Africa Guide

Data Protection

BOWMANS

THE VALUE OF KNOWING

CONTENTS

Foreword

In the digital age, personal data has become one of the most valuable commodities. The rapid adoption of digital technologies has led to an urgent need for robust data protection frameworks that safeguard privacy rights while also facilitating international trade and the free flow of information across borders. As governments, businesses, and civil society increasingly recognise the risks of data misuse, the development and enforcement of comprehensive data protection laws have become a priority.

Since its adoption, the European General Data Protection Regulation (**GDPR**) has had a global impact on how international businesses process, handle, and protect personal data. Several African countries have followed suit and have looked to the GDPR as a benchmark for developing their own data protection laws. These nations are at various stages in their regulatory journeys, with countries like Ghana, Kenya and Mauritius already having well-developed legislation in place, and Botswana, Ethiopia and Malawi having recently enacted new legislation. On the other hand, Namibia has yet to enact a comprehensive data protection framework. In Nigeria, South Africa, Tanzania and Zambia, data protection regulation is still relatively new and developing, as the respective regulators find their feet and seek to enforce the legislation.

The members of our Data Protection Group, a multi-jurisdictional and multi-disciplinary team of experienced lawyers, regularly advise clients on data protection requirements across Africa and assist with data protection compliance, incident response initiatives, training, and disputes.

We also keep abreast of regulatory changes and have prepared this guide to update our clients on the latest developments in this important area of the law. It provides a snapshot of the regulatory landscape in 12 countries and has been prepared in collaboration with our alliance firms in Ethiopia and Nigeria and our relationship firms in Botswana, Ghana, Malawi and Uganda. The information is provided as at May 2025.

Please contact me or any of the key contacts included in the country chapters if you would like to discuss the content of this guide in more detail.

CHLOË LOUBSER
Knowledge and Learning Lawyer – Employment & Data Protection
Cape Town, South Africa

The contents of this publication are for reference purposes only. It is not a substitute for detailed legal advice.

BOTSWANA

The Data Protection Act, 2024 (**DPA 2024**) replaced the Data Protection Act, 2018 in October 2024.

The DPA 2024 commenced on 14 January 2025. It seeks to align Botswana's data protection laws with the General Data Protection Regulation 2016/679 of the EU.

At the date of writing, the Information and Data Protection Commission (**Commission**) is being constituted and is actively spreading data protection awareness across Botswana. The Commission has not yet imposed administrative fines against any organisation. Further, there are no decided cases regarding data protection issues yet.

Main laws	DPA 2024 and the Transfer of Personal Data Order, SI No. 95 of July 2022
Key regulators	The Commission, which is a public office responsible for the enforcement of the DPA 2024
Are there specific requirements applicable to the collection and processing of data?	Yes, in terms of the DPA 2024, the processing of personal data will only be lawful if there is a legal basis for such processing. There are six legal bases provided in section 26 of the DPA 2024.
Is there a requirement for data localisation?	Yes. When transferring personal data outside Botswana, data controllers and processors must ensure that a copy remains in Botswana. This means that data controllers/ processors must store a complete, secure and accessible copy of the personal data within Botswana.
Are there limitations on cross-border transfers of data?	Yes, the DPA 2024 provides for limitations on the cross-border transfer of personal data outside Botswana. Personal data may only be transferred outside Botswana if there is an adequacy decision by the Commission, adequate safeguards (eg, binding corporate rules), or the data controller relies on any of the derogations provided for by section 78 of the DPA 2024.

Are there registration requirements?	No, there are no registration requirements with respect to the processing of personal data, save that data controllers/ processors are required to notify the Commission of their appointment of a Data Protection Officer (**DPO**).
Is a Data Protection Officer required?	Yes, however, it is not a general requirement. A DPO is required where: • processing is carried out by a public authority or body; • the core activities of the data controller or data processor involve processing activities that require regular and systematic monitoring of data subjects on a large scale; or • the core activities of the data controller or data processor consist of processing of sensitive personal data on a large scale or personal data relating to criminal convictions and offences.
Is a risk assessment/ privacy impact assessment required?	Yes, however, this is not a general requirement. In terms of section 65 of the DPA 2024, a data controller is required to conduct a data protection impact assessment (**DPIA**) where a type of processing uses new technologies and is likely to result in a high risk to the rights and freedoms of data subjects. A DPIA is required in the following cases: • a systematic and extensive evaluation of the personal aspects of an individual based on automated processing, including profiling; • processing of sensitive personal data on a large scale; and/ or • systematic monitoring of public areas on a large scale.
Must data breaches be reported?	Yes, personal data breaches must be reported to the Commissioner within 72 hours of the data controller becoming aware of same, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject.

Key enforcement/ sanction provisions	The Commission may issue a warning where satisfied that the intended processing operations are likely to contravene the provisions of the DPA 2024. Additionally, the Commission may issue reprimands, order a data controller/ processor to comply with the DPA 2024, suspend processing activities or impose an administrative fine. The Commission may impose administrative fines of up to BWP 50 million or 4% of the total annual worldwide turnover of group entities.
Is cybercrime regulated in terms of any laws, regulations or directives?	Yes. The Cybercrime and Computer Related Crimes Act [Cap 08:06] governs the interception of non-public transmission of communications on a computer or computer system, disclosure of passwords and cyber offences.
If regulated, are there any cybercrime reporting requirements?	No, there is no general requirement to report cybercrime in Botswana.

SENWELO MODISE
Head of Technology, Cyber and Data Protection
Bookbinder Business Law
Gaborone, Botswana

E: senwelo@bookbinderlaw.co.bw

PHENYO KEDISITSE
Associate
Bookbinder Business Law
Gaborone, Botswana

E: phenyo@bookbinderlaw.co.bw

ETHIOPIA

Data protection in Ethiopia is a developing area of law. A comprehensive personal data protection law was promulgated in July 2024 when the Ethiopian House of Peoples' Representatives (**Parliament**) adopted the Personal Data Protection Proclamation No. 1321/2024 (**Proclamation**). It had been awaiting approval since 2020.

Prior to the adoption of the Proclamation, Ethiopia did not have a unified and comprehensive legal framework governing data protection. Rather, data protection provisions were incorporated in numerous pieces of legislation including the Constitution, the Telecommunications Consumer Rights and Protection Directive, the Financial Consumer Protection Directive, the Computer Crime Proclamation, and the Criminal Code.

Main laws	The Proclamation
Key regulators	The Ethiopian Communications Authority (**ECA** or **Authority**) is mandated under the Proclamation to monitor and ensure compliance by data controllers and processors with the provisions of the Proclamation.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the Proclamation.
Is there a requirement for data localisation?	Yes, in principle, a data controller or data processor is required to store data on a server or data centre located in Ethiopia in so far as the personal data has been obtained or collected locally. Further, the Proclamation provides that some of the data may only be processed on a server or data centre located in Ethiopia. In particular, the Proclamation envisages that the ECA will prescribe categories or personal data as critical personal data, which will only be processed in a server or data centre located in Ethiopia. Such critical personal data will be determined based on grounds of strategic interests of the State.

