

**Baker
McKenzie.**

「Africa Data Security and Privacy Guide」

Contents

Ghana	4
Kenya	9
Madagascar	14
Mauritius	18
Morocco	24
Nigeria	28
Rwanda	39
South Africa	52
Togo	62
Uganda	65
Zimbabwe	70

Overview

The pandemic drove home the high value of personal data to the global economy, while also highlighting its vulnerability to abuse and attack. In response, governments around the world, including those in Africa, have been reviewing their data privacy and protection laws and regulations.

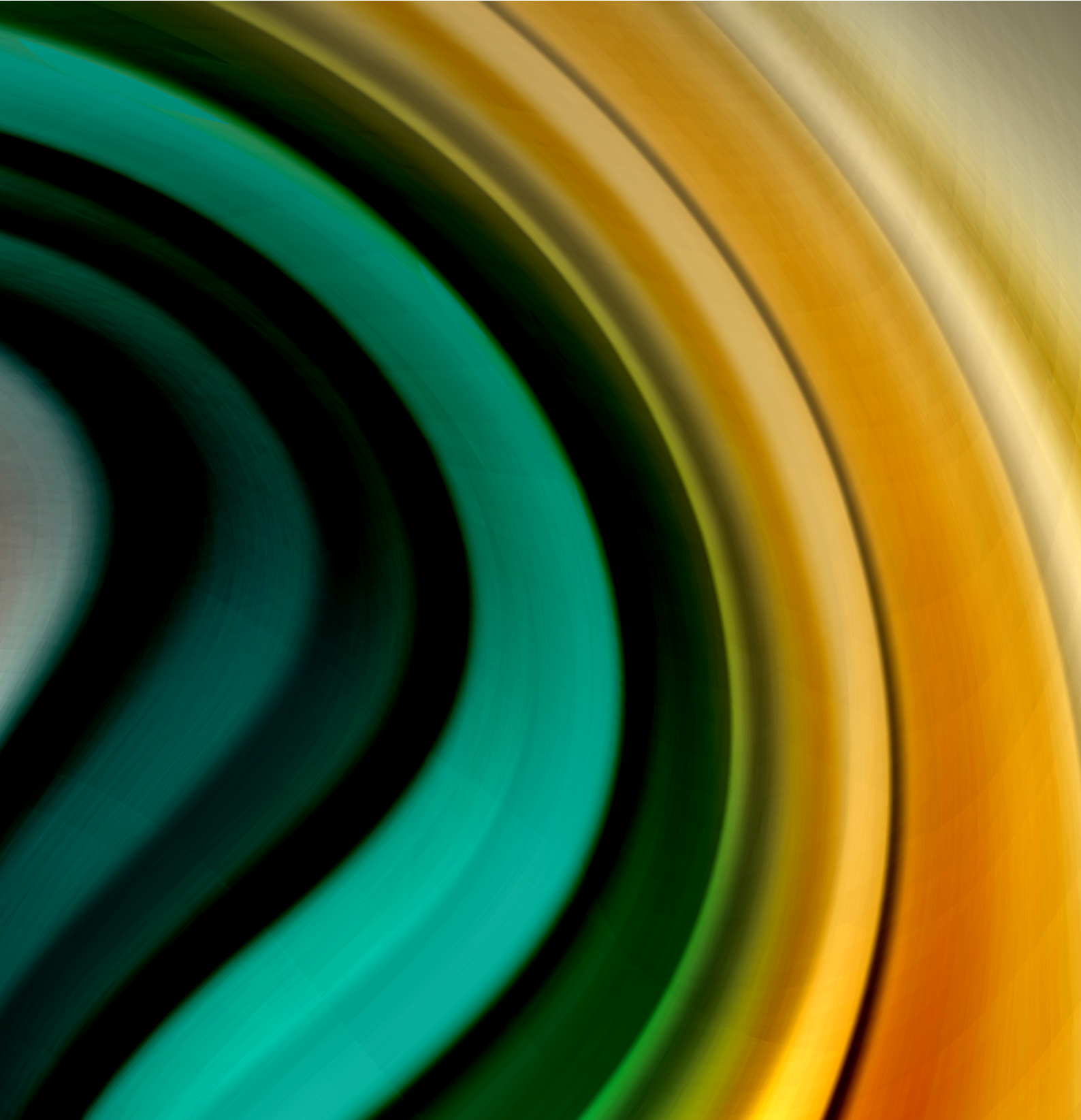
The protection of data in Africa is broadly covered by the Convention of the African Union on Cybersecurity and Personal Data (2014) (Convention), which, at the time of writing, has been ratified by only a small number of the 55 African Union (AU) members - Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal, while 14 countries had signed but not ratified it. South Africa, Kenya and Nigeria have not yet signed the Convention, although all three of these major African economies have privacy laws in place.

Legislation governing the digital economy is essential to protect African citizens in terms of both their digital privacy and security rights, while at the same time ensuring that their online freedoms are not threatened. The AU has been encouraging its member states to sign the Convention and implement balanced local legislation that is fully enforceable and that respects human rights.

To facilitate this process, consultations with stakeholders in government, businesses (local and international) and organisations representing wider society, would ensure a balanced approach during the drafting of these laws. International legislation, such as the European Union's General Data Protection Regulations (GDPR), should be considered alongside local laws, given the borderless nature of the online environment, and consulting with technology experts on policy would allow due consideration to be given to the specific nature of this rapidly developing sector.

Considering the current rapid move to digitally focused business models, the implementation of these legal protections has become urgent. To highlight data security and privacy laws and developments that are already in place, or in progress, across Africa, this comparative guide outlines information on country-specific data privacy and security laws in 11 countries in Africa - Ghana, Kenya, Madagascar, Mauritius, Morocco, Nigeria, Rwanda, South Africa, Togo, Uganda and Zimbabwe.

Ghana



Ghana

What laws currently exist in Ghana to protect and ensure the privacy of data?

In Ghana, data protection is regulated under the Data Protection Act, 2012 (DPA) together with Article 18(2) of the 1992 Constitution, which provides citizens with a fundamental right to privacy.

Are these laws in force?

Yes, these laws are in force.

What are the most recent legal developments, or pending developments, in Ghana around data privacy and protection?

Because data protection is a new area in Ghana, there have not been any recent legal developments. However, we understand that the regulator in Ghana is working on the following:

- Discussions with regulators in other African countries to consolidate and harmonise the data protection laws, and adopt standard data protection laws across the continent due to the emerging discussions on data sovereignty, economization and data localization.
- Pushing data protection certification as an eligibility criterion for running a business in Ghana.
- Discussions with key persons in Ghana to set up a separate data/cyber court to swiftly handle fast growing data breaches and cyber-crime.

Further, the regulator previously published names of persons who were not compliant with the DPA in newspapers, and has recently become more aggressive with enforcement of the DPA.

If Ghana has privacy laws, what constitutes the definition of personal data according to the law?

Under Ghana law, personal data is defined as data about an individual who can either be identified:

- From the data
- From the data or other information in the possession of, or likely to come into the possession of a data controller.

The law further defines special personal data as personal data which consists of information that relates to any of the following:

- The race, colour, ethnic or tribal origin of a data subject
- The political opinion of a data subject
- The religious beliefs or other beliefs of a similar nature, of a data subject
- The physical, medical, mental health or mental condition or DNA of a data subject.
- The sexual orientation of a data subject
- The commission or alleged commission of an offence by a data subject
- Proceedings for an offence committed or alleged to have been committed by a data subject, the disposal of such proceedings or the sentence of any court in the proceedings.

What are the rights of data subjects according to any data privacy law in Ghana?



The rights of data subjects in Ghana are as follows:

- The right to be informed
- The right to give and withdraw consent
- The right of access to personal information
- The right to amend or rectify personal data
- The right to object to the processing of personal data
- The right to prevent processing of personal data for direct marketing
- The freedom from automated decision making
- The right to compensation for breach
- The right to complain to the relevant authorities
- The right to erasure of personal data.

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?



The obligations of a data controller include doing the following:

- Registering with the Data Protection Commission (DPC) and renewing registration every two years
- Implementing appropriate technical and organisational measures
- Implementing data protection policies
- Implementing appropriate security measures
- Appointing a Data Protection Supervisor
- Demonstrating compliance with the DPA and seeking legal advice where required
- Giving instructions to its processors
- Notifying the DPC and data subjects of breaches or compromises.



The obligations of a data processor include the following:

- Processing personal data only on documented instructions from the data controller
- Ensuring that persons authorised to process personal data observe confidentiality
- Taking appropriate security measures
- Respecting the conditions for engaging third party processors
- Assisting the data controller by implementing appropriate technical and organisational measures
- Assisting the data controller in ensuring compliance with the obligations of security of processing
- Deleting or returning all personal data to the controller after the end of the agreement to provide services
- Making available to the controller all information necessary to demonstrate compliance with the data protection laws.

What are the penalties for non-compliance with data privacy law in your country?

- 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 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 both.
- A person who does not comply with the provisions on assessable processing 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 both.
- A person who requires another person to provide a particular record as a condition for the provision of the goods facilities or services to that person 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 both.
- A person who knowingly or recklessly discloses information available to the DPC, which relates to an identifiable person and was not before its disclosure available to the public, commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or a term of imprisonment of not more than five years, or both.
- A person who purchases personal data, knowingly obtains or recklessly discloses personal data 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 both.
- A person who sells or offers to sell personal data of another person commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or a term of imprisonment of not more than five years, or both.
- A person who commits an offence under any data protection regulations enacted by the Minister commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units.
- 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 five thousand penalty units or a term of imprisonment of not more than ten years, or both.

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The data protection regulator in Ghana is the DPC, an independent statutory body established under the Data Protection Act to enforce compliance with the Act.

Does Ghana's data privacy law follow the framework of the EU's General Data Protection Regulations (GDPR)?

Ghana's Data Protection Act was passed in 2012, ahead of the adoption of the GDPR, so it does not expressly follow the GDPR framework. However, the Act regulates the collection and processing of personal data through similar principles provided in the GDPR.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

Although some African countries have implemented laws and regulations to protect personal data, some others offer little to no protection and are yet to implement their own laws.

The AU has adopted the African Union Convention on Cybersecurity and Personal Data Protection (also known as the Malabo Convention), which encourages AU member states to recognise the need to protect critical cyber/ICT infrastructure, personal data and to encourage the free flow of information with the aim of developing a credible digital space in Africa. However, it has not taken effect as only a few countries have ratified it.

In light of the current technological trends and innovations, and digital trade, it is imperative for African countries to implement data privacy and protection policies. African countries must have laws that take care of the local nuances and fit the local context, without simply replicating the provisions of the GDPR and other frameworks.

