless remain in place when people 'exchange' their privacy in different consumer contexts, so to suggest a full trade-off of their privacy has happened is obviously false."[49]

Many people have indeed demonstrated a willingness to give up privacy in exchange for 'first-order needs' such as security or communications.[50] However, surveys also indicate a strong preference for privacy when asked in an abstract sense.[51] For example, 69 per cent of Zimbabweans and 59 per cent of Botswanans agreed that their governments should not be able to monitor their private communications.[52] This may indicate that a potential reason for the supposed low support for privacy in the African context is that it is too often framed as a necessary trade-off for other immediate needs. Perhaps privacy, as it is defined in international and domestic law, simply does not resonate with the average citizen, rather than not being valued. Such a proposition is supported by several stakeholders who mentioned the misconception that people in African countries do not care about the right to privacy but noted the need to talk to individuals in terms they understand, and to link the right with actual harms.

Moreover, how the right to privacy has been conceptualized—as a once-time trade-off or sale of ownership rights for which the consequences are abstract, while the benefits (immediate access to a desirable service) are highly tangible—is problematic. There is a need for a more nuanced and contextualised conceptualization of the right to privacy that takes into account the way that Africans see and value human rights, and under which their agency to exercise the right to privacy can be enabled without misrepresentations.

It is important to note additional possible reasons for the slow development of data protection on the continent, as raised by stakeholders in the interviews for this report. It was noted that the regulation of data protection is a state obligation but that the enactment of such legislation necessarily impacts the ways in which government departments are able to process personal data. Several stakeholders remarked on the extensive use of surveillance by states on the continent, noting that data protection legislation limits this practice. One stakeholder remarked that "state surveillance is common and African states want to engage in state surveillance in an unfettered way. So, they see the right to privacy or data protection laws as a way to stop or to limit the state's approach to surveillance."

---

[48] Daniel Solove, 'The Myth of the Privacy Paradox', 89 George Washington Law Review 1, (2021), available here.
[49] Gabriella Razzano, 'Understanding the Theory of Collective Rights: Redefining the Privacy Paradox,' Research ICT Africa, 2 accessed on 10 May 2021, available here and Daniel Solove, ' The Myth of the Privacy Paradox,' (2020).
[50] 'AD173: In name of security, many Ugandans willing to let government monitor private and religious speech,' AfroBarometer, (2018), available here.
[51] John Martin Kewaza, 'AD165: Majority of Zimbabweans want government out of private communications, religious speech,' AfroBarometer, (2017), available here and Mpho G. Molomo and Wilford Molefe, 'Freedom of information: Batswana back private communication, public accountability,' AfroBarometer, (2017) available here.
[52] *Id*.

An anonymous stakeholder remarked that governments cannot publicly admit to opposing data protection initiatives, so instead they undermine their effectiveness by underfunding the institutions or regulatory authorities tasked with implementing the law. The justification for such underfunding is often publicly noted as a requirement for a developing country that needs to prioritise different concerns. As an anonymous stakeholder pointed out, "Where governments put their money is an indication of their policy priorities." The stakeholder went on to note that this implicates an interesting question: Why is data protection not a concern or priority for states?

The Right to Privacy in Context

The right to privacy must be contextualised alongside other rights such as access to information and freedom of expression. These rights are often bundled together and referred to collectively as 'information rights'. These rights work in concert to enable each other—for example, the rights of an effective remedy, which is an important element of data protection, is enabled through a data subject's right of access to information. The provision of sufficient information empowers a data subject to lay a complaint in the exercise of their right to privacy. On occasion, a tension exists between these rights, which makes it important for data protection legislation to build in safeguards to ensure an appropriate balance is struck between them. As noted by a stakeholder interviewed for this paper who asked to remain anonymous:

> "The whole idea of protecting personal information actually comes out of a pre-accepted commitment to access to information and freedom of expression in the first place. It's precisely because you protect those things, that then you also need to be aware of that nub of personal data and personal information that is protected from that right of access to information and that right of publication and freedom of expression. So, to have the third leg in your law, when your law does not even recognise the basic other two that in all other democracies came first is putting the cart before the horse, I think."

Ensuring an appropriate balance between these rights is particularly important in African countries which have a poor track record for the full realization of access to information and freedom of expression rights. The anonymous stakeholder went on to note:

> "If you go at this focusing on protection of information, rather than seeing that as something that needs to happen as a result of the recognition and enforcement of the other, in my view, more fundamental rights, of access to information, the free flow of information and ideas and freedom of expression; you start with secrecy—that's exactly the wrong starting point and 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, all of that sort of stuff and pretty useless laws on access to information too."

This requisite balance is generally legislated through an exemption for journalistic or artistic purposes, but the enactment and implementation of data protection laws must be cognisant of the need to respect and promote the rights to freedom of expression and access to information in its pursuit of privacy. As noted by the UN High Commissioner for Human Rights, "overbroad privacy regulations may also amount to undue limitations of other rights, in particular freedom of expression, for example when a disproportionate regulation interferes with legitimate news reporting, artistic expression or scientific research."[53] Resultantly, domestic conceptualisations of the right to privacy and data protection are important to consider when analysing the legislative framework.

OVERVIEW OF THE REGULATORY CONTEXT

In this section, the regulatory context is detailed by noting the status of data protection law in the fourteen members and the adoption of international data protection regimes. The specifics are detailed in Table 2 and Table 3.

Out of the fifty-four countries in Africa, only twenty-eight have enacted data protection legislation[54]—ten of these are OGP members.[55] Out of the fourteen OGP members in Africa, ten countries[56] have enacted data protection legislation, two have draft legislation[57] and two have no law at all.[58] Sierra Leone and Liberia remain the only two countries without a draft data protection law. Sierra Leone is said to have drafted a Data Protection and Archives and Records Management Bill, but it has not yet been published or passed.[59] Liberia signed the Supplementary Act on Personal Data Protection which requires signatory states to establish a legal framework for data protection but, despite this, there have been no publicly-available utterances of the intention to implement data protection legislation.

The legislative review conducted by OGP included the legislation of twelve members. It includes each country with legislation, including draft laws and laws that are not in force. Liberia and Sierra Leone are accordingly excluded and any reference to ***members*** in the context of a legislative review, excludes them. At the time of conducting the research, Malawi had not published its draft bill and instead had the Electronic Transactions and Cyber Security Act No 33 of 2016, which contained provisions relating to data protection.

---

[53] Above n 16 at para 11.
[54] As at 3 March 2020, see for example: Privacy International, '2020 is a Crucial Year to Fight for Data Protection in Africa,' available here.
[55] At the time of drafting, South Africa's legislation had not yet come into full force. It has come into force incrementally since 2014 but will be in full force and effect from 1 July 2021 and was accordingly included.
[56] These include Burkina Faso, Cabo Verde, Côte d'Ivoire, Ghana, Kenya, Morocco, Senegal, Seychelles, South Africa, and Tunisia. It is noted that although Seychelles has enacted legislation, it is not in force.
[57] These include Malawi and Nigeria.
[58] These include Liberia and Sierra Leone.
[59] World Bank Group, '"Open Data Readiness Assessment" Prepared for the Government of Sierra Leone,' accessed on 23 May 2021, available here.

Table 2: Adoption of Domestic Data Protection Instruments

Country	Law	Adoption Date	Status of the Law
Burkina Faso	The Protection of Personal Data Act 010-2004/AN (2014)	2004	In force
Cabo Verde	The Data Protection Act, Law 133 of 2001	2001	In force
Côte d'Ivoire	The Protection of Personal Information Act 2013-450	2013	In force
Ghana	Data Protection Act, 2012 (Act 843)	2012	In force
Kenya	The Data Protection Act, 2019	2019	In force
Liberia	No law	-	-
Malawi	No singular data protection law Several data protection provisions are included in the Electronic Transactions and Cyber Security Act No. 33 of 2016 Draft Data Protection Bill, 2021	2016	Electronic Transactions and Cyber Security Act is in full force Data Protection Bill is in draft form
Morocco	Law no. 09-08 of 18 February 2009	2009	In force
Nigeria	The Draft Data Protection Bill, 2020	2019	Draft
Senegal	Law No. 2008-12 of 25 January 2008	2008	In force
Seychelles	Data Protection Act 9 of 2003	2003	Enacted but not in force
Sierra Leone	No law	-	-
South Africa	The Protection of Personal Information Act 4 of 2013	2013	The law has come into effect incrementally and will be in force from 1 July 2021
Tunisia	Law No. 2004-63 of 27 July 2004	2004	In force

Table 3: The Adoption of International Data Protection Regimes

Country	International Covenant on Civil and Political Rights (1966)	Council of Europe Convention 108 on Personal Data (1981)	Council of Europe Convention 185 on Cybercrime (2001)	African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) (2014)	Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010)	Council of Europe Additional Protocol to Convention 108 (Treaty No. 181) (2001)
Description	Article 17 recognizes the right to privacy.	The first binding international instrument which protects the individual against abuses relating to the processing of personal data and which seeks to regulate transfrontier flows of personal data.	The first international treaty on crimes committed via the Internet and other computer networks.	Aims to define the objectives and orientations of the Information Society in Africa and strengthen existing legislation on ICT of members and the regional economic communities.	To fill the legal vacuum created by the use of the internet as a new instrument of communication and establish a harmonized legal framework in the processing of personal data.	Aims to increase the protection of personal data and privacy by improving the original Convention of 1981.
Burkina Faso	Acceded 04/01/1999				Signed 16/02/2010	
Cabo Verde	Acceded 06/08/1993	Acceded 19/06/2018	Acceded 19/06/2018		Signed 16/02/2010	Acceded 19/06/2018
Côte d'Ivoire	Acceded 26/03/1992				Signed 16/02/2010	
Ghana	Signed 07/09/2000 Ratified 07/09/2000		Acceded 03/12/2018	Signed 04/07/2017 Ratified 15/05/2019	Signed 16/02/2010	
Kenya	Acceded 01/05/1972					
Liberia	Signed 18/04/1967 Ratified 22/09/2004				Signed 16/02/2010	
Malawi	Acceded 22/12/1993					
Morocco	Signed 19/01/1977 Ratified 03/05/1979	Acceded 28/05/2019	Acceded 29/06/2018			Acceded 28/05/2019
Nigeria	Acceded 29/07/1993				Signed 16/02/2010	
Senegal	Signed 06/06/1970 Ratified 13/02/1978	Acceded 25/08/2016	Acceded 16/12/2016	Ratified 03/08/2016	Signed 16/02/2010	Acceded 25/08/2016
Seychelles	Acceded 05/05/1992					
Sierra Leone	Acceded 23/08/1996			Signed 29/01/2016	Signed 16/02/2010	
South Africa	Signed 03/10/1994 Ratified 10/12/1998		Signed 23/11/2001			
Tunisia	Signed 30/04/1968 Ratified 18/03/1969	Acceded 18/07/2017		Signed 23/04/2019		Acceded 18/07/2017
Source	Status List.	Chart of Signatures and Ratifications.	Chart of Signatures and Ratifications.	Status List.	Document.	Chart of Signatures and Ratifications.

SCOPE OF APPLICATION

Teki Akuetteh Falconer, during her tenure as a data protection regulator in Ghana, was quoted as remarking that "I'm a data protection regulator but unable to call big tech companies to order because they're not even registered in my country!"[60] As articulated by Falconer, the effectiveness and enforcement of data protection legislation depends significantly on its scope of application.

The nature of the internet and the global market has resulted in the globalisation of personal data.[61] The processing of data is not limited to geographic jurisdiction; rather, it may be collected domestically by a foreign entity, used in another country, and then transferred to several others. Data subjects travel around the world and create personal data in various locations. The scope of application of data protection legislation is accordingly significant—it determines which entities, across the world, are bound by and must comply with domestic legislation. It details whether data protection legislation applies to natural and juristic persons, notes the extent of its application to government departments, and, importantly, regulates whether it applies to foreign entities.

All twelve OGP members explicitly prescribe the scope of application of their data protection law, except for the Seychelles and Malawi. Notably, Burkina Faso, Cabo Verde, Côte d'Ivoire, Kenya, Morocco, Senegal, and South Africa all have similarly worded provisions that prescribe the application to the ***processing of automated and non-automated personal data contained in or intended to form part of a filing system***. Nigeria and Tunisia have similar provisions but neither require that the personal data form part of a filing system. The exclusion of the 'filing system' requirement broadens the scope of application of the law because it applies to all personal data—not just the data that is placed in a structured form that is accessible according to specific criteria. The Seychelles does not have an express provision which details the law's application. Instead, the law's application is scattered and largely undefined, although the legislation does explicitly note that the law applies to public authorities. Malawi's legislation does not prescribe its scope of application.

Significantly, all twelve OGP members require natural persons, juristic persons, and public entities to comply with the law. This is significant as the legislation provides for a broad scope of application by ensuring that all relevant bodies fall within its ambit. However, the scope may be narrowed by specified legislative exclusions. Tunisia, for example, exempts public entities from certain provisions such as the requirements relating to consent and collection directly from a data subject, and the restrictions concerning the transfer of personal data. Importantly, data subjects in Tunisia do not have the right to access data processed by public entities but may request correction or deletion if they are aware of errors.

---

[60] Emma Ruttkamp-Bloem, 'Artificial Intelligence Presents a Moral Dilemma', *Mail & Guardian*, accessed on 21 May 2021, available here.

[61] Lukman Adebisi Abdulrauf, 'Regulating Transborder Flow of Personal Information for Development in the G77+China Group', *Unisa Latin American Report*, vol. 31, iss. 1 (2015), 77.

This section details two focus areas—legislative exclusions and the application of the law to foreign entities. These legislative mechanisms define the ambit of the law by specifying the circumstances which allow for non-compliance with the law and detail its application to foreign entities. These focus areas are discussed in turn below and detailed in Table 4 and Table 5.

Focus 1 | Legislative Exclusions

The scope of application of data protection legislation is limited by exclusions—provisions that expressly exclude certain types of processing from the ambit of compliance. All members—except Malawi—include such exclusions, the most common of which are processing for domestic purposes, national security, and processing for journalistic, literary, or artistic purposes.

Table 4: Applicable Exclusions[62]

Country	Domestic Purposes	National Security	Law Enforcement	Cabinet or Executive Council	Judicial Function	Journalistic, Literary or Artistic Purposes	Temporary Copies
Burkina Faso		X				X	X
Cabo Verde	X						
Côte d'Ivoire	X					X	X
Ghana	X	X	X	X[63]	X[64]	X	
Kenya	X	X				X	
Liberia							
Malawi							
Morocco	X	X					
Nigeria	X	X				X	
Senegal	X					X	X
Seychelles	X	X	X				
Sierra Leone							
South Africa	X	X	X	X	X	X	
Tunisia	X			X	X		

[62] If marked with an X, the country includes such an exclusion in the law.
[63] Note: The law states that the minister may make regulations to prescribe exemptions pertaining to employment by the government or appointments made by the president.
[64] Note: This only applies to processing for the assessment of suitability for office or to confer a national honor.

