AFRICA GUIDE TO DATA PROTECTION
Contents

4 Foreword
6 Ethiopia
12 Ghana
20 Kenya
28 Malawi
34 Mauritius
42 Nigeria
50 South Africa
58 Tanzania
62 Uganda
68 Zambia
74 Our Firm
75 Our Presence in Africa
76 Our Data Protection Services
77 Key Contacts
Foreword

As technology and international trade have developed, so has the need to regulate the processing and cross-border flow of personal information.

The European Union has implemented the General Data Protection Regulation (GDPR), which has had a global impact on how international businesses conduct themselves in relation to individuals protected by the GDPR. In addition, several countries in Africa have recently passed or are considering drafting data protection legislation of their own.

The members of our data protection team regularly advise clients on data protection requirements across Africa. We also keep abreast of regulatory developments and have prepared this guide to support our clients in this important area of the law.

The guide provides a snapshot of the relevant regulations in 10 countries and has been prepared in collaboration with our alliance firms in Ethiopia and Nigeria and our relationship firms in Ghana and Malawi. The information is correct as at March 2022.

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.

Cathy Truter
Head of Knowledge

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

**1. Main Laws**

At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Ethiopia does not currently have a comprehensive data protection law, but data protection provisions are included in the 1995 Constitution of the Federal Democratic Republic of Ethiopia (Constitution), namely Article 26 (right to privacy), the Criminal Code of the Federal Democratic Republic of Ethiopia Proclamation No. 414/2004 (Criminal Code), the Civil Code of the Empire of Ethiopia Proclamation No. 165/1960 (Civil Code), the Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 (Mass Media Proclamation) and the recently promulgated Media Proclamation No. 1238/2021 [which repealed provisions in the Mass Media & Access to Information Proclamation as they related to mass media]. The Ministry of Innovation and Technology (MinT) has recently issued (in April 2020) a Draft Data Protection Proclamation which contains detailed provisions on data collection, use, protection and processing. The Draft Data Protection Proclamation must still be approved and may still be subject to change.

Electronic transactions, cybercrime and cybersecurity are regulated under the Computer Crime Proclamation No. 958/2016 (Computer Crime Proclamation) which sets out the offences and penalties for a person intentionally committing a “computer crime” (i.e. a crime committed against a computer, computer system, data or network; a conventional crime committed by means of a computer, computer data, system or network; or dissemination of illegal computer content data through a computer, computer system or network), and the Electronic Transaction Proclamation No.1205/2020 (which provides that a person who can access electronic messages or any other written documents, has the obligation to keep it confidential). The Ministry of Innovation and Technology (MinT) has recently issued (in April 2020) a Draft Data Protection Proclamation which contains detailed provisions on data collection, use, protection and processing. The Draft Data Protection Proclamation must still be approved and may still be subject to change.

Ethiopia is yet to sign or ratify the AU Convention on Cyber Security and Personal Data Protection or the Budapest Convention on Cyber Crime.

The National Bank of Ethiopia issued the Licensing and Authorisation of Payment Instrument Issuers Directive No. ONPS/01/2020. This directive is aimed at authorising and establishing the framework for Payment Instrument Issuers to operate in Ethiopia and also sets a requirement to notify the National Bank of Ethiopia in cases of data breaches. In addition, the National Bank of Ethiopia also introduced in 2020, the Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020 as well as the Financial Consumer Protection Directive No. FCP/01/2020, both of which incorporate clauses requiring data protection of customers/consumers. Moreover, the Ethiopian Communications Authority promulgated the Telecommunications Consumer Rights and Protection Directive No. 832/2021 in 2021 (TCRP Directive), intended to address consumer protection concerns including data protection aspects.

**2. Key Regulators**

Who are the key regulators, what are their areas of jurisdiction, and what are their contact details?

At present, there is no dedicated data protection regulator in Ethiopia, although some sector specific authorities regulate data protection issues within their regulatory scope. For example, the Ethiopian Communication Authority – a regulator of the telecommunication sector – is empowered to “promote information security, data privacy and protection” while the National Bank of Ethiopia – the banking sector regulator – has certain powers related to privacy and data protection in the financial sector.

However, the Draft Data Protection Proclamation provides for the establishment of a Data Protection Commission.

Ethiopia has established an Information Network Security Agency (INSA) which operates as the cybersecurity agency of Ethiopia, as well as the Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CERT), which operates to defend the national cyber space from accidental and deliberate cyber-attacks by conducting proactive and reactive activities throughout Ethiopia.
3. Recognition of Personal Data
Are there specific definitions for personal data and/ or sensitive personal data?
The Freedom of Mass Media and Access to Information Proclamation defines “personal information” which includes information about an identifiable individual, including, but not limited to: information relating to the medical, educational, academic, employment, professional or criminal history of the individual, information relating to financial transactions involving the individual, any identifying number, symbol or other particular assigned to the individual, as well as the address, fingerprints or blood type of the individual.

The Draft Data Protection Proclamation proposes a new definition for “personal data”: any information relating to an identified or identifiable natural person who can be identified from such data and includes any expression of opinion about the individual. The Draft Data Protection Proclamation also lists certain personal information as “sensitive personal data” including information on racial or ethnic origin, political opinion, religious belief, trade union membership, physical and mental health conditions, sexual life, genetic information, commission of a crime and legal proceedings against the subject.

The recently adopted TCRP Directive provides a definition for “Personal Data” as: any information relating to an identified or identifiable natural person leading to identify such person, directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, telephone number, traffic and billing data, and other personal information in the context of Telecommunications Services.

4. Critical Infrastructure and Databases
The Information Network Security Agency (INSA) is responsible for issuing directives, policies and standards to ensure the security of information & computer based key infrastructures. The Information Network Security Agency Re-establishment Proclamation defines “critical infrastructure” as “an infrastructure that can have considerable damage on public safety and the national interest, if attacked”.

5. Collection and Processing
Are there any specific requirements applicable to the collection and processing of data?
Various sector specific laws in Ethiopia set out that personal data must be collected and processed with due care and only for an intended purpose. As a general rule, the consent of the data subject is required in order to process personal data (unless some other legal basis is present). For example, in terms of the Financial Consumer Directive, a financial service provider should only use and disclose financial consumers’ and security providers’ data consistently with the original purpose of collection or with the explicit and informed consent of the financial consumer.

The TCRP Directive also provides that the collection, processing and maintenance of personal data on consumers shall comply with the laws of the Country and that the processing as well as maintaining Personal Data shall not be for purposes other than those originally identified and communicated to the Consumers.

The TCRP Directive also provides that the collection, processing and maintenance of personal data on consumers shall comply with the laws of the Country and that the processing as well as maintaining Personal Data shall not be for purposes other than those originally identified and communicated to the Consumers.

6. Requirement for Data Localisation
What are the data localisation requirements (if any)?
Various legislation (including legislation regulating the financial sector) provides that any data generated in Ethiopia must be stored in Ethiopia. Further, the Draft Data Protection Proclamation contemplates the Data Protection Commission ordering local processing or storage of “critical personal data” based on the strategic interests of the state. The TCRP Directive also provides that a Consumer’s Personal Data shall only be processed in a server or data centre located in Ethiopia.

7. Cross-Border Transfers
What are the requirements for the cross-border transfers of data (if any)?
While there is currently no specific legislation regulating the cross-border transfer of personal data, the Draft Personal Data Protection Proclamation provides for transfer of data out of the country; i.e. such transfer is only permitted when there is an appropriate level of data protection in the third-party jurisdiction. The Data Protection Commission will assess whether a third-party jurisdiction has an appropriate level of protection by looking at general considerations (such as all circumstances surrounding a specific set of data transfer operations) and particular considerations (such as the nature of the data, purpose and duration of the proposed transfer and the nature of the third-party jurisdiction).

While the TCRP Directive does not particularly relate to Cross-Border Transfers, the directive in general indicates that information on Consumers shall not be transferred to any third party unless there is a court order or the Consumer specifically agrees to the transfer, in writing, or by other verifiable means.

8. Registration and/or Notification
What is the registration and/or notification requirements for the collection and/or processing of data (if any)?
At present, there are no registration and/or notification requirements for data controllers or processors in Ethiopia. The Draft Personal Data Protection Proclamation, however, requires the prior registration of data controllers and data processors.

9. Data Protection Officers
Is a data protection officer required and, if so, what are the key responsibilities?
At present, there is no requirement for the appointment of a data protection officer in Ethiopia, although the Draft Personal Data Protection Proclamation proposes the appointment of a data protection officer.

10. Security Requirements
What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?
The Computer Crime Proclamation requires service providers to implement reasonable and necessary security measures to protect confidential computer traffic data disseminated through their computer systems or communications services from unlawful and unnecessary access.

Certain sectors also contain specific security requirements. For example, the Financial Consumer Protection Directive requires financial service providers to implement appropriate organisational, physical and technical measures to ensure that data is protected against misuse, unauthorised disclosure, accidental loss, destruction or damage.

With respect to telecommunications, the pertinent directive on consumer protection requires taking immediate action necessary to protect and secure the network and the consumer against any adverse impact resulting from a compromise of data.

The Draft Personal Data Protection Proclamation proposes the setting of technical and organisation security measures and the use of data protection impact assessments.

11. Data Breach
There are currently no data breach notification requirements in Ethiopia and no specific measures imposed in operators of critical infrastructure or databases. The Draft Data Protection Proclamation provides notification in cases of data breach to both the Data Protection Commission and the data subject. Notification to the Data Protection Commission would be required when the breach is likely to pose a risk to the rights and freedoms of an individual, while notification to the data subject is required if the breach is likely to pose a “high risk”. In terms of the Draft Personal Data Protection Proclamation, notification must be given without undue delay and only within 72 hours when feasible. When providing breach notifications, data controllers will be required to include information relating to the nature and scope of personal data breached, contact details of the data protection officer, possible consequences of the breach and measures taken or proposed to mitigate the adverse effects of the incident.

However, the Computer Crime Proclamation requires service providers with knowledge that a crime set out in the Proclamation (including breach of privacy following unauthorised access) has been committed by a third party through the computer system it administers to immediately
1. Introduction

2. Key Legislation

3. Data Protection

4. Consent

5. Access

6. Accuracy

7. Purpose Limitation

8. Storage

9. Security

10. Data Portability

11. International Transfers

12. Enforcement and Sanctions

13. Sectoral Issues

14. Trends and Activity

**Health sector**
The Food, Medicine and Healthcare Administration and Control Council of Ministers Regulation provides that a health professional must keep personal health information confidential and may not disclose patient information other than with the written consent of the patient or under certain other specific situations.

**Communications sector**
The Communications Service Proclamation No.1148/2019 permits the Ethiopian Communication Authority to promote information security, data privacy and protection within the telecoms sector. The recently published Draft Consumer Rights and Protection Directive also contains some data privacy protections. The TCRP Directive provides for rules regarding the need for telecom licensed entities to protect the data collected from their consumers and the manner of protecting consumers’ interests, including data.

**Financial sector**
The Financial Consumer Protection Directive No. FCP/01/2020 requires financial service providers to keep the financial consumers’ data confidential and secure. Financial service providers are required to establish and apply (and make available to consumers) policies and procedures to ensure the confidentiality and security of the financial consumers’ data and can only use and disclose consumers’ data for legitimate purposes agreed to by the financial consumer, security provider or as otherwise permitted by law.

**12. Enforcement and Sanctions**

What are the key enforcement and sanctions provisions?

Ethiopian courts are responsible for enforcing data protection provisions in the various sector specific laws. The Criminal Code criminalises the violation of privacy safeguards guaranteed under the Constitution; for example, the sanction for an infringement of the privacy of any correspondence is up to six months imprisonment or a fine.

Further, the Financial Consumer Protection Proclamation provides that financial institutions which contravene the provisions of the Financial Consumer Protection Directive will be subject to a penalty of ETB 10,000 for each violation. The Computer Crime Proclamation provides that anyone who, without authorisation, intentionally secures access to the whole or part of a computer system, computer data, or network will be punishable with imprisonment not exceeding three years and/or a fine.

**13. Sectoral Issues**

Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

**Mass Media Proclamation**
This Proclamation, which protects privacy and personal data through limitations on the right to seek and access any information held by public bodies, applies to all media operating in Ethiopia.

notify INSA, report the crime to the police and take “appropriate” measures.

Further, the Licensing and Authorisation of Payment Instrument Issuers Directive requires payment instrument issuers to report any cybersecurity breach or data loss to the National Bank of Ethiopia.

In addition, the TCRP Directive provides that if and when a Telecom Licensee’s data is compromised, the Licensee is required to notify the Consumer and the Ethiopian Communications Authority, not later than 72 hours after becoming aware of it.

**14. Trends and Activity**

What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system and, at present, enforcement action is not actively pursued.

In recent news, it has been reported that the final version of the Draft Data Protection Proclamation has been submitted to the Attorney-General’s office.
Ghana

1. Main Laws
At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Data protection is regulated in Ghana under the Data Protection Act, 2012 (DPA) together with the 1992 Constitution (Article 18(2) which provides citizens with a fundamental right to privacy). The DPA applies (1) to a data controller established in Ghana and processing personal data in Ghana, (2) to a data controller not established in Ghana but using equipment or a data processor in Ghana to process data, and (3) to processing of information which originates partly or wholly from Ghana. Various sector-specific legislation also contains data protection provisions.

Electronic transactions, cybercrime and cybersecurity are all dealt with under the Electronic Transactions Act, 2008 (ETA) and, more recently, the Cybersecurity Act, 2020. The ETA sets out various cyber offences, including unauthorised access or interception, interference with electronic records, access to stored communications, access to computer programmes or electronic records and disclosure of access codes. Other cyber offences include access to protected computers, denial of service, and causing a computer to cease to function. The Cybersecurity Act establishes the Cyber Security Authority, protects the critical information infrastructure of Ghana, and regulates cybersecurity activities. Ghana also adopted a National Cyber Security Policy and Strategy in 2015.

Ghana has signed (July 2017) and ratified (May 2019) the AU Convention on Cyber Security and Personal Data Protection and has also ratified the Budapest Convention on Cyber Crime.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

The Data Protection Commission (DPC), an independent statutory body established under the DPA to enforce compliance with that Act.

The Cyber Security Authority, established under the Cybersecurity Act, protects the critical information infrastructure of Ghana, regulates cybersecurity activities and develops Ghana’s cybersecurity ecosystem. It is also targeted at positioning Ghana to prevent, manage and respond to cybersecurity incidents.

The National Cyber Security Centre has been established under the Ministry of Communications to liaise with relevant state agencies and the private sector to oversee cyber security operations in Ghana. The Ministry of Communications has also launched a cybercrime/security incident reporting system to provide various channels to report incidents.

Ghana has further established a Computer Emergency Response Team (CERT-GH) at the National Communications Authority (NCA), to provide information and assistance in implementing proactive measures to reduce the risks of computer security incidents, as well as Security Operations Centres at the Bank of Ghana and the National Information Technology Agency (NITA).

3. Recognition of Personal Data
Are there specific definitions for personal data and/or sensitive personal data?

Personal data, as defined in the DPA, means data about an individual who can be identified from the data or other information in the possession of, or likely to come into the possession of, the controller.

The DPA also provides for sensitive (personal) personal data which includes, amongst other things, data relating to race, colour, ethnic or tribal origin, political opinion, religious beliefs, physical medical, mental health or mental condition or DNA, sexual orientation, a commission or alleged commission of an offence, or proceedings of an offence committed or alleged to have been committed, the disposal of such proceeding or the sentence of any court in the proceedings.

KIMATHI & PARTNERS

Kimathi Kuenyehia
E: kimathi@kimathilegal.com

Akua Serwa Asomani-Adem
E: akua@kimathilegal.com

Enid Baaba Dadzie
E: enid@kimathilegal.com
4. Critical Information Infrastructure and Databases
Under the Cybersecurity Act, the Minister of Communications may, on the advice of the Cyber Security Authority, designate a computer system or network as a critical information infrastructure if it is necessary for national security or the economic and social well-being of citizens. In making this designation, the Minister is required to consider if the computer system or computer network is necessary for, amongst other things, the security, defence or international relations of the country, the protection of public safety and public health, including systems related to essential emergency services, the provision of service directly related to, amongst other things, communications and telecommunications infrastructure and banking and financial services.