Enid Baaba Dadzie Solicitor & Barrister

Kimathi Kuenyehia Sr.
kimathi@kimathilegal.com

Akua Serwaa Asomani-Adem
akua@kimathilegal.com

Enid Baaba Dadzie
enid@kimathilegal.com

Mercy Nana Mensah
mercy@kimathilegal.com
+233 (0) 302 770 447

Kimathi & Partners, Corporate Attorneys
Accra, Ghana

Kenya



Kenya

What laws currently exist in your country to protect and ensure the privacy of data?

In 2019, Kenya passed the Data Protection Act (DPA), which is the primary legislation governing the collection and processing of personal data in Kenya. The DPA gives effect to Article 31 (c) and (d) of the Constitution of Kenya, 2010 ("Constitution"), which provides that, "every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed".

The DPA regulates the processing of personal data, provision of rights of data subjects, creation of the obligations of data controllers, as well as establishes the Office of the Data Protection Commissioner (ODPC).

Last year Kenya enacted the Data Protection (Civil Registration) Regulations, 2020 (DPA Regulations), which regulate the processing of personal data by civil registration entities, including the registrars of births, adoptions, persons, marriages and deaths, and entities responsible for issuing passports and any document of identity.

In addition to the DPA and the DPA Regulations, Kenya is also a signatory to the Universal Declaration of Human Rights (UDHR). Article 12 of the UDHR provides that, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour". The same provision is mirrored in Article 17 of the International Covenant on Civil and Political Rights, which Kenya has ratified, and which forms part of the laws of Kenya under the Constitution.

In May 2018, Kenya also ratified the Agreement Establishing the African Continental Free Trade Area (AfCFTA Agreement). Article 15 of the AfCFTA Agreement's Protocol on Trade in Services (the AfCFTA Protocol) provides that member states may adopt and enforce measures necessary to secure compliance with laws or regulations which are not inconsistent with the AfCFTA Protocol, including those relating to the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts. Trading under the AfCFTA began in January 2021.



Kenya also has laws relating to specific sectors that provide for data protection. These include the following:

- Kenya Information and Communications Act, 1998
- Access to Information Act, 2016
- Consumer Protection Act, 2012
- Health Act, 2017
- Health Records and Information Managers Act, 2016
- Banking (Credit Reference Bureau) Regulations, 2020

Are these laws in force?

Yes, all the laws referred to above are in force.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

On 16 November 2020, Kenya appointed its first Data Commissioner who heads the ODPC. Under the guidance of the Commissioner, the ODPC oversees the implementation of the DPA and also ensures that data processors and data controllers comply with their obligations under the DPA.

Under the DPA, the Data Commissioner is empowered to issue guidelines or codes of practice for data controllers, data processors and data protection officers (DPOs). On 24 February 2021, in line with its mandate, the ODPC published the Guidance Notes on Consent and Data Protection Impact Assessment (Guidance Notes) and the Complaints Management Manual (Complaints Manual). Although the Guidance Notes and the draft Complaints Manual have been published on the ODPC's website, they did not undergo public participation, which is necessary under Kenyan law.

Additionally, in April 2021, the ODPC published three sets of draft regulations and invited the public to give their comments. These draft regulations are:

- The Data Protection (General) Regulations, 2021
- The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021
- The Data Protection (Compliance and Enforcement) Regulations, 2021.

It is unclear when the draft regulations will be enacted, but it is anticipated that this will be soon.

If your country has privacy laws, what constitutes the definition of personal data according to the law?

Under the DPA, personal data is defined as, "any information relating to an identified or identifiable natural person".¹

Personal data also includes sensitive personal data, which, under the DPA, is defined as, "data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject".

What are the rights of data subjects according to any data privacy law in your country?

Under the DPA, a data subject has a right to:

- Be informed of the use of their personal data
- Access their personal data, in the custody of the data controller or data processor
- Object to the processing of all or part of their personal data
- The correction of false or misleading personal data
- The deletion of false or misleading personal data about them.²

¹ Section 2 of the DPA.

² Section 26 of the DPA.

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

Under the DPA, the following are the obligations of data controllers and data processors:

- Obtaining consent from data subjects prior to collecting their personal data ³
- Processing personal data in accordance with the principles of data protection ⁴
- Limiting the retention of personal data as much as possible ⁵
- Collecting personal data directly from the data subject and developing policies and practices that ensure that collection of personal data meets the requirements set out in the DPA ⁶
- Registering as a data controller or data processor with the ODPC once the thresholds for mandatory registration are in place ⁷
- Conducting data protection impact assessments prior to carrying out any processing operations where such operations are likely to pose a high risk to the rights and freedoms of data subjects, and submitting the assessment report to the Data Commissioner 60 days prior to the processing of the personal data ⁸
- Complying with any request to restrict personal data issued by a data subject ⁹
- Complying with the requirements on the commercial use of personal data ¹⁰
- Adhering to the restrictions on the processing of sensitive personal data ¹¹
- Reporting data breaches and informing data subjects of such breaches ¹²
- Complying with the requirements applicable to the transfer of personal data outside of Kenya. ¹³

What are the penalties for non-compliance with data privacy law in your country?

Failure to process personal data in accordance with the DPA may, in the case of infringement attract a fine of KES 5,000,000 (approximately USD 45,500) or equivalent to one percent of the annual turnover, whichever is lower. ¹⁴ For offences conducted under the DPA, this may attract a fine of KES 3,000,000 (approximately USD 27,300) or imprisonment for a term not exceeding (ten) 10 years. ¹⁵

The DPA also gives any person who suffers damage (defined as including financial loss and damage not involving financial loss), by reason of a contravention of any requirement under the DPA the right to claim compensation for damage from the data controller or the data processor. Damage is defined as including financial loss as well non-financial loss such as distress. ¹⁶

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The ODPC, headed by the Data Commissioner, oversees the implementation and the enforcement of the DPA. Additionally, the ODPC exercises oversight over data processing operations, either of own motion or at the request of a data subject and verifies whether the processing of personal data is done in accordance with the DPA. ¹⁷

3 Section 30 of the DPA.

4 Section 25 of the DPA.

5 Section 39 of the DPA.

6 Section 28 of the DPA.

7 Section 18 of the DPA.

8 Section 31 of the DPA.

9 Section 34 of the DPA.

10 Section 37 of the DPA.

11 Section 44 of the DPA.

12 Section 43 of the DPA.

13 Section 48 of the DPA.

14 Section 63 of the DPA.

15 Section 73 of the DPA.

16 Section 65 of the DPA.

17 Section 8 of the DPA.

Does your country's data privacy law follow the framework of the EU's GDPR?

Although the provisions of the DPA are similar to those of the GDPR, they are not identical.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

Africa is more connected now than ever to the rest of the world in terms of trade, and the number of foreign entities doing business in Africa continues to increase. The natural consequence of this is that personal data will continue to move across borders. Therefore, it is imperative that data privacy and data protection laws are implemented across the African continent.

With implementation of data protection laws, the resultant effect is that there will be more protections to data subject rights. Additionally, Africa will have more control over those who process personal data of citizens of African countries, both within and outside the continent, limiting what they can do with personal data once collected, and throughout the life cycle of processing personal data.

Furthermore, African countries will be able to exert more influence over the transfer of personal data from African countries, both intra-Africa and inter-Africa. This will ensure that measures are in place to ensure the security of personal data during personal data transfers.

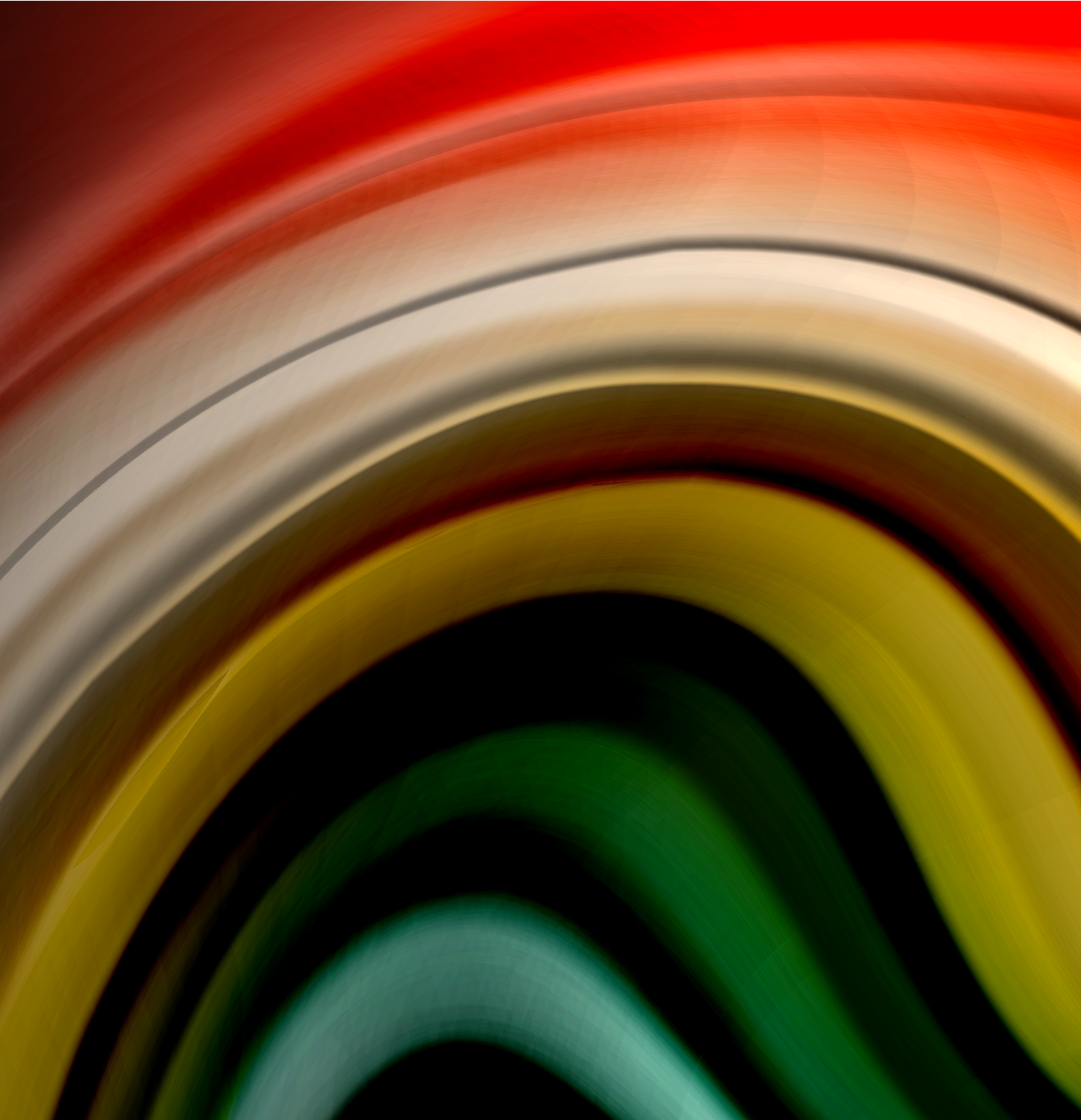
Sonal Sejpal - Partner
ss@africalegalnetwork.com

Jade Makory - Associate
cjm@africalegalnetwork.com
+254 203 640 000

Anjarwalla & Khanna LLP
Nairobi, Kenya



Madagascar



Madagascar

What laws currently exist in your country to protect and ensure the privacy of data?