Most countries included similar exclusions except Burkina Faso, which provides that the law does not apply to research in the field of health and health data. Ghana's legislation includes thirteen exceptions, the most out of the twelve members. Ghana's additional exclusions include personal data that relates to health, education, and social work; processing for the protection against loss or malpractice in the provision of banking, insurance, investment, financial services, or management; personal data for the purposes of research, history, and statistics; legal non-disclosure; examination marks and scripts; and professional privilege. The exclusion of health data may be problematic in light of the particularly sensitive nature of the information. However; the exclusion in Ghana's law is not clear; it bundles health, education, and social work together and instead of noting that the provisions of the law do not apply to them—as it does for all other exclusions—it simply notes the following:

> **Health, education and social work**
>
> 62. Personal data on the following subjects shall not be disclosed except where the disclosure is required by law:
>
> (a) personal data which relates to the physical, mental health or mental condition of the data subject,
>
> (b) personal data in respect of which the data controller is an educational institution and which relates to a pupil at the institution, or
>
> (c) personal data of similar description.

The above clause accordingly appears to prohibit the disclosure of such information, and not to exclude its processing from the ambit of the law. It is included in the exemption section of the law, along with other sections that specifically exclude certain types of processing from compliance with the law but appears to be narrower in its application.

The scope and content of exclusions are important—vague or broad exclusions may be open to abuse. Nigeria's draft bill, for example, includes an exclusion titled 'public interest' in section 35(1) which simply includes the following list: public order; public safety; public morality; national security; public interest; the prevention or detection of crime; apprehension or prosecution of an offender; the assessment or collection of a tax or similar duty; or publication of literary or artistic material. None of these terms are defined in the bill. Although some of these are appropriately clear and certain, several are concerningly vague—it is not clear what would constitute public morality or public interest. The lack of certainty created by such vague terms may be open to abuse and result in diminished and inconsistent application of the law.

The need to exclude processing for journalistic, literary, or artistic expression is an important acknowledgement of the need to balance the right to privacy with other rights, such as freedom of expression and access to information. An effective balance requires that the interpretation of this exclusion is not too narrow, which results in an undue limitation of the right to freedom of expression. In light of the significant penalties included in data protection legislation, cognizance must be had of the possibility for data protection legislation to have a chilling effect on the right to freedom of expression. The fear of the imposition of a penalty for non-compliance with a data protection law may result in self-censorship.

For example, the application of the exclusion for journalistic expression is generally discretionary and entails the weighing up of several factors. The exclusion in South Africa, for example, notes the following:

> This Act does not apply to the processing of personal information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.[65]

It goes on to note that in making such a determination, several factors must be considered, some of which include the importance of the public interest in freedom of expression and the need to secure the integrity of personal data.[66] The application of this exclusion is accordingly uncertain—the weighing up of several factors can produce any determination, particularly for organizations that do not fit squarely within the definition of a journalistic body. An advocacy organization, for example, may publish information, but it arguably does so for the purposes of advocacy as opposed to journalistic expression. The publication of information may entail the processing of personal data—an organization may, for example, collect personal data concerning allegations of corruption of a public official from a whistleblower. This practice may violate the data protection law's requirement that personal data be collected directly from the data subject. Non-compliance with the law carries significant penalties, and the fear of such a consequence—which is likely the imposition of a considerable fine—may deter such an organization from publishing important information.

If the law does not clearly define the scope of the journalistic exclusion, the advocacy organisation may be concerned that the publication of its article would not constitute journalistic expression and they would be penalised. The development of jurisprudence concerning the applicability of this exclusion will create greater certainty and mitigate against the possibility of creating a chilling effect on freedom of expression.

Examples from the Field

South Africa's regulatory authority is mandated to monitor compliance and enforcement of both the data protection law, the Protection of Personal Information Act 4 of 2013, and the access to information law, the Promotion of Access to Information Act 2 of 2000.

This dual role may contribute significantly to ensuring that an appropriate balance is struck between the right to privacy and the right to access information.

[65] Section 7(1) of the Protection of Personal Information Act 4 of 2013.
[66] Section 7(3) of the Protection of Personal Information Act 4 of 2013.

Focus 2 | Application of the Legislation to Foreign Entities

One of the most important aspects of the scope of application of data protection legislation concerns its application to foreign entities. As outlined in Table 5 below, domestic law applies to foreign companies in the data protection legislation of most countries. In most cases, it will not apply to the foreign company if the company just forwards personal data through the country.

Table 5: Scope of Application of Data Protection Legislation to Foreign Entities

Country	Applies to a Foreign Entity?	Circumstances of Application to a Foreign Entity	Transit Exclusion[67] included
Burkina Faso	Yes	The entity "has recourse to methods of processing situated in the territory of Burkina Faso, with the exclusion of data that is not utilized except for transit purposes."	Yes
Cabo Verde	Yes	Applies to controllers outside of Cabo Verde if Cabo Verdean law applies or equipment in Cabo Verde is used for more than just transit purposes.	Yes
Côte d'Ivoire	Yes	Foreign entities, which are not domiciled in Côte d'Ivoire, must comply if they process data in the territory of Côte d'Ivoire.	No
Ghana	Yes	If the entity is not established in Ghana, then it applies if they use equipment or a processor established in Ghana, and if the data is not simply forwarded through Ghana.	Yes
Kenya	Yes	Foreign entities, which are not established in Kenya, must comply if they process the personal data of data subjects located in Kenya.	No
Liberia	No law	No law	No law
Malawi	Not prescribed in the Electronic and Cybersecurity Act, 2016	Not prescribed in the Electronic and Cybersecurity Act, 2016	Not prescribed in the Electronic and Cybersecurity Act, 2016
Morocco	Yes	Foreign entities, which are not domiciled in Morocco, must comply if they conduct activity in Morocco or do more than simply forward personal information through the country.	Yes
Nigeria	Yes	Foreign entities must comply if the data controller is not established in Nigeria, but uses equipment or a data processor in Nigeria to process the personal data of data subjects who reside within or outside Nigeria; or processing is carried out in respect of information relating to data subjects who reside within or outside Nigeria and personal data which originates partly or wholly from Nigeria.	No
Senegal	Yes	Foreign entities, which are not domiciled in Senegal, must comply if they process data using methods of processing in Senegal or do more than simply forward personal information through Senegal.	Yes
Seychelles	Not explicitly prescribed in the legislation	Not explicitly prescribed in the legislation	Not explicitly prescribed in the legislation
Sierra Leone	No law	No law	No law
South Africa	Yes	Foreign entities, not domiciled in South Africa, must comply if they do more than simply forward personal information through South Africa.	Yes
Tunisia	No	The law does not explicitly note whether juristic persons must be domiciled in Tunisia, but Article 22 states that any legal or juristic person wishing to process personal data, or their agents, must be of Tunisian nationality and resident in the country.	No

[67] This means that a foreign entity will not have to comply if it simply forwards personal data through the country. In other words, they must process the personal data in ways beyond transmission.

Mugambi Laibuta, an advocate specialising in privacy and data protection in Kenya, finds that the disjointed approach to data protection legislation in African countries is detrimental for data subjects and data controllers, particularly foreign companies.[68] Not many of the OGP members specify the application of the law beyond their territorial borders, which leaves data subjects without protection. Laibuta notes further that compliance is difficult for foreign companies that work across multiple countries because it entails different compliance measures which involve significant cost. He further suggests that a set of more uniform laws would allow for the development of guidelines and jurisprudence concerning specific aspects of data protection.

[68] Consultation with Mugambi Laibuta, 23 March 2021.

CONTEXTUAL AND LEGISLATIVE ANALYSIS

This section discusses focus areas 3 to 18: the legislative mechanisms which enable or contribute to transparency, accountability, and participation. The purpose of this section is to detail major barriers to their effective implementation, and note concerns raised by various stakeholders. Although these three thematic areas are dealt with separately, they often overlap and bolster each other.

TRANSPARENCY

Transparency is an important tenet of data protection legislation: it builds trust between the data subject and the data controller, empowers the data subject to exercise control over their data, and enables them to seek redress if necessary. Importantly, knowing how personal data is processed, allows a data subject to make an informed decision about whether to enter into an agreement with or use the services provided by a data controller.[69] The United Kingdom Information Commissioner's Office (UK ICO) describes the principle of transparency in data protection as follows:[70]

> Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data.

Importantly, transparency plays an important role in accountability. As noted by Transparency International:[71]

> The demand for accountability is often responded by increasing the level of transparency under the assumption that better and more information would allow citizens, governments or markets to hold institutions accountable for their policies and performance.

Transparency is generally included as a principal in data protection legislation and finds form through the various mechanisms or measures which aim to create greater transparency. These include the provision of a right to be notified that personal data is being processed or that there has been a breach that impacts a person's personal data, the development of a data protection register, and the use of terms of service icons.

The legislation of all OGP members included some commitment to transparency. Five members explicitly include transparency as a condition for the lawful processing of personal data.[72] Its inclusion in such a form may be significant for the enforcement of the principle. In South Africa, for example, non-compliance with openness, which is recognised as condition 6 of the lawful conditions for processing, is considered an interference with the protection of personal data and may carry significant consequences.[73]

---

[69] UK ICO, 'Principle (a): Lawfulness, Fairness and Transparency', accessed on 13 May 2021, available here.
[70] *Id*.
[71] Nieves Zúñiga, 'Does More Transparency Improve Accountability?' U4 Anti-Corruption and Transparency International, 2, accessed on 17 May 2021, available here.
[72] These included: Côte d'Ivoire, Ghana, Kenya, Nigeria, and South Africa.
[73] In this instance, the data protection authority is empowered to serve an enforcement notice which may require the data controller to take specified steps or to stop processing personal data.

In Cabo Verde, it is not expressly included as a condition for lawful processing but is noted in Article, 4 which states that "the processing of personal data shall be carried out transparently."[74] The principle is included, but no consequence appears to be attached to non-compliance with that specific article.[75] Despite not including transparency as a condition for lawful processing, all of the remaining members do require compliance with several measures which contribute to transparency. These are detailed in Table 6 below and discussed in greater detail in this section.

Table 6: The Provision of Transparency Measures

Country	Law Provides a Right to Notification?	Law Requires Notification in the Event of a Breach?	Law Requires a Data Processing Register?	Law Provides for Terms of Service Icons?	Regulatory Authority's Reporting Requirements
Burkina Faso	Yes	No	Yes	No	Annual report to the president of the Country, the president of the National Assembly, and the President of the Constitutional Council. The report is also made public.
Cabo Verde	Yes	No	Yes	No	Annual report. Following an offense, the judgment or public warning of the data controller must be published. Monthly reports must be submitted to the National Assembly.
Côte d'Ivoire	Yes	No	Yes	No	Submission of annual report to the President and the president of the National Assembly.
Ghana	Yes	Yes	Yes	No	None.
Kenya	Yes	Yes	Yes	No	Annual report to be submitted to the cabinet secretary and before the National Assembly.
Liberia	No law	No law	No law	No law	No law.
Malawi	Yes	No	No	No	None.
Morocco	Yes	No	Yes	No	None.
Nigeria	Yes	Yes	No	No	Submission of annual report to the president. Every data controller and processor must submit a data protection audit report to the regulatory authority. The regulatory authority will publish an annual report containing a list of the organisations which submitted their audit reports.
Senegal	Yes	No	Yes	No	Annual activity report to be submitted to the president of the republic and the president of the National Assembly. Deliberations by the regulatory authority must be published in the official journal.
Seychelles	Yes	No	Yes	No	Annual report to be submitted to the minister.
Sierra Leone	No law	No law	No law	No law	No law.
South Africa	Yes	Yes	No	No	Annual report to be submitted to Parliament.
Tunisia	Yes	No	No	No	Submission of annual report to the president.

[74] Article 4 of The Data Protection Act, Law 133 of 2001.
[75] It must be noted, however, that the provision of false information and the failure to comply with notification obligations may result in the provision of a fine.

Focus 3 | The Right to Notification

Significantly, all twelve OGP members provide data subjects with the right to be notified that their personal data is being processed; this right contributes significantly to transparency, which at the very least entails the disclosure of information and openness concerning decisions and actions.[76]

Good to Know

Privacy International recommends, in ***A Guide for Policy Engagement on Data Protection: Rights of Data Subjects*** (2018), that in order for the right of notification to be effective, the data subject should be provided with the following information:

Information as to the identity of the controller (and contact details);
The purpose of the processing;
The legal basis for processing;
The categories of personal data;
The recipients of personal data;
Whether the controller intends to transfer personal data to a third country and the level of protection provided;
The period for which the personal data will be stored;
The existence of the rights of the data subject;
The right to lodge a complaint with the supervisory authority;
The existence of profiling, including the legal basis, the significance and the envisaged consequences of such processing for the data subject;
The existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject;
The source of the personal data (if not obtained from the data subject);
Whether providing the data is obligatory or voluntary; and
The consequences of failing to provide the data.

An anonymous stakeholder noted concerns regarding the practical elements of this right in relation to how it enables other rights. Many correlative rights, such as the right to request the deletion or rectification of personal data, as well as accountability mechanisms—such as the right to lodge a complaint with a regulatory authority—are premised on the data subject being aware that a certain data controller is processing their personal data. If the data controller does not comply with their obligation to notify, it is difficult for a data subject to be aware of such non-compliance. Although the right to request access to personal data goes some way to close this loop, it may in some instances require a data subject to reach out to hundreds of data controllers in order to understand who is processing their personal data. Requiring a data subject to do so may be difficult and entail significant costs. These concerns highlight the difficulties associated with a data protection model that relies on significant data subject participation, as opposed to a model that empowers and encourages a strong regulatory authority, to ensure accountability.

[76] Above n 72.

The anonymous stakeholder opines that regular audits may be a proactive solution to this by consistently confirming whether a data controller is complying with data protection law. Audits are not reactive and triggered, for example, by a data subject being aware of an instance of non-compliance. Such an audit would confirm whether data subjects are being notified that their personal data is being processed and could ensure that the information provided to a data subject is correct. The publication of such audits—or at the very least, confirmation that an audit was conducted and the data controller is compliant—would contribute to increased transparency and greater accountability.