The Cyber Security Authority will register a critical information infrastructure and determine the requirements and procedure for registration and any other matter relating to the registration of a critical information infrastructure. Where there is any change in the legal ownership of a registered critical information infrastructure, its owner must inform the Cyber Security Authority of the change in ownership within seven days. Failure to inform the Cyber Security Authority of the change in ownership within seven days incurs an administrative penalty between 500 penalty units and 10,000 penalty units (a penalty unit is currently GHS 12). The Minister may on the advice of the Cyber Security Authority, withdraw the designation of a critical information infrastructure at any time if the Minister considers that the computer system or computer network no longer satisfies the criteria of a critical information infrastructure.

The Minister will also set minimum standards for prohibitions in respect of the general management of a critical information infrastructure that the Minister considers necessary for the protection of national security (although these have not yet been set) and the Cyber Security Authority will carry out periodic audits and inspection on a critical information infrastructure to ensure compliance with the provisions under the law.

5. Collection and Processing
Are there any specific requirements applicable to the collection and processing of data?

Under the DPA, personal data may only be processed if the purpose for which it is to be processed is necessary, relevant and not excessive. A person who processes data must take into account the privacy of the individual by applying principles including accountability, lawfulness of processing, specification of purpose, compatibility of further processing with the purpose of collection, quality of information, openness, data security safeguards, and data subject participation. A person who processes personal data must ensure that the personal data is processed without infringing the privacy rights of the data subject, in a lawful and reasonable manner.

The DPA provides that personal data must not be processed without the consent of the data subject, unless the purpose for which the personal data is processed is necessary for the purpose of a contract to which the data subject is a party, authorised or required by law, to protect a legitimate interest of a data subject; necessary for the proper performance of a statutory duty; or where it is necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied. If a data subject objects to the processing of personal data, the person who processes the personal data shall stop the processing of the personal data.

The processing of special (sensitive) personal data is prohibited except within the limited scope prescribed in the DPA, such as with the consent of the data subject or where such processing is necessary (e.g. for the exercise or performance of a right or obligation conferred or imposed by law or an employer). A person must not process special (sensitive) personal data unless the processing is necessary for the protection of the vital interests of the data subject where it is impossible for consent to be given by or on behalf of the data subject: the data controller cannot reasonably be expected to obtain the consent of the data subject: or consent by or on behalf of the data subject has been unreasonably withheld.

The DPA provides for a determination of assessable processing by the Minister of Communications who must specify actions which constitute assessable processing. This must be in relation to matters in terms of which processing is likely to cause substantial damage or substantial distress to a data subject or otherwise significantly prejudice the privacy rights of a data subject.

6. Requirement for Data Localisation
What are the data localisation requirements (if any)?

There are currently no data localisation and cross-border transfers of personal data is permitted (see below), as long as the recipients of such data are able to meet the same data protection standards as are required in Ghana.

7. Cross-Border Transfers
What are the requirements for the cross-border transfers of data (if any)?

There are currently no cross-border data transfer restrictions that are applicable, although the sale, purchase, knowing or recklessly disclosure of personal data is prohibited. Further, the DPA applies to processing of information which originates partly or wholly from Ghana (i.e. and cross-border transfers of personal data is permitted provided the recipients of such data are able to meet the same data protection standards as are required in Ghana) and, under the DPA, a data controller or processor is also required to ensure that the personal data of foreign data subjects is processed in compliance with data protection legislation of the foreign jurisdiction of that data subject where personal data originating from that country is sent to Ghana for processing.

8. Registration and/or Notification
What are the registration and/or notification requirements for the collection and/or processing of data (if any)?

In terms of the DPA, a data controller who intends to process personal data is required to register with the DPC, with payment of the registration fee, and will be issued with a certificate of registration which is valid for 2 years and must then be renewed.

The application for registration as a data controller must contain, amongst other things, a description of the personal data to be processed and the category of persons whose personal data will be collected, an indication as to whether the applicant holds or is likely to hold special personal data, a description of the purpose for which the personal data is being processed, a description of the recipient of the personal data, the name of the country to which the applicant may transfer the data, and a general description of measures to be taken to secure the data.

The DPC maintains an online public search register of registered data controllers, which shows the status of the entity with the DPC and the expiry date of its current registration. Though not mandatory, data processors are also encouraged to register with the DPC.

In October 2020, the DPC announced its implementation of an enhanced registration and compliance software to improve the registration and renewal process for data controllers.

9. Data Protection Officers
Is a data protection officer required and, if so, what are the key responsibilities?

Under the DPA, data controllers may appoint data protection supervisors (or officers), but this is not a mandatory requirement. A data protection supervisor is responsible for monitoring the data controller’s compliance with the DPA and may be an employee of the data controller.

While the DPC is empowered to set the qualifications for the appointment of a data protection supervisor, no such minimum qualifications have been set as yet. However, the DPC has indicated that a data controller must appoint a data protection supervisor who has been trained and certified under a DPC-approved training programme. Nevertheless, 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.
10. Security Requirements

What are the requirements relating to the security of data? (if any)? Is there a risk assessment or privacy impact assessment required?

The DPA requires that a data controller takes the necessary steps to secure the integrity of personal data in its possession or under its control through the adoption of appropriate technical and organisational measures to prevent loss of, damage to, or unauthorised destruction, and unlawful access to or unauthorised processing of personal data.

To give effect to this, the DPA requires a data controller to take reasonable measures to (1) identify reasonably foreseeable internal and external risks to personal data under that person’s possession or control; (2) establish and maintain appropriate safeguards against the identified risks; (3) regularly verify that the safeguards are effectively implemented; and (4) ensure that the safeguards are continually updated in response to new risks or deficiencies. A data controller is required to observe generally accepted information security practices and procedure and specific industry or professional rules and regulations.

In terms of the DPA, a person who processes data must take into account the privacy of the individual by applying the data security safeguards. A data controller also has an obligation to ensure that a data processor who processes personal data for the data controller establishes and maintains certain safeguards with the security measures provided for under the DPA; this must be governed by a written contract which must establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data. A person who processes personal data on behalf of a data controller must also only process the data with the prior knowledge or authorisation of the data controller and treat the personal data which comes to the knowledge of the data processor as confidential.

The DPA does not make provision for data protection impact assessments. However, the DPC 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.

The Cybersecurity Act provides that the Cyber Security Authority must develop, establish and adopt standards for cybersecurity (1) education and skills development, (2) hardware and software engineering, (3) governance and risk management, (4) research and development, and (5) practitioners. The Cyber Security Authority must publish standards developed on the website, and must take the necessary measures to ensure that the cybersecurity standards adopted and monitor compliance by the public and private sectors with the cybersecurity standards. A breach of these standards will result in the payment of an administrative penalty.

Under the DPA, a person who fails to secure access or attempt to secure access without authorisation commits an offence and is liable on summary conviction to a fine between 2,500 penalty units and 15,000 penalty units or to a term of imprisonment between two years and five years, or to both.

11. Data Breach

What are the data breach notification requirements? (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

In terms of the DPA, where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a third party who processes data under the authority of the data controller must notify the DPC and the data subject of the unauthorised access or acquisition as soon as reasonably practicable after the discovery.

The notification must provide sufficient information to allow the data subject to take protective measures against the consequences of unauthorised access or acquisition of the data. This should include, if known to the data controller, the identity of the unauthorised person who may have accessed or acquired the personal data. The data controller must take steps to ensure the restoration of the integrity of the information system.

The data controller must delay the notification to the data subject where the security agencies or the DPC inform the data controller that the notification will hinder a criminal investigation. Where the DPC has grounds to believe that publicity would protect a data subject who is affected by the unauthorised access or acquisition of data, the DPC may direct the data controller to publicise the compromise to the integrity or confidentiality of the personal data.

Under the ETA, the NITA is required to use reasonable efforts to notify anyone who is likely to be affected by the occurrence of an adverse event, or to deal with the event or situation in accordance with the procedure specified in its certification practice statement, where in the opinion of the NITA, an event has occurred or a situation has arisen which may materially and adversely affect the integrity of its computer systems or the conditions subject to which a licence was granted.

Under the Cybersecurity Act, an owner of a critical infrastructure is required to report a cybersecurity incident within 24 hours after the incident is detected to the relevant sectoral computer emergency response team, or CERT-GH, conduct an audit on the critical information infrastructure, and submit a copy of the audit report to the Cyber Security Authority. The Cyber Security Authority is required, upon receipt of information in respect of a cyber security incident, to circulate the information to a Sectoral Computer Emergency Response Team, a licensee or any other relevant institution. The Cyber Security Authority is also required to establish a cyber security incident reporting and information sharing platform to enable a Sectoral Computer Emergency Response Team, a licensee and any other relevant institution to report a cyber security incident.

Further, sectoral computer emergency response teams will be required to report cybersecurity incidents to the Cyber Security Authority that may materially and adversely affect the integrity or security of critical information infrastructure, and submit a copy of the audit report to the Cyber Security Authority. The Cyber Security Authority is required to establish a cybersecurity incident point of contact to facilitate this reporting, although this is yet to be done. A breach of these reporting obligations will result in the payment of an administrative penalty of between two hundred and fifty penalty units and ten thousand penalty units (a penalty unit is currently GHS 12).

A person who knowingly or recklessly discloses personal data is liable to a fine of not more than 250 penalty units or to a term of imprisonment of not more than 2 years or to both.

A person who sells or offers for sale personal data is liable to a fine of not more than 250 penalty units or to a term of imprisonment of not more than five years or both. Further, a person who processes personal data but fails to register as a data controller commits an offence and is liable on summary conviction to a fine of not more than two hundred and fifty penalty units or a term of imprisonment of not more than two years or to both.
A person who provides false information to the DPC in support of an application for registration as a data controller commits an offence and is liable on summary conviction to a fine of not more than one hundred and fifty penalty units or a term of imprisonment of not more than one year or to both.

A person who commits an offence under the DPA, in respect of which a penalty is not provided, is liable on summary conviction to a fine of not more than 5000 penalty units or a term of imprisonment of not more than ten years or to both.

Various offences and penalties relating to cybercrimes are set out in the ETA. For example, a person who knowingly and without authority causes a computer to perform any function to secure access to a programme or electronic record held in that computer commits an offence and is liable to a fine of not more than 2500 penalty units or to a terms of imprisonment of not more than 5 years.

Further, any person who intentionally accesses or intercepts an electronic record without authority commits an offence and is liable to a fine of not more than 2500 penalty units or to a term of imprisonment of not more than 5 years. The penalties for other cyber offences, such as those relating to stealing, forgery and appropriation, are set out in the Criminal Offences Act, 1960.

Any contravention of the Cybersecurity Act is subject to a general penalty of a fine of between 250 and 20000 penalty units or to a term of imprisonment of not more than 2 years.

13. Sectoral Issues
Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Communications sector
In terms of the Electronic Communications Act, 2008, a network operator or a service provider who is a holder of a class licence may not use or permit another person to use or disclose confidential, personal or proprietary information of a user, another network operator or service provider without lawful authority unless the use or disclosure is necessary for the operation of the network or service, the billing and collection of charges, the protection of the rights or property of the operator or provider, or the protection of the users or other network operators or service providers from the fraudulent use of the network or service. A person who intentionally uses or discloses personal information in contravention of the Act commits an offence and is liable to a fine of not more than 1500 penalty units or to a term of imprisonment of not more than 5 years or both.

Under the Electronic Communications Regulations, the operator is required to comply with international best practices in the industry to promote privacy, secrecy and security of communications carried or transmitted by the operator or through the communications system of the operator, and the personal and accounts data related to subscribers.

Health sector
In terms of the 7th Schedule to the Public Health Act, 2012: “health information collected or received by a State Party pursuant to these Regulations from another State Party or from WHO which refers to an identified or identifiable person shall be kept confidential and processed anonymously as required by national law.”

Credit reporting
The Credit Reporting Act, 2007 requires the recipient of a credit report to keep such report confidential while ensuring that the information contained in it is used solely for its specified purpose. A credit bureau, data provider or credit information recipient is required to observe the principles of: (a) equality of credit information subjects; (b) confidentiality of information; (c) non-interference in the private life of citizens; (d) respect for the rights, liberties and lawful interests of persons and legal entities; (e) accuracy and transparency of information; and (f) ‘privacy and secrecy of communication.

Financial sector
Various sector-specific legislation within the financial sector, affecting both banks and non-banks, require financial sector entities to ensure confidentiality of customers’ personal information and to ensure the security and integrity of their systems. On 24 October 2018, the Bank of Ghana issued the Cyber & Information Security Directive, which applies to regulated financial institutions licensed or registered or regulated by the Bank of Ghana. The Directive outlines the procedures for risk management and cyber defence security, the appointment of a cyber and information security officer as well as the privacy protection and cyber and information security training for employees. Further, a publication for statistical purposes or any information relating to money or banking that the Bank of Ghana may request from an institution or an individual must not include personal data.

14. Trends and Activity
What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

Data protection, cybercrime and cybersecurity are key focuses in Ghana, which has a fairly developed system including ratification of international instruments.

Because data protection is a new area in Ghana, the regulator is still identifying and sanctioning data controllers for non-compliance. The DPC has, on a previous occasion, published the names of persons who were not compliant with the DPA.

Further, the DPC has become more aggressive with enforcement of the DPA recently.

The Cyber Security Authority has not yet been established; however, the National Cyber Security Centre is currently active and is a coordination center for cybersecurity response in government and the private sector.
KENYA

1. Main Laws

At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Kenya regulates data protection under the Data Protection Act 2019 (DPA), which came into effect on 25 November 2019 and which gave effect to Article 31(c) and (d) of the Constitution of Kenya, 2010 (which deal with the right to privacy). The Data Protection (General) Regulations, Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 and Data Protection (Compliance and Enforcement) Regulations, 2021 (collectively the DP Regulations) also came into effect in early 2022.

The DPA applies to all processing of personal data by any data controller or processor established or resident in Kenya and who processes personal data while in Kenya, or who is not established or residing in Kenya but processes the personal data of data subjects located in Kenya.

Kenya regulates cybercrime under the Computer Misuse and Cybercrime Act, 2018. This Act sets out various offences relating to computer misuse and cybercrime, including unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of computer service, unauthorised modification of computer material, damaging or denying access to computer systems, unauthorised disclosure of passwords, unlawful possession of devices and data, and electronic fraud. It provides for investigations and procedures related to computer misuse and cybercrime.

Electronic transactions and cybersecurity are regulated in Kenya under the Kenya Information and Communication Act, Rev. 2009 (KICA). KICA includes cyber security related provisions that prohibit various actions that would threaten cyber security and prescribes a range of criminal penalties. Kenya developed a National Cybersecurity Strategy, 2014 which sets out guiding factors for the establishment of cybersecurity legislation and guidelines.

Kenya is yet to sign or ratify the AU Convention on Cyber Security and Personal Data Protection or the Budapest Convention on Cyber Crime.

2. Key Regulators

Who are the key regulators, what are their areas of jurisdiction?

The Office of the Data Protection Commissioner (ODPC) was established under the DPA.

The ODPC is responsible for overseeing the implementation and enforcement of the provisions of the DPA, the maintenance of the register of data controllers and processors, receiving and investigating complaints, and carrying out inspections of public and private entities to evaluate the processing of personal data.

The provisions of the various sectoral laws are enforced by the respective sectoral regulatory bodies that are now increasingly requiring compliance with the DPA.

The Computer Misuse and Cybercrimes Act establishes the National Computer and Cybercrimes Coordination Committee which was launched in November 2021. The Committee will be responsible for coordinating national security organs in relation to computer and cybercrimes, receiving and acting on reports relating to computer and cybercrimes, coordination collection and analysis of cyber threats and responses to cyber incidents that threaten Kenyan cyberspace, and establishing codes of cybersecurity practice and standards for performance of implementation by owners of critical national information infrastructure.

KICA creates the Communications Authority which is the regulatory authority in the ICT sector. Under KICA, the Communications Authority has the mandate to develop a national cybersecurity management framework. In this regard, the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), based at the Communications Authority, is a multi-agency collaboration framework responsible for the national coordination of cybersecurity as Kenya’s national point of contact on cybersecurity matters.

The mandate of the National KE-CIRT/CC includes the detection, prevention and response to various cyber threats targeted at Kenya, and technical coordination and response to cyber incidents in collaboration with various actors.
3. Recognition of Personal Data

What is the definition of personal data and/or sensitive personal data?

Personal data is defined as any information relating to an identified or identifiable natural person. Under KICA, personal information includes a person’s full name, identity card number, date of birth, gender, physical and postal address.