In Madagascar, the privacy of data is mainly governed by the Law No 2014-038 dated January 9 2015, on personal data protection ("Malagasy Data Protection Law").

The Law No 2014-006, amended and completed by Law No 2016-031 on the fight against cybercrime, also provides for provisions relating to the obligations and responsibilities of operators and carriers of telecommunications and electronic communication services, as well as specific incriminations for breaches of information systems.

Law No 2016-056 also includes provisions relating to the data protection and retention obligations of electronic money institutions.

Are these laws in force?

These laws are in force. However, the Malagasy Data Protection Law and the Law No 2014-006 on the fight against cybercrime do not yet have implementing decrees.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

The adoption of these laws constitutes the most recent data protection reforms in Madagascar.

The adoption of the implementing decrees of the Malagasy Data Protection Law is awaited in order to ensure its efficiency.

If your country has privacy laws, what constitutes the definition of personal data according to the law?

Article 7 of the Malagasy Data Protection Law defines personal data as any information relating to a natural person whereby that person is or can be identified, directly or indirectly, by reference to a name, an identification number or one or more specific elements. These elements are, in particular, physical, physiological, psychological, economic, cultural or social.

What are the rights of data subjects according to any data privacy law in your country?

According to the Malagasy Data Protection law, the rights of data subjects include:

- The right to object to data processing
- The right to access personal data
- The right to rectify one's personal data
- The right to be informed, in particular, of the identity of the data controller, the purpose of the processing, the recipients and, if applicable, the data transfers.

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?



The Malagasy Data Protection Law defines the general principles relating to data and treatment that must be satisfied when personal data is collected and processed, as the following:

- All personal data must be processed in a fair, lawful and non-fraudulent way, explicit and legitimate purposes.
- All personal data collected must be adequate, relevant and non-excessive with regard to the purposes for which it is collected or used.
- All personal data must be accurate and complete and when necessary, kept up to date.
- All personal data must be retained no longer than is necessary for the purposes for which it is processed.
- All personal data must be kept in a form that allows the identification of the data subjects for no longer than is necessary for the purposes for which it is collected or used.

Moreover, the data controller has an obligation to preserve the security of the data and takes all necessary precautions, taking into account the nature of the data and the risks involved.

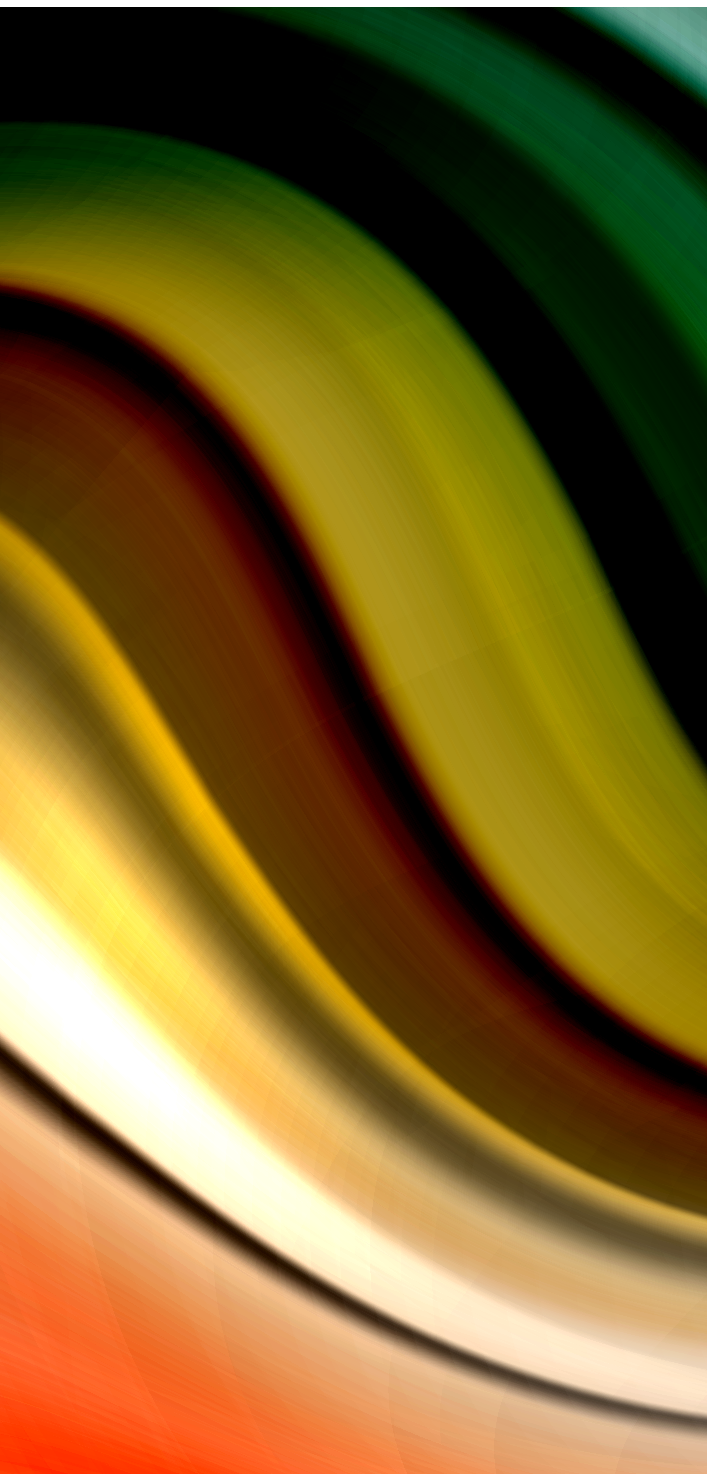
The processing of personal data also requires a prior declaration from the data controller to the national data protection authority - the Commission Malagasy sur l'Informatique et des Libertés (CMIL).

What are the penalties for non-compliance with data privacy law in your country?



In case of non-compliance by the controller with the provisions of the law, the following sanctions may be imposed by the national data protection authority:

- A warning
- An injunction to cease processing or withdrawal of the authorization granted
- A financial penalty.



What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The data protection law provides for the creation of the CMIL, the national data protection authority responsible for ensuring that personal data processing is carried out in accordance with the provisions of the Malagasy Data Protection Law. However, to date, the CMIL has not yet been established.

Does your country's data privacy law follow the framework of the EU's GDPR?

The Malagasy Data Protection Law is based on the 1995 European General Data Protection Directive (95/46/EC). However, as the 1995 European General Data Protection Directive was repealed by the GDPR when adopted in 2018, the Malagasy Data Protection Law is no longer up to date.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

It is essential for African countries, such as Madagascar, to adapt to the evolution of technologies and the new realities of digital development. Indeed, these new issues raise new risks and problems that African countries must imperatively address, and to which they must respond through the adoption of modern and updated regulations.

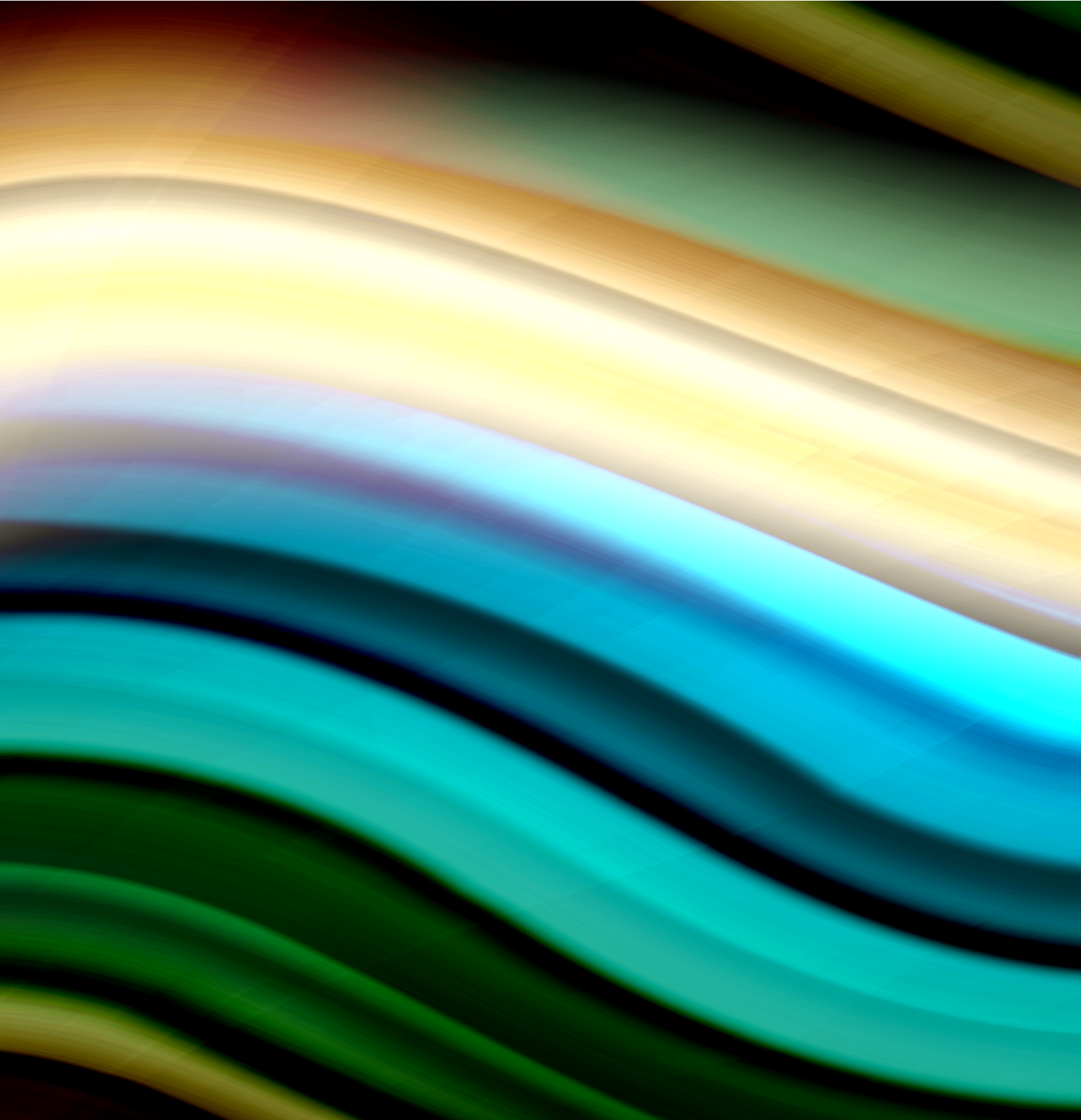
Raphael Jakoba - Managing Partner

Ranty Ambinintsoa - Legal Counsel
conseils@cabinet-mci.com
+261 20 22 295 25

MCI Law Firm – Madagascar
Conseil International
Antananarivo, Madagascar



Mauritius



Mauritius

What laws currently exist in your country to protect and ensure the privacy of data?