Are there limitations on cross-border transfers of data?	A data controller or data processor may transfer personal data to a third-party jurisdiction upon: • providing proof to the Authority of the existence of an appropriate level of protection in that third-party jurisdiction; • the data subject giving explicit consent to the proposed transfer; • the transfer being necessary: for the performance of a contract between the data subject and the data controller/ processor; for the conclusion or performance of a contract concluded in the interest of the data subject; or for important reasons of public interest; or • the transfer being made from a register which, according to law, is intended to provide information to the public. While prior approval of the Authority is not required for cross-border transfers, provided that the above conditions are fulfilled, the prior approval of the Authority is required to transfer sensitive data. In addition to the Proclamation, there are also sector-specific requirements regarding data transfers in the case of the telecommunications sector.
Are there registration requirements?	Yes. The Proclamation requires the prior registration of data controllers and data processors. The Proclamation empowers the Authority to register data controllers and/ or processors if they are to engage in data processing. Also, the Authority is mandated to cancel a registration if it finds any information given to it to be false or misleading or if the registration holder fails to comply with any requirement. The Authority is yet to issue a directive outlining details on registration requirements.
Is a Data Protection Officer required?	Yes, a data controller or processor is required to appoint a data protection officer (**DPO**) where: • the processing is carried out by a government body, except for courts acting in their judicial capacity; • the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale; or • the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.

	Any data controller/ processor that falls under any of the categories above is required to designate a DPO. As such, not all data controllers/ processors are required to appoint a DPO. That said, the Proclamation does not define what constitutes 'large scale'. We expect this requirement to be further clarified in a future directive to be issued by the Authority.
Is a risk assessment/ privacy impact assessment required?	Yes, the Proclamation dictates that data controllers or processors, in cases where processing operations may result in a risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes, are required to carry out an assessment of the impact of the intended processing operations on personal data protection. The Proclamation further provides for the specific elements that must be considered in carrying out the assessment, including assessments of the necessity of the processing operations, the risks to the rights and freedoms of the data subjects and measures to address the risks and safeguards as well as security measures. Moreover, data controllers and data processors are required to implement the appropriate technical and organisational measures, including performing a data protection impact assessment.
Must data breaches be reported?	A data processor is required to notify the data controller without undue delay, after becoming aware of a personal data breach. A data controller is also required to notify the Authority and the data subject, in the case of a personal data breach, within 72 hours after having become aware of the breach. In notifying the personal data breach, the Proclamation requires the data controller to provide information relating to the nature of the personal data breach, the name and contact details of the DPO, likely consequences of the breach and measures taken or proposed to be taken by the data controller addressing the breach. In addition to the above requirements under the Proclamation, there are also other sector-specific requirements for reporting data breaches.

Key enforcement/ sanction provisions

The Proclamation mandates the Authority to impose administrative penalties on persons contravening the Proclamation and other implementing legal instruments.

A subsidiary regulation is projected under the Proclamation to lay out the details of administrative offences and fines in cases where an offence is committed by an institution, in relation to sensitive data, or against the personal data of a minor. In such cases, the administrative offence results in a fine of up to 4% of a company's total worldwide turnover in the preceding financial year, with any gains made going to the Government.

In addition to the administrative sanctions, the Proclamation dictates that failure to notify a data breach, failure to implement technical and organisational measures in a case of breach, or processing personal data in contravention of the Proclamation, constitutes a criminal offence entailing simple imprisonment and/ or fines.

Other categories of criminal offences, such as failing to erase personal data against the rights of the data subject, restricting processing, selling or offering to sell personal data, and transferring personal data outside Ethiopia in violation of the Proclamation, are some among a list of those identified under the Proclamation, which entail criminal sanctions of imprisonment ranging from simple to serious and the imposition of fines.

A much more stringent criminal sanction of a fine of up to 4% of a company's total worldwide turnover in the preceding financial year is imposed for offences committed by an institution; causing damage making it a serious offence; committed in relation to sensitive personal data; or committed in relation to the personal data of a minor.

In addition to the above, sector-specific laws contain sanction provisions. The Criminal Code also criminalises the violation of privacy safeguards guaranteed under the Constitution.

ETHIOPIA

Is cybercrime regulated in terms of any laws, regulations or directives?	Yes, the Computer Crime Proclamation No. 958/2016 (**Computer Crime Proclamation**) and the Criminal Code set out offences and penalties for persons committing a 'computer crime'. The Information Network Security Agency has been established to take all appropriate measures to defend cyber or electromagnetic attacks on information and computer infrastructures as well as preventing and investigating cybercrimes, among other things.
If regulated, are there any cybercrime reporting requirements?	Yes, the Computer Crime Proclamation imposes the duty to report on any service provider or government organ that becomes aware of the commission of crimes under the Computer Crime Proclamation or dissemination of illegal content data by third parties through computer systems.

MICAEL SEHUL
Partner
Aman & Partners LLP
Addis Ababa, Ethiopia

E: micael.sehul@aaclo.com

TILAHUN WELDIE
Principal Associate
Aman & Partners LLP
Addis Ababa, Ethiopia

E: tilahun.weldie@aaclo.com

REDEAT STIPHANOS
Senior Associate
Aman & Partners LLP
Addis Ababa, Ethiopia

E: redeat.stiphanos@aaclo.com

GHANA

Data protection is a key focus area in Ghana, which has a fairly developed system including the ratification of international instruments. As the country gradually adopts a more digitalised economy, the protection of personal data has become ever more important.

The regulator of data protection in Ghana is the Data Protection Commission (**DPC**). The DPC has recently become more aggressive in its enforcement of the Data Protection Act and has, on previous occasions, published the names of persons who were not compliant in the media. It is understood that the regulator is working with regulators in other African jurisdictions to harmonise the data protection laws and adopt standard data protection laws across the continent.

Main laws	Data Protection Act, 2012 (**DPA**)
Key regulators	The DPC, an independent statutory body established under the DPA to enforce compliance with the DPA
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the DPA.
Is there a requirement for data localisation?	There are no requirements for data localisation.
Are there limitations on cross-border transfers of data?	There are currently no cross-border data transfer restrictions. However, as the DPA applies, *inter alia*, to the processing of information that originates partly or wholly in Ghana, data recipients in other jurisdictions will be required to meet the same data protection standards that are required in Ghana.
Are there registration requirements?	Yes, a data controller who intends to process personal data is required to register with the DPC. Although not mandatory, data processors are also encouraged to register with the DPC.