Similar to the GDPR, the DPA refers to sensitive personal data as special categories of data. Special categories of data include personal data pertaining to any of the following about a data subject: race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, or the sexual orientation of the data subject.

4. Critical Information Infrastructure and Databases

Under the Computer Misuse and Cybercrime Act, the Director of the National Computer and Cybercrimes Coordination Committee may designate certain systems as critical infrastructure e.g. if disruption of the system would result in an adverse effect on the Kenyan economy, or which would result in a failure or substantial disruption of the Kenyan money market. As of January 2022, these now include (but are not limited to) mobile communication infrastructure systems, data centres, international internet gateways, systems supporting emergency healthcare and systems supporting Kenya’s financial system.

Upon designation, the Director is further required to issue directives to regulate the protection of, the storing of and archiving of the data held by the critical information infrastructure as well as cyber security incident management by the critical information infrastructure, and the minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure.

5. Collection and Processing

Are there any specific requirements applicable to the collection and processing of data?

In terms of the DPA, the processing of personal data must comply with the following principles:

- processed in accordance with the right to privacy of the data subject;
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Consent of the data subject for any processing is generally required. Alternatively, processing of personal data may take place under a contract with the data subject, in the fulfilment of legal obligations, for the protection of the interests of the data subject, when in the public interest, or when in the legitimate interests of the data controller. The processing of sensitive data is permitted, but subject to further restrictions.

The ODPC has a duty to conduct periodical audits on processes and systems of data controllers or processors, which may require controllers and processors to maintain their processing records for purposes of providing sufficient information for such audits.

6. Requirement for Data Localisation

What are the data localisation requirements (if any) i.e. does data have to be stored locally?

In terms of the DPA, the Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or data centre located in Kenya. The data localisation requirements under the DP Regulations apply to certain sectors, for example, education, healthcare and designated critical infrastructure. Additionally, under the Health Information System Policy (which is persuasive albeit not legally binding) there is a requirement that health data should not be stored outside Kenya.

The DPA also provides for certain restrictions on cross-border transfers of personal data and different restrictions on the cross-border transfer of sensitive personal data.

7. Cross-Border Transfers

What are the requirements for the cross-border transfers of data (if any)?

The DPA regulates the cross-border transfer of personal data outside Kenya. Prior to any transfer the data controller or processor must provide proof to the ODPC in relation to the appropriate safeguards with respect to the security and protection of the personal data, including jurisdictions with similar data protection laws. Data transfers may also be permissible where an adequacy decision has been issued by the ODPC, for the performance of pre-contractual measures of a contract or the conclusion or performance of a contract, to protect the vital interests of the data subject, for compelling legitimate interests pursued by the data controller or processor (that are not overridden by the rights of the data subject) or with the consent of the data subject.

The consent of the data subject is required for the transfer of sensitive personal data out of Kenya, as well as confirmation of appropriate safeguards. The Draft DP Regulations prescribe the terms that must be contained in any cross-border transfer agreements.

8. Registration and/or Notification

What are the registration and/or notification requirements (if any)?

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 propose a threshold of an annual turnover exceeding KES5 million and more than 10 employees, as well as those controllers and processors engaged in specified activities under the Third Schedule to these regulations (such as telecommunication network or service providers, hospitality industry firms, insurance administration, etc). The ODPC is required to maintain the register and issue certificates of registration.

An application for registration must include the following: a description of the personal data and the purpose for which that data is to be processed, the category of data subjects, the contact details of the data controller or processor, a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data, and any measures to indemnify the data subject from the unlawful use of data by the data processor or controller. The grace period for registration expires in mid-July 2022.

Prior consultation with the ODPC is required where a data protection impact assessment indicates that the processing of the data would result in a high risk to the rights and freedoms of the data subject.

9. Data Protection Officers

Is a data protection officer required and, if so, what are the key responsibilities?

The DPA makes provision for the designation of data protection officers but this obligation is not mandatory (i.e. it is dependent on the conditions and activities of the data controller or processor e.g. if the core activities consist of the processing of sensitive categories of personal data).

Data protection officers can be members of staff and may perform other roles. The contact details of the data protection officer must be published on the organisation’s website and communicated to the ODPC.

10. Security Requirements

What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

In terms of the DPA, data controllers and processors are required to implement the appropriate organisational and technical measures to implement data protection principles in an effective manner and to integrate necessary safeguards into the processing. These measures...
must ensure that, by default, only personal data
which is necessary for each specific purpose
is processed taking into consideration the
amount of personal data collected, the extent
of its processing, the period of its storage, its
accessibility, and the cost of processing data
and the technologies and tools used.

To give effect to this, the data controller or
processor is required to consider measures
such as (1) identifying reasonably foreseeable
internal and external risks to personal data;
(2) establishing and maintaining appropriate
safeguards against the identified risks, (3)
pseudonymising and encrypting personal data,
(4) ability to restore the availability and access
to personal data in a timely manner in the event
of a physical or technical incident, (5) verifying
that safeguards are effectively implemented, and
(6) ensuring that the safeguards are continually
updated in response to new risks or deficiencies.

The data controller must also have regard to
the state of the technological development available,
the cost of implementing security measures, the
special risks that exist in the processing of data,
and the nature of the data being processed.
A data controller must ensure that a data
processor provides sufficient guarantees in
respect of the security measures.

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
purposes of the processing), the data controller
or processor must carry out a data protection
impact assessment. A data protection impact
assessment must include: a systematic description
of the processing operations and purpose of
processing, an assessment of the necessity and
proportionality of the processing, an assessment
of the risks to the rights and freedoms of data
subjects, and the measures to address the risks
and the safeguards, security measures and
mechanisms to ensure the protection of the
personal data.

The National Computer and Cybercrimes
Coordination Committee will be expected
to develop a framework to facilitate the
availability, integrity and confidentiality of critical
national information infrastructure including
telecommunications and information systems
in Kenya. As at March 2022, we note that the
Committee has not yet done so. This Committee
also has an obligation to, in consultation with the
operators of critical infrastructure, conduct an
assessment of the threats, vulnerabilities, risks,
and probability of a cyberattack across all critical
infrastructure sectors and identify other risk-
based factors appropriate for the protection of
public health, safety or national security.

11. Data breach
What are the data breach notification
requirements and what are the specific measures
imposed on operators of critical infrastructure or
databases?

Data controllers are required to notify the ODPC
of any breaches within 72 hours of becoming
aware of a breach where there is a real risk of
harm to the data subject.

The notice must include: the description and
nature of the data breach, a description of the measures
that the data controller or processor has
taken to address the data breach, a
recommendation on the measures to be taken by
the data subject to mitigate the adverse effects
of the security compromise, the identity of the
unauthorised person who may have access or
acquired the personal data, and the name and
contact details of the data protection officer. On
the other hand, data processors are required to
inform data controllers of any breach within 48
hours of becoming aware of such a breach. The
data controller is required to record the facts
relating to a breach of personal data, the effects
and the remedial action it takes.

The data controller must notify the data subject
of such breach without undue delay (within a
reasonable time), unless the identity of the data
subject cannot be established. The communication
of the breach to the data subject shall not be
required where the data controller or data
processor has implemented appropriate security
safeguards which may include encryption of
affected personal data.

Service providers under KICA have an obligation
under the Kenya Information Communications
Regulations to notify the data subject if there
is a risk of breach of security to its network,
if the risk is outside the scope of measures that
can be undertaken by the provider, the provider
must inform the data subject of the possible
remedies (including the likely costs). Under KICA,
licensed service providers also have an obligation
to notify the Communications Authority of any
cybersecurity incidents within 24 hours of the
incident, detailing the threat and measures taken
or intended to be taken to prevent the threat.

Financial institutions should notify the
Central Bank of Kenya within 24 hours of any
cybersecurity incidents that could have a
significant and adverse impact on the institution’s
ability to provide adequate services to its
customers, its reputation or financial condition.

Further, the Data Protection (General) Regulations
provide that financial service providers are
obliged to notify the ODPC of any breach
involving a data subject’s account identifier and
password, two-step authentication data or
biometric data.

Under the Computer Misuse and Cybercrimes
Act, any operations identified and gazetted as
critical infrastructure have an obligation to report
to the Committee any cyber threats (although no
process, timeline or other formalities are provided
for). Further, a person who operates a computer
system or network whether public or private has
an obligation to report to the National Computer
and Cybercrimes Coordination Committee any
attacks, intrusions and other disruptions to the
functioning of another computer system within
24 hours of the attack. The report should include
information about the breach, how the breach
occurred if known, an estimate of the number of
people affected by the breach, an assessment of
the risk and harm to the affected persons, an
explanation of circumstances that would lead to
delay in informing the affected persons of the
breach. The National Computer and Cybercrimes
Coordination Committee may propose the
isolation of any computer systems or network
suspected to have been attacked or disrupted
pending the resolution of the issues.

12. Enforcement and sanctions
What are the key enforcement and sanctions
provisions?

The ODPC has the duty to ensure the
implementation and enforcement of the DPA,
which provides for various offences and sanctions.
Additional sanctions are enforced by various
sectoral regulators which may include fines and
the revocation or suspension of licences. Where
the ODPC is satisfied that any person has violated
the provisions of the DPA, the ODPC may issue 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, a failure to register with the ODPC as
a data controller or processor, unlawful disclosure,
processing of personal data without lawful
purpose, and the sale of personal data, where a
penalty is not provided attracts a fine of up to
KEs 3 Million or imprisonment for up to 10 years
or both a fine and imprisonment. A data subject
is entitled to compensation for damage from the
data controller or processor for any violation of
rights.

Under the Computer Misuse and Cybercrimes
Act, unauthorised access is an offence with a
fine of KES5 million or imprisonment for 3 years,
or both; access with intent to commit a further
offence is an offence with a fine of KES 10 million
or imprisonment for 10 years; unauthorised
interference is an offence with a fine of KES10 million
or imprisonment for a period of 5 years.
Where the offence results in significant financial
loss, threatens national security or public health,
the penalty increases to KES 25 million or 20
years imprisonment.

KICA includes cyber security related provisions
that prohibit various actions that would threaten
cyber security and prescribes a range of criminal
penalties, from between KES200,000 to KES 1
million and/or a jail term of up to 5 years.
13. Sectoral Issues
Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Communications sector
KICA outlines the requirements and compliance standards by which licensed information and communication service providers who are data collectors and controllers must abide. For example, all licensed providers are required to obtain and retain information required for the registration of subscribers and SIM cards and ensure that this information is stored in a manner that is secure and confidential. The ICT Policy 2020, gazetted by the Ministry of ICT, recognises cybercrime and cybersecurity vulnerabilities as key factors in the development of the ICT sector.

Health sector
The processing of medical data is regulated under the Public Health Act 2012, the Health Act 2017 and the HIV and AIDS Prevention and Control Act, 2006 (which requires that customer data must be anonymised before processing to protect the patient/data subject privacy). The Health Information System Policy guides the collection and processing of medical data of patients, including requiring the deidentification of patient data before processing. Further, a Guidance Note on Access to Personal Data During COVID-19 Pandemic – expected to provide a policy guidance on processing personal data to actualise responses to and research on the COVID-19 pandemic – was published for public comment in January 2021.

Financial sector
In the financial sector, processing of financial data is regulated under the National Payment Systems Act, 2011 and the National Payment Systems Regulations, 2014. The Central Bank of Kenya’s Prudential Guidelines for Institutions Licensed under the Banking Act provide basic standards that financial institutions must implement to safeguard customer data (such as ensuring the security and confidentiality of their customer’s information and transactions), while the Central Bank of Kenya’s Guideline on Cybersecurity for Payment Service Providers (PSPs) requires a risk assessment to address customer privacy. The Guidelines of PSPs set out the minimum requirements that PSPs need to adhere to for cybersecurity purposes, including the designating of a Chief Information Security Officer, creating and implementing written cybersecurity policies, strategies and frameworks, implementing risk assessment procedures, incident response and cyber resilience, and vulnerability assessment and penetration testing.

14. Trends and Activity
What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system and, at present, enforcement action is not actively pursued. However, important steps are being taken in the data protection space in Kenya demonstrating a commitment to ensuring the proper regulation of personal data.

With the newly enacted DP Regulations, we expect more developments in this area of the law as the ODPC seeks to enforce the provisions of the DPA.
**Malawi**

1. Main Laws

At a high-level, what are the main privacy, data protection, cybercrime, cybersecurity and/or data breach notification legislation and/or regulations?

Malawi does not currently have a comprehensive data protection law, but data protection provisions are included in the Constitution of Malawi (Article 21, regarding the right to personal privacy) and in the Electronic Transactions and Cybersecurity Act, 2016 (ETC Act). A draft Data Protection Bill, 2021 (draft DP Bill) was published for public comment in early 2021. The draft DP Bill’s proposed scope of application includes a data controller or processor who is domiciled, ordinarily resident or ordinarily operating in Malawi, is processing personal data within Malawi or, subject to some limitations, is processing personal data of a data subject who is in Malawi (e.g. targeted offerings of goods or services, or the monitoring of the behaviour of a data subject). The draft DP Bill proposes the repeal of the provisions relating to data protection in the ETC Act, but there is no indication as to when the draft DP Bill is likely to come into effect.

Electronic transactions, cybercrime and cybersecurity are all dealt with under ETC Act and the Communications Act 2016. One of the objectives of the ETC Act is “to put in place mechanisms that safeguard information and communication technology users from fraud, breach of privacy, misuse of information and immoral behaviour brought by the use of information and communication technology” and criminalises unauthorised access, interception or interference with data, prohibits hacking, cracking and introducing virus, as well as unlawfully disabling a computer system, while the Communications Act criminalises unlawful interception and interference with the transmission of electronic communications. Malawi has also adopted a National Cyber Security Strategy.

Malawi is yet to sign or ratify the AU Convention on Cyber Security and Personal Data Protection or the Budapest Convention on Cyber Crime.

2. Key Regulators

Who are the key regulators, what are their areas of jurisdiction, and what are their contact details?

At present, there is no dedicated data protection regulator in Malawi.

The Malawi Communications Regulatory Authority (MACRA) is responsible for the implementation of the ETC Act (and, accordingly, data protection and cybersecurity) and may impose administrative penalties for violations.

Malawi’s National Computer Emergency Response Team (mwCERT), a department established under the ETC Act, is responsible for taking charge of critical information infrastructure protection actions and serving as a base for national coordination to respond to cybersecurity threats, including assistance for responses to incidents.

The draft DP Bill designates MACRA as the authority to regulate and monitor personal data protection and privacy in Malawi and oversee the implementation and enforcement of the Act. It is proposed that a Data Protection Office will be established within MACRA, which will be primarily responsible for the activities relating to data protection under the Bill.

3. Recognition of Personal Data

Are there specific definitions for personal data and/or sensitive personal data?

Personal data, as defined in the ETC Act, means any information relating to an individual who may be directly identified, or if not directly identified, may be identifiable by reference to an identification number or one or several elements related to his physical, physiological, genetic, psychological, cultural, social or economic identity. There is no definition for sensitive personal data.

The draft DP Bill proposes the following definition for personal data: any information relating to an individual who can be identified or is identifiable, directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.
The draft DP Bill also recognises a further category of special personal data, namely sensitive personal data i.e. personal data relating to an individual’s biometric data, race or ethnic origin, religious or similar beliefs such as those reflecting conscience or philosophy, health status, sex life or sexual orientation, political opinions or affiliations, or any other prescribed personal data.

4. Critical Databases
The term ‘critical data’ is defined under the ETC Act as data which is declared by the Minister of Information to be of importance to the protection of national security of Malawi or the economic and socio well-being of its citizens.

The Minister may declare certain classes of information to be critical data, may establish procedures for identification of databases with critical data, deal with the registration of databases with critical data, prescribe minimum standards regarding management, access to transfer and control of databases with critical data, and the inspection of databases by MACRA.

5. Collection and Processing
Are there any specific requirements applicable to the collection and processing of data?

The ETC Act sets out principles governing the processing of personal data, legal bases for the processing activities, data subjects’ rights, and security measures that a data controller must put in place when processing personal data. Although MACRA is the competent authority for the enforcement of the ETC Act, the Government is also authorised to adopt the necessary regulations in order to establish a legal framework to ensure the confidentiality of personal data.