The Data Protection Act 2017 ("DPA 2017") which is aligned with international standards, namely the GDPR and the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") was passed on 8 December 2017. Prior to the DPA 2017, there was the Data Protection Act 2004 which was based on the EU Data Protection Directive (Directive 95/46/EC).

Are these laws in force?

Yes, the DPA 2017 came into force on 15 January 2018 and is still in force.

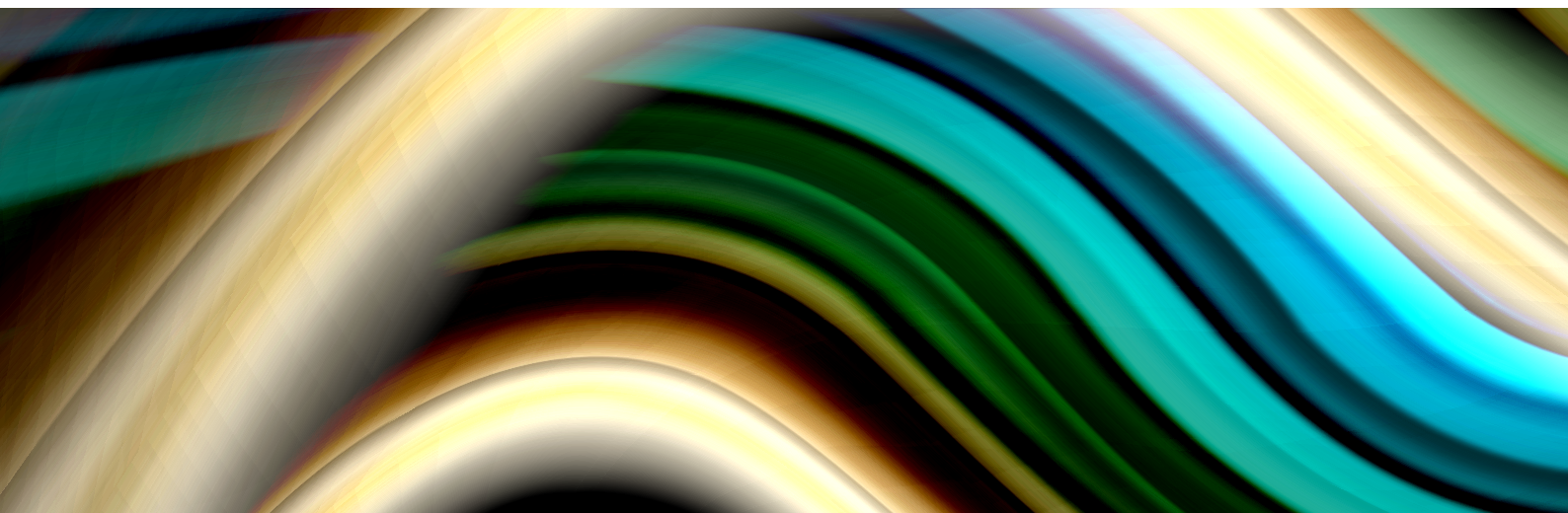
What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

In September 2020, Mauritius signed and ratified the Amending Protocol to the Convention for the Protection of Individuals with regard to the Processing of Personal Data.

If your country has privacy laws, what constitutes the definition of personal data according to the law?

Personal data refers to any information relating to a data subject, i.e., an identified or identifiable individual, in particular by reference to an identifier 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 individual.

The DPA 2017 also makes mention of special categories of personal data (such as personal data pertaining to racial or ethnic origin and, physical or mental health or condition) which are subject to more stringent processing requirements under the DPA 2017.



What are the rights of data subjects according to any data privacy law in your country?



The data subjects have the following rights in Mauritius:

- **Right to be informed:** The controller must inform the data subjects of the categories of personal data that are being processed and the reason for the processing. The data subjects have the right to know to whom their personal data has been disclosed or will be disclosed to. The data subjects are also entitled to know for how long the personal data will be stored.
- **Right to access:** The data subjects may ask the controller, free of charge, for confirmation as whether the controller is processing personal data pertaining to them, and if the controller does, to provide a copy. The controller has one month to comply with such request.
- **Right to object:** Data subjects may, at any time, object in writing to the processing of their personal data unless the controller can demonstrate that there are compelling grounds for the processing which override the data subjects' rights, or the processing is required for the establishment, exercise or defence of a legal claim.
- **Right to correction and erasure:** Data subjects have the right to request the controller to rectify any inaccurate personal data which the controller holds on the data subjects. The data subjects can also request the controller to erase personal data concerning the data subjects if, for example, the purpose of the collection of such data no longer exists, or the data subjects withdraw the consent on which the processing is based and there are no other legal grounds for the processing.
- **Right not to be subject to automated decision-making:** Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects concerning the data subjects or significantly affects the data subjects. This prohibition does not apply if the decision is based on the data subjects' explicit consent.
- **Right to make a complaint:** Data subjects have the right to make a complaint to the DPO if they have concerns with the manner their personal data is being processed. They must be informed of this right at the time of collection of their personal data.

The above rights are available to all data subjects irrespective of nationality or country of residence.

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?



Data Protection Principles:

Both the controller and processor must process personal data in accordance with the following data protection principles:

- Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly and in a transparent manner.
- Purpose limitation: Personal data must be collected for a specified purpose or purposes and not further processed in a way incompatible with those purposes.
- Data minimisation: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Data must not be held more than needed for the purpose(s) the data have been collected.
- Data accuracy: Personal data must be accurate and, where necessary, kept up to date and steps must be taken to erase or rectify personal data without delay.
- Storage limitation: Personal data must not be kept longer than is necessary for the purposes for which the personal data are processed.
- Security: Appropriate security measures must be implemented to prevent unauthorised access to, and the disclosure of personal data. These measures may include encrypting the personal data and regularly testing and evaluating the effectiveness of the measures.
- Accountability: Must take responsibility of what is done with the data and adopt policies and implement measures to be able to demonstrate compliance. If the processor becomes aware of a personal data breach, the processor must notify the controller without undue delay, describing the nature of the personal data breach, including, if possible, the approximate number of data subjects and personal data records concerned.



Data Protection Impact Assessment:

If the data processing operations are likely to result in a high risk to the rights and freedoms of the data subject by virtue of the nature, scope, context and purposes, the controller must, before conducting the processing, carry out an assessment of the impact of the intended processing operations. The assessment must be reviewed if there is a significant change in the data processing operations.

What are the penalties for non-compliance with data privacy law in your country?

A breach of the DPA 2017 constitutes, in certain cases, a criminal offence and, on conviction, the offender may be sentenced to a fine or a term of imprisonment. Examples of non-compliance with data privacy law which constitute a criminal offence under the DPA 2017 are:

- Failure, without reasonable excuse, or refusal to comply with an enforcement notice issued by the Data Protection Commissioner may entail to a fine not exceeding MUR 50,000 and to imprisonment for a term not exceeding 2 years.
- Knowingly providing information which is false or misleading at the time of registration may entail to a fine not exceeding MUR 100,000 and to imprisonment for a term not exceeding 5 years.
- Processing personal data in breach of the DPA 2017 may entail to a fine not exceeding MUR 100,000 and to imprisonment for a term not exceeding 5 years.

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The Data Protection Office (DPO) is a public office created by the DPA 2017 and is under the administrative control of the Data Protection Commissioner (DPC). In the discharge of its functions under the DPA 2017, the DPO acts with complete independence and impartiality and is not subject to the control or direction of any other person of authority.

The DPC is empowered to investigate a complaint that the DPA 2017 or any data protection regulations have been contravened or are being contravened or are likely to be contravened, unless the DPC holds the view that the complaint is frivolous or vexatious.

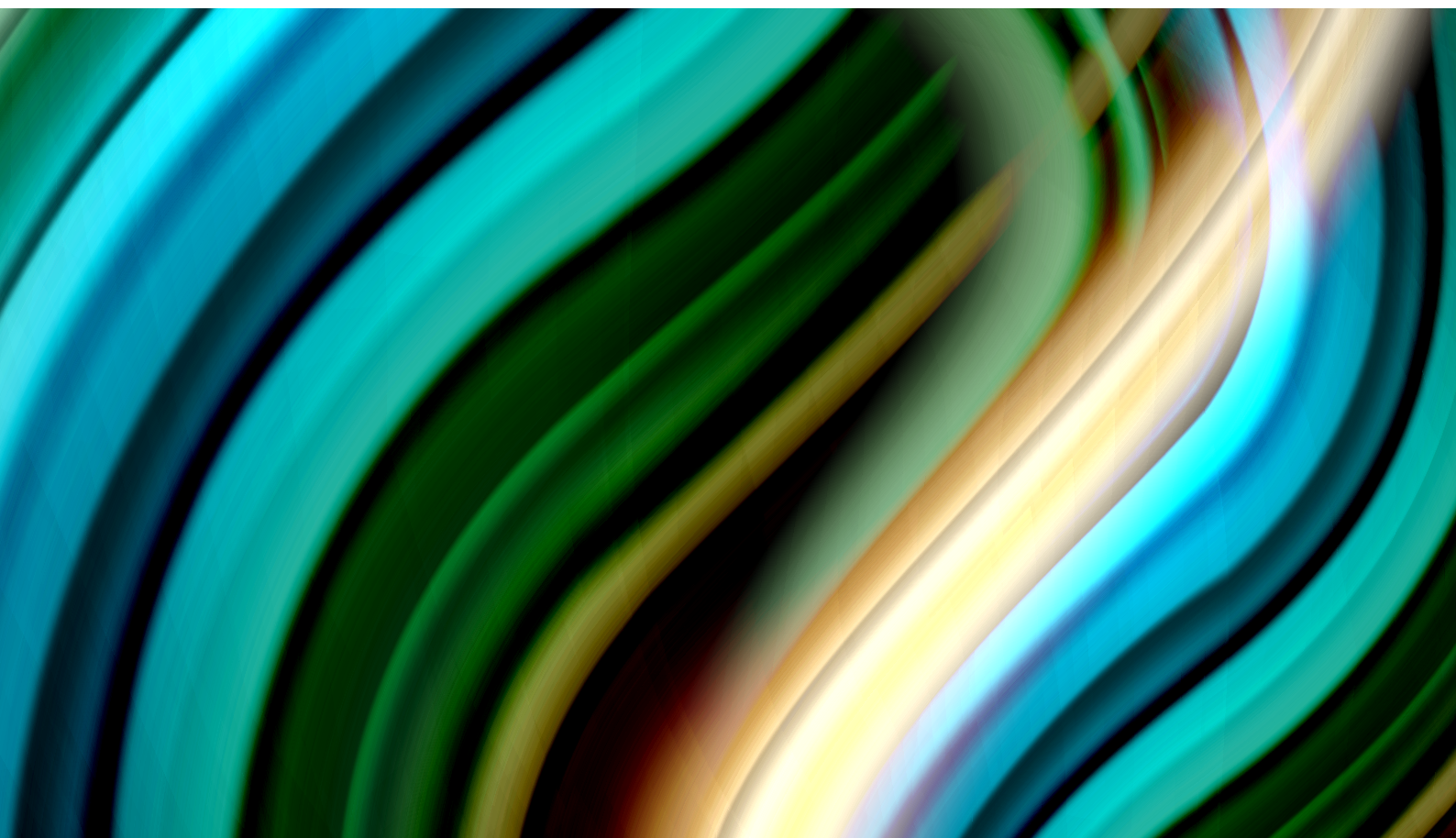
It is noteworthy that by law the DPO must publish an annual report on its activities before the National Assembly of Mauritius not later than three months after the end of every year. The annual report is also published on the website of the DPO. Finally, the DPO, being a public office, it is subject to scrutiny by the Director of Audit and the Public Accounts Committee of the National Assembly.