GHANA

Is a Data Protection Officer required?	Under the DPA, data controllers may appoint data protection supervisors (or officers). The appointed data protection supervisor must be trained and certified under a DPC-approved training programme. The DPC has indicated that although the appointment of a data protection supervisor is not a mandatory requirement for the initial registration, the appointment is necessary for the renewal of a registration with the DPC. A data controller registering with the DPC for the first time may appoint an ultimate decision maker (such as a CEO or director) as its data protection supervisor, in order to be registered.
Is a risk assessment/ privacy impact assessment required?	The DPA does not make provision for data protection impact assessments. However, the regulator has indicated that a data controller must submit a data protection impact assessment and provide documentary evidence on its personal information management system and information security management system.
Must data breaches be reported?	Yes, the data controller, or a third party who processes data under the authority of the data controller, must notify the regulator and the data subject/s of any unauthorised access or acquisition of personal data.
Key enforcement/ sanction provisions	Under the DPA, where the DPC is satisfied that a data controller has contravened or is contravening any of the data protection principles, it may serve an enforcement notice on the data controller. A person who fails to comply with an enforcement notice commits an offence and is liable on summary conviction to a fine of not more than 150 penalty units or to a term of imprisonment of not more than one year or to both. A penalty unit is equivalent to GHS 12 (approximately USD 0.82). Sanctions may also be imposed where a person knowingly or recklessly discloses personal data or sells or offers for sale personal data; or in circumstances where a person who processes personal data fails to register as a data controller.

GHANA

Is cybercrime regulated in terms of any laws, regulations or directives?	Yes, cybercrime is regulated in Ghana mainly by the Cyber Security Authority of Ghana (**CSA**) as established under the Cybersecurity Act, 2020. The Cybersecurity Act regulates cybersecurity activities and cybercrimes such as crimes related to children, including publication of indecent images and photos of a child, sexual extortion through electronic means, non-consensual sharing of intimate images, threats to distribute prohibited intimate images or visual recordings, etc. The Cybersecurity Act also regulates cybersecurity threats and incidents, and owners of critical information infrastructure, among others. The Electronic Transactions Act, 2008, as amended, also contains laws on cybercrime, and regulates offences such as stealing, charlatanic advertisements, forgery, and electronic trafficking among others.
If regulated, are there any cybercrime reporting requirements?	Yes. An owner of critical information infrastructure is required to report cybersecurity incidents within 24 hours of detecting the incident to: • the relevant Sectoral Computer Emergency Response Team; or • the National Computer Emergency Response Team, in the case of a critical information infrastructure that does not belong to a Sectoral Computer Emergency Response Team. It is also required to conduct an audit on the critical information infrastructure and submit a copy of the audit report to the CSA. A breach of this requirement is subject to an administrative penalty between 250 penalty units and 10 000 penalty units. A Sectoral Computer Emergency Response Team is required to report a cybersecurity incident to the CSA through the National Computer Emergency Response Team. A person in charge of an institution is required to report a cybersecurity incident to the relevant Sectoral Computer Emergency Response Team or the National Computer Emergency Response Team within 24 hours after the incident is detected. A breach of this requirement is subject to an administrative penalty between 250 penalty units and 500 penalty units.

GHANA

KIMATHI KUENYEHIA
Managing Partner
Kimathi & Partners
Accra, Ghana

E: kimathi@kimathilegal.com

ENID BAABA DADZIE
Managing Counsel
Kimathi & Partners
Accra, Ghana

E: enid@kimathilegal.com

VANESSA ALABI
Associate
Kimathi & Partners
Accra, Ghana

E: vanessa@kimathilegal.com

KENYA

The Kenyan authorities are demonstrating a commitment to ensuring the proper regulation of personal data. The Office of the Data Protection Commissioner (**ODPC**) has been active in publishing various Guidance Notes to aid in the implementation and interpretation of the Data Protection Act. Some examples include Guidance Notes for electoral purposes, on registration requirements and on data protection impact assessments, as well as sector-specific Guidance Notes touching on education, health and communication.

Since the enactment of the Data Protection Act, 2019 (**DPA**), and more notably from 2022 onwards, the ODPC has increasingly exercised its investigative and enforcement powers, issuing several decisions addressing compliance with the DPA particularly regarding lawful consent, the exercise of data subject rights, and reliance on appropriate legal bases for data processing.

The Kenyan courts have also been dealing with data protection matters and have offered clarity on the right to privacy and enforcement of the DPA in several recent decisions.

Main laws	The DPA, read with the Data Protection (General) Regulations, 2021, Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021, and the Data Protection (Civil Registration) Regulations, 2020 (together **DP Regulations**)
Key regulators	The ODPC established under the DPA The provisions of the various sectoral laws are enforced by the respective sectoral regulatory bodies, which are now increasingly requiring compliance with the DPA.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the DPA.

Is there a requirement for data localisation?	In terms of the DPA, the Cabinet Secretary may prescribe, based on grounds of strategic interests of the State or protection of revenue, certain types of processing that must only be effected through a server or data centre located in Kenya. There are also data localisation requirements under the DP Regulations that apply to certain sectors, for example, education and healthcare or otherwise where the purpose of processing is for the strategic interests of the Kenyan State.
Are there limitations on cross-border transfers of data?	Yes, the DPA regulates the cross-border transfer of personal data outside Kenya.
Are there registration requirements?	Yes, under the DPA, data controllers and processors are required to be registered with the ODPC, although the ODPC has discretion to prescribe the thresholds for mandatory registration based on: • the nature of the industry; • the volumes of data processed; and • whether sensitive personal data is being processed. The Data Protection (Registration of Data Controllers and Data Processors) Regulations contain applicable thresholds in this regard.
Is a Data Protection Officer required?	The DPA makes provision for the designation of data protection officers, but this obligation is not mandatory and depends on the conditions and activities of the data controller or processor.
Is a risk assessment/ privacy impact assessment required?	Yes, where a processing operation is likely to result in high risk to the rights and freedoms of a data subject (based on the nature, scope, context or purpose of the processing), the data controller or processor must carry out a data protection impact assessment.
Must data breaches be reported?	Yes, data controllers are required to notify data breaches to the ODPC where there is a real risk of harm to the data subject. In certain circumstances, notification must also be made to the impacted data subject/s. Data processors must inform data controllers of any breaches.

Key enforcement/ sanction provisions	Where the ODPC is satisfied that any person has violated the provisions of the DPA, the ODPC may serve an enforcement notice and a penalty notice requiring the person to pay a penalty of an amount up to a maximum of KES 5 million or 1% of an entity's annual turnover the preceding year, whichever is lower. In addition, penalties may also be levied for failing to register as a data controller or processor, unlawful disclosure, processing of personal data without lawful purpose and the sale of personal data.
Is cybercrime regulated in terms of any laws, regulations or directives?	Yes, cybercrime is regulated under the Computer Misuse and Cybercrimes Act, 2018 (**CMCA**), the DPA, the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime) Regulations, 2024, and the Kenya National Cybersecurity Strategy (2022 – 2027).
If regulated, are there any cybercrime reporting requirements?	The CMCA imposes a reporting obligation on any person who operates a computer system or a computer network, whether public or private, to immediately inform the National Computer and Cybercrimes Co-ordination Committee (**NC4**) of any attacks, intrusions and other disruptions to the functioning of another computer system or network within 24 hours of such attack, intrusion or disruption.