Under the ETC Act, personal data processing may only occur with unambiguous consent (freely given specific and informed indication of wishes by agreement) from the data subject or if processing is necessary for:

- compliance with a legal obligation to which the controller is subject;
- the performance of a public interest mission or the exercise of public authority;
- the commencement or performance of a contract in the data subject’s interests or to which he, she or they are a party;
- safeguarding the interests or fundamental rights and freedoms of the data subject; or
- the pursuit of legitimate interests of the controller or third-party data processor, provided these interests preserve the fundamental rights and freedoms of the data subject.

The draft DP Bill proposes a comprehensive framework for data protection in Malawi. It requires a data controller or data processor to process data fairly and in a transparent manner and only where (1) the data subject has given and not withdrawn his consent, and (2) the data is required for legitimate purposes outlined in the draft DP Bill.

The draft DP Bill further limits the processing of sensitive personal data. All processing of personal data must adhere to internationally recognised data protection principles.

6. Requirement for Data Localisation
What are the data localisation requirements (if any)?

There are no current data localisation requirements, although the draft DP Bill does provide for certain restrictions on cross-border transfers of personal information as discussed below.

7. Cross-Border Transfers
What are the requirements for the cross-border transfers of data (if any)?

There are currently no cross-border data transfer restrictions that are applicable in Malawi.

However, the draft DP Bill contains prohibitions on the transfer of personal data outside Malawi unless the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection in respect of the personal data (i.e. a level of protection which upholds principles that are substantially similar to those contained in the draft DP Bill). A data controller or processor will be required to record the basis for the transfer of the personal data to another country and the adequacy of protection (if applicable). MACRA may make rules requiring data controllers and processors to notify it of the measures in place and explain their adequacy.

In the absence of adequacy of protection, the draft DP Bill provides that cross-border transfers may only take place if – (1) the data subject has given and not withdrawn his consent, and (2) the data is required for legitimate purposes outlined in the draft DP Bill

The draft DP Bill proposes that cross-border transfers must be adequate by providing that transfers of personal data may only take place if – (1) the data subject has given and not withdrawn his consent, and (2) the processing is necessary for the performance of a contract to which the data subject is a party, or which is in the interest of the data subject, or (3) the transfer is for the benefit of the data subject and it is not possible to obtain the consent of the data subject and if it were reasonably practicable, the data subject would likely give it.

8. Registration and/or Notification
What are the registration and/or notification requirements for the collection and/or processing of data (if any)?

At present, there are no registration and/or notification requirements for data controllers or processors in Malawi.

The draft DP Bill envisages the registration of data controllers and processors “of major importance” with MACRA which will be valid for a period of 3 years. This refers to a controller or processor domiciled, ordinarily resident or ordinarily operating in Malawi which processes or intends to process personal data of more than 10,000 data subjects who are within Malawi or such other controller or processor who is processing personal data of particular value or significance to the economy, society or security of Malawi.

It is proposed that registration will be made by notifying MACRA of the name and address of the controller or processor or any representative, a description of the personal data and the categories and number of data subjects to which the personal data relate, the purposes for which the personal data is processed, the categories of recipients to whom the data will be disclosed, any country to which the personal data will be transferred, and a general description of risks, safeguards, security measures and mechanisms to ensure the protection of the personal data.

Payment of a prescribed fee will also be required. MACRA will be required to maintain and publish a register of such registered controllers and processors. It may be possible to obtain an exemption from this registration requirement for a class of controllers or processors under the draft DP Bill.

As discussed further below, notification of the results of a data protection impact assessment must be made to MACRA, in certain circumstances, under the draft DP Bill.

9. Data protection officers
Is a data protection officer required and, if so, what are the key responsibilities?

At present, there is no requirement for the appointment of a data protection officer in Malawi. Similarly, the draft DP Bill does not require the appointment of a data protection officer.

10. Security Requirements
What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

In terms of the ETC Act, a data controller must implement technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures are required to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. No further detail is provided regarding such technical and organisational measures.

The draft DP Bill sets out that each data controller and processor will be required to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorised disclosure or access, taking into account: (1) the amount and sensitivity of personal data, (2) the degree and likelihood of harm to data subjects, (3) the extent of the processing, (4) the period of data retention, and (5) the cost of any technologies, tools or other measures to be implemented relative to the size of the data controller or processor. Measures can include pseudonymisation, encryption, periodic risk assessments to processing systems and services, regular testing and evaluation and regular updates.
11. Data Breach

What are the data breach notification requirements (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

There are currently no data breach notification requirements in Malawi, and no specific measures imposed on operators of critical infrastructure or databases.

However, the draft DP Bill proposes specific measures for personal data breaches (although there will be a 2-year delay in the coming into operation of this section). In the event of a data breach, where such breach is likely to result in a risk to the rights and freedoms of individuals, a data controller will be required to notify MACRA of the breach within 72-hours of having become aware of it, describing the nature of the personal data breach including the categories and approximate numbers of data subjects and personal data records concerned. If there is a high risk to the rights and freedoms of a data subject, the data controller will be required to communicate such breach to the data subject (or in the form of a public communication in certain circumstances) without undue delay in plain and clear language, including advice about measures the data subject could take to mitigate the possible adverse effects of the data breach.

The draft DP Bill also provides that a data processor is required to notify a data controller of a data breach within 72-hours of becoming aware of it and will be required to respond without undue delay to all information requests from the data controller.

12. Enforcement and Sanctions

What are the key enforcement and sanctions provisions?

In terms of the ETC Act, no person is permitted to gain unauthorised access to, or intercept, or interfere with, data. Exceeding authorised access, or interference with data, are offences which are subject to sanction. A data controller or processor who produces, sells or utilises any device or computer program to overcome security measures designed to protect data are offences which are subject to sanction on conviction. Hacking, introducing or spreading viruses and rendering a computer system ineffective are also all considered to be offences in Malawi. Similarly, any other violation of a provision of the ETC Act (including the provisions relating to the protection of personal data) is an offence. ETCA also caters for the appointment of cyber inspectors.

The draft DP Bill proposes that MACRA may initiate an investigation on its own accord or upon reference by the data subject and make appropriate compliance and enforcement orders against the violating data controller or processor. A data controller or processor who fails to comply with a compliance or enforcement order under the draft DP Bill will be liable for a fine of K5 million and imprisonment for two years.

13. Sectoral Issues

Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data).

Communications sector

The Communications Act, 2016 criminalises unlawful interception or interference by service providers.

Financial sector

The Reserve Bank of Malawi implemented the Information and Cyber Security Risk Management Guidelines, under the Financial Services Act 2010, replacing the previous IT risks management policies. The guidelines outline minimum requirements which banks are expected to put in place for managing information and cyber security risk, as well as strengthening banks’ information system security and protection of critical information infrastructure.

14. Trends and Activity

What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system and, at present, enforcement action is not actively pursued.

The draft DP Bill has been subjected to stakeholder consultations and has been presented to Cabinet for approval, before being tabled in Parliament. It is likely that the draft DP Bill will be tabled in Parliament later this year or early next year.
MAURITIUS

1. Main Laws
At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Mauritius has a strong legal framework in place to protect personal data. Mauritius regulates data protection under the Data Protection Act 2017 (DPA), which came into effect on 15 January 2018 and which ensures alignment with the General Data Protection Regulation (GDPR), together with the Data Protection (Fees) Regulations, 2020 (which sets out various fees and forms for registration under the DPA). The DPA applies to a controller or a processor who is established (ordinarily resident or carries out data processing activities through an office branch or agency in Mauritius) and processes data in the context of that establishment. If the controller or processor is established outside Mauritius but uses equipment in Mauritius to process data, such controller or processor will have to nominate a representative which is established in Mauritius.

Electronic transactions are regulated in Mauritius under the Electronic Transactions Act, 2000 which provides a legal framework to facilitate electronic transactions and communications by regulating electronic records, electronic signatures and the security of these.

Mauritius regulates cybercrime under the Computer Misuse and Cybercrime Act, 2003. This Act sets out various offences relating to computer misuse and cybercrime, including unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of computer service, unauthorised modification of computer material, damaging or denying access to computer systems, unauthorised disclosure of passwords, unlawful possession of devices and data, and electronic fraud.

It provides for investigations and procedures related to computer misuse and cybercrime. Mauritius also developed a Cybercrime Strategy 2017-2019 to, amongst other things, develop a more effective legal framework to tackle and prosecute cybercrime.

To address cyber security matters, Mauritius developed a National Cyber Security Strategy: 2014-2019 falling under the Ministry of Information & Communication Technology. There is no separate cybersecurity legislation in Mauritius at present, although a Cybersecurity Bill was introduced to Parliament in November 2020.

Mauritius ratified the AU Convention on Cyber Security and Personal Data Protection in March 2018 and ratified the Budapest Convention on Cyber Crime in November 2013. Mauritius has also ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

Under the DPA, the Data Protection Office (DPO) - an independent and impartial public office - is responsible for data protection oversight. The DPO is headed by the Data Protection Commissioner (Commissioner) with the assistance of public officers. The Commissioner is responsible for the enforcement of the DPA.

The Mauritian Computer Emergency Response Team (CERT-MU), a division of the National Computer Board operating under the Ministry of Technology, Communication and Innovation, is the advisory body for information security issues in Mauritius and is responsible for handling and coordinating cyber security incidents, providing information and encouraging organisations and individuals to report cyber security incidents.

The Mauritian Cybercrime Online Reporting System (MAUCORS) is one of the key initiatives of the National Cybercrime Strategy that sets out the Government’s approach to combat cybercrime in Mauritius. It is a platform administered by the CERT-MU and is designed to make cybercrime reporting easier and convenient. It is a centralised system that connects the CERT-MU, the Cybercrime Unit (Mauritius Police Force), the DPO and the Information Communication Technologies Authority (ICTA) and allows citizens to report incidents on one platform that can connect with the respective institutions.
3. Recognition of Personal Data
What is the definition of personal data and/or sensitive personal data?

**Personal data** is defined as any information relating to a data subject. A data subject is a natural person who is identified or identifiable, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Similar to the GDPR, the DPA refers to **sensitive personal data** as special categories of data. Special categories of data include personal data pertaining to any of the following about a data subject: racial or ethnic origin; political opinion or adherence; religious or philosophical beliefs; membership of a trade union; physical or mental health or condition; sexual orientation, practices or preferences; genetic or biometric data that is uniquely identifying; or commission or proceedings related to the commission of a criminal offence.

4. Critical Infrastructure and Databases
Mauritius’ National Cyber Security Strategy includes the development and implementation of a critical information infrastructure protection framework for Mauritius, which will help sectors defend against a range of cyber threats.

5. Collection and Processing
Are there specific requirements applicable to the collection and processing of data?

In terms of the DPA, every data controller or processor needs to ensure that personal data is:
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in accordance with the rights of data subjects.

All data controllers and processors are required to keep a record of all processing operations under their responsibility.

In terms of the DPA, data subject consent (any freely given, specific, informed and unambiguous indication of the data subject’s wishes, either by statement or affirmative action) is required for processing. Alternatively, personal data may be processed (amongst other grounds) when it is necessary for the purposes of the performance of a contract; to ensure compliance with a legal obligation imposed on the data controller, to protect the vital interests of the data subject, or for the legitimate interests of the data controller or a third party to whom the data is disclosed (except if the processing is unwarranted having regard to the harm and prejudice to the rights, freedoms or legitimate interests of the data subject).

6. Requirement for Data Localisation
What are the data localisation requirements (if any)?

There are no specific data localisation requirements applicable in Mauritius, although cross-border restrictions are imposed under the DPA.

7. Cross-Border Transfers
What are the requirements for the cross-border transfers of data (if any)?

In terms of the DPA, a data controller or processor may transfer personal data to another country, where the data controller or processor has provided proof of appropriate safeguards with respect to the protection of the personal data (Mauritius has obtained adequacy with the EU) to the Commissioner, or where the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer given the absence of appropriate safeguards.

A cross-border transfer is also permissible, amongst other grounds, where it is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request; in order to protect the vital interests of the data subject; or for the purpose of compelling legitimate interests pursued by the data controller or the processor (which are not overridden by the interests, rights and freedoms of the data subjects involved and where the transfer is not repetitive and concerns a limited number of data subjects and the data controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data).

The transfer may also be made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case (such transfer must not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer must be made only at the request of those persons or in case they are to be the recipients).

The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as the Commissioner may determine.

8. Registration and/or Notification
What are the registration and/or notification requirements (if any)?

Every person who intends to act as a data controller or processor must register with the Commissioner in the prescribed form and pay the prescribed registration fee. Registration certificates are valid for three years.

Every registration application must include the following: name and address (including of a representative, where applicable); a description of the personal data, the category of data subjects, the purpose for which the personal data is to be processed, and any recipient of the data; a statement as to whether the data controller or processor holds, or is likely to hold, special categories of personal data; the name, or a description of, any country to which the data may be transferred; and a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data e.g. physical access control, firewall, antivirus, encryption of data, employee awareness programs. The Data Protection Register is kept by the Commissioner and is available for inspection free of charge.

Every data controller and processor is required to obtain prior authorisation from the DPO where appropriate safeguards are not in place for the cross-border transfer of personal data. Certain processing activities are also subject to prior consultation e.g. where a data protection impact assessment indicates that processing operations are likely to present a high risk due to their nature, scope or purposes.

9. Data Protection Officers
Is a data protection officer required and, if so, what are the key responsibilities?

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). There can be one data protection officer for a group of companies, provided that person is accessible.

The data controller is also required to keep records that contain the name and contact details of the data protection officer. At the time of collecting personal data, an individual must be informed of the identity and contact details of any data protection officer if there is one.
The data protection officer can be an employee (provided this does not lead to any conflicts of interest) or may be outsourced, but the person must act with complete independence and impartiality and must have professional experience and knowledge of data protection laws and standards.

10. Security Requirements

What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

Under the DPA, a data controller or processor must implement and maintain appropriate security and organisational measures for the prevention of unauthorised access to, alteration, disclosure or destruction of, or the accidental loss of the personal data. The data controller or processor must ensure that the measures provide a level of security appropriate to the harm that may result and the nature of the personal data concerned, including: (1) pseudonymisation and encryption; (2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and/or (4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data controller must have regard to: the state of technological development available, the cost of implementation of the security measures, special risks that exist in the processing of the data, and the nature of the data being processed.

Where a data controller is using the services of a processor, the controller must choose a processor that is able to provide sufficient security and organisational measures to ensure the protection of personal data, and the processor must be contractually bound to providing such measures. Interestingly, the Commissioner has introduced a voluntary certification process for assessing the implementation of appropriate technical and organisational measures, which is renewable after 3 years.

Further, 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 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.

11. Data Breach

What are the data breach notification requirements (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

Under the DPA, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner. A data processor must, once aware of a personal data breach, notify the controller without undue delay. The breach notification must: (1) describe the nature of the personal data breach, including the categories and approximate number of data subjects and categories and approximate number of personal data records concerned, (2) the name and contact details of any appropriate data protection officer, and (3) recommend measures to address the personal data breach as well as remedial measures taken.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller must, after having notified the Commissioner, inform the individual in clear language, of the breach without undue delay. There are circumstances which do not require the controller to notify the individual of the personal data breach: e.g. if such notification would involve a disproportionate effort and the controller has made a public communication of the breach whereby the data subject is informed.

The communication of a personal data breach to the data subject is also not required where: the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption; the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise; or it would involve disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

Cybercrime incidents can be reported on the CERT-MU website through the online reporting form as well as at CERT-MU’s office.

12. Enforcement and Sanctions

What are the key enforcement and sanctions provisions?

The Commissioner may investigate a complaint that the DPA or any regulations in respect thereof have been contravened. The Commissioner may serve an enforcement notice on a data controller or processor in contravention requiring them to take remedial steps within a set period. The Commissioner may also inspect and assess security and organisational measures which a controller is required to have in place prior to starting processing or the transfer of personal data, and may carry out periodical audits of the systems of data controllers to ensure compliance with the provisions of the DPA. Further the Commissioner may designate an authorised officer to enter and search any premises on which the authority of a warrant issued by a Magistrate. In addition, if the Commissioner has reasonable grounds to believe that data is vulnerable to loss or modification, an application may be made to a Judge in Chambers for an order for the expedient preservation of the data.

The Computer Misuse and Cybercrime Act also sets out various offences related to computer misuse and cybercrime and provides for necessary investigations and procedures.

13. Sectoral Issues

Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Health sector

The DPO published a Guide on Data Protection for Health Data and Artificial Intelligence Solutions in the context of the COVID-19 Pandemic which helps controllers and processors to determine the basis for processing health data.