Does your country's data privacy law follow the framework of the EU's GDPR?

The DPA 2017 is aligned with international standards, namely the GDPR and the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data. However, there are certain instances in the DPA 2017 where the provisions are not the same as contained in the GDPR, for example, the hefty administrative penalties under the GDPR have not been reflected in the DPA 2017. The Mauritian legislator has adopted a criminal regime for sanctioning contravention of the DPA 2017. However, if an individual has suffered prejudice as a result of a breach of the DPA 2017 by a controller or processor, e.g., following a personal data breach, the individual may claim damages or that breach under the law of tort.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

Increasingly, a wide range of activities (economic, political and social) are moving online. In the area of international trade, the use of information and communication technologies is transforming the way business is done and the way people interact amongst themselves. The globalisation and decentralisation of production and distribution have made cross-border movement of personal data crucial for the production and provision of goods and services. To attract foreign investors, in particular, from the European Union, it is imperative that African countries have robust data protection legislation. Data protection is regarded as a fundamental right in the European Union. The cross-border flows of personal data have become essential for international trade. With the ever-increasing push for international trade agreements to have a solid data protection component, it is imperative that African countries implement data privacy and protection legislation.



Ammar Oozeer - Barrister at Law
Ammar.Oozeer@blc.mu

Satyan Ramdoo - Barrister at Law
Satyan.Ramdoo@blc.mu
+230 403 2400

BLC Robert & Associates
Cybercity, Ebene, Mauritius

Morocco



Morocco

What laws currently exist in your country to protect and ensure the privacy of data?

The following laws govern the protection of personal data in Morocco:

- Dahir No. 1-09-15, dated 18 February 2009, promulgating the Law No. 09-08 on the protection of individuals with regard to processing personal data ("Law 09-08")
- Decree No. 2-09-165, dated May 21, 2009, implementing the Law 09-08
- The decisions of the Moroccan data protection authority, i.e. the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) or National Commission for the Protection of Personal Data.

Are these laws in force?

Yes.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

To the best of our acknowledgment there is no recent legal update.

If your country has privacy laws, what constitutes the definition of personal data according to the law?

Personal data is defined by article 1.1 of the Law 09-08 as any information relating to an identified or identifiable natural person (data subject), irrespective of the form or medium of said information, and including sound and images - very close to the definition provided by the GDPR.

What are the rights of data subjects according to any data privacy law in your country?

The rights of data subjects include:

- Access to the data processing information (kind of data, purposes, entities to which data are sent)
- The update, correction, deletion (for legitimate reasons) or locking of data
- The opposition to, for legitimate reasons, the processing of data
- The right of access, which allows the data subject to request that the data controller provide such access at no cost, without constraint and without delay.

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

Under the Law 09-08, a data controller's obligations include:

- Collecting consent to the data processing
- Processing the data loyally, collected for determined, explicit and legitimate purposes and not be diverted from such purposes
- Ensuring that the data is relevant, adequate and not disproportionate to the declared purposes
- Ensuring that the data is accurate and updated
- Ensuring that the data processing has been subject either to prior declaration or prior authorization.

In addition, under the Law 09-08, the data processor is required to take technical and organizational measures in order to comply with data regulation applicable to data processing (against loss, destruction, dissemination or non-authorized access).

What are the penalties for non-compliance with data privacy law in your country?

The penalties against individuals include:

- The withdrawal of authorization to process
- Fines between EUR 1,000 to EUR 20,000 depending on the offence
- Imprisonment of anywhere between three months to one year depending on the offence.

The penalties against companies include:

- The above fines against individuals are doubled when a company breaches the Moroccan data protection laws
- A company can be seized or even shut down by a court order
- A company's legal representatives may be sanctioned if they are personally involved in an offence.

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

Yes, the National Control Commission for the Protection of Personal Data, the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) established by the Law 09-08.

The CNDP enforces the protection of personal data in Morocco (with Moroccan jurisdiction) and issues decisions to help data subjects to better understand their rights, and reinforces data controllers/processors' obligations.

The CNDP has seven members – a president appointed by the King and six members, also appointed by the King, following a proposal by The Prime Minister (two members); by the President of the House of Representatives (two members) and by the President of the House of Councillors (two members).

Does your country's data privacy law follow the framework of the EU's GDPR?

Current data privacy law in Morocco follows the "declarative" framework of the EU Directive n°95/46 which prevailed in Europe before the GDPR was passed.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

Having strong regulation on data protection is nowadays crucial in Africa in general, and specially in Morocco, regarding the exponential rise of data processing due to the use of smartphones and e-commerce this past decade. On the one hand, it ensures the protection of citizens and their fundamental rights. On the other hand, a solid data protection law helps to reassure the foreign investor/interlocutor who wishes to exchange personal data for business purposes.

Having a strong data privacy regulation should be seen by African countries and businesses as a competitive advantage in a globalized word, where local and international data processing is key to gain profitability.



Pierre Deprez – Associate
Pierre.Deprez@bakermckenzie.com

Saad Khaldi – Associate
Saad.Khaldi@bakermckenzie.com
+212 522 77 95 95

Baker McKenzie
Casablanca, Morocco

Nigeria



Nigeria

What laws currently exist in your country to protect and ensure the privacy of data?

The Nigeria Data Protection Regulation 2019 (NDPR) is the principal privacy and data protection legislation in Nigeria. The NDPR was issued by the National Information Technology Development Agency (NITDA) or ("Agency") in January 2019, pursuant to Section 32 of the NITDA Act 2007 as a subsidiary legislation to the NITDA Act 2007. The NITDA Act establishes the Agency, the official government body that develops and regulates information technology in Nigeria. In 2020, NITDA released the NDPR Implementation Framework (NDPRIF) to ensure the effective implementation and enforcement of the NDPR.

Other laws which regulate the use and processing of personal data in Nigeria are as follows:

- The Constitution of the Federal Republic of Nigeria, 1999 (as amended) - It establishes the foundation of data privacy and protection in Nigeria. Section 37 of the Constitution guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. This right is deemed enforceable in the court of law when breached.
- The National Identity Management Commission Act, 2000 - Prior authorisation of the National Identity Management Commission (NIMC) is required before accessing data or information contained in the National Identity Database.¹⁸ Section 5 also mandates the NIMC to ensure security (including cyber-security) of any data collected and stored in the National Identity Database.
- Freedom of Information Act No. 4 of 2011 (FOIA) - the FOIA, mandates public institutions in custody or possession of any information, to make such information available to any person who applies for it, but deny an application for information that contains personal information, unless the individual involved consents to the disclosure, or where such information is publicly available.¹⁹ Also, a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law.²⁰
- The Nigeria Communication Commission Consumer Code of Practice Regulations 2007 – this mandates telecommunication service providers to take measures to ensure customer information is stored securely and protected from improper or accidental disclosure.²¹ Moreover, unless required or permitted by other relevant laws, customer information is not to be transferred to any party.²²
- Cybercrimes Act 2015 – this Act provides a legal and regulatory framework for the prevention, detection, and subsequent punishment of cybercrimes in Nigeria such as identity theft, cybersquatting, hacking etc. Sections 14 and 16 of the Act prohibits dealing with data stored in a computer system or network in a fraudulent manner for fraudulent purposes.

¹⁸ Section 26 NIMC Act 2000

¹⁹ Section 14 Freedom of Information Act 2011/20 Section 39 of the DPA

²⁰ Section 16 Freedom of Information Act 2011

²¹ Section 35(1)(g) Nigeria Communication Commission Consumer Code of Practice Regulations 2007

²² Section 35(1)(h) Nigeria Communication Commission Consumer Code of Practice Regulations 2007

- Child Rights Act 2003 – this Act protects and guarantees the right of every child to privacy, family life, home, correspondence, telephone conversation and telegraphic communications subject to the supervision or control of the parents or guardian.²³
- The National Health Act 2014 – This Act limits the disclosure of the personal data of users of health services in their records and mandates healthcare providers to protect such data.
- The Federal Competition and Consumer Protection Act, 2019 – In the event of investigation carried out by the Federal Competition and Consumer Commission, any information/secret uncovered in any stage of inquiry is protected by this Act.²⁴
- The NCC Registration of Telephone Subscribers Regulations, 2011 – under this regulation, information of telephone subscribers is protected, and records of subscribers stored in the central database or database of licensees are confidential.
- The Central Bank of Nigeria –Act, 2007 – Pursuant to this Act, the Central Bank of Nigeria issued the Consumer Protection Framework, 2016, which requires financial institutions to ensure adequate protection of customer data.

Are these laws in force?

Yes, all of the above referenced laws and regulations are currently in force.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

The most significant development regarding data protection and privacy in Nigeria so far has been the Nigerian Data Protection Regulation, 2019. Prior to the release of the NDPR, Nigerians could only rely on the general provisions of section 37 of the Constitution on privacy, as well as a largely fragmented/sector-specific data protection framework for the enforcement of privacy rights.

The NDPR Regulation successfully provided a body of rules specifically for the protection of personal data and privacy. The regulation explicitly sets out the rights of data subjects, prescribes the development of security measures to protect data, and strengthens the powers of the primary data protection authority called National Information Technology Development Agency (NITDA).

Closely following the issuance of the NDPR, NITDA also issued an Implementation Framework in November 2020, aimed at providing clearer information on the requirements of the NDPR and compliance requirements.