JOHN SYEKEI
Head of IP and Technology
Bowmans
Nairobi, Kenya

E: john.syekei@bowmanslaw.com

ARIANA ISSAIAS
Director
Bowmans
Nairobi, Kenya

E: ariana.issaias@bowmanslaw.com

MALAWI

In 2024, Malawi enacted the Data Protection Act, 2024 (**DPA**) which, among other things, provides for the protection of personal data of natural persons and the regulation of the processing and movement of such data in the country.

Main laws	The DPA is the main law for data protection in Malawi. The DPA provides the principles relating to the processing of personal data, rights of data subjects, processing of personal data relating to criminal offences and convictions, complaints about data processing, data security and cross-border transfers of personal data. The Electronic Transactions and Cyber Security Act, 2016, (**ECTA**) provides specifically for the regulation of the processing of personal data, electronically. The ECTA provides for several rights of data subjects, including the need to obtain the consent of data subjects, and provide data security.
Key regulators	The DPA has designated the Malawi Communications Regulatory Authority (**MACRA**), which is established under the Communications Act, 2016, as the data protection authority in Malawi.
Are there specific requirements applicable to the collection and processing of data?	Yes, data is required to be collected and processed lawfully, fairly and in a transparent manner. Data is to be collected for a specific and legitimate purpose. No data is to be stored for longer than its required period. Data integrity and confidentiality is to be observed at all times. Data subjects are to be informed of the details of the data controller and the legal basis for processing the personal data of the data subject.
Is there a requirement for data localisation?	There are no data localisation requirements. However, a data controller must inform a data subject if personal data is to be transferred to a place outside of Malawi.

MALAWI

Are there limitations on cross-border transfers of data?	The DPA applies to cross-border transfers of data. But the DPA does not impose limitations on cross-border transfers of personal data. Although the DPA does not impose any limitations, it empowers MACRA to assess and decide whether cross-border transfers provide adequate levels of protection of personal data.
Are there registration requirements?	Yes. Only 'data controllers of significant importance' must be registered by MACRA and operate within the requirements of their registration. The DPA defines a 'data controller of significant importance' as a data controller: • who is ordinarily resident or operates in Malawi and processes or intends to process personal data of at least 10 000 data subjects resident in Malawi; or • who processes or intends to process personal data of significance to the Malawian economy, society or security.
Is a Data Protection Officer required?	The DPA requires a data protection officer to act as the contact point between MACRA, as the authority, and various data controllers and data processors within a data processing entity on compliance matters under the DPA.
Is a risk assessment/ privacy impact assessment required?	A risk assessment is required under the DPA. Data controllers and data processors must conduct a periodic risk assessment/ privacy assessment of the data processing system and service including if data processing involves the transmission of personal data over electronic communication networks, and conduct regular testing, assessment and evaluation of the effectiveness of the measures.
Must data breaches be reported?	Yes, in terms of the DPA, a data controller must, in the case of a personal data breach, notify MACRA within 72 hours of becoming aware of the breach.

MALAWI

Key enforcement/ sanction provisions	The DPA empowers MACRA to impose sanctions if a data controller or data processor contravenes the provisions of the DPA. In terms of the ECTA, no person is permitted to gain unauthorised access to, or intercept, or interfere with, data, and to do so is an offence that is subject to sanction. Violation of any provision of the ECTA, including the data protection provisions, is an offence.
Is cybercrime regulated in terms of any laws, regulations or directives?	Cybercrime is currently regulated under the DPA and the ECTA. However, Malawi has a Cybersecurity Bill, 2024 that, if enacted, will regulate cybercrime in Malawi.
If regulated, are there any cybercrime reporting requirements?	In Malawi, cybercrime reporting is part of the general reporting requirements under the DPA and the ECTA.

ELTON JANGALE
Partner
PFI Partnerships
Blantyre, Malawi

E: eltonjangale@pfi.mw

MAURITIUS

Mauritius has a strong, well-developed legal framework in place to protect personal data. The 2024 ITU Global Cybersecurity Index classified the country as being role-modelling and in Tier 1 (the highest tier of performance) in terms of cybersecurity-related actions and commitment to cybersecurity.

According to the Annual Report of the Data Protection Office, for the period ending in December 2023, 11 415 certificates of registration were issued, and 97 new complaints were received, most of which related to unauthorised use of CCTV cameras, unlawful processing of data, rights of access and telemarketing. The Data Protection Office closed 42 cases during this period, five through amicable resolution. In addition, 56 personal data breaches were reported to the Data Protection Office. An analysis of the type of breaches received showed that email misuse and unlawful disclosure remain the main causes of breaches reported.

Main laws	Data Protection Act, 2017 (**DPA**), read with the Data Protection (Fees) Regulations, 2020
Key regulators	The Data Protection Office (**DPO**), an independent and impartial public office responsible for data protection oversight. The DPO is headed by the Data Protection Commissioner (**Commissioner**), who is responsible for the enforcement of the DPA.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the DPA.
Is there a requirement for data localisation?	There are no data localisation requirements.
Are there limitations on cross-border transfers of data?	Yes, the DPA regulates the cross-border transfer of personal data outside Mauritius.
Are there registration requirements?	Yes, every person who intends to act as a data controller or processor must register with the Commissioner.

MAURITIUS

Is a Data Protection Officer required?	The DPA provides that every data controller must adopt policies and implement appropriate technical and organisational measures so as to ensure, and be able to demonstrate, that the processing of personal data is performed in accordance with the DPA. One of these measures is the requirement to designate a data protection officer (although this is not a compulsory requirement).
Is a risk assessment/ privacy impact assessment required?	In terms of the DPA, if the data processing operations are likely to result in a high risk to the rights and freedoms of the individual by virtue of its nature, scope, context and purposes, the data controller must, before conducting the processing, carry out an assessment of the impact of the intended processing operations.
Must data breaches be reported?	Yes, data breaches must be reported to the Commissioner, and in certain circumstances, to the data subject/s. A data processor must notify the data controller of any data breach.
Key enforcement/ sanction provisions	The Commissioner may serve an enforcement notice on a data controller or processor who contravenes the DPA. The Commissioner may also inspect and assess the security and organisational measures that a controller is required to have in place prior to processing or transferring personal data, and may carry out periodical audits of the systems of data controllers to ensure compliance with the provisions of the DPA.
Is cybercrime regulated in terms of any laws, regulations or directives?	Cybercrime is regulated by the Cybersecurity and Cybercrime Act, 2021. This legislation creates a framework for dealing with cybercrime by, among others, creating cybercrime offences and establishing bodies to advise on, investigate and act on reports relating to cybersecurity and cybercrime.