Communications sector

In terms of the Information and Communication Technologies Act, 2001 a licensee, including its employees and agents, must treat as confidential any message or any information relating to a message in the course of their duties. A person who, otherwise than in the course of his/her duties, makes use of, or records, the contents or substance of a message that comes to their knowledge, or to which they have access, by reason of their position as a licensee, or as an employee or agent of a licensee, commits an offence.

Financial sector

In terms of the Banking Act, 2004 a person including a service provider, who, by virtue of professional relationship with a financial institution, has access to the books, accounts, records, financial statements or other documents, whether electronically or otherwise, of a financial institution cannot, during or after that relationship with the financial institution, disclose directly or indirectly to any person any information relating to the affairs of any of its customers including any deposits, borrowings or transactions or other personal, financial or business affairs, without the prior written consent of the customer or the customer’s personal representative.

The disclosure of banking information is permissible in circumstances specifically specified in the Banking Act. For example, the duty of confidentiality does not apply if a customer who had been issued a credit card or charge card by a financial institution, has their card suspended or cancelled by the financial institution by reason of their default in payment, and the financial institution discloses information relating to the customer’s name and identity, the amount of their indebtedness and the date of suspension or cancellation of their credit card or charge card to other financial institutions issuing credit cards or charge cards in Mauritius.
In terms of the Guides on Outsourcing by Financial Institutions (revised in March 2018) (the BOM Outsourcing Guidelines) issued by the Bank of Mauritius (BOM), a financial institution must report any unauthorised access or breach of confidentiality and security by an outsourcing service provider to the BOM and state the action(s) it proposes to take to deal in consequence.

A mobile banking or mobile payment service provider which provides services to a customer who does not hold a bank account must submit monthly reports which must, among other things, cover any loss of confidential data, to the BOM. In addition, under the BOM Outsourcing Guidelines, a financial institution must avoid cross-border outsourcing arrangements with countries that do not have legislation on the confidentiality of information. Financial institutions should obtain their clients’ consent for their information to be stored in the cloud in specified jurisdictions.

14. Trends and Activity
What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

Mauritius has a developed system and ranks among the top three in Africa in the 2018 ITU Global Security Index.

A proposal has been submitted for the amendment of the Computer Misuse and Cyber Crime Act to provide a legal mandate to CERT-MU to operate as a separate legal entity and to act as a watchdog on critical information infrastructure protection. This will shift CERT-MU from an advisory role to overseeing national cyber security issues.
1. Main Laws
At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Nigeria does not currently have a principal data protection legislation, but data protection provisions are included in the Constitution of the Federal Republic of Nigeria 1999 (Section 37, regarding the right to privacy) and the Nigerian Data Protection Regulation, 2019 (NDPR). Other laws with data protection provisions include the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Cybercrimes Act), the Implementation Framework for the NDPR, 2020 (Framework) and the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020, the Child Rights Act 2003, the Freedom of Information Act 2011, the National Health Act 2014 and the HIV and AIDS (Anti-Discrimination) Act 2014.

There are also laws that apply to specific sectors and industries in Nigeria that contain data protection provisions. For example, the telecommunication sector has specific data protection provisions that are applicable to all companies operating in the sector. These provisions are set out in the Nigeria Communications Commission (NCC) Consumer Code of Practice Regulations 2007, the NCC Registration of Telephone Subscribers Regulations 2011, the Central Bank of Nigeria (CBN) Consumer Protection Regulations 2020, the NCC Lawful Interception of Communications Regulations, 2019 and the Official Secrets Act 1962.

The NDPR applies to all transactions intended for the processing of personal data of natural persons in Nigeria and also applies to natural persons residing in Nigeria or outside Nigeria who are citizens of Nigeria.

The Framework issued in November 2020, serves as a guide to data controllers and processors to understand the standards required for compliance within their organisations.

Electronic transactions, cybercrime and cybersecurity are all dealt with under the Cybercrimes Act which provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. It also requires financial institutions to retain and protect data and criminalises the interception of electronic communications.

The Cybercrimes Act promotes cybersecurity, the protection of critical national information infrastructure, computer systems and networks, electronic communications, data and computer programs, and privacy rights. Nigeria also adopted a new National Cybersecurity Policy and Strategy in February 2021.

The National Cybersecurity Policy and Strategy proposes the amendment of the Cybercrimes Act to, amongst other things, adopt timelines for cyber incident reporting and to allot powers to the National Cybersecurity Coordination Centre (NCCC), once established, to coordinate national cybersecurity and anchor investigation of cyber breaches.

Nigeria is yet to sign or ratify the AU Convention on Cyber Security and Personal Data Protection and the Budapest Convention on Cyber Crime.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

Under the NDPR, the National Information Technology Development Agency (NITDA), which is the national authority for planning, developing and promoting the use of information technology in Nigeria, is the main regulator for data protection in each of their sectors. For example, the Central Bank of Nigeria oversees matters relating to protecting financial data, while the Nigerian Communications Commission (NCC) regulates data collected or processed by internet service providers and telecommunications companies.

On 4 February 2022, the President of the Federal Republic of Nigeria, President Muhammadu Buhari announced the establishment of a dedicated data protection agency for Nigeria, the Nigerian Data Protection Bureau (NDPB). This means that, going
forward, the NDPB and not the NITDA will be responsible for the enforcement of data protection regulations and for the administration of all related data protection matters in Nigeria. The NDPB will, until the substantive data protection regulation is passed, continue to operate within the existing regulatory framework, i.e. the NDPR and the NDPB Implementation Framework. Enacting a substantive Data Protection Bill will create a regulatory framework for the establishment and administration of the NDPB and related data protection matters is one of the top priorities of the NDPB. Pending the establishment of the framework and the stabilisation of operations, the NITDA continues to regulate data protection in Nigeria on a transitional basis.

There is no specific regulatory authority for the enforcement of the provisions of the Cybercrimes Act in Nigeria, rather it is the obligation of all security agencies in Nigeria to enforce the provisions of the Cybercrimes Act. The Office of the National Security Adviser (ONS,A) is responsible for coordinating the implementation of the Cybercrimes Act by the security agencies.

The Nigeria Computer Emergency Response Team (ngCERT), established under the Cybercrimes Act, is the focal point for Nigerian cyber incident management and will supervise the establishment of sectoral cybersecurity incident response teams. The National Cybersecurity Policy and Strategy proposes (1) establishing processes, protocols and timelines for reporting and escalating cybersecurity incidents across all levels from individual users, sectoral teams and critical information infrastructure operators to ngCERT, and (2) establishing and operating a National Register of Cybersecurity Incidents.

3. Recognition Of Personal Data

Are there specific definitions for personal data and/or sensitive personal data?

The NDPR defines personal data as any information relating to an identified or identifiable natural person and would include information such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The NDPR defines sensitive personal data as data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trade union membership, or criminal records. The Bill proposes the introduction of a larger definition for sensitive data which would include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning health, data concerning a natural person’s sex life, and personal data concerning a child.

4. Collection and Processing

Are there any specific requirements applicable to the collection and processing of data?

The NDPR sets out the governing principles of data processing including that personal data must be:

• collected and processed in accordance with a specific, legitimate and lawful purpose consented to by the data subject;
• adequate, accurate and without prejudice to human dignity;
• stored only for the period within which it is reasonably needed; and
• secured against all foreseeable hazards and breaches.

Personal data processing is lawful if it is carried out under any of the bases set out below:

• where the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
• where the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
• where the processing is necessary for compliance with a legal obligation to which the data controller is subject;
• where the processing is necessary for the protection of vital interests of the data subject or of another natural person; and
• where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official public mandate vested in the data controller.

Consent must be a freely given, specific, informed and unambiguous indication of the data subject’s wishes. The legal age of consent, as stated in the provisions of the NDPR Implementation Framework is 13 (thirteen) years.

The NDPR requires all public and private organisations in Nigeria that control data of natural persons to make available to the general public their respective data protection policies within 3 months after the date of issuance of the NDPR.

5. Critical Databases

The Cybercrimes Act defines the term “critical infrastructure” as systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, and national public health and safety of the country.

Under the Cybercrimes Act, the President, on the recommendation of ONSA, may declare certain assets to be critical national infrastructure. In the National Cybersecurity Policy and Strategy, the President identifies 13 critical information infrastructure sectors, namely:

• power and energy;
• water;
• information infrastructure operators to ngCERT;
• telecommunications and electronic communications;
• banking/finance and insurance; health;
• transportation and storage; food and agriculture;
• safety and emergency services; industrial and manufacturing; and
• mines and steel.

The Cybercrimes Act makes it an offence for anyone to destroy or interfere with critical national information infrastructure. The offender will be liable, upon conviction, to imprisonment for not more than ten years, without an option of a fine.

6. Requirement for Data Localisation

What are the data localisation requirements (if any)?

The NITDA’s mandatory Guidelines for Nigerian Content Development in Information and Communication Technology require:

• all telecommunications companies and network service companies to host all subscriber and consumer data in Nigeria;
• all data and information management companies to host all sovereign data in Nigeria;

There are also certain restrictions on cross-border transfers of personal data, as discussed further below.

7. Cross-Border Transfers

What are the requirements for the cross-border transfers of data (if any)?

Cross-border transfers of personal data are supervised by the Honorable Attorney General of the Federation (HAGF) upon an application by the proposed transferor submitted to the HAGF through the NITDA. In terms of the NDPR, cross-border transfers of personal data are permitted where the HAGF determines that a foreign country, territory or specific sector(s) within a foreign country or international organisation provide adequate levels of personal data protection.

The determination is based on the HAGF’s consideration of the foreign country’s legal system, rule of law, respect for human rights and fundamental freedoms, the implementation of equivalent legislation, the existence and effectiveness of an independent supervisory authority in the foreign country responsible for compliance with data protection, and the commitments of the foreign country to data protection through conventions, instruments, participation in multilateral or regional systems.

An application is required to be made to the HAGF through the NITDA and the NITDA will decide whether the country where personal data is to be transferred to has adequate data protection laws that can safeguard the privacy of the personal data of Nigerian citizens and residents.
9. Data Protection Officers

Is a data protection officer required and, if so, what are the key responsibilities?

The NDPR and the Framework require data controllers and data processors to designate a data protection officer who will be responsible for ensuring compliance with the NDPR, data privacy policies of the organisation and other applicable data protection directives. The data controller or processor may outsource this responsibility to a competent firm or person. A data controller or processor must ensure continuous capacity building for its data protection officers and its personal involved in any form of data processing.

10. Security Requirements

What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

In terms of the NDPR, anyone involved in data processing or the control of data has the responsibility to develop security measures to protect data, including but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policies for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff. Further, the Cybercrime Act requires non-financial institutions to put in place effective counter-fraud measures to protect sensitive information.

11. Data Breach

What are the data breach notification requirements (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

There is no mandatory requirement to report data security breaches or losses to the authorities or to data subjects under the NDPR. However, the Framework requires that data controllers notify NITDA of personal data breaches within 72 hours of becoming aware of the breach, and to immediately notify a data subject where the breach will likely result in high risks to the freedoms and rights of the data subject. The notification of a data breach to NITDA must include the following: a description of the circumstances of the breach and the personal data involved; the date or time period; an assessment of the risk of harm to data subjects and the likely scope; a description of steps taken to reduce the risk of harm and to notify individuals of the breach; and the name and contact information of a suitable contact person.

Furthermore, the Cybercrimes Act provides that any person or institution who operates a system or a network, whether public or private, must immediately inform ngCERT of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network. The Cybercrimes Act does not provide the process or formalities that need to be followed, but ngCERT’s website sets out the following information regarding whether the cyber attack is ongoing, the impact and nature of the cyber attack, the date and time of occurrence, and countermeasures taken. The Cybercrimes Act provides that any person or institution who fails to report any such incident to ngCERT within 7 (seven) days of its occurrence, commits an offence, will be liable to denial of Internet services, and will be required to pay a fine of NGN 2 million into the National Cyber Security Fund.

Banks and other financial institutions have an obligation to report data breaches to the Central Bank of Nigeria, while telecommunications companies and internet service providers are required to report data breaches to the NCC. Further, the Internet Industry Code of Practice of 2019 issued by the NCC requires internet access service providers to notify affected customers of any breach within 48 hours of its occurrence.

12. Enforcement and Sanctions

What are the key enforcement and sanctions provisions?

NITDA is authorised to set up an administrative redress panel to investigate allegations of breaches of the NDPR, which is considered to be a breach of the NDPR Act, 2007. Penalties vary in amount, depending on the number of data subjects whose personal data the data controller or processor processes. The NDPR provides as follows: (1) in the case of a data controller dealing with more than 10,000 data subjects, payment of a fine of 2% of annual gross revenue for the preceding year or payment of the sum of NGN10,000.

Where the NITDA considers an application to transfer personal data outside Nigeria, the HAGF will issue an adequacy decision upon a satisfactory review of the following information or documents which the applicant will be required to provide: (1) a list of countries where the Personal Data of the Nigerian citizens and residents are in the regular course of business; (2) the data protection laws observed by the data protection office / administration of such countries; (3) the privacy policy of the data controller, which must be NDPR compliant; (4) an overview of the encryption method and data security standards which will be deployed by the data controller or processor; and (5) any other detail or information which can assure that the privacy of such personal data will be adequately protected in such country.

Where the HAGF issues an adequacy decision based on the application above, such adequacy decision permits a cross-border transfer of personal data outside Nigeria or the onward transfer to a party in a country stated in the White List. The White List is the list of countries which the NITDA has confirmed to have adequate data protection laws and which the NITDA has annexed as a schedule to the Framework. The HAGF may, however, refuse an application for the transfer of the personal data of Nigerian citizens or residents to countries where it is of the opinion that such country’s data protection laws are inadequate or incompatible with the provisions of Nigerian law.

Where a data controller or processor wishes to transfer personal data to countries that are not included in the White List, the HAGF shall subject such an application to further scrutiny to ensure that the personal data of Nigerian citizens and residents will be adequately protected in the country where the personal data is intended to be transferred.

Personal data transfers may also take place without NITDA and HAGF’s authorisation in certain recognised circumstances, including (1) where the data subject expressly consents to the proposed transfer after being informed of associated risks in the absence of an adequacy determination, the lack of appropriate safeguards, and that there are no alternatives, (2) where transfer is necessary for the performance of a contact or (3) where the transfer is necessary to protect the vital interests of the data subject (4) where the transfer is necessary for important reasons of public interest, or (5) the transfer is necessary for the establishment, exercise or defence of legal claims. Nevertheless, the NDPR requires that the data subject must, in all circumstances be made to understand the specific principle(s) of data protection that are likely to be violated in the event of the transfer of their personal data to a third country in the above stated circumstances.

8. Registration and/or Notification

What are the registration and/or notification requirements for the collection and/or processing of data (if any)?

At present, there are no registration and/or notification requirements for data controllers or processors in Nigeria. Under the NDPR, however, data controllers are required to carry out periodic data protection audits and to submit a data protection audit report to NITDA if they process the data of more than 1000 data subjects in 6 months (in which case a soft copy of the summary of the audit must be submitted to the NITDA), or more than 2000 data subjects in 12 months (in which case a summary of the data protection audit must be submitted to the NITDA) on or before 15 March, every year.

In addition, the NDPR requires every data controller or processor to engage the services of a Data Protection Compliance Organisation (DPCO). A DPCO is a firm licenced by the NITDA to provide data protection compliance services to organisations in Nigeria. One of such services is conducting the data protection and privacy audit. Only DPCOs are permitted under the NDPR to conduct audits and to file reports on behalf of data controllers and processors.

The White List is the list of countries which the NITDA has confirmed to have adequate data protection laws and which the NITDA has annexed as a schedule to the Framework. The HAGF may, however, refuse an application for the transfer of the personal data of Nigerian citizens or residents to countries where it is of the opinion that such country’s data protection laws are inadequate or incompatible with the provisions of Nigerian law.
The NDPR further provides that any breach of its provisions will be construed as a breach of the provisions of the NITDA Act 2007. Consequently, the penalties stipulated in the NITDA Act would also apply in such circumstances. The NITDA Act stipulates that any entity that commits an offence is liable on conviction to the following: (1) for a first offence, a fine of NGN200,000 or imprisonment for a term of 1 year or to both such fine and imprisonment; and (2) for any subsequent offence, a fine of NGN500,000 or imprisonment for a term of 3 years or to both such fine and imprisonment.