Focus 4 | Breach Notification

Several stakeholders noted that effective transparency in data protection requires the provision of information to a data subject concerning how their personal data is used. This includes information concerning an event, such as a data breach, which impacts the integrity, availability, or confidentiality of a data subject's personal data.[77]

A breach notification is a mechanism that requires a data controller to provide notice if the personal data in their control has been accessed or acquired by an unauthorized person. Data protection laws generally require that notice be provided to the regulatory authority as well as to affected data subjects.

The purpose of the notification is to allow affected data subjects to take necessary measures to mitigate against any potential harm they may suffer as a result of the breach. Identity theft is a common example of the type of harm that may result.[78] As noted by the Information Policy Institute:[79]

> Identity theft and identity fraud have emerged as serious crimes for consumers, citizens and business [...] Given the peculiar nature of this type of theft – namely, that it can be perpetrated by accessing information stored in places uncontrolled by the victim and in places of which the victim is often unaware – legislators have passed or are considering passing laws which require that the consumer be notified in the event of a data breach.

Surprisingly, the legislation of only four of the twelve OGP members requires notification in the event of a data breach. The specifics of the obligation are detailed in Table 7.

[77] UK ICO, 'What is a personal data breach?' Accessed on 25 May 2021, available here.
[78] Michael Turner, 'Towards a Rational Personal Data Breach Notification Regime,' Information Policy Institute (June 2006), accessed on 25 May 2021, available here.
[79] *Id*.

Table 7: Obligations Concerning Notification in the Event of a Data Breach

Country	Obligation to Report to the Regulatory Authority?	Obligation to Report to the Data Subject?	Time frame specified?	Additional Things to Note
Burkina Faso	No	No	No	No
Cabo Verde	No	No	No	No
Côte d'Ivoire	No	No	No	No
Ghana	Yes	Yes	As soon as reasonably possible after the discovery of the compromise.	If known, the data controller must disclose the identity of the unauthorized person who gained access to the data. The commission may direct the data controller to publicise the data compromise.
Kenya	Yes	Yes	The regulatory authority must be notified within 72 hours of becoming aware of the breach; the data subject must be notified within a reasonably practical period.	A data controller does not have to notify the data subject of a breach if the data controller or processor has implemented appropriate security safeguards, which may include encryption of the affected data.
Liberia	No law	No law	No law	No law
Malawi	No	No	No	No
Morocco	No	No	No	No
Nigeria	Yes	Yes	Data subjects must be notified within 48 hours after notification to the regulatory authority; there is no time frame specified for the notification.	Nothing to note
Senegal	No	No	No	No
Seychelles	No	No	No	No
Sierra Leone	No law	No law	No law	No law.
South Africa	Yes	Yes	Notice must be provided to the regulatory authority and the data subjects as soon as reasonably possible.	The regulatory authority may direct the publication of the fact of the compromise if doing so would protect a data subject.
Tunisia	No	No	No	No

Several stakeholders noted concerns regarding the ways in which the obligation to notify may be undermined. According to the stakeholders, this may occur in three ways: first, through the absence of a prescribed timeframe for notification; second, through the use of vague terms for the notification period; and third, through the inclusion of exceptions which allow for non-reporting. All three of these concerns are evident in Kenya's data protection legislation.

In Kenya, the legislation requires notification of a breach to be provided to the regulatory authority within seventy-two hours of becoming aware of it, but there is no time-frame prescribed for notification to a data subject, the legislation simply requires that the data subject be notified 'within a reasonably practical period.' The obligation for notification to a data subject accordingly provides no prescribed timeframe and instead includes a vague notification period. Mugambi Laibuta, an advocate specialising in privacy and data protection in Kenya, remarked that the way in which legislation is crafted is important—laws that require notification 'within a reasonable time' or 'as soon as practically possible' could be interpreted differently to mean a day or a whole year. The lack of a prescribed time frame may be open to abuse and undermine the purpose of the notification; for instance, a lengthy delay in the notification would not allow a data subject to take the necessary measures to mitigate against such risk. It further undermines accountability by excluding a clear prescription period: a data subject or the regulatory authority would struggle to hold a non-compliant data controller accountable without the evidence of the effluxion of time. It is difficult to prove that an ***unreasonable period of time*** has passed.

All four members that require notification in the event of a breach, provide vague time-frames for notification. Kenya is the only exception—by requiring notification to the regulatory authority within seventy-two hours—but its use of a vague time frame for notification to data subjects is concerning. As pointed out by Grace Bomu, a Research Fellow at the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University in Kenya, who noted that it is the data subject's rights that are affected by a breach.

The third concern stakeholders raised relates to the inclusion of circumstances that exempt a data controller from compliance. Kenya's legislation provides that a data controller does not have to notify the data subject of a breach if the data controller has **"*implemented appropriate security safeguards which may include encryption of affected personal data*."**[80] Amrit Labhuram, a research assistant at CIPIT, Strathmore University in Kenya, notes that beyond encryption, the law does not specify the requirements for what would constitute **"*appropriate security safeguards*"** which provides a loophole for non-compliance. Again, the use of vague terms may be open to abuse and allow for non-compliance. He notes that encryption does not guarantee the security of personal data and opines that such a caveat should be removed from the legislation.

Examples from the Field

The legislation in Ghana and South Africa includes a provision which may work to significantly increase transparency. In both countries, the regulatory authority is empowered to direct a data controller to publish information concerning the fact of the breach.

Although discretionary, the power may work to mitigate some of the concerns surrounding the vague time periods for reporting a breach to data subjects.

[80] Section 43(6) of The Data Protection Act, 2019.

Focus 5 | Data Processing Registers

This section focuses on the use of data processing registers, a mechanism included in data protection legislation that may work to increase transparency.

Good to Know

In terms of the GDPR, a data processing register must be developed and maintained by organisations that employ 250 or more employees, and in certain other circumstances.

The register must contain specific information concerning the processing of personal data by the organisation, some of which includes:

- The name and contact information of the data controller;
- The purpose of the processing;
- A description of the categories of the data subjects; and
- The categories of recipients to whom the data will be disclosed.

Article 30 of the GDPR specifies the requirements of the register in detail. Across the African members, different terms are used for a document that takes a similar form.

The legislation of eight of the twelve members require the development of a document or register similar to that of a data processing register. In some instances, the information that is included differs substantially from the information included in a data processing register in terms of the GDPR. The use of the term ***data processing register*** may accordingly be inaccurate but is used in this report to reflect a consolidated bundle of information that is developed and maintained by a regulatory authority. Table 8 provides more detail concerning the content and availability of such a register.

Table 8: Data Processing Register

Country	Law Requires a Data Processing Register?	Content Included in the Register	Register Available to the Public?	Does Public Access Require the Payment of a Fee?
Burkina Faso	Yes	The law or regulatory act mandating its creation or the date of its declaration, its name, and its purpose; the service to which the right of access is exercised and the categories of identifiable information recorded and the recipients or categories of recipients authorised to receive communication of this information.	No	Not applicable
Cabo Verde	Yes	Information concerning the controller, the category of data which is processed, the purpose of processing, the entities to whom it will be disclosed, the manner of exercising the right of access and rectification, combination of personal data processing, and any proposed transfer to third parties.	Yes	Not specified
Côte d'Ivoire	Yes	Not specified in the law.	Yes	Not specified
Ghana	Yes	Particulars of the data controller, a description of the personal data they process, the purpose for the processing, a description of the recipients of the data, the countries to which the data may be transferred, and a general description of the security measures.	Yes	Payment of a prescribed fee appears to only apply to the receipt of particulars from the register, inspection appears to be free.
Kenya	Yes	A description of the personal data, the purpose for the processing, risks and safeguards, and any other details prescribed by the data commissioner.	Yes	Not specified
Liberia	No law	No law	No law	No law
Malawi	No	Not applicable	Not applicable	Not applicable
Morocco	Yes	The files that public authorities are responsible for processing, files processed by private persons; references to published laws or regulations establishing public records, the authorizations issued, and data relating to files which are necessary to enable data subjects to exercise their rights to information, access, rectification, deletion and objection.	Yes	Not specified
Nigeria	No	Not applicable	Not applicable	Not applicable
Senegal	Yes	Not stated in the law.	Yes	No

Table 8: Data Processing Register (continued)

Country	Law Requires a Data Processing Register?	Content Included in the Register	Register Available to the Public?	Does Public Access Require the Payment of a Fee?
Seychelles	Yes	Particulars of the data controller, a description of the personal data and the purpose for processing it, a list of the sources from whom the data will be collected, a list of the persons to whom the data will be disclosed, a list of the foreign countries the data controller intends to transfer the data to, and one or more addresses to which data subjects can direct their requests for access to their data.	Yes	Yes
Sierra Leone	No law	No law	No law	No law
South Africa	No	Not applicable	Not applicable	Not applicable
Tunisia	No	Not applicable	Not applicable	Not applicable

Grace Bomu, a research fellow at CIPIT, Strathmore University, Kenya, notes that transparency, at a bare minimum, requires the publication of information, specifically relating to data controllers and data processors.[81] This basic information is included in the registers of Cabo Verde, Ghana, and the Seychelles. The description of the content provided by Burkina Faso and Morocco is unclear but seem to differ substantially from the type of content included in a data processing register as envisaged by the GDPR. Côte d'Ivoire does not specify the content of the register.

Notably, eight of the members that provide for a register, except Burkina Faso, require that it be made available to the public. This is significant, as a register must be accessible to members of the public in order for the public to benefit. It appears that only the Seychelles requires the payment of a prescribed fee, which may limit access to some members of the public.

Amrit Labhuram[82] notes that data processing registers significantly contribute to transparency by providing data subjects with a consolidated list of data controllers. This allows a data subject to confirm which data controllers are bound by the obligations of the act and determine which data controllers they may exercise their rights against. Labhuram stressed the need for the register to be accessible, suggesting that it includes a digital copy. He observed that many public registers in Kenya are only available in physical form, which may limit accessibility. He observed further that a digital register will provide greater transparency and access to foreign individuals who are not located in Kenya.

[81] Consultation with Grace Bomu, a research fellow at CIPIT, Strathmore University, Kenya, 9 March 2021.
[82] Consultation with Amrit Labhuram, a research assistant at CIPIT, Strathmore University in Kenya, 17 March 2021.

Focus 6 | Terms of Service Icons

This section focuses on terms of service icons, which may contribute to increased transparency and participation but are surprisingly not utilised by any of the members.

Under the GDPR, Recital 60 provides for the dissemination of information to a data subject through a combination of text and icons. Their purpose is to provide a meaningful overview of the processing in an "easily visible, intelligible and clearly legible manner."[83] The intention behind the use of such icons is to enable free, prior, and informed consent for data processing in a way that is comparable and user-friendly by using easily identifiable icons. The rationale for such icons is explained by the European Commission Data Protection Working Party: [84]

> The purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject.

Their effective use depends upon the standardization and universal nature of such icons or images which are easily identifiable. Under the GDPR, the European Commission is responsible for the development of these standard icons.[85]

None of the OGP members in Africa provide for the use of terms of service icons in their legislation, and the reason for their exclusion is unclear. Interestingly, it was not mentioned by any of the stakeholders we engaged with as a means to bring about greater transparency. No equivalent means were included in the data protection legislation of the members.

Recommendations to Strengthen Transparency

- Proactive audits of data controllers should be conducted in order to confirm their compliance with data protection legislation. Such audits are useful to ensure that data subjects have been notified that their personal data is being processed, which will enable the exercise of additional rights. It is envisaged that members will be the implementing actors, although private sector actors may also consider conducting such audits.
- The obligation to notify the regulatory authority and data subjects in the event of a breach must prescribe specific and certain time-frames. The use of vague time-frames is open to abuse and may lead to non-compliance. It is envisaged that members will be the implementing actors.
- Data processing registers should be made available to the public. Any prescribed fee must not limit access to certain members of the public. The mechanism which provides access to the register must be accessible, and it is recommended to include digital access. It is envisaged that members will be the implementing actors.
- The mechanisms or processes that enable the exercise of the right to access information must be accessible. It is envisaged that data controllers will be the implementing actors.

[83] European Commission Article 29 Data Protection Working Party 'Guidelines on Transparency Under Regulation 2016/67,' adopted on 29 November 2017, at para 52, accessed on 30 May 2021, available here.
[84] *Id.*
[85] *Id.*

ACCOUNTABILITY

> "Accountability is the way to ensure checks and balances . . . to enable responsible behaviour."[86]

Gabriella Razzano appropriately noted that the reality of effective accountability is context-dependent. Although this makes it difficult to develop uniform rules or standards for an institutional framework for accountability, certain common measures have been included in the data protection legislation of the African OGP members—the most prominent of which includes the appointment of a regulatory authority tasked with enforcing compliance with the law.

Accountability is also actor-dependent, where the effectiveness of the measures depends on the nature of the relationship. As noted by Transparency International:[87]

> The notion of accountability refers to a relationship between the agent (who does the action) and the principal (on whose behalf the agent is supposed to act), in which the principal is able to hold the agent responsible for its actions and the proper execution of its powers.

In the context of accountability in data protection, three important relationships emerge: the first is between **the data subject and the data controller**—where the data controller is responsible for processing a data subject's personal data in compliance with the law. This relationship concerns the legislative mechanisms which enable a data subject to hold the data controller accountable.

The second relationship is between the **data controller and the regulatory authority**—where the regulator is mandated to ensure that the data controller processes personal data in compliance with the law. This relationship concerns the legislative mechanisms which enable a regulatory authority to hold the data controller accountable.

The third relationship exists between **the regulatory authority and the public**—where the regulatory authority has a duty to monitor and enforce compliance with the data protection legislation and accordingly give effect to the right to privacy on behalf of the state. This relationship concerns the mechanisms which enable the public to hold the regulatory authority accountable.

Data protection legislation provides for several accountability measures and mechanisms that allow different actors to hold the various principals in these three relationships accountable. These are discussed in more detail throughout this section.

---

[86] OECD, 'The Governance of Regulators – Creating a Culture of Independence: Practical Guidance Against Undue Influence,' accessed on 28 May 2021, available here.

[87] Nieves Zúñiga, 'Does More Transparency Improve Accountability?' Transparency International, 3, accessed on 17 May 2021, available here.

Mechanisms for the Data Subject to Hold the Data Controller Accountable

Focus 7 | Civil Liability

One of the most important accountability mechanisms available to a data subject is civil liability. This allows a data subject to institute legal proceedings against a data controller if the controller violates the law and causes the data subject harm or loss. The data subject can use this legal action to claim a monetary amount from the data controller in damages for the harm or loss they suffered. Such a court action is time-consuming and expensive, and will likely carry significant reputational harm for a data controller.