Another notable development on privacy and data protection is the introduction of the Data Protection Bill, 2020. The proposed Bill primarily seeks to establish an effective regulatory framework for the protection of personal data, regulate the processing of information concerning data subjects and safeguard their fundamental rights and freedoms as guaranteed under the Constitution.²⁵

²³ Section 8 Child Rights Act 2003

²⁴ Section 34(6) The Federal Competition and Consumer Protection Act 2019

²⁵ Section 1 of the proposed Data Protection Bill 2020

On applicability, compared to the NDPR, the Bill provides more certainty on the category of persons it covers, as this has been clearly expanded to include: ²⁶

- Data subjects who are citizens of Nigeria
- Data subjects who are ordinarily resident in Nigeria
- Entities incorporated under the laws of Nigeria
- An unincorporated joint venture or association operating in part or in whole in Nigeria
- Any person who does not fall within the above mentioned, but maintains an office, branch or agency through which business activities are carried out in Nigeria
- Foreign entities targeting persons resident in Nigeria.

Also, compared to the NDPR, the category of data covered by the Bill has been expanded to include amongst others, personal subscription data which reveals data subject behaviour, personal banking and accounting records; personal data revealing a data subject's flight reservation or itinerary; student's academic transcripts records; such other categories of data usually processed by service providers and commercial entities as may be determined by the guidelines of the Commission. ²⁷

Furthermore, an independent commission known as the Data Protection Commission, which would help to promote and enforce the provisions of the Bill, data protection in general, as well as advise on international best practices is to be established under the proposed Bill. ²⁸

Most recently in 2021, another significant development has been the Lagos State Data Protection Bill, which seeks to promote the protection of information processed by public and private bodies, and establish minimum requirements for the processing and protection of personal information on a state level. ²⁹ Similar to the Data Protection Bill 2020, the Lagos State Data Protection Bill 2021 seeks to establish a local Data Protection Commission for the enforcement and implementation of provisions of the Bill. ³⁰ Notable provisions include rights of data subjects, ³¹ detailed obligations of data controllers and processors, particularly registration with the Commission, ³² and the conduct of periodic audits of the systems of data controllers and data processors to ensure compliance with data protection principles. ³³

Although there are significant gaps in the current regulations around data protection and privacy, it is interesting to note that Nigeria has made significant strides in the enforcement of the rights of data subjects. Very recently, the NITDA sanctioned an online lending platform for privacy invasion of its clients. This action goes to show that the NITDA is poised to fully enforce the provisions of the NDPR and ensure that the personal information of data subjects is protected.

²⁶ Section 2(3) of the proposed Data Protection Bill 2020

²⁷ Section 2(4) of the proposed Data Protection Bill 2020

²⁸ Section 7(9) of the proposed Data Protection Bill, 2020

²⁹ Preamble to the proposed Lagos State Data Protection Bill 2021

³⁰ Section 3 of the proposed Lagos State Data Protection Bill 2021

³¹ Part VII of the proposed Lagos State Data Protection Bill 2021

³² Section 37(1) and (2) of the proposed Lagos State Data Protection Bill 2021

³³ Section 18 of the proposed Lagos State Data Protection Bill 2021

If your country has privacy laws, what constitutes the definition of personal data according to the law?

Personal data under the NDPR is defined as “any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular, by reference to an identifier 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. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.”³⁴

Personal data under the Data Protection Bill means any information relating to a data subject.³⁵ It includes but is not limited to:³⁶

- Personal and biometric data revealing a data subject’s identity, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership
- Personal banking and accounting records
- Personal data revealing a data subject’s flight reservation or itinerary
- Student’s academic transcripts records
- Personal medical and health records
- Telephone calls, call data records, messages, websites, and other information stored on any electronic device
- Personal subscription data which reveals data subject behaviour.

³⁴ Section 1.3(xix) of the NDPR, 2019

³⁵ Section 2(4) of the Data Protection Bill, 2020

³⁶ Section 2(4) of the Data Protection Bill, 2020

What are the rights of data subjects according to any data privacy law in your country?



The rights of data subjects under Nigerian law include: ³⁷

- The right to information relating to data processing, in writing, and in a manner that is easily understandable
- The right to opt out/withdraw consent to the processing of their personal data at any time
- The right to be informed of the appropriate safeguards for data protection in a foreign country, in the instance that the personal data is being transferred to a foreign country or an international organisation
- The right to have incomplete personal data completed, in relation to data processing
- The right to rectification, erasure, and restitution of inaccurate, false or unlawfully processed personal data, without delay and free of charge from the data controller
- The right to request deletion of personal data at any time
- The right to data portability i.e., the right to receive personal data of a subject from a data controller, in a structured, commonly used and machine-readable format, and furthermore the right to transmit such data to another controller without any hindrance
- The right of to obtain confirmation as to whether personal data of a subject has been processed and the reasons for processing
- The right to be informed of the existence of and logic behind automated decision- making including profiling significantly affecting a data subject
- The right to object at any time to the processing of personal data including for the purposes of direct marketing at no cost.

³⁷ Articles 2-3 of the NDPR, 2019

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

Under the NDPR, data controllers and processors are required to comply with the general requirements of the NDPR on lawful processing, data security, protection of data subject rights, etc.



Specifically, however, the data controller is required to observe the following obligations: ³⁸

- Ensure that consent of a data subject has been obtained without fraud, coercion, or undue influence
- Designate a Data Protection Officer for the purpose of ensuring adherence to the Regulation, and relevant data privacy instruments
- Ensure the processing of personal data is proportionate to the purpose for which it was processed
- Take into consideration the risks arising from the interests, rights and fundamental freedoms of data subjects, according to the nature, volume, scope and purpose of processing the data
- Examine the likely impact of the intended processing of personal data on the rights of data subjects before commencement of such processing
- Only use a data processor who provides sufficient guarantee to implement appropriate technical and organisational measures and ensure the protection of rights of the data subjects
- Design the data processing in such a manner that prevents or minimises the risk of interference with data subject's rights and fundamental freedoms
- Be liable for the processing of personal data carried out on its behalf by a data processor.

Data controllers are also required to send a soft copy of the summary of an audit containing information about processed data to NITDA, where it processes the personal data of more than 1,000 data subjects in a period of six months or submit a summary of its data protection audit to NITDA where it processes the personal data of more than 2,000 data subjects within 12 months by 15 March of the following year.

What are the penalties for non-compliance with data privacy law in your country?

Failure to comply with the NDPR is generally treated as a breach of the NITDA Act, which may attract fines and possible criminal penalties upon conviction. A first offence attracts a fine of NGN 200,000 (approximately USD 360) or imprisonment for a term of one year, or both a fine and imprisonment. Subsequent offences attract a fine of NGN 500,000 (approximately USD 900) or imprisonment for a term of three years, or both. Specifically, the NDPR provides penalties for data controllers who are subject to the regulation and are found to be in breach of the data privacy rights of any data subject. The penalties are as follows:

- 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 of the preceding year or payment of the sum of NGN 10 million (approximately USD 18,020), whichever is greater
- In the case of a data controller dealing with less than 10,000 data subjects, payment of a fine of 1% of the annual gross revenue of the preceding year or payment of the sum of NGN 2 million (approximately USD 3,605) whichever is greater. ³⁹

³⁸ Regulation 4.1 of the NDPR, 2019

³⁹ Regulation 2.10 of the NDPR, 2019

Other penalty provisions in sector specific legislation are:



Credit Reporting Act

- Any person who intentionally or negligently discloses credit information commits an offence and is liable, upon conviction, to a fine of not less than NGN 10 million (approximately USD 18,020). ⁴⁰
- In the instance that the Credit Reporting Act fails to provide a penalty for the contravention of any of its provisions, a fine of not less than NGN 10 million (approximately USD 18,020), or a prison term of 10 years, or both, may be imposed. ⁴¹



National Identity Management Commission Act

- Anyone who unlawfully accesses data or information in the National Identity Database, shall upon conviction be liable to imprisonment for a term of not less than ten years without the option of a fine. ⁴²



Cybercrime Act

- By virtue of Section 38(6), any service provider who breaches the provisions concerning maintenance of traffic data and subscriber information, shall be liable, on conviction, to imprisonment for a term of not more than three years or a fine of not more than NGN 7 million (approximately USD 12,610), or both.

⁴⁰ Section 21 Credit Reporting Act 2017

⁴¹ Section 23 Credit Reporting Act 2017

⁴² Section 28(1)(a) National Identity Management Commission Act, 2007

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

There is no sole appointed agency tasked with the duty to enforce compliance of the data protection or privacy laws, rather there are various authorities, or statutory bodies, authorised by law to act as “Data Protection Authority” in their relevant sectors.

These authorities include:

National Information Technology Development Agency (NITDA)

The NITDA is statutorily mandated by the NITDA Act of 2007 to develop regulations for electronic governance and monitoring of the use of information technology and electronic data.⁴³ Following issuance of the NDPR by NITDA, it is safe to say that NITDA is currently the primary data protection authority in Nigeria, as the Agency is charged with ensuring compliance with data protection requirements under the NDPR. In this regard, NITDA primarily undertakes the following:

- Review of complaints filed, conduct surveillance/investigation to identify any breach, impose administrative sanctions were necessary⁴⁴
- NITDA is expected to set up an administrative redress panel to help with such investigation and facilitate resolution of pending disputes⁴⁵
- NITDA also registers and issues licenses to Data Protection Compliance Organisations (DPCOs), which monitor, and audit Data Controllers on its behalf.

Nigerian Communications Commission (NCC)

The Nigerian Communications Act, 2003 gives the NCC power to act as a data regulator within the telecommunications sector.⁴⁶ The Commission can investigate any matter it deems to be a breach of the provision of the Act and enforce the prescribed sanction.

National Identity Management Commission (NIMC)

Section 5 of the National Identity Management Commission Act mandates the Commission to ensure security (including cyber-security) of any information or data collected and stored in the National Identity Database. In enforcing such regulatory measures, the Commission has power to issue fine or commit to prison anyone found guilty and convicted of a breach of the data protection provisions in Act.⁴⁷

Central Bank of Nigeria (CBN)

The CBN has the overall power within the Nigerian financial services sector to regulate, investigate and subject to the enabling law, sanction banks, financial institutions, and any other licensee for breach of data security requirement.

⁴³ Section 6, NITDA Act 2007

⁴⁴ Article 11 NDPR Implementation Framework, 2020

⁴⁵ Article 4.2 Nigerian Data Protection Regulation, 2019

⁴⁶ Section 3 Nigerian Communications Commission Act, 2003

⁴⁷ Section 5 National Identity Management Commission Act, 2000

Does your country's data privacy law follow the framework of the EU's GDPR?