The Cybercrimes Act creates various offences and imposes various penalties for cybercrimes. For example, under the Cybercrimes Act it is an offence for any person, without authorisation, to access a computer system with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information. The penalty, upon conviction, is a period of imprisonment for 7 (seven) years or a fine of not more than NGN 7 million, or both.

13. Sectoral Issues
Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Communications sector
The NCC issued the Consumer Code of Practice Regulations 2007 (NCC Regulations) to require all licensees to take reasonable steps to protect customer information against improper or accidental disclosure and to ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information without the customer’s consent. The General Consumer Code was issued by the NCC as a schedule to the NCC Regulations.

This Code provides mechanisms for detailed complaint submission and handling processes for the resolution of consumers’ complaints by licensees.

In addition, the NCC Registration of Telephone Subscribers Regulations, 2011 require providers of mobile telephone services to collect and transmit subscriber information to the central database. The Regulations further require mobile telephone service providers to retain and use subscriber information collected by them pursuant to the Regulations, solely for their operations and in accordance with the protection of consumer information provisions of the General Consumer Code of Practice for Telecommunications Services and any other regulations of the NCC or any law regulating the specific purposes for which the personal information may be used.

Financial sector
The Consumer Protection Regulations 2020 were enacted under the Central Bank of Nigeria Act, 2007. The Regulations contain provisions that prohibit financial institutions from disclosing customers’ personal information. The Regulations further require that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

The Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, issued in 2016 by the Central Bank of Nigeria, advise deposit money banks and payment service providers on the implementation of their cybersecurity programmes. This Framework also mandates such entities to appoint a chief information security officer who will be responsible for the day-to-day cybersecurity activities and exposure of the company.

Health sector
Under the National Health Act 2014, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The National Health Act further imposes restrictions on the disclosure of user information and requires persons in charge of health establishments to set up control measures for preventing unauthorised access to information. The National Health Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

Cloud computing
The Nigerian Cloud Computing Policy classifies data into the various categories depending on the sensitivity of the data. The Policy provides that cloud service providers servicing public institutions must comply with the cloud security certification programmes that the Nigerian Government will establish, including ISO 27001 (the international standard that sets out the specification for an information security management system) and ISO 27018 Code of Practice (which deals with the protection of personally identifiable information in public clouds).

In respect of the operations of a cloud service provider, the Policy provides that a cloud service provider must maintain the utmost integrity to protect the data and meet the security requirements set out by the NITDA.

Employment sector
Under the HIV and AIDS (Anti-Discrimination) Act 2014, employers are prohibited from requiring an HIV test as a precondition to an offer of employment, access to opportunities or services, except if an employer is able to demonstrate to the court, on the certification of two competent medical authorities working independently, that the employee’s failure to take a test constitutes a clear and present danger of HIV transmission to others.

14. Trends and Activity
What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

As explained above, on 4 February 2022, the President announced the establishment of the NDPB. The NDPB will, until the substantive data protection regulation is passed, continue to operate within the existing regulatory framework, i.e. the NDPR and the NITDA Implementation Framework. Enacting a substantive Data Protection Bill which will create a regulatory framework for the establishment and administration of the NDPB and related data protection matters is one of the top priorities of the NDPB. Pending the establishment of the framework and the stabilisation of operations, the NITDA continues to regulate data protection in Nigeria on a transitional basis.

Further, while the National Cybersecurity Policy and Strategy proposes the amendment of the Cybercrimes Act, no such amendments have yet been proposed or published.
South Africa

1. Main Laws
At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Data protection is regulated under South Africa's comprehensive data protection statute, the Protection of Personal Information Act 4 of 2013 (POPIA), together with the regulations and guidelines published under POPIA from time to time (including the Regulations Relating to the Protection of Personal Information), as well as the Constitution of the Republic of South Africa (section 14, the right to privacy) and the common law right to privacy.

POPIA became fully enforceable with effect from 1 July 2021. POPIA is applicable to data controllers domiciled in South Africa as well as outside South Africa where means are used to process personal data in South Africa.

Electronic transactions are regulated in South Africa under the Electronic Communications and Transactions Act, 2002 (ECTA) which provides a legal framework to facilitate electronic transactions and communications by regulating electronic records, electronic signatures and the security of electronic records. ECTA also includes provisions on the protection of critical databases. The Regulation of Interception of Communications and Provision of Communication-related Information Act, 2003 regulates the interception and monitoring of communications.

South Africa also regulates cybercrime under the recently enacted Cybercrimes Act 19 of 2020. Most of the provisions of the Act came into effect on 1 December 2021.

Previously, cybercrime was regulated under ECTA, but the relevant provisions of ECTA which dealt with cyber crimes were repealed by the Cybercrimes Act, with effect from 1 December 2021. The Cybercrimes Act introduces a framework for detecting and combating cybercrimes by creating new cybercrime and extending the jurisdiction of and expanding the power of law enforcement agencies to investigate and prosecute cybercrimes.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

Under POPIA, the Information Regulator of South Africa – an independent and impartial authority - is responsible for data protection oversight and enforcement of POPIA. The Information Regulator is headed by a Chairperson.

Cyber inspectors may be appointed under ECTA. A cyber inspector may, amongst other things, monitor and inspect any website or activity on an information system in a public domain and report any unlawful activity to the appropriate authorities.

To date, no cyber inspectors have been appointed. In terms of the Cybercrimes Act, members of the South African Police Service must receive basic training in aspects relating to the detection, prevention and investigation of cybercrime.

The Cybercrimes Act criminalises the unlawful and intentional access to, or interference with, data, a computer program, a computer data storage medium, or a computer system. The Cybercrimes Act also criminalises the unlawful and intentional interception of data, any act of cyber fraud and malicious communications.

South Africa does not currently have a comprehensive cybersecurity law and cybersecurity is addressed under a number of different laws. South Africa adopted the National Cybersecurity Policy Framework in 2012, which sets out the measures and mechanisms for coordination of cybersecurity across government.

South Africa signed the Budapest Convention on Cyber Crime in November 2001 but is yet to sign or ratify the AU Convention on Cybersecurity and Personal Data Protection.
collaboration for cybersecurity incidents. It is also established to promote a coordinated approach to cybersecurity including incident coordination, information sharing, awareness building, sector computer security incident response team establishment, and creation and promotion of national standards.

It was intended that a Cybersecurity Response Committee would be established to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters; however, this legislation did not progress through the South African legislative process.

A National Cybersecurity Advisory Council has been established which, amongst other things, develops an annual report on cybersecurity risk assessment measured against international best practices.

3. Recognition of Personal Data

What is the definition of personal data and/or sensitive personal data?

Personal data is referred to as “personal information” under POPIA and includes information relating to both an identifiable, living natural person and, where applicable, an identifiable existing juristic person or legal entity. This includes information about a person’s race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, and religion, as well as information relating to the education, medical, financial, criminal or employment history of a person, any identifying number, symbol, address or online identifier, the biometric information of the person, the personal opinions, views or preferences of the person, and correspondence sent by the person.

POPIA also refers to “special personal information” i.e. sensitive personal data, which includes all information relating to a person’s religious, philosophical beliefs, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour.

4. Critical Information Infrastructure and Databases

ECTA applies to critical database administrators and critical databases i.e. a collection of data that is declared by the Minister of Communications to be of importance to the protection of the national security of South Africa or the economic and social well-being of its citizens. In terms of ECTA, the Minister may publish the requirements for the registration of critical databases and the procedures to be followed for such registration, as well as the minimum standards or prohibitions in respect of access to, transfer and control of critical databases, infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data, procedures and technological methods to be used in the storage or archiving of critical databases, and disaster recovery plans in the event of loss of critical databases.

To date, no such standards or prohibitions have been published. In terms of ECTA, audits may be performed at a critical database administrator to evaluate compliance, either by a cyber inspector or independent auditor.

5. Collection and Processing

Are there any specific requirements applicable to the collection and processing of data?

In terms of POPIA, personal data must be processed lawfully and in a reasonable manner that does not unnecessarily infringe on the privacy of the data subject. Personal data may only be processed if, given the purpose for which it is processed, the processing is adequate, relevant and not excessive. The justified bases on which personal data may be processed include, amongst others, if the person to whom the personal data relates consents to such processing (where consent must be a voluntary, specific and informed expression of will), or if the processing protects a legitimate interest of the data subject or it is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied.

The processing of sensitive personal data, including the transfer of that information to third parties, is prohibited unless consent has been obtained from the data subject (or as otherwise specified in POPIA).

6. Requirement for Data Localisation

What are the data localisation requirements (if any) i.e. does data have to be stored locally?

There are no specific data localisation requirements applicable in South Africa, although cross-border restrictions are imposed under POPIA.

The Minister of Communications and Digital Technologies published a Draft National Data and Cloud Policy for public comment on 1 April 2021. The Draft Policy suggests that new data localisation requirements will be introduced in terms of which a copy of all data generated in South Africa will need to be kept in South Africa. If these policy proposals are adopted, this will probably result in some amendments to POPIA to give effect to the policies.

7. Cross-Border Transfers

What are the requirements for the cross-border transfers of data (if any)?

POPIA includes specific provisions regarding the transfer of personal data across borders to countries outside of South Africa. POPIA provides that a data controller may only transfer personal data about a data subject to a third party in a foreign country if:

- the recipient is subject to a law, binding corporate rules, or contract which upholds principles of reasonable processing of the information that are substantially similar to the principles contained in POPIA; and includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- the transfer is for the benefit of the data subject and it is reasonably practicable to obtain the consent of the data subject to that transfer; and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

8. Registration and/or Notification

What are the registration and/or notification requirements (if any)?

There are no specific registration or notification requirements for the processing of personal data, although prior authorisation is required with regard to certain limited categories of processing under POPIA. For example, prior authorisation is required for processing which relates to the cross-border transfer of special personal information or personal information concerning children (to a third party in a foreign country that does not provide an adequate level of protection).

Prior authorisation is also required for the processing of any unique identifiers of data subjects where this is processed for a purpose other than the one for which the identifier was specifically intended at collection, and with the aim of linking the information together with information processed by other data controllers. The Guidance Note on Applications for Prior Authorisation, published by the Information Regulator on 1 March 2021, provides guidance on the completion of the relevant application form, the manner of submission and the proposed timelines for the processing of applications.

In terms of POPIA, information officers must be registered with the Information Regulator prior to taking up their duties under POPIA.

While the relevant Minister may determine the requirements for the registration of critical databases under ECTA, no such requirements have yet been determined.
9. Data Protection Officers
Is a data protection officer required and, if so, what are the key responsibilities?

A data protection officer (referred to in POPIA as an “information officer”) is a requirement for both public and private bodies, although an information officer may delegate its responsibilities to a deputy information officer. Information officers are, by virtue of their positions in an organisation, appointed automatically e.g. the Chief Executive Officer of a private body will automatically be appointed as the information officer for that private body (but may authorise another person to act as the information officer).

As discussed above, information officers, and deputy information officers, must be registered with the Information Regulator. The Information Regulator published a Guidance Note on Information Officers and Deputy Information Officers on 1 April 2021. This Guidance Note includes, amongst other things, practical details on the procedure for registering information officers. Whilst the Guidance Note encourages registration via the online registration portal, many technical difficulties were experienced with this platform at the time of construction. Manual registrations are accordingly now recommended, with registration forms to be sent to a dedicated email address.

10. Security Requirements
What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

A data controller is required under POPIA to ensure that it has implemented sufficient security measures to ensure the integrity and confidentiality of the personal data that it processes. This requires the data controller to take appropriate and reasonable technical and organisational measures to prevent the loss, damage to, or unauthorised destruction of personal information and the unlawful access to or processing of personal information. In this regard, the data controller is required to take reasonable measures to: (1) identify all reasonably foreseeable internal and external risks to personal data in their possession or under their control; (2) establish and maintain appropriate safeguards against the risks identified; (3) regularly verify that the safeguards are effectively implemented; and (4) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The data controller is also required to have due regard to generally accepted information security practices and procedures that may apply to it generally or be required in terms of specific industry or professional rules and regulations.

In terms of the regulations published under POPIA, an information officer is required to ensure that a personal information impact assessment is carried out to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal data. A data controller must also, in terms of a written contract between the data controller and the processor, ensure that the processor processes personal information in accordance with the security measures required under POPIA.

In general, ECTA does not impose positive obligations on corporate entities to prevent cybercrime. However, in the financial services sector, in terms of the Banks Act, read with Prudential Authority Directive 2/2019, banks, controlling companies and branches of foreign institutions must comply with the following proactive compliance requirements:

• establish and maintain robust governance structures, which include coverage of IT, to ensure adequate management and operational oversight over critical business functions, resources and infrastructure; and
• implement a sufficiently robust incident management framework to manage and report IT and cyber incidents.

The Prudential Authority and Financial Sector Conduct Authority have also recently published a Joint Standard on Cybersecurity and Cyber Resilience Requirements for consultation, which sets out the minimum standards for sound practices and processes of cybersecurity and cyber resilience for categories of specified financial institutions. The draft Joint Standard seeks to ensure that these financial institutions implement processes and have tools and technology which will prepare them for cyber-attacks as well as respond to and recover from such attacks.

Further, the King IV Report requires the board of a company to monitor the security of information continually and to exercise ongoing oversight of technology and information management. Furthermore, the King IV Report requires that the board proactively monitor intelligence to identify and respond to incidents, including cyberattacks, and manage the performance of, and risks pertaining to, third-party and outsourced services.

11. Data Breach
What are the data breach notification requirements (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

There is a general data breach notification obligation under POPIA. Under POPIA, where there are reasonable grounds to believe that a data subject’s personal information has been accessed or acquired by an unauthorised person, the data controller must notify the Information Regulator and the data subject, unless the identity of the data subject cannot be established.

This notification must be made as soon as reasonably possible after the discovery of the data breach. The data controller may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Information Officer determines that notification will impede a criminal investigation by the public body concerned.

The notification to the data subject must be in writing and must contain enough information to allow the data subject to take protective measures against the breach. The Information Regulator may also tell a data controller to publicise the fact of any security compromise if it believes that such publicity would protect a data subject who has been affected by the security compromise.

A data processor is required to notify the data controller immediately where there are reasonable grounds to believe that the personal data of the data subject has been accessed or acquired by an unauthorised person.

In the financial services sector, in terms of Directive 2/2019, the Prudential Authority has implemented minimum reporting requirements for banks, controlling companies and branches of foreign institutions in terms of material IT and cyber incidents. The classification of materiality must be performed in accordance with the bank’s risk profile, based on the nature, size and complexity of its business. In accordance with the Banks Act, 1990, banks are required to:

• comply with the reporting requirements in relation to material IT and/or cyber incidents including: (i) completing a prescribed IT and/or cyber incident Form at various stages of the process of remediating an IT and/or cyber incident, and submitting this form to the Prudential Authority; (ii) submitting a root cause and impact analysis report, with available information, to the Prudential Authority within 14 calendar days from the date of submission of the IT and/or Cyber Incidents Form; and (iii) submitting further updates to the Prudential Authority on agreed timelines;
• establish and maintain robust governance structures, which include coverage of IT, to ensure adequate management and operational oversight over critical business functions, resources and infrastructure;
• implement a sufficiently robust incident management framework to manage and report IT and cyber incidents; and
• notify the Prudential Authority, as soon as practically possible, but not later than one day, following the discovery of a material IT and/or cyber incident.

There are no other sectors with enhanced responsibilities in relation to cybercrime, although the Cybercrimes Act imposes an obligation on electronic communications service providers or financial institutions that are aware, or that become aware, that their computer system is involved in the commission of any category or class of offences to report the offence to the South African Police Service within 72 hours of having become aware of the offence and to preserve any information that may assist law enforcement agencies investigating the offence. Such entities will be liable for any failure to report cybercrimes committed using their services (with a fine of up to ZAR 50,000), although this obligation must not be interpreted as imposing an obligation on an electronic communications service provider or financial institution to monitor the data that it transmits or stores, or to actively seek facts or circumstances indicating any unlawful activity.
12. Enforcement and Sanctions

What are the key enforcement and sanctions provisions?

The Information Regulator is responsible for the investigation and enforcement of POPIA. The Information Regulator may conduct assessments, on its own initiative or upon request, of a public or private body in respect of the processing of personal information by that body. In addition, the Information Regulator is empowered to receive and investigate complaints on alleged violations of the provisions of POPIA. The Information Regulator may issue enforcement notices requiring that the data controller take specific steps or refrain from taking such steps, or to stop processing personal information in the manner set out in the notice.