The legislation of six OGP members provides for civil liability. It must be noted, however, that the exclusion of civil liability in the data protection law does not necessarily preclude a data subject from bringing such an action, as the law of the member may provide for it elsewhere.

The legislation does not provide significant detail on such liability, except for South Africa's, which states that a data controller may be liable if they acted with intent or were negligent. Most members, however, do note the circumstances or defences which would preclude liability. Concerningly, the following vague defense is common: a data controller will be exempt from liability if they can prove that reasonable care was taken. It is unclear what would constitute ***reasonable care*** and, if interpreted broadly, it may create an easy avenue for data controllers to escape liability. Further detail concerning civil liability is provided in Table 9.

Table 9: Civil Liability

Country	Does the Law Provide for Civil Liability?[88]	What is The Fault Requirement for Civil Liability?	The Exemptions from Liability
Burkina Faso	No	Not applicable	Not applicable.
Cabo Verde	Yes	Not specified in the law	The data controller may be exempted from liability if they can prove they are not responsible for the fact that gave rise to the damage.
Côte d'Ivoire	No	Not applicable	Not applicable.
Ghana	Yes	Not specified in the law	Evidence that reasonable care was taken to comply.
Kenya	Yes	Not specified in the law	The data controller may be exempted from liability if they can prove that they are not responsible for the event that gave rise to the damage.
Liberia	No law	No law	No law
Malawi	No	Not applicable	Not applicable
Morocco	No	Not applicable	Not applicable
Nigeria	Yes	Not specified in the law	The data controller may be exempted from liability if they can prove that they took reasonable care.
Senegal	No	Not applicable	Not applicable
Seychelles	Yes	Not specified in the law	It is a defense to prove that reasonable care was taken in the circumstances to prevent the loss, destruction, disclosure, or access.
Sierra Leone	No law	No law	Not applicable
South Africa	Yes	Intention or negligence	Any of the following defences may exclude liability: vis major, consent of the plaintiff, fault on the part of the plaintiff, compliance was not reasonably practicable in the circumstances or the data controller has been granted an exemption by the regulator in terms of section 37.
Tunisia	No	Not applicable	Not applicable

The effectiveness of civil liability relies on the outcome of the judicial process. Concerningly, several stakeholders noted that accountability is undermined by the court system. Fatou Jagne, the Regional Director for Senegal and West Africa at Article 19, noted that the technical and evolving nature of data protection issues has meant that judges are ill-equipped to preside over such matters.[89] She remarked that she has observed this trend across multiple jurisdictions in Africa. This point was expanded on by Teki Akuetteh Falconer[90] who stated that "we shouldn't think of data protection as a law which ends with the regulator."[91] She pointed out that effective accountability requires the whole ecosystem—the regulatory authority, the police service, the courts, and lawyers—all of whom require a level of specialization.

[88] Note: Even though the legislation does not specifically provide for civil liability, it may still be possible to pursue this through different avenues of law which exist in the country. Table 9 only details whether it is noted in the data protection law.
[89] Consultation with Fatou Jagne Regional Director for Senegal and West Africa, Article 19, 18 March 2021.
[90] Founder and Director of Africa Digital Rights' Hub, Ghana and former member of the regulatory authority of Ghana.
[91] Consultation with Teki Akuetteh Falconer, 19 May 2021.

In light of these concerns, several stakeholders noted the importance of providing specialised training for actors who assist data subjects in the realisation of their right to redress and who bring about accountability. Such actors were recognised to include members of the regulatory authority, members of the police service, lawyers, and judges. = It was noted that the provision of education and training must equip these actors to determine whether a violation has occurred and to understand and enforce appropriate remedies. In relation to the judiciary, it was recommended that specialised courts, or specialised units and registries within courts, be set up to adjudicate on these matters. = It was further noted by Fatou Jagne that there is insufficient jurisprudence on the African continent concerning data protection matters.[92]

Good to Know

One of the first things that Teki Akuetteh Falconer did as Ghana's data protection commissioner was to reach out to the chief justice to set up a specialised court that was able to preside over data protection matters.

In addition, her office ran training for the bar association to raise awareness and capacity around data protection issues.

Mechanisms for the Regulatory Authority to Hold the Data Controller Accountable

This section concerns a regulatory authority's capacity to monitor and enforce compliance with the data protection law and hold data controllers accountable. All twelve OGP members have designated a regulatory authority that is mandated to do so. The regulatory authority holds data controllers accountable through its powers of sanction, which include the imposition of administrative penalties, such as a fine, and criminal penalties. Further detail on the power of the regulatory authorities is included in Table 10.

Despite the powers afforded to regulatory authorities, there are several—often overlapping—factors that undermine their ability to perform their function. Concerns around the ways in which the regulatory authority's capacity is undermined formed the bulk of engagements with stakeholders. Such a strong focus demonstrates the significant role that regulatory authorities play in the effective implementation of the data protection law. The ability of the regulatory authority to effectively execute its mandate depends on three overlapping factors: its powers, its structure, and its capacity. Subsequently, this paper discusses in greater detail the ways in which these factors are undermined and contribute to the regulatory authority's diminished capacity to execute its mandate.

[92] Above n 91.

The Powers of the Regulatory Authority

This section discusses focus areas 8 and 9:the regulatory authority's power to investigate and the power to sanction. The provision of such powers in the members' legislation is detailed in Table 10.

Table 10: Powers of the Regulatory Authority

Country	Does the Law Establish a regulatory authority (RA)?	Is the RA Empowered to Investigate?	Is the RA Empowered to Subpoena or Request the Provision of Evidence or Explanation?	Does the Law Provide for Criminal Penalties?	Does the Law Provide for Administrative Penalties?
Burkina Faso	Yes, the ***Commission de l'Informatique et des Libertés*** (the Commission for Informatics and Freedoms).	Yes	Yes	Yes	No
Cabo Verde	Yes, the National Data Protection Commission.	Yes	Yes	Yes	Yes
Côte d'Ivoire	Yes, the Personal Data Protection Authority.	Yes	No	No	Yes
Ghana	Yes, the Data Protection Commission.	Yes	No	Yes	No
Kenya	Yes, the Office of the Data Protection Commissioner.	Yes	Yes	Yes	Yes
Liberia	No law	No law	No law	No law	No law
Malawi	The law is unclear. The Malawi Communications regulatory authority is responsible for the implementation of the Act. The Act also establishes the Malawi Computer Emergency Response Team which is mandated to respond to information and communication technology security threats. Neither body is specifically mandated to ensure compliance.	The law is unclear	The law is unclear	Yes	No
Morocco	Yes, the National Commission for the Control of the Protection of Personal Data.	Yes	Yes	Yes	Yes
Nigeria	Yes, the Bill establishes the Data Protection Commission.	Yes	Yes	Yes	Yes
Senegal	Yes, the Law establishes the Commission for Data Protection.	Yes	Yes	Yes	No
Seychelles	Yes, the Data Protection Commissioner.	Yes	Yes	Yes	No
Sierra Leone	No law	No law	No law	No law	No law
South Africa	Yes, the Office of the Information Regulator.	Yes	Yes	Yes	Yes
Tunisia	Yes, the National Authority for the Protection of Personal Data.	Yes	Yes	Yes	Yes

Focus 8 | The Power to Investigate

Importantly, the legislation of eleven of the twelve OGP members empowers a regulatory authority to investigate instances of non-compliance with the law. This power may be triggered by a complaint laid by a data subject or may be instituted on the initiative of the regulatory authority. In some instances, the regulatory authority is empowered to apply for a warrant, may subpoena individuals, and seize documents or property. Notably, nine of the twelve members provide regulatory authorities with such powers of access and seizure.

This power significantly impacts on a regulatory authority's ability to sanction and requires it to have the necessary resources and capacity, as investigations into non-compliance may entail a high level of technical expertise. For example, such expertise is often necessary to determine whether a breach has occurred in an instance where the data controller has not reported one.

Focus 9 | The Power to Sanction

One of the most effective ways for a regulatory authority to hold data controllers accountable is through their power to sanction. If a data controller violates the data protection law, they may be criminally liable or liable to an administrative sanction, which may include the payment of a fine. The legislation of eleven of the twelve members also provides for criminal sanctions. Although the legislation of each member provides for different offenses, common examples include the unauthorised sharing of data with a third party or accessing data without authorization; collecting data in a fraudulent, unfair, or illegal manner; and obstructing the powers of the regulatory authority. Common sanctions include imprisonment or a fine.

In Burkina Faso, for example, the offense of unauthorized sharing of data or unauthorized access to data carries a penalty of imprisonment of between three months and five years and a fine of between 1,000,000 francs CFA (1,861 US dollars) and 3,000,000 francs CFA (5,585 US dollars). The same offense in Ghana carries a penalty of a fine of not more than 250 penalty units[93] or imprisonment not exceeding two years, or both.

In some instances, the regulatory authority can direct that a data controller must comply with certain instructions which is commonly done through an enforcement notice. The data protection laws in South Africa, Ghana, and Nigeria provide for this, and the regulatory authority in South Africa may direct that the data controller take specified steps, refrain from taking certain steps, or must stop processing personal data. The enforcement notice specifies a time-frame within which the data controller must comply and allows the regulatory authority to order compliance on an urgent basis. Failure to comply with an enforcement notice is generally considered an offense.

[93] In Ghana, when a provision is made for the imposition of a fine as a penalty, the amount of the fine is expressed in terms of a number of penalty units. The law prescribes a monetary value for a penalty unit which may change from time to time.

Each member's legislation clearly distinguishes between criminal and administrative offenses. Seven of the twelve members provide for administrative penalties which generally include the imposition of a fine. In Nigeria, the only administrative offence is the failure to comply with an enforcement notice and carries the penalty of a fine, the amount of which is determined by the regulatory authority. Senegal also only has one administrative offence which is the failure to comply with a formal notice sent by the regulatory authority, but it interestingly carries a penalty of a temporary withdrawal of authorisation to process for three months. After the three-month period, the withdrawal may become final and a fine of up to 100,000,000 francs CFA (181,446.30 US dollars) may be imposed.

Stakeholders noted two concerns relating to the regulatory authority's power to sanction. The first concerns the need to guard against a culture of impunity, where a country exhibits a lack of accountability for non-compliance with the law. 'Gbenga Sesan, the Executive Director of Paradigm Initiative, Nigeria, considers this the most important element for an effective data protection regime. He noted: "I think the one which may be more important than all is the war against impunity, making sure that there are examples of people who breach data rights and are poached for it."[94] He went on to note that if an individual violates the law and is not punished, it is likely that someone else will commit the same offence again. Mugambi Laibuta, an Advocate of the High Court of Kenya, concurred and noted that "a weak regulatory environment will of course, breed impunity."

The second concern relates to the effectiveness of the sanction itself. Mugambi Laibuta[95] submitted that for the sanction to be effective, it must be prohibitive, which requires that the amount must be sufficiently high. An anonymous stakeholder agreed and referred to the fine in Kenya as a slap on the wrist. He remarked that those who can afford it may choose to pay the fine instead of complying with the law.

Good to Know

In Kenya's data protection law, a fine may not exceed five million Kenyan shillings which equates to just under fifty thousand American dollars.

Mugambi Laibuta, an advocate of the High Court of Kenya, refers to this as 'tea money' for big companies—small pocket change that is usually used to purchase office basics such as coffee and tea. He notes that this legislatively low amount weakens the role of the regulatory authority.

[94] Consultation with 'Gbenga Sesan, Executive Director of Paradigm Initiative, Nigeria, 3 March 2021.
[95] *Id*.

The Structure of the Regulatory Authority

This section discusses the legislative structure of the regulatory authority and notes how three institutional or operational concerns—budget, security of tenure, and the structural and reporting requirements—may undermine institutional independence, which in turn work to undermine adjudicatory independence. This ultimately impacts the regulatory authority's ability to enforce compliance with the data protection law.

Focus 10 | Independence

Kuda Hove, a Policy Officer at Privacy International noted:

> "There's this general distrust in having independent institutions in Africa. 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."

The regulatory authority's independence is a crucial element in its ability to perform its function. As noted by the Organisation for Economic and Co-operation and Development (OECD):

> Regulators need to make and implement impartial, objective and evidence-based decisions that will inspire trust in public institutions [...]. Undue influence, whether real or perceived, can undermine a regulator's ability to behave in this way, impinge on its independence, and ultimately, on its performance.[96]

Unsurprisingly, the independence of the regulatory authority was mentioned by every stakeholder and was regarded as fundamentally important for the effectiveness of data protection. Mugambi Laibuta, an advocate of the High Court of Kenya, noted the importance of the law providing for the independent structure of the regulatory authority. The legislation of seven of the members use language that explicitly describes the regulatory authority as independent but, as remarked on by 'Gbenga Sesan, the Executive Director of Paradigm Initiative in Nigeria, the letter of the law doesn't always align with the spirit of the law. Several factors may work to undermine the independence of the regulatory authority and contribute to the disjunct between ***de jure*** and ***de facto*** independence, and ultimately impinge on the authority's performance.

Alison Tilley, a member of the regulatory authority in South Africa, drew attention to the two distinct elements of independence—institutional and adjudicatory independence—and was concerned about how the two linked together. Institutional independence implicates structural and operational concerns, such as funding and personnel capacity, which directly impact the regulatory authority's ability to function. Adjudicatory independence relates to independence in their decision-making.

[96] Above n 88.

Three institutional or operational concerns—the collaboration and reporting requirements, budget, and security of tenure—were noted by stakeholders to undermine the institutional independence of the regulatory authority, which, in turn, works to undermine its adjudicatory independence. These three concerns are dealt with in turn below.