If regulated, are there any cybercrime reporting requirements?

The owner of critical information infrastructure must report to the National Cybersecurity Committee on any cybersecurity incident impacting national security, public safety or public interest and the action the owner intends to take to mitigate the cybersecurity incident.

'Critical information infrastructure' is defined as an asset, facility, system, network or process, whose incapacity, destruction or modification would have:

- a debilitating impact on the availability, integrity or delivery of essential services, including those services whose integrity, if compromised, could result in significant loss of life or casualties; or
- a significant impact on national security, national defence, or the functioning of the State.

Users may also voluntarily report cybercrimes on the Mauritian Cybercrime Online Reporting System (**MAUCORS+**), a national online system that also acts as a secure channel for reporting cybercrimes. Depending on the nature of the incident, it will be escalated to the relevant institution for investigation.

SHIANEE CALCUTTEEA
Partner
Bowmans
Moka, Mauritius

E: shianee.calcutteea@bowmanslaw.com

CHETAN ANCHARAZ
Associate
Bowmans
Moka, Mauritius

E: chetan.ancharaz@bowmanslaw.com

NAMIBIA

Namibia does not have a comprehensive data protection framework that aligns with its constitutional right to privacy (Article 13) at present, which leaves the processing of personal data largely unregulated. However, there is a draft Data Protection Bill (2023) in the early stages of the legislative process that must undergo further parliamentary review before becoming law.

While the Bill is not yet in force, lessons from neighbouring countries in Southern African and other jurisdictions with established privacy laws, highlight the need for the Government and organisations in Namibia to take proactive measures to prepare for the Bill's enactment. Once enacted, the Bill will bring significant changes to Namibia's privacy landscape and reshape how Government and organisations handle and store personal data.

Main laws	There is currently no dedicated legislation in Namibia regulating data protection. However, the Electronic Transactions Act, 2019 (**ETA**) provides a framework for electronic transactions, including the following: • Chapter 3 covers the legal recognition and effect of data messages and electronic transactions, including provisions on electronic signatures and retention of electronic records. • Chapter 4 focuses on consumer protection, which includes obligations related to data security in electronic commerce. • Chapter 6 addresses the liability of service providers for unlawful material, which has certain aspects of data protection.
Key regulators	While the Communications Regulatory Authority of Namibia (**CRAN**) plays a role, to an extent, in cybersecurity and electronic communications, it does not serve as Namibia's dedicated data protection authority. There is currently no dedicated regulator in Namibia. However, in terms of the draft Data Protection Bill, a Data Protection Supervisory Authority will be created and will oversee compliance with data protection laws and enforce regulations.

NAMIBIA

Are there specific requirements applicable to the collection and processing of data?	There are none at present, but the draft Data Protection Bill establishes obligations for data controllers and processors, requiring them to ensure transparency, lawfulness and fairness in data collection and processing.
Is there a requirement for data localisation?	There is no explicit requirement for data localisation in Namibia, and none is catered for in the draft Data Protection Bill.
Are there limitations on cross-border transfers of data?	There are none at present, but the draft Data Protection Bill includes provisions for transborder flows of personal data, requiring compliance with certain safeguards, such as ensuring adequate protection in the receiving country.
Are there registration requirements?	There are none at present, but the draft Data Protection Bill proposes a register of approved codes of conduct for data controllers and processors, ensuring compliance with data protection requirements.
Is a Data Protection Officer required?	The draft Data Protection Bill does not explicitly mandate a Data Protection Officer, but it does establish a Data Protection Supervisory Authority to oversee compliance as mentioned above.
Is a risk assessment/ privacy impact assessment required?	The draft Data Protection Bill includes provisions for security measures and accountability, which will imply risk assessments for high-risk data processing activities.
Must data breaches be reported?	While fraudulent and/ or suspicious transactions must be reported to Namibia's Financial Intelligence Centre, there is no statutory obligation to report other general data breaches. The draft Data Protection Bill, however, will require notification of personal data breaches to affected individuals and the supervisory authority.
Key enforcement/ sanction provisions	There are none at present, but the draft Data Protection Bill outlines penalties and enforcement mechanisms, including fines and corrective actions for non-compliance.

NAMIBIA

Is cybercrime regulated in terms of any laws, regulations or directives?	Namibia does not have dedicated cybercrime legislation, but sector-specific regulations may apply as mentioned above. The draft Cybercrime Bill includes provisions for investigation and enforcement which cover cyber-related offences.
If regulated, are there any cybercrime reporting requirements?	It is not regulated at present, but the draft Cybercrime Bill includes provisions for reporting cyber-related offences.

COBUS VISSER
Partner
Bowmans
Windhoek, Namibia

E: cobus.visser@bowmanslaw.com

NIGERIA

Data protection in Nigeria is a developing area of law. The principal data protection legislation is the Nigeria Data Protection Act, 2023 (**NDPA**), which was enacted in June 2023. It established the Nigeria Data Protection Commission (**NDPC**) as the country's data protection authority.

The NDPC issued the NDPA General Application and Implementation Directive 2025 (**GAID**) on 20 March 2025. The GAID has a six-month transition period and will become effective as of 19 September 2025. The GAID will replace the Nigerian Data Protection Regulation, 2019 (**NDPR**) and the Nigerian Data Protection Regulation 2019: Implementation Framework (**Implementation Framework**), which will continue to apply until the GAID becomes effective.

Currently, the data protection landscape is regulated by the NDPA, NDPR, Implementation Framework as well as other national and sector-specific laws containing data protection and privacy obligations.

Main laws	The NDPA, the GAID, the NDPR and the Implementation Framework
Key regulators	The NDPA established the NDPC as the data protection authority in Nigeria. The NDPC is responsible for the enforcement of the NDPA and other subsidiary regulations. Various sector-specific regulatory authorities are also responsible for data protection in each of their sectors.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the NDPA.
Is there a requirement for data localisation?	Yes, the mandatory Guidelines for Nigerian Content Development in Information and Communication Technology issued by the National Information Technology Development Agency have certain data localisation requirements, including, for example, that all data and information management companies host all sovereign data in Nigeria.