POPIA provides for various criminal offences, such as a failure to comply with an enforcement notice or for making false statements. Penalties for criminal offences include a fine or imprisonment of up to 12 months and 10 years. The Information Regulator may also issue administrative fines of up to ZAR 10 million.

The Cybercrimes Act provides for sentencing for specific contraventions of the Cybercrimes Act; for example, if a court convicts a person of being in possession of data which has been unlawfully intercepted, such person will be liable to a fine or to imprisonment for not more than 5 years.

13. Sectoral Issues

Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Communications sector

In addition to the provisions of POPIA, the Electronic Communications Act 2005 and its regulations include various data protection provisions regarding the privacy and confidentiality of subscribers’ personal data.

Health sector

In addition to the provisions of POPIA, there are various data protection provisions in the applicable health legislation regarding the privacy and confidentiality of patients’ personal data. The National Digital Health Strategy for South Africa 2019-2024 also provides for the development of new regulations focusing on data protection, data sharing between private and public sectors, as well as cybersecurity and also provides for the establishment of a cybersecurity policy that will include developing the required leadership capacity and decision-making structures in order to build effective threat assessment and mitigation strategies as part of the Strategy’s implementation.

Financial sector

In addition to the provisions of POPIA, and the data breach obligations set out above, South Africa’s financial sector legislation includes various data protection provisions regarding the privacy and confidentiality of customers’ personal data. The South African Reserve Bank has also issued a Directive and Guidance Note on Cloud Computing and Offshoring of Data (Directive 03/2018) which is applicable to all banks, controlling companies, branches of foreign institutions and auditors of banks or controlling companies. In terms of this Directive, banks are required to put in place a formally defined and board approved data strategy and data governance framework and must also ensure that their risk and control frameworks, including their application, are designed and operating effectively to manage risks associated with the use of cloud computing and/or the offshoring of data.

14. Trends and Activity

What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system and, to date, enforcement action has not been actively pursued.

The Information Regulator has published draft codes of conduct (for, among others, banks and the credit sector) for public comment. These codes of conduct are developed for the purpose of setting out the manner in which the conditions for the lawful processing of personal information are to be applied or compiled within particular sectors. It is expected that additional sectors will develop such codes of conduct in due course.

The Cybercrimes Act was signed by the President and published in the Government Gazette on 1 June 2021 and most of its provisions came into force with effect from 1 December 2021. It is expected that a further bill will be published in due course specifically in relation to cybersecurity matters.

The Minister of Communications and Digital Technologies published a Draft National Data and Cloud Policy for public comment on 1 April 2021. The Draft Policy suggests that new data localisation requirements will be introduced in terms of which a copy of all data generated in South Africa will need to be kept in South Africa. The Draft Policy also suggests that some limited data sovereignty requirements will be introduced in terms of which certain “critical infrastructure data” (which is not defined) will need to be stored only in South Africa. If these policy proposals are adopted, this will probably result in some amendments to POPIA to give effect to the policies.
1. Main Laws
At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Tanzania does not currently have a comprehensive data protection law, but data protection provisions are included in the Constitution of the United Republic of Tanzania (in Article 16), which guarantees the right to privacy, and in the Electronic and Postal Communications Act, 2010 (EPOCA) which, amongst other things, guards against the violation of a person’s private communications, including electronic communications (although under the EPOCA Regulations, 2017, state law enforcement organs are authorised to tap into private telecommunications for purposes of investigation after obtaining a warrant). Tanzania’s data protection requirements are also located in certain sector-specific legislation.

Electronic transactions, cybercrime and cybersecurity are all dealt with under the Electronic Transactions Act, 2015 (ETA), EPOCA and the Cybercrimes Act, 2015. The Cybercrimes Act aims to criminalise offences related to ICT and computer systems and, for example, provides that it is an offence to access or cause a computer system to be accessed without permission. It is also an offence to intentionally and unlawfully remain in a computer system or continue to use a computer system after no longer being allowed to do so. The Cybercrimes Act further prohibits the interception of personal communications and the interference with data by damaging, deleting, altering, obstructing and interrupting it. Further, the Cybercrimes Act prohibits operators and other service providers from monitoring activities or data being transmitted in their systems. This Act was unsuccessfully challenged in the case of Jamii Media Company Ltd v Attorney General and Another [2017] TLS LR 447 on the grounds that several provisions allow law enforcement to search and seize computer systems, data and information without a court order, eroding the constitutional right to privacy. Tanzania does not currently have a National Cyber Security Strategy.

Tanzania is yet to sign or ratify the AU Convention on Cyber Security and Personal Data Protection or the Budapest Convention on Cyber Crime, although it is a member of the Global Forum on Cyber Expertise.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

At present there is no dedicated data protection regulator in Tanzania.

Instead, the specific sectoral authorities (where applicable) administer the data protection provisions e.g. the Tanzania Communications and Regulatory Authority (TCRA) is empowered to ensure the enforcement of EPOCA, while the Bank of Tanzania is responsible for the Banking and Financial Institutions Act. The Cybercrimes Act is enforced by the criminal law authorities of the government.

The TCRA has established the Tanzania National Computer Emergency Response Team (TZ-CERT), under EPOCA, which is responsible for ensuring high and effective network and information security, coordinating and responding to cybersecurity incidents at the national level, and protecting people against abuse and other risks related to ICT by responding to computer emergencies and dealing with security risks.

3. Recognition of Personal Data
What is the definition of personal data and/or sensitive personal data?

There is no definition of personal data or sensitive personal data under Tanzanian law. However, the EPOCA Investigation Regulations, 2017 define the term “data” in relation to any communication as any information identifying or purporting to identify any person.

4. Critical Infrastructure and Databases
In terms of the Cybercrimes Act, the Minister responsible for Information and Communication Technology may designate a computer system as critical information infrastructure (assets, devices, computer systems or networks, physical or virtual, which may affect national security or the economy and social well-being of citizens if incapacitated). The Minister may also prescribe guidelines for, amongst other things, the registration, protection or preservation of critical information infrastructure; access to, transfer and control of data in any critical information infrastructure; and disaster recovery plans in the event of loss of the critical information infrastructure.
The Cybercrimes Act also sets out offences relating to critical information infrastructure.

5. Collection and Processing

Are there any specific requirements applicable to the collection and processing of data?

As a general rule, consent is required in order to collect personal data. There are also legal obligations under various sector-specific laws regarding the collection of personal data in those sectors.

6. Requirement for Data Localisation

What are the data localisation requirements (if any)?

There are no data localisation requirements in Tanzania at present.

7. Cross-Border Transfers

What are the requirements for the cross-border transfers of data (if any)?

There are currently no laws governing cross-border data transfers that are applicable in Tanzania.

8. Registration and/or Notification

What are the registration and/or notification requirements (if any)?

At present, there are no registration and/or notification requirements for data controllers or processors in Tanzania.

9. Data Protection Officers

Is a data protection officer required and, if so, what are the key responsibilities?

At present, there is no requirement for the appointment of a data protection officer in Tanzania.

10. Security Requirements

What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

There are currently no specific requirements applicable to the security of data and no risk assessment or privacy impact assessment is required.

However, the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018, developed by the TCRA, require internet service providers, telecommunications operators and other service providers to provide a secure environment against information security threats. The term “information security” means the administrative and technical measures taken to ensure that data is only accessible to those who are entitled to use it.

11. Data Breach

What are the data breach notification requirements (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

There are currently no specific data breach notification requirements in Tanzania and no specific measures are imposed in operators of critical infrastructure or databases.

12. Enforcement and Sanctions

What are the key enforcement and sanctions provisions?

Under the Cybercrimes Act, accessing or causing a computer system to be accessed without permission is an offence punishable by at least one year of imprisonment, a fine of at least three million Tanzanian Shillings, or both. It is also an offence under the Cybercrimes Act to intentionally and unlawfully remain in a computer system or to continue to use a computer system after the expiration of the time which one was allowed to do so.

Intercepting personal communications and interfering with data by damaging, deleting, altering, obstructing and interrupting it is punishable by a fine of between TZS 2 million and 20 million, and three times the value of the undue advantage received by the offender, whichever is greater, or at least three years in prison.

13. Sectoral Issues

Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Communications sector

• The Consumer Protection Regulations provide that a licensee may collect and maintain consumers’ or subscribers’ information where it is reasonably required for business purposes.

• Rule 4 of the Electronic and Postal Communications (Investigation) Regulations, 2017 guard against the violation of any person’s entitlement to respect and protection of his person, his privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications. Further, rule 6 of the Electronic and Postal Communications (Consumer Protection) Regulations, 2018 sets out certain restrictions under which customer’s information may be collected and used by licensee companies e.g. where it is reasonably required for business purposes. These regulations provide further that the collection and maintenance of information on individual shall be fairly and lawfully collected and processed, processed for identified purposes, accurate, protected against improper or accidental disclosure, and not transferred to any other party other than as permitted by the consumer or under any permission of approval or the TCRA.

• Under the EPOCA (Online Content Regulation), 2020 an obligation is imposed on online content providers to use passwords to protect any user equipment, access equipment or hardware to prevent unauthorised access or use by unintended persons and the use of moderating tools to filter prohibited content.

• The EPOCA (Investigation) Regulations, 2017 prohibit any person from intercepting any communication at any place in the country except as provided under the Regulations and repeat the right to privacy as set out in the Constitution. However, a person’s communications may be intercepted in certain recognised circumstances e.g. the preservation or protection of national security or the preservation of public safety, economic well-being or interest of the country. Contravention of regulation 6(1) is an offence with a possible penalty of a five million Shillings or imprisonment for not less than one year or both.

Financial sector

• Section 48(1) of the Banking and Financial Institutions Act, 2006 prohibits banks from disclosing their customers’ affairs and information unless required by law. Further, under the Bank of Tanzania (Credit Reference Bureau) Regulations, 2012, credit reference bureaus are prohibited from maintaining any information relating to a borrower’s race, creed, colour, ancestry, ethnic origin, religious or political affiliation, state of health or criminal record except financial fraud or other similar offences.

Health sector

• Rule 4 of the Code of Ethics and Professional Conduct For Medical and Dental Practitioners In Tanzania, 2005 provides that medical practitioners and dentists are required to maintain secrecy and security of client’s private information, use professional judgment and responsibility in sharing the client’s confidential information among colleagues, and ensure that subordinate and any other member of staff observe confidentiality.

14. Trends and Activity

What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system and, at present, enforcement action is not actively pursued.

There have been two failed attempts to enact comprehensive data protection laws in Tanzania: the ZD06 Freedom of Information Draft Bill, and the Draft Data Protection Bill 2014 (which was to be modelled on the SADC Model Law and the EU Directive, but which omitted consent as a condition for processing and was widely criticised). There is now a new Data Protection and Privacy Bill, 2021 which has been published for public consultation. Among other things, the Bill proposes the establishment of a Data Protection Office, a registration requirement for data controllers and data processors, the regulation of the collection and processing of personal data, restrictions on the transfer of personal data and the creation of data subject rights regarding, inter alia, access, rectification, data portability and transmission.
UGANDA

1. Main Laws
At a high-level, what are the main privacy, data protection, cybercrimes, cybersecurity and/or data breach notification legislation and/or regulations?

Data protection in Uganda is regulated under the Data Protection and Privacy Act, 2019 (DPPA), read with the Data Protection and Privacy Regulations, 2021 (Regulations). The DPPA supplements the constitutional right to privacy in the Constitution of the Republic of Uganda (Article 27, which prohibits interference with the privacy of a person’s home, correspondence, communication or other property). The DPPA regulates the collection, processing, use and disclosure of personal data and applies to any person, entity or public body in or outside Uganda (although the application to entities outside Uganda is restricted to personal data relating to Ugandan citizens).

Electronic transactions, cybercrime and cybersecurity are all dealt with under the Electronic Transactions Act, 2011 (ETA) and the Computer Misuse Act, 2011. The Computer Misuse Act makes provision for the safety and security of electronic transactions and information systems, the prevention of unlawful access, abuse or misuse of information systems, and making provision for security the conduct of electronic transactions. Computer misuse offences include unauthorised access, unauthorised modification of computer material, unauthorised use or interception of computer services, unauthorised disclosure of information and unauthorised use or interception of a computer service. Uganda has also developed a National Information Security Policy (February 2014) which deals with, amongst other things, information security (including the mandatory minimum security controls that all public and private sector organisations that use, own and/or operate protected computers, handle official communications and personal data must apply to reduce their vulnerability to cyber threats).

The Uganda Communications (Computer Emergency Response Team) Regulations, 2019, which came into effect on 5 July 2019, establish the Computer Emergency Response Team (CERT.UG). The CERT.UG is responsible for managing cyber security incidents in the communications sector and for identifying and protecting critical communications infrastructure. The Regulations also provide for emergency response measures to respond to cyber and any other network threats in the communications sector.

Uganda is yet to sign or ratify the AU Convention on Cyber Security and Personal Data Protection and the Budapest Convention on Cyber Crime. However, Uganda concluded a Memorandum of Understanding, Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Integration Projects Partner States in June 2015, which is a cyber security collaboration framework between Kenya, Rwanda, Uganda and South Sudan, which includes establishing a Northern Corridor CIRT and serves as a collaborative framework to share cyber security information and coordinate incident handling.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

The Personal Data Protection Office (DP Office), in the National Information Technology Authority-Uganda (NITA-U) is the regulator responsible for personal data protection and privacy. However, it is the Ministry of Information Communications Technology and National Guidance which has the mandate to formulate regulations to provide for the accountability and enforcement mechanisms of the data protection law.

The CERT.UG is established under the Uganda Communications (Computer Emergency Response Team) Regulations, 2019 and is a unit within the Ugandan communications regulator, the Ugandan Communications Commission.

Brian Kalule
E: brian.kalule@bowmanslaw.com
3. Recognition of Personal Data
What is the definition of personal data and/or sensitive personal data?
Personal data, as defined in the DPPA, is information about a person from which the person can be identified, such as information relating to nationality, age, martial status, education level, occupation, an identification number or symbol and identity data.
Sensitive personal data is data relating to the religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records of an individual.

5. Collection and Processing
Are there any specific requirements applicable to the collection and processing of data?
The DPPA restricts personal data collection and processing by:
• requiring entities to obtain informed consent prior to personal data collection or processing;
• prohibiting the collection or processing of special personal data unless specifically permitted by law;
• requiring that personal data be collected directly from the data subject, and only for a lawful or specific purpose related to the functions or activities of the data collector or controller;
• requiring data collectors, processors, and controllers to ensure that personal data is complete, accurate, up-to-date and not misleading;
• requiring that further processing of personal data be for a specific purpose related to the purpose for which personal data was collected;
• prohibiting personal data retention for a period longer than necessary to achieve the purpose for which data was collected and processed, unless specifically authorised by the DPPA;
• requiring destruction or de-identification of personal data records at the end of the retention period to prevent reconstruction of personal data in an intelligible form; and
• prohibiting the collection and processing of sensitive personal information other than in certain specific circumstances.

6. Requirement for Data Localisation
What are the data localisation requirements (if any)?
The DPPA and Regulations permit the processing or storage of data outside Uganda provided:
1. adequate measures for the protection of personal data are in place in the country in which the data is processed or stored, at least equivalent to the protections provided under the DPPA;
2. the data subject has consented to the processing or storing of data. Under the Regulations, the DP Office is required to publish a list of countries which meet the criteria of equivalent protections, although this has yet to be done.

7. Cross-Border Transfers
What are the requirements for the cross-border transfers of data (if any)?
In terms of the DPPA, processing or storage of personal data outside Uganda is permitted if:
1. adequate measures are in place in the country in which the data is processed or stored, at least equivalent to the protections under the DPPA; or
2. data subject consent is obtained in a manner and form that takes into consideration the nature of the personal data sought to be processed or stored outside Uganda.

8. Registration and/or Notification
What are the registration and/or notification requirements (if any)?
The NITA-U is authorised to maintain a data protection register of every person, institution or public body that collects or processes personal data, including the purpose of data collection or processing. This register can be accessed by the public for purposes of inspection. These registration requirements are not yet in effect and are pending implementation of regulations to be enacted by the Minister of Information and Communications Technology. The Regulations provide that the register must contain information relating to data collectors, processors and controllers (name and address), including the name of the personal data and the purpose for which the personal data is collected or processed.