Table 11: Institutional Structure of the Regulatory Authority

Country	Does the Law Establish a regulatory authority?	Structure	Funding Source
Burkina Faso	Yes, the ***Commission de l'Informatique et des Libertés*** (the Commission for Informatics and Freedoms).	Independent body (they do not receive instructions).	The regulatory authority's budget is funded by the state or by any other resource that could be assigned to it. It may not receive funding from an individual, an entity, or a foreign state unless it is intermediated by the cooperation structures of Burkina Faso.
Cabo Verde	Yes, the National Data Protection Commission.	Independent body which operates within the National Assembly.	Not stated
Côte d'Ivoire	Yes, the Personal Data Protection Authority.	The mandate of the Personal Data Protection Authority is entrusted to the independent administrative authority in charge of telecommunications regulation and Information and communication technologies.	Unclear, but it appears to be funded out of the state budget.
Ghana	Yes, the Data Protection Commission.	Not detailed in the law. The governing body is a Board consisting of members from various government departments and industries.	Funds are received from: money approved by parliament, donations and grants, money that accrues in the performance of its functions; and any other money approved by the minister responsible for finance.
Kenya	Yes, the Office of the Data Protection Commissioner.	It is designated as a State Office in terms of Article 260 (q) of the Constitution.	Funds are received from, money allocated by the National Assembly; grants, gifts or donations and funds that accrue in the performance of its functions.
Liberia	No law	No law	No law
Malawi	The law is unclear. The Malawi Communications regulatory authority is responsible for the implementation of the Act. The Act also establishes the Malawi Computer Emergency Response Team which is mandated to respond to information and communication technology security threats. Neither body is specifically mandated to ensure compliance.	No additional information is provided for in the law.	Not stated

Table 11: Institutional Structure of the Regulatory Authority (continued)

Country	Does the Law Establish a Regulatory Authority?	Structure	Funding Source
Morocco	Yes, the National Commission for the Control of the Protection of Personal Data.	Article 27 provides for the National Commission's establishment "nearby to" the prime minister. This seems to mean that it either sits within the prime minister's office or is under its authority. The regulations do require that the members are chosen for their "impartiality" and expertise.	The budget is included in the budget of the prime minister. They may receive donations and bequests from national and international public or private organisations.
Nigeria	Yes, the Bill establishes the Data Protection Commission.	An independent, corporate body.	Funds are received from: 5 per cent of the revenue generated for specific items by the National Identity Management Commission, the Federal Road Safety Commission, the Nigerian Immigration Service, the National Information Technology Development Fund, the Nigeria Communications Commission, and Service Wide Vote, gifts, loans, and grants; assets that accrue to the commission and licensing fees, penalties, and fines.
Senegal	Yes, the Law establishes the Commission for Data Protection.	An independent administrative authority.	The regulatory authority receives a budgetary allocation from the state and may only receive donations or subsidies from an individual, an organisation, or a foreign State through the cooperation structures of the state of Senegal.
Seychelles	Yes, the Data Protection Commissioner.	Not specified, but the commissioner appears to be a role fulfilled by a natural person, who may seek assistance from additional officers.	Funds are provided for by an Appropriation Act.
Sierra Leone	No law	No law	No law
South Africa	Yes, the Office of the Information Regulator.	An independent, juristic entity that is accountable to the National Assembly of Parliament.	Funds are provided by Parliament and through fees specified in section 111.
Tunisia	Yes, the National Authority for the Protection of Personal Data.	The regulatory authority is noted to have legal personality and financial autonomy.	The regulatory authority's budget is attached to the budget of the minister of human rights and it receives money from subsidies granted by the state, revenue from its own activities and services, donations provided to the authority, and any other revenues provided to it by law or regulation.

Focus 10.1 | Collaboration and Reporting Requirements

In some instances, the law undermines the independence of a regulatory authority by requiring it to collaborate with certain departments. As remarked on by Mugambi Laibuta, an advocate of the High Court of Kenya, the regulatory authority in Kenya is legislatively obligated to collaborate with national security organs. He finds this requirement problematic because such organs "are key violators of the right to privacy" and such collaboration would undermine the regulator's ability to perform its function.

Mustafa Mahmoud, a Programme Manager at Namati in Kenya, a legal empowerment network, remarked on the data protection law in Kenya which requires the regulatory authority to consult with the cabinet secretary, a cabinet member, to draft directorates. He notes that this kind of legislative collaboration and reporting structure immediately establishes a chain of authority—one where the regulatory authority is a subsidiary. In Ghana, for example, the law provides that the minister may give directives to the board, which is the governing body of the regulatory authority, on matters of policy. This structure may undermine the independence of the regulatory authority's independence if the board feels obligated to act on or enforce such directives.

Commenting on the reporting structure—and the law's requirement that independent bodies report to a minister, 'Gbenga Sesan, the Executive Director of Paradigm Initiative in Nigeria, noted that "on paper agencies are independent but, in reality, it comes down to the human factor. If the minister respects the rule of law, and he respects independence, then it works that way." In addition, the collaboration and reporting requirements stipulated in the law may provide for undue influence, which ultimately undermines the independence of the regulatory authority.

Focus 10.2 | Budget

Several stakeholders noted that a lack of financial independence undermines the regulatory authority's independence. Mustafa Mahmoud, Programme Manager at Namati in Kenya, noted that cutting the budget of an independent body is used as a way to punish them or ensure their allegiance. Drawing from examples in Kenya, he remarked that the government cut the budget of the judiciary by 25 per cent in response to several rulings the judiciary made against the government. He noted that "because [regulatory authorities] are solely dependent on a government budget, it means they're financially dependent, so they can be blackmailed."

Consequently, a regulatory authority may treat a government department differently, for example by choosing to turn a blind eye to instances of non-compliance. This has significant implications for the effective functioning of the regulatory authority because, as noted by several stakeholders, government departments are often the biggest violators of data protection laws. The regulatory authority's reliance on certain government departments for funding may impact on their decision-making, and ultimately undermine their adjudicatory independence. Commenting on the impact of the budget structure in Nigeria, 'Gbenga Sesan, the Executive Director of Paradigm Initiative, noted that "[i]f you get your money directly from the national budget, you have more power. If you get your money from the ministry, you have no power." In light of this, suitable measures should be taken to ensure a sustainable financial model that secures the regulatory authority's financial independence.

Focus 10.3 | Security of Tenure

Concerning the regulation of government departments, Teki Akuetteh Falconer noted that during her time at the regulatory authority in Ghana:

> "Our biggest and toughest challenges were with government bodies— a lot of them were sister regulatory bodies. I remember receiving a letter from a regulator saying they are also a regulator so they will not comply with the law. You need to be very strategic around how to engage with government. In Africa, we have undermined our institutions, and this undermines our ability to push for some of these requirements."

This section discusses focus area 10.3—the security of tenure of the regulatory authority, which is another critical component of institutional independence. As noted by Alison Tilley, who is a member of the South African regulatory authority, security of tenure provides security for a regulator, which allows them to make difficult or unpopular decisions. Teki Akuetteh Falconer, a previous member of the regulatory authority of Ghana, agreed and stated that "security of tenure enables regulatory bodies to stand firm when it comes to government practices which undermine the [accountability] ecosystem." In this section, we are concerned with the composition and appointment of the regulatory authority, the term of office and the process and grounds for removal of the members of the regulatory authority, the details of which are outlined in Table 12.

Table 12: Security of Tenure of the Regulatory Authority

Country	Composition of the regulatory authority	Appointment Process	Term of Office	Removal Process
Burkina Faso	The regulatory authority comprises nine members. With the exception of the chairperson, the members of the committee do not hold a permanent position.	Commissioners are appointed by the president of the republic, upon the nomination of a court. After their designation by their structure of origin, the commissioners are appointed by decree taken in the council of ministers.	A term of five years; renewable once.	The law is confusing but it notes that members enjoy full immunity for opinions concerning their work.
Cabo Verde	The regulatory authority comprises three persons. The presidency of the regulatory authority is held by each of its members in turn in alphabetical order for a period of two years.	Members are elected by the National Assembly, by a two-thirds majority of the members of parliament.	A term of six years; renewable once.	The members are not removable, and their functions cannot cease before the end of their term of office, except in the case of resignation, loss of office, death, permanent physical incapacity, or incapacity that is expected to exceed the term of office. The law is silent on what constitutes 'loss of office.'

Table 12: Security of Tenure of the Regulatory Authority (continued)

Country	Composition of the Regulatory Authority	Appointment Process	Term of Office	Removal Process
Côte d'Ivoire	The regulatory authority comprises seven members.	The organization and appointment of the members are governed by ordinance. It is run by a regulatory council appointed by the council of ministers	A term of six years, not renewable.	The members of the Regulatory Council cannot be dismissed before the end of their mandate except for gross negligence that is duly justified.
Ghana	The regulatory authority comprises a board of eleven members.	Members are appointed by the president in accordance with article 70 of the Constitution.	A term of three years, renewable once.	A member of the board may resign at any time. If a member of the board is absent from three consecutive meetings without sufficient cause, they cease to be a member. This does not apply to the executive director. The president may revoke a member's appointment by addressing a letter to the member.
Kenya	The regulatory authority comprises the data commissioner as its head and accounting officer, and other staff appointed by the data commissioner.	The president nominates and appoints the data commissioner, with the approval of the National Assembly. The additional members are appointed by the data commissioner, in consultation with the Public Service Commission.	A six-year term, not renewable.	The office of the data commissioner shall become vacant if the data commissioner dies, resigns, is convicted of an offence and sentenced to a term exceeding six months without the option of a fine, or if they are removed from office on one of the listed grounds. The listed grounds include the inability to perform the functions of the office, non-compliance with Chapter 6 of the Constitution, bankruptcy, incompetence, or gross misconduct. The Public Service Commission will consider a complaint of one of the listed grounds and make a recommendation to the cabinet secretary.
Liberia	No law	No law	No law	No law
Malawi	The law is unclear.	The law is unclear.	The law is unclear.	The law is unclear.

Table 12: Security of Tenure of the Regulatory Authority (continued)

Country	Composition of the Regulatory Authority	Appointment Process	Term of Office	Removal Process
Morocco	The regulatory authority comprises seven members: a president and six ordinary members. The modalities and conditions of appointment of the members are determinable by decree.	The president and members are appointed by His Majesty the King, on the proposal of the prime minister.	A term of five years, renewable once.	The law and decree are silent on this question.
Nigeria	The regulatory authority comprises sixteen members.	The data protection commissioner is appointed by the president, subject to the confirmation of the Senate.	A term of five years, renewable once.	The data protection commissioner may resign or be removed from office by the President for one of the following reasons: inability to discharge the functions of the office due to physical or mental infirmity, any act of gross misconduct, or if it is established that it is not in the interest of the regulatory authority or the public for the data commissioner to continue in the office.
Senegal	The regulatory authority comprises eleven members.	The members are designated by the President of the Republic. After their designation, they are appointed by decree in the Council of Ministers.	A term of four years, renewable once.	Membership can only be terminated in the event of resignation or incapacity noted by the regulatory authority.
Seychelles	The regulatory authority comprises an officer known as the data protection commissioner. It is noted that the President may provide for the provision of officers to assist the data protection commissioner; it does not prescribe their appointment process or the number of officers.	The data protection commissioner is appointed by the president.	A term of five-years, renewable.	The data protection commissioner may resign at any time and may be removed by the president.

Table 12: Security of Tenure of the Regulatory Authority (continued)

Country	Composition of the Regulatory Authority	Appointment Process	Term of Office	Removal Process
Sierra Leone	No law	No law	No law	No law
South Africa	The regulatory authority comprises five members: a chairperson and four ordinary members. The chairperson and two of the ordinary members are appointed in a full-time capacity, the remaining two may be full-time or part-time.	Members are appointed by the president, on the recommendation of the National Assembly.	A term of five years, which may be renewed.	Through resolution of the National Assembly, with the supporting vote of a majority of the members. The president must remove a member from office upon adoption of the resolution by the National Assembly.
Tunisia	The regulatory authority comprises Thirteen members: The President and twelve ordinary members. The president may charge one or more members to study or monitor certain projects within its responsibility. The president may also instruct additional specialists in the field of personal data to assist with the regulatory authority's duties.	The chairman and members are appointed on a proposal from the minister charged with human rights. There is also a permanent secretariat, run by a secretary general which is appointed by decree, on a proposal from the minister charged with human rights.	A term of three years, which may be renewed.	The law is silent on this.

Composition and Appointment of the Regulatory Authority

As evidenced in Table 12 above, the general trend for the composition of the regulatory authority is for it to be comprised of several members, as opposed to one single commissioner. The composition of the regulatory authorities ranges in number of members from three to sixteen, as provided for in Nigeria's legislation. There are two exceptions: Kenya and the Seychelles, both of which note that the regulatory authority comprises one person, the data protection commissioner. Notably, however, both countries provide for the appointment of additional staff members to assist with the regulatory authority's functions. Kenya's law allows the data protection commissioner to make such additional appointments, whereas the Seychelles provides for such appointments to be made at the president's discretion.

Interestingly, the regulatory authority in Ghana comprises a board of eleven members and the legislation prescribes the sectors and rank of several members. It requires that six members must be representatives from each of the following departments: the National Communications Authority not below the rank of director; the Commission on Human Rights and Administrative Justice, not below the rank of a deputy commissioner; the Ministry of Communications, not below the rank of a director; the National Information Technology Agency, not below the rank of director; the Bank of Ghana, not below the level of deputy governor; and the Statistical Service, not below the rank of director. One representative must be elected by the Industry Forum and two members must be nominated by the president. The law does not define 'Industry Forum' and it is not mentioned elsewhere in the law.

Nigeria's draft law also prescribes the designation of members of the board, but notably requires representatives from sectors outside of government. It prescribes that one member must be nominated by private sector data controllers, one member must be nominated by independent data protection professional service providers, and one member must be nominated by civil society organisations involved in data and privacy protection. Importantly, it notes that the member must be ***nominated*** by these sectors and not that the member be a representative from such a sector.

Prescribing certain designations of membership may ensure a diversity of knowledge and skill within the regulatory authority, and may contribute to increased cooperation between government departments and stakeholders. This may, in turn, result in increased buy-in across sectors.

Nigeria's law is significant in this regard through its legislated inclusion of non-governmental actors, including the private sector and civil society. It is important to note, however, that the prescription of designation may undermine the independence of the regulatory authority. In both countries, the prescribed designation results in a majority of the regulatory authority's members comprising of members of government. In Ghana, six of the eleven members are representatives from government departments and in Nigeria, eleven of the sixteen members are government representatives.

The inclusion of government officials, who assumedly maintain their role in the government department, may severely undermine the independence of the regulatory authority whose function is to monitor and enforce compliance with the data protection legislation—including compliance by government departments. Such a majority-government membership may influence the decisions of the regulatory authority when acting against government departments.

Term of Office of the Regulatory Authority

As noted in Table 12, the shortest term of office is for a period of three years as provided for by Ghana and Tunisia. The general trend prescribes the term of office for a period of five years, which may be renewed only once. Notably, three countries—the Seychelles, South Africa, and Tunisia—provide for the renewal of the members' term of office, but do not state the number of times that renewal may occur, which undermines legal certainty.