	In addition, there are certain data localisation provisions in some sector-specific laws. For example, the Central Bank of Nigeria (**CBN**) mandates that bank verification number (**BVN**) data must be stored in Nigeria and must not be routed outside the country without the approval of the CBN.
Are there limitations on cross-border transfers of data?	Yes, the NDPA governs the cross-border transfer of personal data outside Nigeria. Cross-border transfers of personal data are overseen by the NDPC and are only allowed where the data controller or data processor relies on the bases for transfer stipulated in the NDPA.
Are there registration requirements?	Yes, there are registration requirements under the NDPA. Entities deemed to be data controllers and processors of major importance (**DCPMI**) must register with the NDPC. The NDPC has issued a Guidance Notice (**Notice**), which defines the entities that are deemed to be DCPMIs. According to the Notice, a DCPMI is a data processor or controller that keeps or has access to a filing system (whether analogue or digital) for the processing of personal data, and: • processes the personal data of more than 200 data subjects in six months; or carries out commercial information communication technology (**ICT**) services on any digital device that has storage capacity and belongs to another individual; or • processes personal data as an organisation or a service provider in any of the following sectors: financial, communication, health, education, insurance, export and import, aviation, tourism, oil and gas, and electric power sectors. In addition, the Notice classifies DCPMIs into three levels or categories, namely: • Major data processing-ultra high level (**MDP-UHL**): These are entities that process the personal data of over 5 000 data subjects in a six-month period. In addition, entities such as commercial banks operating at national or regional level, telecommunication companies, insurance companies, multinational companies, electricity distribution companies, oil and gas companies, public social media app developers and proprietors, public email app developers and proprietors, communication device manufacturers, payment gateway providers, and fintechs are also deemed to be MDP-UHLs.

	• Major data processing-extra high level (**MDP-EHL**): These are entities that process the personal data of over 1 000 data subjects within six months. In addition, entities such as ministries, departments, and agencies of government (**MDAs**), microfinance banks, higher institutions (Universities, Polytechnics, Colleges of Education, etc), hospitals providing tertiary or secondary medical services, and mortgage banks are also designated MDP-EHL. • Major data processing-ordinary high level (**MDP-OHL**): These are entities that process the personal data of over 200 data subjects within a six-month period. In addition, entities such as primary and secondary schools, primary health centres, agents, contractors, and vendors who engage with data subjects on behalf of other organisations/ entities (**third-party data processors**) are deemed to be MDP-OHL.
Is a Data Protection Officer required?	Yes, the NDPA requires data controllers and data processors of major importance to designate data protection officers with expert knowledge of data protection laws and practices.
Is a risk assessment/ privacy impact assessment required?	Yes. Under the NDPA, where the processing of personal data may likely result in a high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes, a data controller must, prior to processing, carry out a data privacy impact assessment.
Must data breaches be reported?	Yes, the NDPA requires data controllers to notify the NDPC within 72 hours of becoming aware of a breach that is likely to result in a risk to the rights and freedoms of individuals. Certain institutions, such as banks, also have obligations to report data breaches under their sector-specific laws.
Key enforcement/ sanction provisions	Breaches of the NDPA may result in penalties that vary in amount, depending on whether the entity is a DCPMI. If it is a DCPMI, there is a fine of 2% of annual gross revenue for the preceding year or payment of the sum of NGN 10 million, whichever is greater. In the case of a data controller or data processor not of major importance, a fine of 2% of the annual gross revenue for the preceding year or payment of the sum of NGN 2 million, whichever is greater, may be imposed.

NIGERIA

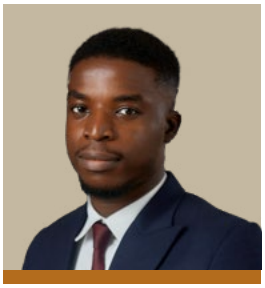
Is cybercrime regulated in terms of any laws, regulations or directives?	Yes, cybercrime is primarily regulated under the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 (as amended by the 2024 Amendment Act) (**Cybercrimes Act**).
If regulated, are there any cybercrime reporting requirements?	Yes, the Cybercrimes Act requires that any person or institution operating a computer system or network, whether public or private, inform the National Computer Emergency Response Team (**CERT**) Coordination Centre of any attacks, intrusions, or other disruptions that could hinder the functioning of computer systems or networks within seven days of the occurrence. Reports to the CERT Coordination Centre must be routed through the respective sectoral CERTs or sectoral Security Operations Centres.

JUMOKE LAMBO
Partner
Udo Udoma & Belo-Osagie
Lagos, Nigeria

E: jumoke.lambo@uubo.org

BABATUNDE OLAYINKA
Senior Associate
Udo Udoma & Belo-Osagie
Lagos, Nigeria

E: babatunde.olayinka@uubo.org



JOEL ADEYEMI ADEFIDIPE
Associate
Udo Udoma & Belo-Osagie
Lagos, Nigeria

E: joel.adefidipe@uubo.org

SOUTH AFRICA

South Africa's data protection legislation, the Protection of Personal Information Act, has been fully enforceable for approximately four years (since 1 July 2021), and this is still a developing area of law.

The Information Regulator has been proactive in educating members of the public on their rights when it comes to data protection and access to information, and enforcement action has picked up steadily in recent years.

The Information Regulator has conducted several assessments into the manner in which responsible parties are processing personal information, both in response to complaints received and on its own initiative. This has resulted in several enforcement notices being issued to organisations, and administrative fines being imposed on organisations that have not complied with these notices. The highest administrative fine imposed to date has been ZAR 5 million.

Main laws	Protection of Personal Information Act, 2013 (**POPIA**), read with the regulations and guidelines published under POPIA from time to time, including the Regulations Relating to the Protection of Personal Information, 2018 (as amended in 2025) (**Regulations**)
Key regulators	The Information Regulator, an independent and impartial authority responsible for data protection oversight and the enforcement of POPIA
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under POPIA.
Is there a requirement for data localisation?	Not at present. According to the National Policy on Data and Cloud (**Policy**), government data that incorporates content about the protection and preservation of national security and sovereignty of the Republic must only be stored in digital infrastructure located within the borders of South Africa. The Policy has not yet, however, been approved by Cabinet and still needs to be implemented.

SOUTH AFRICA

Are there limitations on cross-border transfers of data?	Yes, POPIA regulates the cross-border transfer of personal data from South Africa to a third party in a foreign country.
Are there registration requirements?	Responsible parties (known as 'data controllers' in some other jurisdictions) are not required to be registered with the Information Regulator. However, responsible parties must register an information officer (and, if applicable, any deputy information officers) with the Information Regulator prior to such officers taking up their duties under POPIA.
Is a Data Protection Officer required?	Yes, a data protection officer (referred to in POPIA as an 'information officer') is a requirement for both public and private bodies. Information officers may delegate their responsibilities to one or more deputy information officers.
Is a risk assessment/ privacy impact assessment required?	Yes, the Regulations require an information officer to carry out a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for lawful processing of personal information. In addition, the information officer is required to prepare and implement a compliance framework, which must be continually updated.
Must data breaches be reported?	Yes, data breaches must be reported to the Information Regulator and the impacted data subject/s (if known). Operators (referred to as 'data processors' in some other jurisdictions) must notify the responsible party in the event of a data breach.
Key enforcement/ sanction provisions	Following an investigation or assessment (on its own initiative or upon request), the Information Regulator may issue an assessment or enforcement notice requiring a responsible party to: • take specific steps; or • refrain from taking such steps; or • stop processing personal information in the manner set out in the notice. Failure to comply with an assessment or enforcement notice is an offence. Other offences include making false statements or unlawful acts relating to the processing of data subjects' account numbers. Committing an offence may result in a fine, or imprisonment of between 12 months and 10 years, or both, or an administrative fine of up to ZAR 10 million.