9. Data Protection Officers
Is a data protection officer required and, if so, what are the key responsibilities?
Entities or institutions are required to appoint a data protection officer who is responsible for ensuring compliance with the DPPA. The Regulations provide that a data protection officer will be required where the activities 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 where the core activities involve the processing of sensitive personal data. The term “large scale” will be determined based on the number of data subjects, the volume of data, the duration or permanence of the processing, or the geographical extent of the processing. Under the Regulations, the responsibilities of the data protection officer are: to conduct regular assessments and audits to ensure compliance with the DPPA; to serve as a point of contact between the institution and the DP Office; to maintain records of all data processing activities conducted by the institution; and to respond to data subject requests for information and erasure of data.

10. Security Requirements
What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?
The DPPA provides that data controllers, collectors and processors must secure the integrity of personal data in their control or possession by adopting appropriate, reasonable technical and organisational measures to prevent loss and unauthorised destruction, processing or access to personal data. Data controllers are specifically required to use measures that: identify reasonably foreseeable risks to personal data in their possession or control; and maintain appropriate precautions against the risks identified, regularly verify the effective implementation of the precautions and ensure that the safeguards are continually updated in response to new risks and deficiencies.

Data controllers are required to observe generally accepted information security practices and procedures, and specific industry or professional...
11. Data Breach
What are the data breach notification requirements (if any)? Are there specific measures imposed on operators of critical infrastructure or databases?

In terms of the DPPA, it is mandatory for data collectors, controllers and processors to immediately notify NITA-U of any reasonable belief that personal data has been accessed or acquired by an unauthorised person, as well as the remedial action taken. The Regulations set out that the following should be notified: the nature of the personal data breach, the personal data that is the subject of the breach, the categories and approximate number of data subjects affected by the personal data breach, the likely consequences of the personal data breach, the appropriate remedial measures taken or proposed to address the personal data breach, and the name and contact details of the data protection officer.

The DP Office will determine whether the data subject should be notified of the breach and/or whether publicity of the data breach is required.

12. Enforcement and Sanctions
What are the key enforcement and sanctions provisions?

The DPPA empowers the NITA-U to enforce penalties for violations of the Act (e.g. 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) which include remedial orders and requiring compliance with data subject requests. Enforcement is generally triggered by complaints lodged with the NITA-U by aggrieved individuals or by data subjects seeking to enforce rights under the DPPA.

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 award compensatory damages to persons harmed by data collector, controller or processor violations of the DPPA.

There are no specific cybersecurity provisions that are applicable in any sectors.

13. Sectoral Issues
Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Sector specific laws regulate data protection in the context of certain regulated activities.

For example, in the telecommunications sector, the Uganda Communications Act 2013 criminalises privacy violations and provides for the punishment of unlawful interception and disclosure of communications by a service provider. There are no specific provisions regarding the notification of a personal data breach in the health or financial sectors. The National Payment Systems Regulations, 2020, however, do provide in general terms that a payment services provider must collect, process, control and manage personal data in accordance with the DPPA.

There are no specific cybersecurity provisions that are applicable in any sectors.

14. Trends and Activity
What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system and it is expected that enforcement action will be more rigorously pursued going forward.

For example, in February 2021, following an investigation under the DPPA by the NITA-U, Safeboda (a platform that connects motorcycle taxi riders with passengers) was found to have unlawfully shared clients’ data with third parties. NITA-U opted not to impose any penalty but made several recommendations for implementation by Safeboda. Should Safeboda not implement these recommendations, criminal prosecution under the DPPA may be explored.
Zambia has not yet signed or ratified the Budapest Convention on Cyber Crime. In January 2016, Zambia signed (but has not yet ratified) the AU Convention on Cyber Security and Personal Data Protection.

2. Key Regulators
Who are the key regulators, what are their areas of jurisdiction?

The Office of the Data Protection Commissioner (the DPC), within the Ministry responsible for communications, will be responsible for the regulation of data protection and privacy in Zambia. The office of the DPC is yet to be operationalised.

The Zambia Information and Communications Technology Authority (ZICTA) is the regulator responsible for the implementation of the provisions of the Cyber Act and the ECT Act.

The Zambia Computer Incidence Response Term (zmCIRT), established under ZICTA, serves as a central point for collaboration between industry, government and civil society on all cybersecurity related incidents in Zambia.

3. Recognition of Personal Data
What is the definition of personal data and/or sensitive personal data?

The Data Act defines personal data as data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. “Sensitive personal data” is defined as personal data which by its nature may be used to suppress the data subject’s fundamental rights and freedoms and includes: the race, marital status, ethnic origin or sex of a data subject; genetic data and biometric data; child abuse data; a data subject’s political opinions; a data subject’s religious beliefs or other beliefs of a similar nature; whether a data subject is a member of a trade union; or a data subject’s physical or mental health or physical or mental condition.
4. Critical Databases and Infrastructure
The relevant Minister has the power under the Cyber Act to declare information which is of importance to the protection of national, security, economic or social wellbeing of Zambia, to be critical information and any infrastructure containing critical information will accordingly be declared as critical information infrastructure.

The Data Act provides, amongst other things, that any critical information infrastructure must be registered with ZICTA and that any change of ownership will require the prior approval of ZICTA. Further, the Cyber Act requires a controller of critical information infrastructure to annually appoint an information technology auditor to audit the critical information infrastructure and to establish mechanisms and processes, in accordance with published security standards, as are necessary for the detection of a cyber security threat in respect of its critical information infrastructure. ZICTA may also conduct cyber security exercises for the purpose of testing the state of readiness of owners of different critical information infrastructure in responding to significant cyber security incidents at national level.

5. Collection and Processing
Are there any specific requirements applicable to the collection and processing of data?

The Data Act, which provides for the protection of personal data being processed wholly or partly by automated means or by other means other than by electronic means provides, amongst other things, that a data controller or processor must ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
- accurate and where necessary kept up to date;
- stored in a form which permits identification of data subjects for no longer than is necessary;
- processed in accordance with the rights of a data subject; and
- processed in a manner that ensures appropriate security of the personal data.

In terms of the Data Act, a data controller may process personal data where the data subject has given consent (which must be a written, freely given, specific, informed and unambiguous indication of the data subject’s wishes) to the processing or, for example, where the processing is necessary for the performance of a contract or for compliance with a legal obligation. The processing of sensitive personal data is only permitted in very particular circumstances. A data controller is also required to keep and maintain, in writing, a record of processing activities and meta data under its responsibility, and all categories of processing activities carried out.

6. Requirement for Data Localisation
What are the data localisation requirements (if any)?

The Data Act 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 Zambia). There are also proposed restrictions on cross-border transfers of personal data, as discussed below. Further, the Cyber Act requires a controller of critical information to store all critical information on a server or data centre located in Zambia (unless otherwise authorised by the Minister).

7. Cross-Border Transfers
What are the requirements for the cross-border transfers of data (if any)?

Under the Data Act, personal data (excluding sensitive personal data) may be transferred outside Zambia only where the data subject has consented and the transfer is subject to standard contracts or intragroup schemes that have been approved by the DPC or where the Minister has prescribed that transfers outside Zambia is permissible (e.g. where there is an adequate level of protection and the enforcement of data protection laws is effective). OR where the DPC approves a particular transfer or set of transfers as permissible due to a situation of necessity. Personal data may also be transferred outside Zambia in certain other defined circumstances e.g. in the case of an emergency, to a particular person or entity engaged in the provision of health services or emergency services.

A data controller or processor, taking into account the nature, scope and purpose of processing personal data, the associated risks, and the likelihood and severity of harm that may result, implement appropriate security safeguards including:

- (1) maintaining integrity of personal data using methods such as pseudonymisation and encryption;
- (2) ensuring ongoing confidentiality, integrity and implementation of measures necessary to protect the integrity of personal data;
- (3) measures necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data; and
- (4) implementation of appropriate data protection policies. A periodic review of security safeguards will be required.

A data controller must only use data processors providing sufficient guarantees to implement these appropriate technical and organisational measures.

The Data Act further provides that 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.

9. Security Requirements
What are the requirements relating to the security of data (if any)? Is a risk assessment or privacy impact assessment required?

The Data Act requires a data controller or processor to provide guarantees regarding the technical and organisational security measures employed to protect the personal data and must ensure strict adherence to such measures.

A data controller or processor is required to notify to ZICTA within 24 hours of any security breach affecting personal data processed. A data processor will be required to notify the data controller as soon as reasonably practicable of any security breach affecting personal data processed on behalf of the data controller. A data controller or processor must notify the data subject as soon as practicable of any security breach.
Under the Cyber Act a controller of critical information infrastructure is required to report to ZICTA on or after the occurrence of: a cyber security incident concerning such critical information infrastructure and a cyber security incident in respect of any computer or computer system under the controller’s control that is interconnected with or communicates with the critical information infrastructure. A monthly cyber security incident and threat report must also be submitted to ZICTA.

12. Enforcement and Sanctions

What are the key enforcement and sanctions provisions?

There are a number of proposed offences set out under the Data Act for breach by a data controller or processor (for which the penalty is a fine not exceeding two percent of annual turnover of the preceding financial year or to ZMW 600,000), whichever is higher, and under the Cyber Act, e.g. the intentional introduction or spread of malicious software into a computer system (for which the penalty is a fine not exceeding five hundred thousand penalty units or imprisonment for a period not exceeding 5 years).

13. Sectoral Issues

Are there any specific sectoral issues to consider? (e.g. financial data, health data, communications data, educational or school data)

Health sector

Health data is regulated under the Data Act as a category of sensitive personal information. Further, the National Health Research Act No 3 of 2013 (NHRA) regulates health research conducted in Zambia or health research undertaken outside Zambia under the direction of a person or body established in Zambia.

The NHRA requires that written consent of a person participating in health-related research must be obtained. Prior to obtaining the consent, the person must be informed of the objectives of the research and any potential risks or benefits on that person’s health.

Communications section

The telecommunications sector is regulated under ZICTA, which is established by the ICT Act. ZICTA imposes a duty on service providers under its binding Consumer Protection Guidelines not to monitor or disclose or allow any person to monitor or disclose any information of any customer transmitted by the subscriber through the service provider’s system unless as provided under the law.

Financial sector

Banks and financial institutions in Zambia are regulated under the Banking and Financial Services Act (BFSA). The Bank of Zambia is established as the regulator of the sector and may impose sanctions and penalties in the event of contraventions of the applicable sectoral legislation.

The BFSA provides that, subject to the Financial Intelligence Centre Act, 2020, a financial service provider must maintain the confidentiality of information obtained in the provision of a service to a customer (including, for example, the nature, amount or purpose of any payment made by or to a person, or the recipient of a payment made by a person) and must not divulge any information except in accordance with the express consent of a customer, or any other recognised legal grounds e.g. in compliance with a court order or where the interest of the financial service provider requires disclosure.

The BFSA also prohibits banks from disclosing to a third person information regarding the affairs of a customer of a financial service provider that was obtained in the performance of the bank’s functions, unless lawfully required to do so.

14. Trends and Activity

What are the key developments in law, regulatory activity, enforcement, litigation or public attention in this space? (e.g. Is the applicable system developing or highly developed? Is enforcement action pursued actively?)

This is a developing system, and, at present, enforcement action is not actively pursued.
Our Firm

We help our clients manage legal complexity and unlock opportunity in Africa.

We have an enviable track record of providing legal services to the highest professional standards in Africa. We work for clients across numerous African jurisdictions on corporate, finance, competition, taxation, employment, technology and dispute resolution matters.

With eight offices in six African countries and over 400 specialist lawyers, we draw on our unique knowledge of the business and socio-political environment to advise clients on a wide range of legal issues.

Everywhere we work, we offer clients a service that uniquely blends expertise in the law, knowledge of the local market, and an understanding of their businesses. Our aim is to assist clients to achieve their objectives as smoothly and efficiently as possible while minimising the legal and regulatory risks.

Our clients include domestic and foreign corporates, multinationals, funds and financial institutions, across almost all sectors of the economy, as well as state-owned enterprises and governments.

Our expertise is frequently recognised by independent research organisations. Most recently, our Kenyan practice won the 2022 Chambers Africa Award for Law Firm of the Year in Kenya. In 2022, Bowmans won six IFLR Africa Awards including overall M&A Team of The Year; Jurisdictional Firm of the Year: South Africa; Loans Firm of the Year: South Africa; M&A Firm of the Year: South Africa; and Project Finance Firm of the Year: South Africa. We also advised on the deal named M&A Deal of the Year. At the 2022 Africa Legal Awards, we won four practice awards including Banking and Finance Team of the Year; Capital Markets Team of the Year; Tax Team of the Year and Transportation and Infrastructure Team of the Year.

Recognising the size and enormous diversity of Africa, our approach to providing legal services across the continent is intended to offer on-the-ground advice in the countries that matter for our clients. Our presence in Africa is always evolving to meet the changes that are shaping the future of this vast continent.

Currently, we have our own offices in six African countries: Kenya (Nairobi), Mauritius (Moka), South Africa (Cape Town, Durban, Johannesburg), Tanzania (Dar es Salaam), Uganda (Kampala) and Zambia (Lusaka).

We work closely with our Bowmans Alliance firms in Ethiopia (Aman & Partners LLP) and Nigeria (Udo Udoma & Belo-Osagie). These are two of the leading corporate and commercial law firms in their jurisdictions.

We have a special relationship with a competent practitioner in Mozambique. We also have a non-exclusive co-operation agreement with French international law firm Gide Loyrette Nouel that provides our clients access to assistance in francophone west and north Africa. The arrangement provides complementary access for Gide’s clients and lawyers to markets in central, southern and eastern Africa.

On the global front, Bowmans has long-standing and excellent relationships with a range of international law firms with whom we often work on Africa-focused client mandates. We are also a member firm of Lex Mundi, a global association of more than 160 independent law firms in all the major centres across the globe. Lex Mundi gives us the ability to connect our clients with the best law firms in each of the countries represented.
Our Data Protection Services

Our data protection group, which includes lawyers skilled in technology, media, telecommunications, employment and corporate investigations law, regularly advises clients on data protection requirements across Africa.

Our highly experienced lawyers are able to assist clients needing specialist advice on their statutory obligations as well as data protection issues in the context of particular transactions. We conduct reviews of our clients’ business policies, protocols, processes and procedures to ensure compliance with current data protection requirements and new requirements under pending legislation. We help our clients to find practical ways of implementing data protection obligations in their businesses.

Our clients include international financial institutions and banks, telecommunications companies and equipment manufacturers, mining companies, pharmaceutical companies, and retailers.

Specialist services:

• advice on the data processing requirements set out in the applicable laws and the implications for client businesses, including reviewing and preparation of contracts, policies, processes and procedures, and other data protection and privacy controls;
• assistance with the appointment and training of information officers, and their registration with the relevant regulatory authorities;
• training and awareness sessions with employees, in order to ensure compliance with data protection, privacy, incident response and other data processing requirements;
• assistance with conducting impact assessments, the preparation and implementation of compliance frameworks and the development of incident response plans;
• advice to employers in respect of the obligations pertaining to the processing of the personal information of employees;
• representing clients and providing dispute resolution advice;
• advice on the implications of data protection laws on corporate transactions and the obligations arising from ownership, sharing and transfer of personal information;
• advice on the cross-border transfer of personal information and cloud data processing;
• advice on the competition law aspects pertaining to the processing and the use of personal information; and
• advice on data protection concerns in the context of due diligences.

Bowmans’ specialist Cybersecurity and Major Incidents Group provides advice on crisis management and the handling of major incidents that arise from data breaches and the consequences of those breaches. We advise boards on governance surrounding incident response decisioning, reporting obligations and resulting litigation risk exposure.

Key Contacts

CATHY TRUTER
Head of Knowledge Management
Johannesburg, South Africa
T: +27 11 669 9336
E: cathy.truter@bowmanslaw.com

CHLOÈ LOUBSER
Knowledge and Learning Lawyer: Employment & Data Protection
Cape Town, South Africa
T: +27 21 480 7846
E: chloe.loubser@bowmanslaw.com
Cape Town, South Africa  
T: +27 21 480 7800  
E: info-cpt@bowmanslaw.com

Dar es Salaam, Tanzania  
T: +255 76 698 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

Kampala, Uganda  
T: +256 41 425 4540  
E: info-ug@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

Follow us on Twitter:  
Twitter: @Bowmans_Law  
LinkedIn: Bowman-Gilfillan

www.bowmanslaw.com

Alliance Firms:

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

Udo Udoma & Belo-Osagie, Lagos, Nigeria  
T: +234 1 2774920-2, +234 1 2719811-3  
E: uubo@uubo.org