Process and Grounds for Removal

The process and grounds for removal of members of the regulatory authority impact its independence. 'Gbenga Sesan, the Executive Director of Paradigm Initiative in Nigeria, noted that "as long as the president can remove very easily, then there is no independence."[97] Out of fear of losing their job, a regulator may respond to a government department differently, for example, by choosing to ignore evidence of non-compliance with the law. The ability to remove the members of the regulatory authority gives certain government departments or individuals significant power over the members of the regulatory authority which may result in undue influence over their adjudicatory independence.

As detailed in Table 12, there appears to be insufficient legal certainty concerning the removal of members of the regulatory authority across the members. In some instances, the law is silent on the removal process as is the case in Morocco and Tunisia. Cabo Verde vaguely notes that members may be removed due to 'loss of office' but the law does not stipulate the scope of what constitutes a loss of office. The countries that do prescribe the grounds of removal generally include incapacity and gross negligence as justifications for removal. Interestingly, Ghana provides that if a member is absent from three consecutive meetings, without just cause, they cease to be a member.

Concerningly, the legislation of several members provides for removal by the president, without the provision of inherent safeguards to mitigate against an abuse of power. Ghana's legislation provides that the president may revoke the appointment of a member of the board of the regulatory authority by addressing a letter to the member. It does not prescribe that such a decision be made with the approval of or based on the recommendation of an additional oversight body and is accordingly a prerogative power of the president. There do not appear to be any mechanisms included in the legislation to enable accountability or guard against the possibility of the abuse of such a power. Further, the law does not provide for grounds of justification for such a removal which would inherently circumscribe the power of the President. This is also the case in the Seychelles, which simply notes that the data protection commissioner may be removed by the president.

[97] Above n 96.

Nigeria's legislation also provides for the removal of the data protection commissioner by the president. Although the legislation prescribes the grounds on which the president may remove the member—inability to discharge the functions of the office or gross misconduct—it also provides a vague and broad ground that may be open to abuse. It notes that the data protection commissioner may be removed from office by the president "where it is established that it is not in the interest of the commission or the public for the data commissioner to continue in the office."[98] The law does not stipulate what would constitute such an interest nor does it prescribe any factors that must be considered when making such a determination. Such a broad justification may be open to abuse and arguably undermines the purpose of including grounds of justification for removal—such a broad ground does not circumscribe the president's power.

As demonstrated above, the structural and operational concerns relating to budget, collaboration and reporting requirements, and security of tenure impact the institutional independence of the regulatory authority, which, in turn, may undermine its adjudicatory independence. This ultimately impacts on the regulatory authority's ability to enforce compliance with the data protection law.

[98] Section 12(b)(iii) of the Data Protection Bill, 2020, Nigeria.

The Capacity of the Regulatory Authority

Remarking on the independence of South Africa's regulatory authority, Alison Tilley noted:

> "I'm not concerned about adjudicatory independence; in terms of institutional independence, that's going to be a longer process than I had realised. It is certainly going to be a number of years before a lot of those institutional issues can be resolved. Will that impact on adjudicatory independence? I don't think so. But it's always an interesting question as to how the one impacts on the other."

The final factor that contributes to the regulatory authority's ability to execute its mandate and enforce compliance with the data protection law concerns its capacity. This relates to the resources, both human and capital, provided to a regulatory authority to enable it to function effectively.

Good to Know

As noted by Chawki Gaddes, the president of Instance nationale de protection des données personnelles (INPDP), Tunisia, the Association of Francophone Data Protection Authorities (AFAPDP) determines whether a regulatory authority has sufficient independence to be accepted as a member in the association.

Focus 11 | Resources

Various stakeholders noted the enormous expense required for the regulator to operate. This is because the technical nature of data protection requires hiring employees with the requisite technical capacity—investigating non-compliance with data protection laws, for example, may entail determining whether a data breach has occurred. As noted by an anonymous stakeholder, these skilled individuals are paid well in the private sector and government departments do not have enough resources to offer them a competitive salary.

An anonymous stakeholder also noted that regulatory bodies are deliberately undermined by governments—they are under-funded and staffed with employees who have little experience in the field in order to subvert their ability to function. Another stakeholder noted that "there is a reason these things don't get funded. Governments always find money for the army, always. They always find money for defense, for police, for jails—where governments put their money is an indication of their policy priorities."

In light of these concerns, stakeholders recommended that regulatory authorities must be appropriately capacitated in order to function. This requires sufficient funding to draw the requisite expertise. As noted in the sections above, the regulatory authority's ability to hold data controllers accountable depends on its ability to function effectively. This, in turn, requires the appropriate powers, structure, and capacity of the regulatory authority.

The Regulatory Ecosystem

One anonymous stakeholder noted that the structural undermining of the regulatory authority is often linked to the origin and development of the law. They find the under-funding and under-capacitating of the regulatory authority an obvious reality. On this point, they remarked:

> "That's just so obvious; that can't be the level at which we enter the debate. The debate is, why is that happening? And also, for me, it's to go one step back and say, if you're not committed to this, why do it in the first place? Why have the laws in the first place? And when you go back and have a look, a lot of the stuff is donor driven."

As noted by several stakeholders, data protection laws in African countries are often written or funded by an external party. Such a process may be triggered by a need to access aid or to participate in the market. As noted by a stakeholder who requested to remain anonymous:

> "People who are not living in country, write the laws and the government is then pressurized 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."

Several stakeholders expanded on this point to note that the practice undermines the legitimacy of the law and results in a disconnect between the law's drafting and implementation. Nigeria was cited as an example of this where the law lacks legitimacy for those on the ground because it is not one the people feel a sense of ownership over. The use of a multistakeholder deliberative body to develop legislation or guidelines domestically may mitigate some of the concerns posed by the use of external consultants.

In light of this, Chawki Gaddes, President of the regulatory authority in Tunisia, commented on the importance of the legislation being implemented because of a culture or public demand. This links with the observation made by several stakeholders that the effective implementation of data protection laws requires political buy-in or good-will from the government.

Mechanisms for the Public to Hold the Regulatory Authority Accountable

The regulatory authority is mandated to monitor and enforce compliance with the data protection law. In so doing, it ensures that personal data is processed lawfully, data subjects' rights are respected, and the right to privacy is protected. There is accordingly a public interest in ensuring that the regulatory authority executes this mandate effectively. This section is concerned with how the regulatory authority may be held accountable—including by members of the public and members of civil society.

Focus 12 | Regular Reporting

Several stakeholders noted that to hold the regulatory authority accountable, the public must have access to information concerning its functions. Such information may be provided through the obligation to report. The prescribed reporting requirements are detailed in Table 13.

Table 13: regulatory authorities Reporting Requirements

Country	Regulatory Authority's Reporting Requirements
Burkina Faso	Annual report to the President of the country, the President of the National Assembly and the president of the Constitutional Council. The report is also made public.
Cabo Verde	Annual report. Following an offence, the judgment or public warning of the data controller must be published. Monthly reports must be submitted to the National Assembly.
Côte d'Ivoire	Annual report to be submitted to the president and the president of the National Assembly.
Ghana	None
Kenya	Annual report to be submitted to the cabinet secretary and before the National Assembly.
Liberia	No law
Malawi	None
Morocco	None
Nigeria	Annual report to be submitted to the president. Every data controller and processor must submit a data protection audit report to the regulatory authority. The regulatory authority will publish an annual report containing a list of the organisations which submitted their audit reports.
Senegal	Annual activity report to be submitted to the President of the Republic and the president of the National Assembly. Deliberations by the regulatory authority must be published in the official journal.
Seychelles	Annual report to be submitted to the Minister.
Sierra Leone	No law
South Africa	Annual report to be submitted to Parliament.
Tunisia	Annual report to be submitted to the President.

The legislation of nine of the twelve OGP members requires the regulatory authority to submit an annual report. Such submissions are either made to the president, the National Assembly, or to a specified minister. It is assumed that the regulatory authority reports to the body that is tasked with its oversight in terms of domestic law.

The obligation to report generally provides little detail concerning the content of such reports. South Africa, for example, simply notes that the regulatory authority must report "on all its activities" in terms of the data protection legislation.[99] Tunisia does not provide any detail on the content of the report.

Concerningly, none of the members—except Burkina Faso—specify whether the report will be made publicly available. The lack of transparency concerning its functions undermines the public's ability to hold the regulatory authority accountable. Gabriella Razzano, a Senior Research Fellow at Research ICT Africa in South Africa, noted that the most important thing for a regulatory authority to release is the information that allows other parties to monitor them—particularly in a context where institutional accountability might be lacking. This concern was shared by Amrit Labhuram, a Research Assistant at CIPIT, Strathmore University, in Kenya, who noted that the absence of reporting on internal functions undermines the regulatory authority's transparency. His concern is based on the fact that no one would know how many complaints they received versus the number of decisions or outcomes they issued, and there would be no way to interrogate the rationale behind their decisions. He notes that the absence of an obligation to report on the regulatory authority's functions is an omission in the Kenyan legislation and warrants a possible amendment. It is noted that the use of an enforcement and compliance history database, which tracks and assesses compliance, may mitigate such concerns. Grace Bomu, Research Fellow at CIPIT, Strathmore University, in Kenya, reiterated the importance of the regulatory authority releasing such information and noted that it will allow civil society to monitor the enforcement of the law and play an oversight role. She recommended that regulatory authorities submit quarterly reports instead of annual reports and suggested that the reports provide disaggregated statistics.

On accountability, Teki Akuetteh Falconer noted:

> **"**Accountability is the true path to ensure respect for data protection. When you hold the data and process it, you respect where it has come from, you understand it relates to a person and you understand your obligations to that data. To be able to push for a system where people truly see and respect this, you as the regulator have to do this yourself—you have to build trustworthy systems which facilitate compliance and encourage accountability. If the regulator is corrupt—by virtue of that corruption, they have no integrity or trust – you are going to get to a place where you will have a collapse of the law. People will be ticked as complying, not because they are compliant, but because they are in bed with the regulator or support their agenda. When you do that, you undermine the institution. It doesn't happen quickly, it comes over a long period of time. The industry begins to believe that you are an institution that is not worth its time. An Industry can see that kind of corruption and it will undermine your institution. There is a lot of corruption in African countries and if we allow these regulatory bodies to take on the nature of existing institutions which have been labelled as corrupt, then data protection won't be effective."

[99] Section 40(1)(b)(v) of the Protection of Personal Information Act 4 of 2013.

Recommendations to Strengthen Accountability

- All key-players in the accountability ecosystem should have the requisite technical capacity and knowledge to handle data protection matters. This includes members of the regulatory authority, members of the police service, lawyers, and judges. All of these actors must be appropriately trained to equip them to determine whether a data protection violation has occurred and to understand and enforce the appropriate remedies. It is envisaged that members, regulatory authorities, and professional bodies will be the implementing actors.
- Specialised courts, or units and registries within courts, should be designated to adjudicate on data protection issues. It is envisaged that members will be the implementing actors.
- Sanctions in terms of monetary fines must be sufficiently high to act as a deterrent. It is envisaged that members will be the implementing actors.
- The institutional independence of the regulatory authority must be secured in order to ensure adjudicatory independence; this requires a sustainable financial model that secures the financial independence of the regulatory authority. It is envisaged that members will be the implementing actors.
- The regulatory authority must be appropriately capacitated. This requires sufficient funding to employ technically skilled staff. Members of the regulatory authority should consider alternative ways to draw in technical skills, such as public-private partnerships, the development of networks, and internships. It is envisaged that members and regulatory authorities will be the implementing actors.
- The regulatory authority should publicly report on its activities and functions to enable external actors to hold it accountable. It is recommended that such reports be released quarterly and should include disaggregated statistics and information. It is envisaged that regulatory authorities will be the implementing actors.

PARTICIPATION

Participation in the data protection framework occurs in the following three ways: the first is the data subjects' participation in, and control over, the processing of their personal data; the second concerns the participation of the regulatory authority domestically through its engagement with stakeholders and its ability to participate in legislative and policy developments; and the third concerns the participation of the regulatory authority regionally through its cooperation in regional associations and organizations.

Data Subject Participation

Data subject participation may be enabled through the provision of three rights: the right to access personal data; the right to request the correction of their personal data; and the right to request the deletion of their personal data—focus areas 13 and 14. The participation of data subjects is further enabled through the requirements concerning data subject consent—focus area 15. The members' inclusion of these rights is detailed in Table 14 and the specifics relating to consent are outlined in Table 15.

Table 14: The Inclusion of Rights That Enable Data Subject Participation

Country	Does the Law Provide a Right to Access Personal Data?	Does the Law Provide a Right to Request the Correction of Personal Data?	Justification Required for a Request for Correction	Does the Law Provide a Right to Request the Deletion of Personal Data?	Justification Required for a Request for Deletion
Burkina Faso	Yes	Yes	Personal data is incomplete or incorrect.	No	Not applicable
Cabo Verde	Yes	Yes	Personal data is incomplete, inaccurate or does not comply with the law.	No, but it does provide for blocking.	Not applicable
Côte d'Ivoire	Yes	Yes	Personal data is inaccurate, incomplete, ambiguous or expired, or whose collection, use, disclosure or retention is prohibited.	Yes	Personal data is inaccurate, incomplete, ambiguous or expired, or whose collection, use, disclosure or retention is prohibited.
Ghana	Yes	Yes	Personal data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or has been obtained unlawfully.	Yes	Personal data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or has been obtained unlawfully.

Table 14: The Inclusion of Rights that Enable Data Subject Participation (continued)

Country	Does the Law Provide a Right to Access Personal Data?	Does the Law Provide a Right to Request the Correction or Personal Data?	Justification Required for a Request for Correction	Does the Law Provide a Right to Request the Deletion of Personal Data?	Justification Required for a Request for Deletion
Kenya	Yes	Yes	Personal data is inaccurate, out of date, incomplete or misleading.	Yes	Personal data is irrelevant, excessive, obtained unlawfully, or the data controller is no longer authorised to retain it.
Liberia	No law	No law	No law	No law	No law
Malawi	Yes	Yes	The processing does not comply with the provision of the Cybersecurity Act, or the personal data is incomplete or inaccurate.	Yes	The processing does not comply with the provision of the Cybersecurity Act, or the personal data is incomplete or inaccurate.
Morocco	Yes	Yes	The processing does not conform with the law, notably by being incomplete or incorrect.	Yes	The processing does not conform with the Law, notably by being incomplete or incorrect.
Nigeria	Yes	Yes	The personal data is inaccurate, false or has been unlawfully processed.	Yes	The personal data is inaccurate, false or has been unlawfully processed.
Senegal	Yes	Yes	Personal data is incorrect, incomplete, ambiguous, out of date or illegally collected or processed.	Yes	Personal data is incorrect, incomplete, ambiguous, out of date or illegally collected or processed.
Seychelles	Yes	Yes	Following an application for compensation for the inaccuracy of personal data, a court may order the rectification or erasure of data	Yes	Following an application for compensation for the inaccuracy of personal data, a court may order the rectification or erasure of data.
Sierra Leone	No law	No law	No law	No law	No law
South Africa	Yes	Yes	Personal data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.	Yes	Personal data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.
Tunisia	Yes	Yes	The personal data is inaccurate, ambiguous, or the processing is prohibited.	Yes	The personal data is inaccurate, ambiguous, or the processing is prohibited.