SOUTH AFRICA

Is cybercrime regulated in terms of any laws, regulations or directives?	Cybercrime is regulated by the Cybercrimes Act, 2020. This legislation creates a framework for detecting and combating cybercrimes by creating cybercrime offences and expanding the jurisdiction and powers of law enforcement agencies to investigate and prosecute cybercrimes.
If so, are there any cybercrime reporting requirements?	Under the Cybercrimes Act, electronic communications service providers and financial institutions (as defined) have a legal obligation to report cybercrimes to the South African Police Service within 72 hours of becoming aware of them. There is, however, no general obligation on organisations against which cybercrimes have been committed to report those offences.

NADINE MATHER
Partner
Bowmans
Johannesburg, South Africa

E: nadine.mather@bowmanslaw.com

TALITA LAUBSCHER
Partner
Bowmans
Johannesburg, South Africa

E: talita.laubscher@bowmanslaw.com

TANZANIA

The Personal Data Protection Act, 2022 (**PDPA**), has been in force since 1 May 2023 and is actively enforced by the Personal Data Protection Commission (**Commission**), the regulatory authority under the legislation.

With data protection still at a developing stage, the Commission has been hosting nationwide training initiatives and has published guidelines and forms to assist users and regulated individuals with their compliance obligations under the PDPA.

There have already also been a number of cases in courts of law involving the interpretation of the PDPA, notably *Tito Magoti v Honourable Attorney General* which sought to challenge the constitutionality of a number of the provisions under the PDPA; *Alexander J. Barunguza v Personal Data Protection Commission and two others* in which the Commission was sued for failure to exercise jurisdiction over a personal data complaint; and *Fatna Faradji Kayunga v MIC Tanzania (PLC) Ltd* involving a personal data breach.

Main laws	The PDPA
Key regulators	The Commission and various sector-specific regulatory authorities are also responsible for data protection in each of their sectors.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the PDPA.
Is there a requirement for data localisation?	There are no data localisation requirements.
Are there limitations on cross-border transfers of data?	Yes, the PDPA regulates the cross-border transfer of personal data outside Tanzania.

TANZANIA

Are there registration requirements?	Yes, personal data collectors and processors are required to be registered by the Commission.
Is a Data Protection Officer required?	Yes, a personal data collector or processor is required to appoint a personal data security officer who will ensure that security measures are taken to protect personal information that is collected or processed.
Is a risk assessment/ privacy impact assessment required?	Yes, a data controller or a data processor is required to conduct an impact assessment where it is determined that the processing of personal data is likely to affect the rights and freedoms of the data subject.
Must data breaches be reported?	Yes, personal data collectors or processors must inform the Commission in the event of a security breach that affects the safety of personal data.
Key enforcement/ sanction provisions	Disclosing personal data contrary to law is an offence which, upon conviction, is punishable by a fine of between TZS 100 000 and TZS 20 million, or imprisonment for a term not exceeding 10 years, or both. For an offence committed by a body corporate, a fine between TZS 1 million and TZS 5 billion may be imposed. The offences of destruction, erasure, concealment, or modification of personal data contrary to law, are punishable by a fine of between TZS 100 000 and TZS 10 million, or to imprisonment for a term not exceeding five years, or both. Where an offence has been committed by a body corporate, any officer who knowingly authorises the commission of such offences will be held liable. For any breach of the conditions of the PDPA for which no punishment has been prescribed, the offence shall be punishable by fine between TZS 100 000 and TZS 5 million; or to imprisonment not exceeding five years, or both.

TANZANIA

Is cybercrime regulated in terms of any laws, regulations or directives?	Cybercrimes are dealt with under the Cybercrimes Act, 2015, which has created a number of offences that may be prosecuted under the legislation. The Act regulates investigations and prosecution of offences involving cybercrime, among other things.
If regulated, are there any cybercrime reporting requirements?	There are no express cybercrime reporting requirements under the Cybercrimes Act.

WILBERT KAPINGA
Senior Partner
Bowmans
Dar es Salaam, Tanzania

E: wilbert.kapinga@bowmanslaw.com

FRANCIS KAMUZORA
Consultant
Bowmans
Dar es Salaam, Tanzania

E: francis.kamuzora@bowmanslaw.com

UGANDA

The right to privacy is a fundamental human right guaranteed under Article 27 of the Constitution of Uganda.

The primary law governing data protection is the Data Protection and Privacy Act, Cap 97 (**DPPA**) and the Data Protection and Privacy Regulations, S.I. No. 21 of 2021 (**Regulations**) made thereunder.

The Personal Data Protection Office (**PDPO**) is the statutory body responsible for personal data protection. In recent years, there has been a notable increase in enforcement activity, including Investigation Reports and recommendations by the PDPO, public sensitisation campaigns and registration drives for data controllers and processors.

While challenges remain in ensuring full compliance across sectors, Uganda is steadily moving from policy to practice, signalling growing institutional commitment to data privacy.

Main laws	The 1995 Constitution of Uganda under Article 27 guarantees the right to privacy, forming the constitutional foundation for data protection. The DPPA, read with the Regulations, are the primary laws governing personal data.
Key regulators	The PDPO in the National Information Technology Authority – Uganda (**NITA-U**) is the regulator responsible for personal data protection and privacy.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the DPPA. There should be a lawful basis for the processing of the personal data. The primary basis is consent. Mandatory consent of the data subject is required before the collection and processing of personal data unless it is exempted by the DPPA. Consent is defined by the DPPA to mean any freely given, specific, informed and unambiguous indication of the data subject's wish (ie, that they, by a statement or by a clear affirmative action, signify agreement to the collection or processing of personal data relating to them). Consent should therefore be obtained in a manner that fulfils the requirements in this definition.

UGANDA

Is there a requirement for data localisation?	The DPPA and Regulations permit the storage of data outside of Uganda in certain limited circumstances.
Are there limitations on cross-border transfers of data?	Yes, the DPPA regulates the cross-border transfer of personal data outside Uganda. Section 19 of the NDPPA and Regulation 30 of the Regulations provide the criteria for the transfer of personal data outside Uganda. In particular, personal data and special personal data can be transferred outside Uganda where: • the country to which the personal data is to be transferred has adequate measures in place for the protection of the data equivalent to the protections in Uganda; or • the data subject has consented to the processing or storing of personal data outside Uganda. This consent must be obtained in a manner and form that takes into consideration the nature of the personal data sought to be processed or stored outside Uganda. Any personal data already transferred out of Uganda shall not be further transferred to or processed in a third country without the express consent of the data subject.
Are there registration requirements?	Yes. All data collectors, data controllers and data processors to whom the DPPA applies are required to register with the PDPO.
Is a Data Protection Officer required?	Entities or institutions are required to appoint a data protection officer, who is responsible for ensuring compliance with the DPPA, depending on the nature of the entity or institution's activities.
Is a risk assessment/ privacy impact assessment required?	Where the collection or processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the data collector, controller, or processor is required (before collection or processing) to carry out an assessment of the impact of such operations on the protection of personal data. The PDPO is yet to publish a list of the processing operations that will be subject to a data protection impact assessment.