The NDPR is significantly modelled after the GDPR. Both laws are reasonably similar in terms of rationale and core principles. The NDPR and the GDPR both aim to provide data subjects with a certain level of protection regarding their personal data. The material scope of the laws are consistent, with common definitions and principles on processing of personal data in general.

Some other similar provisions between both laws relate to:

- Requirement of consent of a data subject for processing of personal data
- Provision of obligations for data controllers and data processors
- Both provide for similar rights of data subjects
- Both laws have similar timeframes for report of data breach
- The appointment of a data protection officer is provided for under both laws
- The GDPR require data controllers to report a data breach within 72 hours after becoming aware of such breach. The same provision can be found in the NDPR implementation framework.⁴⁸

Beyond the similarities, both laws also have notable differences. Unlike the NDPR, the GDPR is a more unified framework. Although the NDPR and the Data Protection Bill aim to achieve this goal, Nigeria laws on data protection and privacy are currently not as comprehensive or unified.

Other notable differences in the framework of the two laws include:

- Varied personal and territorial scope of application of the laws. NDPR applies to Nigerian citizens and non-Nigerian residents. However, the GDPR applies to data processing of EU residents by a controller or processor who is not established in the EU.⁴⁹
- Sanctions under the NDPR vary depending on the number of data subjects a company handles. For example, financial penalties can amount of an organisation's annual gross revenue of the preceding year, or of NGN 10 million (approximately USD 18,020), whichever figure is greater, but the organisation handles over 10,000 data subjects. However, under the GDPR national supervisory authorities in Europe can fine an organisation up to 4% of annual gross revenue.⁵⁰
- The NDPR and the GDPR differ in their provisions regarding the responsibilities of supervisory authorities. Unlike the NDPR, which focuses powers on NITDA, the HAGE, and the Administrative Redress, Under the GDPR, it is left to each Member State to establish a supervisory authority.

48 Article 10 NDPR Implementation Framework, 2020

49 Article 33 GDPR, 2019

50 Article 83(5) GDPR, 2019

How imperative do you think it is for African countries to implement data privacy and protection, and why?

It is absolutely imperative that African countries enact comprehensive laws and regulations for protection of personal data and privacy of its citizens. The landscape of trade and commerce has significantly evolved, and technology now allows companies, organisations, public bodies and individuals to make use of data on a large scale to pursue their daily activities. In performing such activities, personal information is made available publicly and globally through the internet. Technological advancements have also revolutionised the economy and social life, thus making more information readily accessible.

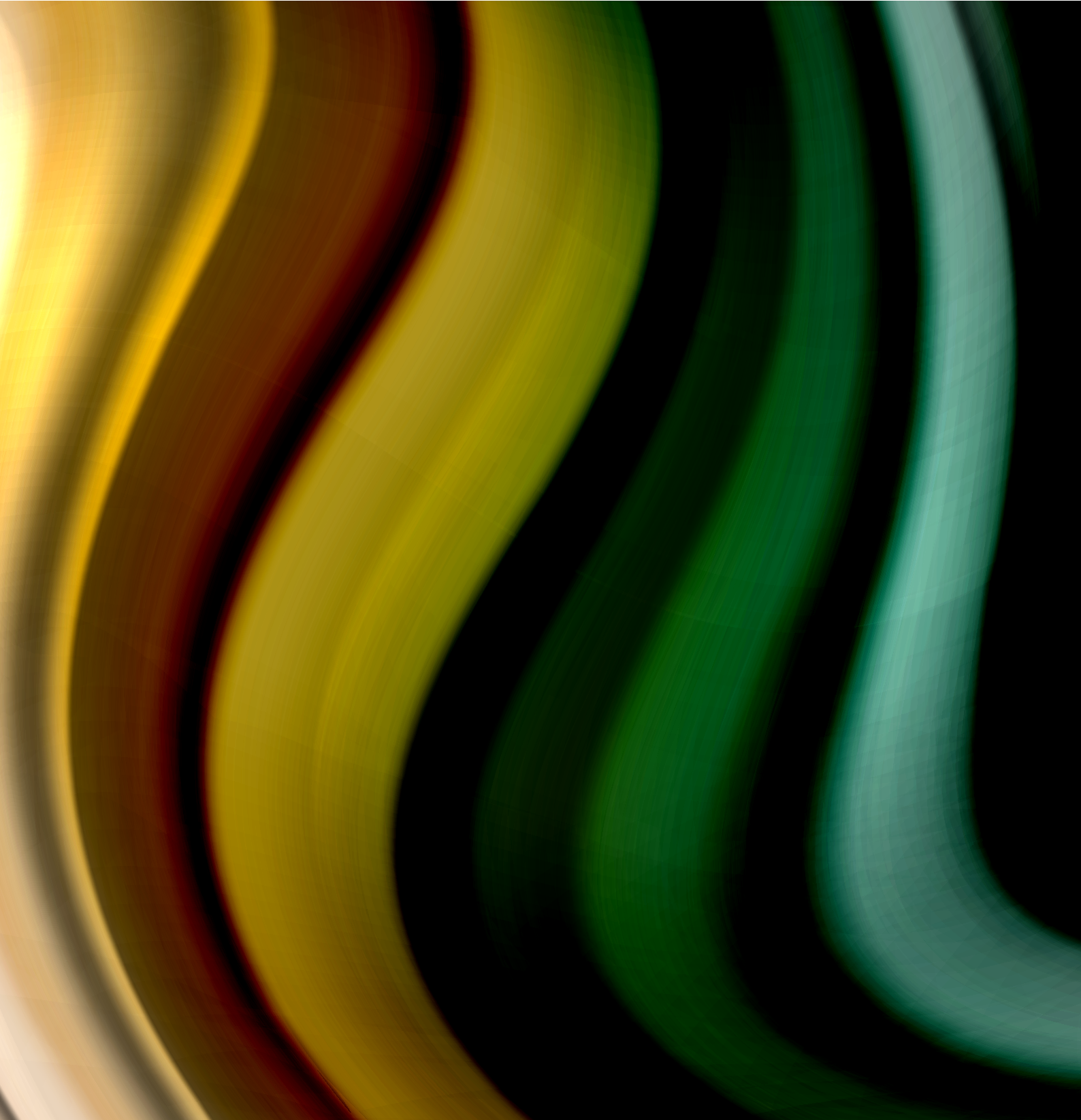
As a result, there is an increased risk of sensitive information getting into the wrong hands or the likelihood of data gathering for dubious purposes, reports of data breaches, data abuse and misuse by both governments and private corporations. Aside from these risks, the absence of data protection laws could hinder business operations on an international scale. The growth of e-commerce and business in general in African countries makes the need for data protection more pressing. Multinational organizations looking for investment opportunities in these countries may limit their business explorative activities in Africa due to the absence of or lack of clarity around data protection law. This is particularly because several multinational companies collect and process a large amount of personal data in the ordinary course of their business. Thus, in order to conduct business effectivity and safely in Africa, organizations need to understand the scope of data protection laws in such countries. Furthermore, in order to keep up with the dynamic realities of our world and its impact, African countries need to develop a strong and more coherent framework for data protection and privacy.

Ijeoma Uju - Partner
ijeoma.uju@templars-law.com
+234 1 2703 982
+234 802 307 7640

Templars
Lagos, Nigeria

TEMPLARS

Rwanda



Rwanda

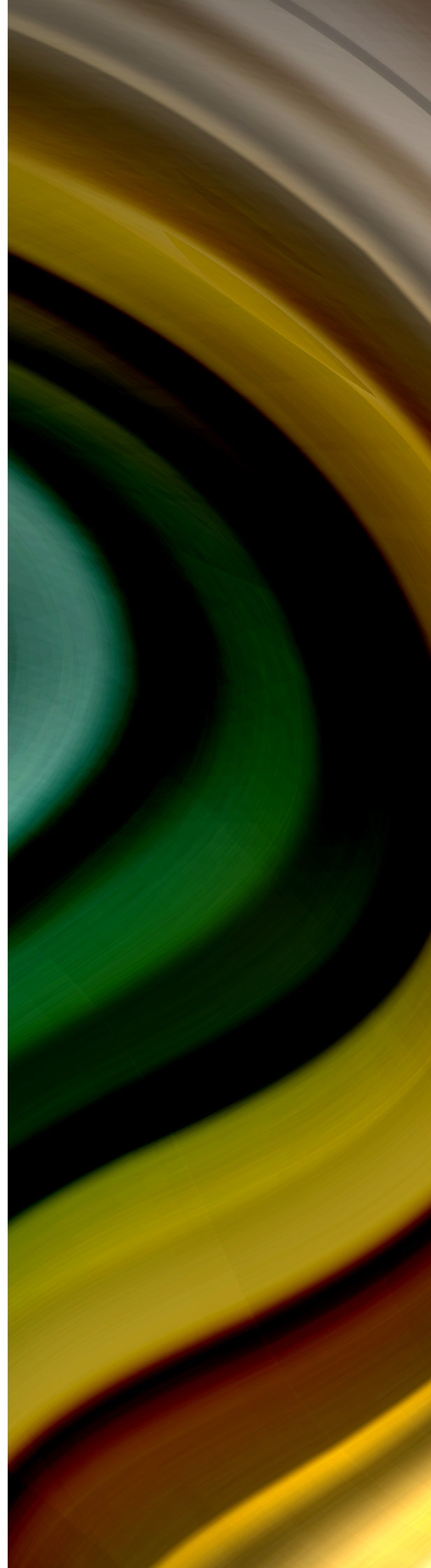
What laws currently exist to protect and ensure the privacy of data?

There are numerous laws that deal with the protection of data privacy in Rwanda, including:

- The Constitution of Rwanda, 2003, as revised in 2015
- Law n° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy.
- Law N° 04/2013 of 08/02/2013 relating to Access to Information
- Law N°24/2016 of 18/06/2016 governing Information and Communication Technologies
- Law N° 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes
- Law N°60/2013 OF 22/08/2013 regulating the Interception of Communications
- Law N°02/2013 OF 08/02/2013 regulating media
- Law N° 73/2018 of 31/08/2018 governing Credit Reporting System
- Law N° 75/2019 of 29/01/2020 on Prevention and Punishment of Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction
- Law N° 017/2021 of 03/03/2021 relating to Financial Service Consumer Protection
- Law N°02/2017 of 18/02/2017 establishing Rwanda Information Society Authority and determining its mission, organization and functioning
- Law N°26/2017 of 31/05/2017 establishing the National Cyber Security Authority and determining its mission, organization and functioning
- Law N°09/2013 of 01/03/2013 establishing Rwanda Utilities and Regulatory Authority (RURA) and determining its mission, organization and functioning
- Regulation N° 02/2018 of 24/01/2018 on Cybersecurity
- Cybersecurity Regulation N° 010/R/CR-CSI/RURA/020 of 29/05/2020
- Regulation N° 31/2019 of 16/12/2019 on Protection of Payment Users
- Draft Regulation Governing use of Personal data in Rwanda 2019.