Focus 13 | The Right to Access Personal Data

Significantly, all twelve OGP members provide data subjects with the right to access their personal data. Privacy International notes that in order for the right to be effective:

> The data subject must be able to obtain (i.e., to request and be given) information about the collection, storage, or use of their personal data. The information should include, at least, confirmation of whether a controller processes data about them, the purpose of processing, the legal basis for processing, where the data came from, who it has been/might be shared with, how long it will be stored for, and information about how their data is being used for profiling and automated decision-making.[100]

The right to access plays an important role in enabling the exercise of other rights, such as the right to an effective remedy. Hlengiwe Dube, a Programme Manager for Expression, Information and Digital Rights, at the Centre for Human Rights, University of Pretoria, South Africa, notes that the right, coupled with the right to notification, forms part of a data controller's broader obligation to be accountable for the personal data which they process. It further contributes to transparency, which entails the disclosure of information and an openness concerning decisions and actions.[101]

Stakeholders noted two concerns regarding the ways in which such a right is undermined in practice. The first relates to the content of the information provided. An anonymous stakeholder observed that there is a gap between the information that a data subject has access to and the type of information that is required to lay a complaint. They noted that data subjects often do not have access to sufficient information, which makes it difficult or impossible to lay a substantive complaint. This accordingly undermines their right to an effective remedy. They recommended that an audit be conducted to align the information required to lodge a complaint with the information made available to a data subject.

The second relates to the mechanism used by data subjects to physically request access to information. This concern was raised by several stakeholders who, drawing on experience with access to information legislation, noted that the right to access is undermined by inaccessible processes. Such processes may be uncertain, be complicated, or provide complex language and literacy hurdles. As noted by Kuda Hove, a Policy Officer at Privacy International:

> "In a country with 16 official languages, the request for information has to be reduced to writing by the person making the application and the writing has to be in English, which is a barrier in itself."

It was pointed out that these difficulties are compounded by a culture around access to information where private and state entities do not feel obligated to provide information, and

[100] Privacy International, 'A Guide for Policy Engagement on Data Protection: Rights of Data Subjects,' accessed on 31 May 2021, available here.
[101] Above n 72.

individuals assume they are not entitled to it. The stakeholder noted that to enable access to information required a culture shift:

> "It's really an issue of shifting people's cultures. On the one hand, you make the public more willing to access that information that is held by different entities. On the other hand, you make entities understand that they do have an obligation to release information as it is requested, [and] they should think about issues around accessibility."

Another stakeholder commented on the reasons why undermining the right to access information undermines the right to privacy:

> "There are a lot of gaps in terms of access to information, which become profoundly important for the realities of privacy. If you think about it, data subject access is a fundamental part of privacy rights. So not having these legislative foundations for access in place and not having the cultural and bureaucratic foundations in place for access are a huge problem for privacy, but also continue to be a problem for access to information."

In order for the right to access personal data to be meaningful, a data subject must be able to exercise the right through an accessible mechanism which considers contextual language and literacy barriers. Literature on the right to access information concerning personal data notes that the disclosure of information is not enough—the information must also be "reliable, accessible, of good quality and on time" to be effective.[102] Accordingly, Privacy International recommends that the law should provide the following minimum requirements:[103]

- **Timeframe:** this should be within a reasonable and stated time.
- **Cost**: individuals should bear no cost for obtaining information about processing and a copy of their personal data.
- **Format:** the information provided to the data subject should be in a form that is readily intelligible to them and does not require them to have any expertise or knowledge in order to comprehend the information they are provided with.

It is also important that data subjects be provided with reasons for any denial of access, and they must be provided with the right to challenge or appeal such a decision.

[102] Above n 72 at page 2.
[103] Above n 103 at page 4.

Focus 14 | The Rights to Request the Correction or Deletion of Personal Data

All twelve members provide data subjects with the right to request the correction or deletion of their personal data. Although the justifications for such a request differ slightly, the general trend in the members' laws is to allow for this if the personal data is inaccurate, is false, or has been unlawfully processed.

Seychelles' law is substantially different from the laws of the other countries. Although premised on the inaccuracy of personal data, it requires a data subject to launch a court application for compensation for such inaccuracy following which a court may order rectification or erasure. The court may also order erasure following a claim for damages due to unlawful disclosure or access of personal data if there is a substantial risk of further disclosure. Requiring a data subject to launch a court application, which is both costly and time-consuming, places a significant barrier on the exercise of such rights.

There are a few anomalies in the scope of application of this right. Côte d'Ivoire extends the right to the descendants of a deceased person whose data they believe has not been updated. This would be unnecessary in a country, such as South Africa, that limits the scope of application of the data protection law to personal data concerning living natural people, which excludes the personal data of the deceased. Côte d'Ivoire goes even further by providing data subjects with a right to request the erasure and cessation of the dissemination of data which was made available when they were a minor. In Morocco, the right to request correction, destruction, or erasure extends to third parties with whom the personal data has been communicated. In such cases, the data controller must undertake the corrections at no cost to the applicant within ten days. In Kenya, in cases where the data has been shared with a third party, the data controller or processor must take reasonable steps to inform the third party of the request for rectification, erasure, or destruction. If such data is required for evidence, the data subject must be informed of that.

The exercise of this right implicates other important rights such as access to information and freedom of expression. Importantly, as noted by Privacy International:

> It is essential that provision is made to ensure among other safeguards, that when processing the request, the data controller will consider the public interest of the data remaining available. It is essential that any such right clearly provides safeguards and in particular exemptions for freedom of expression. The Construction of this right and how it will play out in the national context must be considered very carefully to ensure that it is not open to abuse.[104]

South Africa and Ghana provide an interesting solution that may mitigate any concerns relating to the removal of such information. Their laws provide that on receipt of a request to correct or delete personal data, the data controller must comply or provide credible evidence in support of the data. Where agreement cannot be reached between the data controller and the data subject, and if requested to do so by the data subject, the data controller must attach to the record an indication that a request was made but not complied with.

[104] Above n 103 at page 5.

Importantly, this right relies on the data subject's awareness that a data controller is processing their personal data and is accordingly enabled through their right to request access and their right to notification. The undermining of their access and notification rights accordingly diminishes their capacity to exercise the right to request the correction or deletion of their personal data.

Focus 15 | Consent

Data subject consent is one of the lawful justifications provided for the processing of personal data. It is accordingly a mechanism that enables participation by allowing a data subject to control the ways in which their personal data is used.

Table 15: Data Subject Consent

Country	Does the Law Define the Requirements for Consent?	Requirements for Consent	Does the Law Require Opt-in Consent?
Burkina Faso	No	Not applicable	Not specified
Cabo Verde	Yes	It must be a free, specific, and informed expression of will.	No
Côte d'Ivoire	Yes	It must be express, unambiguous, free, specific and informed.	Not specified
Ghana	No	The minister is empowered to make regulations which specify the conditions that must be satisfied for consent to be given.	No
Kenya	Yes	It must be express, unequivocal, free, specific, and informed.	Yes
Liberia	No law	No law	No law
Malawi	Yes	It must be freely given, specific and informed.	No
Morocco	Yes	it must be free, specific, and informed.	Not specified
Nigeria	Yes	It must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes.	The law is not clear
Senegal	Yes	It must be an express, unequivocal, free, specific, and informed manifestation of will.	Not specified
Seychelles	No	Not applicable	No
Sierra Leone	No law	No law	No law
South Africa	Yes	It must be a voluntary, specific, and informed expression of will.	No
Tunisia	Not specifically	The law does state certain specific conditions for consent in some provisions which require that it is written and must be express and specific.	No

The legislation of eight of the twelve members provide requirements for valid consent. Ghana ascribes the power to determine the requirements to the minister to be included in regulations. Tunisia does not include a single definition of consent, but specific provisions contain certain requirements for consent. All eight members require that consent must be ***voluntarily*** and ***freely given*** and that it is ***specific*** and ***informed***. With regards to consent being ***voluntarily*** and ***freely given***, the UK ICO notes:

> Consent means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given and it will be invalid.
>
> This means people must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time. It also means consent should be unbundled from other terms and conditions (including giving separate granular consent options for different types of processing) wherever possible.[105]

In order for consent to be specific and informed, the data subject must be provided with sufficient information. Such information should include: the identity of the data controller, the purpose for the processing and the right to withdraw consent.[106] Notably, Kenya 's law is the only one that expressly requires opt-in consent.

As noted above, the right to access personal data and request the correction or deletion of it empowers the data subject to control the ways in which their personal data is used, and ultimately increase their participation. Several stakeholders, however, have noted the general lack of awareness of data protection measures that exist amongst data subjects. This lack of awareness likely contributes to diminished participation from data subjects because they are unaware of their rights.

Such a lack of awareness is often misconstrued as a lack of concern for data protection amongst people in African countries. This idea has been debunked by several stakeholders who note that people in Africa articulate such concerns but there is often a need to link the issues around data protection to real harms. In light of this, Grace Bomu, a Research Fellow at CIPIT, Strathmore University, in Kenya, recommends that effective data protection requires awareness-raising. Chawki Gaddes, president of the regulatory authority in Tunisia, observed that a culture of data protection has started to develop and grow in Africa. He noted that as awareness grew in Tunisia, the number of complaints received by the regulatory authority increased. This provides some evidence that increased awareness correlates with increased participation by data subjects.

[105] UK ICO, 'What is Valid Consent?' Accessed on 31 May 2021, available here.
[106] *Id.*

The Regulatory Authority's Domestic Participation

Focus 16 | Stakeholder Engagement

Gabriella Razzano, Senior Research Fellow at Research ICT Africa in South Africa, noted that transparency is facilitated by public participation. An effective data protection regime requires the facilitation of spaces where the regulatory authority can engage with multiple stakeholders and requires direct access to the regulatory authority. Several stakeholders noted the important need for the regulatory authority to engage with various stakeholders. In commenting on this, Teki Akuetteh Falconer, a Founder and Director of Africa Digital Rights' Hub and former member of the regulatory authority in Ghana, noted:

> "When I was in the regulator, I saw the role of all stakeholders as important in the ecosystem. The role of civil society is extremely important. Looking at the lack of resources and the ability of CSOs to bring different groups together to facilitate a driven agenda, I believe CSOs in the space of data protection will create an enabling environment – the regulator and the private sector can't do it alone. CSOs also brings a certain accountability standard to the table. If it is able to look at the ecosystem from a fair and objective point of view, it will be able to bring all stakeholders to account—and this isn't just about complying with a law. It's broader—they ask if what is being done is helping citizens, is it enabling our citizens? CSO's are in a better position to call these people to order to say: 'You aren't respecting x or doing y.'"

Mugambi Laibuta, an advocate of the High Court of Kenya, agreed and noted that it is important for the regulatory authority to have the power to engage with multiple industry players and that data protection should be a participatory process. He noted that it is important for these bodies to consult with stakeholders before releasing guidelines or notes on specific things such as consent or data protection impact assessments. He also observed with concern that the regulatory authority in Kenya released guidance notes on consent and a manual on complaints without engaging with stakeholders beforehand. Public participation is a constitutional imperative in Kenya, so the lack of public participation means that these guidelines may be challenged and declared unconstitutional.

Gabriella Razzano, pointed out the importance of the regulatory authority having a cross-cutting mandate which enables them to facilitate multi-stakeholder conversations. She commented: "What are regulators there for? They're there to intervene in the economy and that's how they're different from other powers." She went on to note that "they require the ability to facilitate multi stakeholder conversations. Whether they have the capacity to do that then becomes the further question and whether there's a political will to listen to them is a separate question." Drawing on the example of South Africa's regulatory authority being excluded from the regulations concerning contact tracing, she noted: "What does that mean about their ability to convene the kinds of cross-sector conversations that they need to when national government doesn't know they're there?"

Focus 17 | The Regulatory Authority's Mandate to Participate in Policy Formulation

The section concerns focus area 17: the regulatory authorities' capacity to participate in domestic policy. Table 16 notes which of the members are empowered to do so and details the specifics of their participation.

Table 16: The Capacity of the Regulatory Authority to Participate in Policy

Country	Is the Regulatory Authority Mandated to Participate in Policy Formulation?	What is the Scope of the Regulatory Authority's Participation?
Burkina Faso	Yes	The regulatory authority is empowered to propose legislative or regulatory measures to the government that aim to protect freedoms in response to technological developments.
Cabo Verde	Yes	The regulatory authority must be consulted on legislative initiatives concerning personal data processing.
Côte d'Ivoire	Yes	The regulatory authority is empowered to determine the essential guarantees and measures appropriate for the protection of personal data, to give its opinion on any draft legal text in relation to the protection of freedoms and privacy, and to develop rules of conduct relating to the processing and protection of personal data.
Ghana	The law is unclear	The minister may give directives to the board, which is the governing body of the commission, on matters of policy.
Kenya	The law is unclear	The regulatory authority is required to research developments in data processing to minimise risk, but it does not specify whether such research will inform legislation or policy.
Liberia	No law	No law
Malawi	No	Not applicable
Morocco	Yes	The regulatory authority is empowered to provide its opinion to the government and parliament on legal or regulatory propositions or projects relating to the processing of personal data.
Nigeria	Yes	The regulatory authority is empowered to review guidelines and regulations made under the Bill.
Senegal	Yes	The regulatory authority is empowered to present suggestions to the government to simplify or improve the legislative and regulatory framework with regard to the processing of personal data.
Seychelles	No	Not applicable
Sierra Leone	No law	No law
South Africa	Yes	The regulatory authority is required to keep up to date with any legislative, policy, or technological developments which may impact the protection of personal information, and must further submit a report to parliament on any necessary action to be taken.
Tunisia	Yes	The regulatory authority is mandated to "determine the essential guarantees and appropriate measures for the protection of personal data" as well as provide opinions, develop rules of conduct, and participate in research, training, and study activities.