UGANDA

Must data breaches be reported?	Yes, it is mandatory for data collectors, controllers or processors to notify the NITA-U of any data breach. The PDPO shall determine whether the data subject should be notified of the breach and/ or whether publicity of the data breach is required.
Key enforcement/ sanction provisions	The DPPA empowers the PDPO to enforce penalties for violations of the Act (eg, the unlawful obtaining or disclosure to another person of personal data held or processed by a data collector, controller or processor, and the unlawful destruction, deletion, alteration to or concealment of personal data). These include remedial orders and requiring compliance with data subject requests. Ugandan courts may award compensatory damages to persons harmed by data collector, controller or processor violations of the DPPA. Entities that breach the DPPA are subject to a fine of up to UGX 4.9 million. If an entity is a corporation, Ugandan courts may penalise the corporation's violations of the DPPA by ordering a fine of up to 2% of the corporation's annual gross turnover.
Is cybercrime regulated in terms of any laws, regulations or directives?	Yes. The Computer Misuse Act, Cap. 96 provides for the safety and security of electronic transactions and information systems. The Computer Misuse Act provides for offences such as cyber harassment and cyber stalking.
If regulated, are there any cybercrime reporting requirements?	Yes, cybercrime incidents in Uganda must be reported to the Uganda Police Force's Cyber Crimes Unit under the Computer Misuse Act. If the incident involves a breach of personal data, it must also be reported to the PDPO within 72 hours, as required by Section 31 of the DPPA.

BRIAN KALULE
Partner
AF Mpanga
Kampala, Uganda

E: brian.kalule@afmpanga.com

RACHEL ASABA
Senior Associate
AF Mpanga
Kampala, Uganda

E: rachel.asaba@afmpanga.com

JUDITH KAGERE
Associate
AF Mpanga
Kampala, Uganda

E: judith.kagere@afmpanga.com

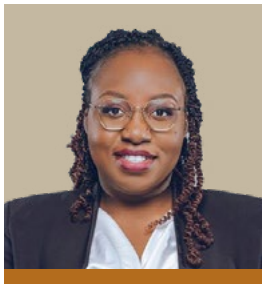
ZAMBIA

Zambia's principal data protection legislation, the Data Protection Act, 2021, is still a relatively new piece of legislation, having only come into effect on 1 April 2021. At present, the Office of the Data Protection Commissioner (**ODPC**) is operational and registration of data controllers and processors is ongoing.

Main laws	Data Protection Act, 2021 (**DPA**)
Key regulators	The ODPC, within the Ministry responsible for communications, is responsible for the regulation of data protection and privacy in Zambia.
Are there specific requirements applicable to the collection and processing of data?	Yes, requirements exist under the DPA.
Is there a requirement for data localisation?	Yes, the DPA requires a data controller to process and store personal data, including sensitive personal data, on a server or data centre located in Zambia (although the Minister may prescribe categories of personal data that may be stored outside of Zambia).
Are there limitations on cross-border transfers of data?	Yes, the DPA regulates the cross-border transfer of personal data outside Zambia.
Are there registration requirements?	Yes, the DPA requires any person who controls or processes (or intends to control or process) personal data to register as a data controller or data processor with the ODPC.
Is a Data Protection Officer required?	Yes, a data controller or processor is required to appoint a data protection officer.

ZAMBIA

Is a risk assessment/ privacy impact assessment required?	Where a type of processing uses new technologies (taking into account the nature, scope, context and purposes of the processing) and is likely to result in a high risk to the rights and freedoms of an individual, a data controller must (prior to the processing) carry out an assessment of the impact of the processing operations on the protection of personal data. The DPC must establish a list of the kinds of processing operations that will require data protection impact assessments.
Must data breaches be reported?	Yes, data controllers are required to notify the DPC and the impacted data subject/s of any data breach. Data processors are required to notify the data controller of any data breach affecting personal data processed on behalf of the data controller.
Key enforcement/ sanction provisions	There are a number of offences set out under the DPA for breach by a data controller or processor (for which the penalty is a fine not exceeding 2% of the annual turnover of the preceding financial year or ZMW 600 000, whichever is higher).
Is cybercrime regulated in terms of any laws, regulations or directives?	Yes, cybercrime is regulated under the Cyber Crimes Act, 2025 (**CCA**). The CCA provides for offences relating to computers, and computer systems, the protection of persons against cybercrimes and for child online protection.
If regulated, are there any cybercrime reporting requirements?	Yes, the cybercrime reporting requirements are outlined in the Cyber Security Act, 2025 (**CSA**). A controller (person who controls or is responsible for critical information or critical information infrastructure that is registered under the CSA) is required to immediately report to the Cybersecurity Agency a perceived or actual occurrence of any cybersecurity incidence.



BWALYA CHILUFYA- MUSONDA
Partner
Bowmans
Lusaka, Zambia

E: bwalya.musonda@bowmanslaw.com

JOSHUA MWAMULIMA
Partner
Bowmans
Lusaka, Zambia

E: joshua.mwamulima@bowmanslaw.com

PRECIOUS MWANSA-CHISHA
Associate
Bowmans
Lusaka, Zambia

E: precious.mwansa-chisha@bowmanslaw.com

BOWMANS
THE VALUE OF KNOWING

Cape Town, South Africa
T: +27 21 480 7800
E: info-cpt@bowmanslaw.com

Dar es Salaam, Tanzania
T: +255 76 898 8640
E: info-tz@bowmanslaw.com

Durban, South Africa
T: +27 31 109 1150
E: info-dbn@bowmanslaw.com

Johannesburg, South Africa
T: +27 11 669 9000
E: info-jhb@bowmanslaw.com

Lusaka, Zambia
T: +260 211 356 638
E: info-zb@bowmanslaw.com

Moka, Mauritius
T: +230 460 5959
E: info-ma@bowmanslaw.com

Nairobi, Kenya
T: +254 20 289 9000
E: info-ke@bowmanslaw.com

Swakopmund, Namibia
T: +264 64 406 320
E: info-na@bowmanslaw.com

Windhoek, Namibia
T: +264 61 382 800
E: info-na@bowmanslaw.com

Follow us on:
LinkedIn: bowmans-law
X: @bowmans_law

www.bowmanslaw.com

Alliance Firms:

Aman & Partners LLP, Addis Ababa, Ethiopia
T: +251 11 470 2868
E: info@aaclo.com

Udo Udoma & Belo-Osagie, Lagos, Nigeria
T: +234 1 277 4920-2, +234 1 271 9811-3
E: uubo@uubo.org