Eight of the twelve members are empowered to participate in domestic policy, albeit in different ways. The purpose of the participatory policy-making process is to "facilitate the inclusion of individuals or groups in the design of policies via consultative or participatory means to achieve accountability, transparency and active citizenship."[107] Importantly, the regulatory authority will have the relevant expertise to guide data protection policy. Their inclusion in the process provides an opportunity to strengthen weaknesses that exist in the regulatory system.

[107] Rietberger-McCracken, J., 'Participatory Policy Making,' page 1, accessed on 31 May 2021, available here.

The Regulatory Authority's Regional and International Participation

Focus 18 | Regulatory Authority Participation

Various stakeholders noted the importance of the regulatory authority's regional and international participation. Importantly, Senegal's law specifically provides that the regulatory authority is empowered to cooperate with regulatory authorities from other countries and participate in international organisations relating to the protection of personal data. An anonymous stakeholder noted that effective data protection requires the regulatory authority to be integrated into regional associations in order to assist with coordination and the development of jurisprudence and resources. They noted that effective regional cooperation is particularly important for regional concerns such as cross-border data transfers, and noted that Senegal, Mauritius, and Ghana are examples of countries that are effectively cooperating at a regional level.

Regional bodies do exist, but they are not at a stage where they are providing technical support to each other. Alison Tilley, a member of the regulatory authority in South Africa, noted that there are several regional and international associations[108] that the South African regulatory authority is part of. She noted that the engagements currently focus on knowledge and experience sharing and are not technical discussions about issues such as cross-border data transfers and adequacy findings. Chawki Gaddes, a former president of the regulatory authority in Tunisia, noted that the Association of Francophone Data Protection Authorities is not making joint determinations on technical matters such as cross-border data transfers, but rather making resolutions on conceptual ideas such as whether or not a data subject owns their personal information and is able to sell it.

In light of this, stakeholders have recommended regional coordination at the African Union level, possibly through the African Commission on Human and Peoples Rights or through the establishment of a new division within the African Union Commission. It was noted that because data protection issues concern matters of justice, privacy, and technology, it is important that any coordinating body is housed in the right contextual space that is able to deal with the multifaceted nature of data protection. It was suggested that an office similar to the European Data Protection Board should be established.

Greater regional cooperation was posed as a possible solution to the lack of legitimacy of the law, which stems from it being drafted by external actors or funders. It has been noted that some of the concerns may be mitigated if the process is African-lead, and if jurisprudence is developed regionally. Regional cooperation was also recommended to harmonise legislative standards and to facilitate and enable technical aspects such as cross-border data transfers.

---

[108] An example is the African Network of Data Protection Authorities, Réseau Africain Des Autorités De Protection Des Données Personnelles, (RAPDP), which was established in 2016 at the African Forum on personal data protection. It comprises several regulatory authorities from different geographical and linguistic areas and aims to set up a platform for exchanges and cooperation between its members. The following African OGP members are members of the RAPDP: Burkina Faso, Cape Verde, Côte d'Ivoire, Ghana, Morocco, Senegal, South Africa, and Tunisia.

Recommendations to Strengthen Participation

- Audits should be conducted to determine what information a data subject has access to and what information is required in order to lay a complaint. The two must align to enable a data subject to exercise their right to an effective remedy. It is envisaged that data controllers will be the implementing actors.
- Data controllers must ensure that the process they implement to realise a data subject's right to request access to their personal data is clear, is certain, and considers contextual language and literacy barriers. The law should provide for minimum requirements that notes a timeframe for a response, it should not entail a cost, and the information should be provided in an intelligible format. It is envisaged that data controllers and members will be the implementing actors.
- Data subject participation is undermined by a lack of awareness of data subject rights. Awareness campaigns should be undertaken to facilitate data subject participation. It is recommended that linking data protection concerns to real-life harms makes the content more accessible. It is envisaged that the regulatory authorities, members, and civil society organizations will be the implementing actors.
- The regulatory authority should have a cross-cutting mandate and the capacity to facilitate multi-stakeholder conversations. It is envisaged that members and the regulatory authorities will be the implementing actors.
- Data protection should be a participatory process and in order to enable this, regulatory authorities should consult with stakeholders before releasing regulatory documents such as guidance notes. It is envisaged that regulatory authorities will be the implementing actors.
- A body or mechanism should be established to enable greater regional cooperation. It is recommended that such coordination take place at the African Union level and an office similar to the European Data Protection Board should be established. Such a body could provide regional guidance to states on data protection issues. It is envisaged that members and the African Union will be the implementing actors.

AUTOMATED PROCESSING

In this section, we briefly discuss the regulation of automated processing by members. The increased use of artificial intelligence has created a need for greater protection concerning the automated processing of personal data. As noted by Privacy International:[109]

> Because of the heightened risks to human rights and freedoms and issues such as fairness, transparency, and accountability, data protection frameworks may impose restrictions and safeguards on the ways in which data can be used to make decisions. These safeguards should include a right not to be subject to certain automated decisions as this is important where these decisions are consequential for individuals, and in particular where they affect their rights.

The members' regulation of automated processing in their data protection legislation is detailed in Table 17 and is discussed briefly in this section.

Table 17: Automated Processing

Country	Does the Law Provide Data Subjects with a Right Not to Be Subject to Automated Decision-Making?	Is Automated Decision-Making Regulated Elsewhere in the Data Protection Law?	Exceptions to the Prohibition
Burkina Faso	Yes	Not applicable	None
Cabo Verde	Yes	Not applicable	None
Côte d'Ivoire	No	Yes	None
Ghana	Yes	Not applicable	Decisions made in the course of considering whether to enter into a contract, in the performance of a contract, for a purpose required or authorised by an enactment, or in other circumstances prescribed by the minister.
Kenya	Yes	Not applicable	When it is necessary for entry into or performance of a contract between the data subject and the data controller, when the data controller is authorized to do so by law, and such law includes suitable safeguards for the data subject's rights, and when the data subject consents to it.
Liberia	No law	No law	No law

[109] Above n 103 at page 58.

Table 17: Automated Processing (continued)

Country	Does the Law Provide Data Subjects with a Right Not to Be Subject to Automated Decision-Making?	Is Automated Decision-Making Regulated Elsewhere in the Data Protection Law?	Exceptions to the Prohibition
Malawi	No	No	Not applicable
Morocco	Yes	Not applicable	Decisions taken for the conclusion or performance of a contract, and decisions made at the request of the data subject.
Nigeria	Yes	Not applicable	In considering whether to enter into a contract with the data subject, in the performance of such a contract, for a purpose authorised by an enactment, and in other circumstances prescribed by the regulatory authority.
Senegal	No	Yes	Decisions taken in the context of the conclusion or execution of a contract and for which the data subject has been able to present concerns.
Seychelles	No	No	Not applicable
Sierra Leone	No Law	No law	No law
South Africa	Yes	Not applicable	When the decision has been taken in connection with the conclusion or execution of a contract, or when the decision is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.
Tunisia	No	Yes, the law provides data subjects with a right of access.	Not applicable

Seven out of the twelve members provide data subjects with a right not to be subject to automated decision-making. Three out of the remaining five members regulate automated decision-making in other ways in the law. The data protection law in Côte d'Ivoire, for example, stipulates that no court decision involving an assessment of the behaviour of a natural person may be based on automatic processing of personal data intended to assess certain aspects of their personality. It further provides that no administrative or private decision involving an assessment of the behaviour of a natural person may be based solely on automatic processing.

In Tunisia, the only specification in the law for automated decision-making requires that if a data subject's information is being processed with the aid of automated processes, then the data subject has the right to access their information in an intelligible form. This includes implementing the technical means necessary to allow the data subject to send their request for correction or deletion of personal data by electronic means. It accordingly does not provide data subjects with a right not to be subject to decisions based on automated decision-making, including those that create a profile about a data subject. From the text of the law, it appears that data controllers are able to use automated decision making, and no redress mechanisms are provided to data subjects to challenge such a decision.

In Burkina Faso, no exceptions to the prohibition are included but automated processing of personal data on behalf of the state, a public entity, a local authority, or a juristic person governed by private law and managing a public service are decided by decree after reasoned approval of the regulatory authority. It appears that automated processing on behalf of these entities is treated differently.

Cabo Verde does not note any exceptions to the prohibition, and it includes a requirement that data controllers notify the regulatory authority before carrying out any wholly or partially automated data processing operations. An exemption from notification is allowed if the sole purpose of the processing is for the maintenance of a register intended to provide information to the public and which is open to consultation by the public or by any person demonstrating a legitimate interest

It is noted that when automated decision-making is permitted, the data subject must still be afforded the right to obtain human intervention.[110] The data subject must also be provided with a right to an effective remedy.

[110] *Id* at page 59.

CONCLUSION

African OGP members have taken commendable strides in their pursuit of the protection and promotion of the right to privacy. Their adoption of data protection legislation far outweighs the adoption rate of other African states. However, some work is still required for all fourteen members to have data protection laws in force: three remain in draft form and two states—Liberia and Sierra Leone – have yet to publish draft bills.

On the whole, the African OGP members provide a robust and effective legislative framework with some notable inclusions. All twelve members provide data subjects with the right to be notified that their personal data is being processed—a right that contributes significantly to transparency and increased accountability. They also all provide data subjects with the right to access their personal data and to request the correction and deletion of it—rights that enable data subject participation. The establishment of a regulatory authority by all twelve members ensures that compliance with the law is monitored and enforced and when coupled with the provision of sanctions, it may pave the way for an accountable framework.

However, there is often a disconnect between the legislative text and the implementation of the law. Serious concerns have been raised regarding the deliberate undermining of the regulatory authority through the erosion of its institutional independence, which cripples its adjudicatory independence. Accountability is further diluted by the lack of appropriate expertise—in the regulatory authority, the police service, and the judicial system. These factors may work to create a culture of impunity, which is noted as a significant barrier to effective data protection.

Much work is required to ensure the effective functioning of the data protection regime. Teki Akuetteh Falconer, reflecting on her time as a member of the regulatory authority in Ghana, remarked that “if your objective is to create an ecosystem of respect for personal data which minimizes risk of harm to humanity, then it’s fairly easy to measure everything by that yardstick.” She recommends that every regulator should ask themselves everyday about what they are trying to achieve, and in answering that question, they should try to be as objective and fair as possible because it is not a personal agenda, it is a country’s agenda.

REFERENCE LIST

Academic and research texts

Adebisi Abdulrauf, L., Regulating Transborder Flow of Personal Information for Development in the G77+China Group,' Unisa Latin American Report, Volume 31, Issue 1, 2015, 77-96.

Andagalu, R., 'Kenya High Court rules constitutional amendment bill unconstitutional,' Jurist, (16 May 2021).

Banisar D., World Bank Institute, 'The Right to Information and Privacy: Balancing Rights and Managing Conflicts.'

Boniface Makulio, A., 'Privacy and Data Protection in Africa: A State of the Art 2021,' International Data Privacy Law Vol. 2. No.3.

Boshe, P., 'Data Protection Legal Reform in Africa,' 2017, Passau University.

Cuijpers, C., 'A Private Law Approach to Privacy: Mandatory Law Obliged?' (2007) 4/4 SCRIPTed 304–18.

De Hert, P. and Gutwirth, S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action,' in S Gutwirth, et al. (eds), Reinventing Data Protection? (Springer, New York 2009) 3–44.

Karanja, SK., 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation,' PhD Thesis, Faculty of Law, University of Oslo, (2006).

International Network of Privacy Law Professionals, 'A Brief History of Data Protection: How Did it All Start?' 22 May 2021.

Razzano, G., Research ICT Africa, 'Understanding the Theory of Collective Rights: Redefining the Privacy Paradox,' page 5.

Rietbergen-McCracken, J., 'Participatory Policy Making,' CIVICUS.

Roos, A., 'Core Principles of Data Protection Law,' The Comparative and International Law Journal of Southern Africa Vol. 39, No. 1: 102.

Solove, D., 'The Myth of the Privacy Paradox,' 89 George Washington Law Review 1, (2021), available here.

Turner, M., Information Policy Institute, 'Towards a Rational Personal Data Breach Notification Regime,' June 2006.

Tzanou, M., 'Data protection as a fundamental right next to privacy? Reconstructing' a not so new right,' (2013).

United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide.'

World Bank Group, 'Open Data Readiness Assessment' Prepared for the Government of Sierra Leone.'

Legal resources and guidelines

European Commission Article 29 Data Protection Working Party, 'Guidelines on Transparency Under Regulation 2016/67,' adopted on 29 November 2017.

OECD, 'The Governance of Regulators: Creating a Culture of Independence, Practical Guidance Against Undue Influence.'

Report of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age,' 3 August 2018.

Legal texts

Burkina Faso: The Protection of Personal Data Act 010-2004/AN of 2014.

Cabo Verde: The Data Protection Act, Law 133 of 2001.

Côte d'Ivoire: The Protection of Personal Information Act 2013-450.

Ghana: Data Protection Act, 2012, Act 843.

Kenya: The Data Protection Act, 2019.

Malawi: The Electronic Transactions and Cyber Security Act, 2016.

Morocco: Law no. 09-08 of 18 February 2009.

Nigeria: The Draft Data Protection Bill, 2020.

Senegal: Law No. 2008-12 of 25 January 2008.

Seychelles: Data Protection Act 9 of 2003.

South Africa: Protection of Personal Information Act 4 of 2013.

Tunisia: Law No. 2004-63 of 27 July 2004.

Web-based resources

'AD173: In name of security, many Ugandans willing to let government monitor private and religious speech,' AfroBarometer (2018).

'AD165: Majority of Zimbabweans want government out of private communications, religious speech,' AfroBarometer (2017).

'Freedom of information: Batswana back private communication, public accountability,' AfroBarometer, (2017).

Bulao J., 'How Much Data is Created Every Day in 2021?' *Techjury*.

'Data Protection Africa,' ALT Advisory (2020), available here.

Privacy International, '2020 Is a Crucial Year to Fight for Data Protection in Africa.'

Privacy International, 'A Guide for Policy Engagement on Data Protection: Rights of Data Subjects,' accessed on 31 May 2021.

Privacy International, 'The Right to Privacy in Morocco,' (2016).

Privacy International, 'What Is Privacy?' 23 October 2017.

Ruttkamp-Bloem, E., 'Artificial Intelligence Presents a Moral Dilemma,' *Mail & Guardian*.

U4 Anti-Corruption and Transparency International, 'Does More Transparency Improve Accountability?'

UK ICO, 'Principle (a): Lawfulness, Fairness and Transparency,' accessed on 13 May 2021, available here.

UK ICO, 'What is a Personal Data Breach?'

UK ICO, 'What is Valid Consent?'

Zúñiga, N., Transparency International, 'Does More Transparency Improve Accountability?'