Are these laws in force?

Yes.



What are the most recent legal developments, or pending developments around data privacy and protection?

The draft Law on Data Protection and Privacy 2020 was submitted to Parliament and adopted by the Chamber of Deputies⁵¹ on May 6, 2021.

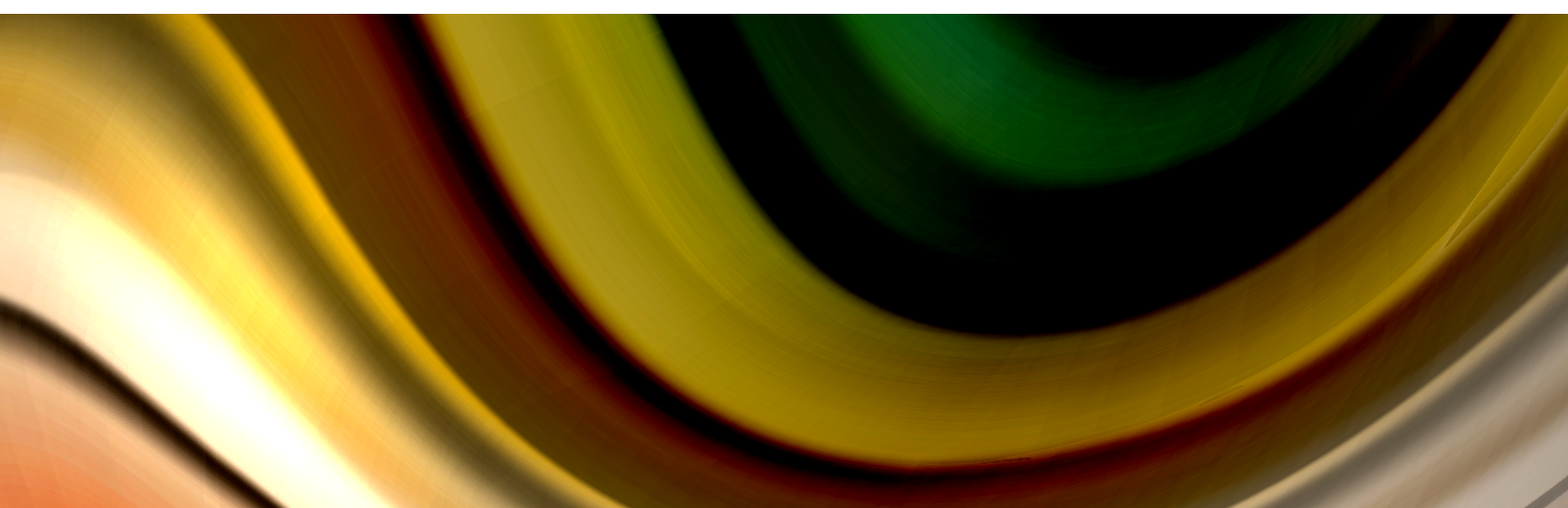
The draft law then proceeded to the parliamentary committee⁵² and Plenary Session⁵³.

The draft Law on Data Protection and Privacy 2020 passed through all the Parliamentary processes on 12 August 2021 and then underwent translation in the three official languages before submission for presidential assent. The law came into force on 15 October 2021 and is titled Law n° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy.

If your country has privacy laws, what constitutes the definition of personal data according to the law?

Law n° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy defines personal data as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

The draft Regulation Governing the use of Personal Data in Rwanda 2019, defines personal data as any information relating to an identified or identifiable individual.



51 Parliament of Rwanda is composed of two Chambers: 1° the Chamber of Deputies (Lower Chamber) and 2° the Senate (Upper Chamber). The Chamber of Deputies is elected by the people and represents them, pass legislation and oversees the executive. Its major business is conducted in Committees and adopted in Plenary Session.

52 The Chamber of Deputies consists of 11 Parliamentary Commissions (also referred to as standing committees). Where the relevance is approved, the Speaker of the Chamber of Deputies refers to the relevant Standing Committee a bill within five (5) days of the closing of debates on its relevance in the plenary sitting.

53 Article 70 of the Constitution of Rwanda states that for each Chamber of Parliament to duly sit, it must hold its meetings at designated buildings, upon official invitation, with an agenda, during sessions, and with a presence of at least three fifths (3/5) of its members. Article 90 further states that draft laws determined by the plenary sitting to have relevance are transmitted to the relevant parliamentary committee of the Chamber of Parliament for examination prior to their consideration and adoption in the plenary sitting. During the consideration of the relevance of a draft law, the Chamber of Parliament may decide if the draft law may be adopted in the plenary sitting without prior consideration by the relevant Committee.

What are the rights of data subjects according to any data privacy law?

Chapter III of Law n° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy, provides for the rights of the data subject as below:



Right to personal data

Without prejudice to other relevant laws, the data subject may, in writing or electronically, request from the data controller or the data processor the following:

- To provide them with the information relating to the purposes of the processing of personal data
- To provide them with a copy of their personal data
- To provide them with a description of personal data that the data controller or the data processor holds, including data on the contact details of a third party or the categories of third parties who have or have had access to personal data
- To inform them of the source of the personal data in case their personal data has not been obtained from the data subject
- To inform them in case their personal data has been transferred to a third country or to an international organization.

The right of the data subject to obtain a copy of their personal data is overridden:

- If it may adversely affect the rights and freedoms of other persons
- Where legal professional privilege or another legal obligation of confidentiality applies
- If the data relates to information management or information about the data subject or relates to ongoing negotiations with the data subject requester
- If the data relates to the data subject's confidential references, examination scripts or examination marks.

The data controller or the data processor must provide the data subject with their personal data in a clear and concise manner.

A data subject who is not satisfied with the response of the data controller or the data processor may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority is required to respond to the appeal within sixty (60) days from the date of receipt of the appeal.



Right to object

The data subject, at any time in writing or electronically, may request the data controller or the data processor to stop processing their personal data which causes or is likely to cause loss, sadness or anxiety to the data subject.

However, this right does not apply if the data controller or the data processor demonstrates compelling legitimate grounds for the personnel data processing, which override the interests, rights and freedoms of the data subject or for the establishment of the legal claim.

The data subject, at any time in writing or electronically, may request the data controller or the data processor to stop processing personal data of the data subject if personal data are processed for direct marketing purposes, including profiling to the extent that it is related to such direct marketing.

The data controller or the data processor, within thirty (30) days from the date of receipt of the request, must inform the concerned data subject in writing or electronically of the compliance with the request or reasons for non-compliance.

The data subject who is not satisfied with the response of the data controller or the data processor may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority responds to their appeal within sixty (60) days from the date of receipt of the appeal.



Right to personal data portability

The data subject has the right to request the data controller in writing or electronically to resend the personal data concerning them as it was provided to the data controller, in a structured and readable format.

The data subject also has the right to request the data controller in writing or electronically to have their personal data transmitted to another data controller, where technically feasible, without hindrance.

The data controller, within thirty (30) days from the date of receipt of the request, must inform the concerned data subject in writing or electronically of personal data portability.

The data subject who is not satisfied with the response of the data controller may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority must respond to the appeal within sixty (60) days from the date of receipt of the appeal.



Right not to be subject to a decision based on automated data processing

The data subject has the right not to be subject to a decision based solely on automated personal data processing, including profiling, which may produce legal consequences or significant consequences to them.

However, these provisions do not apply if the decision:

- Is based on the data subject's explicit consent
- Is necessary for entering into, or for the performance of, a contract between the data subject and the data controller
- Is authorised by laws to which the data controller is subject and also puts in place suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Any automated processing of personal data intended to evaluate certain personal aspects relating to a natural person is not based on sensitive personal data unless one of the grounds set out in Article 10 of this Law is met.



Right to restriction of processing of personal data

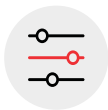
The data subject or the supervisory authority has the right to restrict the data controller from processing personal data for a given period if:

- The accuracy of personal data is contested by the data subject, pending the verification of their accuracy
- The processing is unlawful and the data subject requests the erasure of the personal data or the restriction of the use of some of them
- The data subject has objected to the processing of personal data pending the verification whether the legitimate grounds of the controller override those of the data subject.

The right to restriction of processing of personal data described above is not exercised if the processing of personal data:

- Is necessary for the protection of the rights of another person
- Is necessary for reasons of public interest.

The data controller must, before lifting the restriction of processing of personal data referred to in item 1 above, inform the data subject in writing or electronically.



Right to erasure of personal data

The data subject has the right to request the data controller in writing or electronically for erasure of their personal data where:

- The personal data is no longer necessary in relation to the purposes for which it was collected or processed
- The data subject withdraws consent on which the personal data processing is based and where there is no other legal ground for the processing
- The data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing
- The personal data has been unlawfully processed.

The data controller who has disclosed personal data to a third party or has posted the personal data in the public domain must, in writing or electronically, inform a third party processing such data that the data subject has requested the erasure of any links to, or copy of, those personal data.

However, the right to request the erasure of personal data does not apply to the extent that processing is necessary for:

- Reasons of public interest
- Historical or scientific research purposes or statistical purposes
- Compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller
- The establishment, exercise or defence of legal claims in the interest of the data controller.

The data controller, within thirty (30) days from the date of receipt of the request, must inform the concerned data subject in writing or electronically of the erasure of their personal data.

The data subject who is not satisfied with the response of the data controller may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority must respond to the appeal within sixty (60) days from the date of receipt of the appeal.



Right to rectification

The data subject has the right to request the data controller the rectification of their personal data.

The data subject has the right to have incomplete personal data completed, where necessary.

The data controller, within thirty (30) days from the date of receipt of the request, must inform the data subject in writing or electronically of the rectification of their personal data. The data subject who is not satisfied with the response of the data controller may appeal to the supervisory authority within thirty (30) days from the date of receipt of the response.

If the data subject appeals, the supervisory authority must respond to the appeal within sixty (60) days from the date of receipt of the appeal.



Right to designate an heir to personal data

The personal data of the data subject are not subject to succession.

However, where the data subject had left a will, the data subject provides their heir with full or restricted rights relating to the processing of personal data kept by the data controller or the data processor, if such personal data still need to be used.



Right to representation

The right of the data subject to representation is exercised where:

- The data subject is under sixteen (16) years of age, in which case they are represented by a person who has parental authority over them or who was appointed as their guardian
- The data subject has a physical impairment and is unable to represent themselves, in which case they are represented by their parent, adopter, a centre or an association that caters for them or the guardian appointed by a court
- The data subject has a medically determinable mental impairment and is unable to represent themselves, in which case they are represented by their parent, adopter, a centre or an association that caters for them or the guardian appointed by a court
- There is any other reason, in which case they are represented by another person authorised in writing by the data subject in accordance with relevant law.

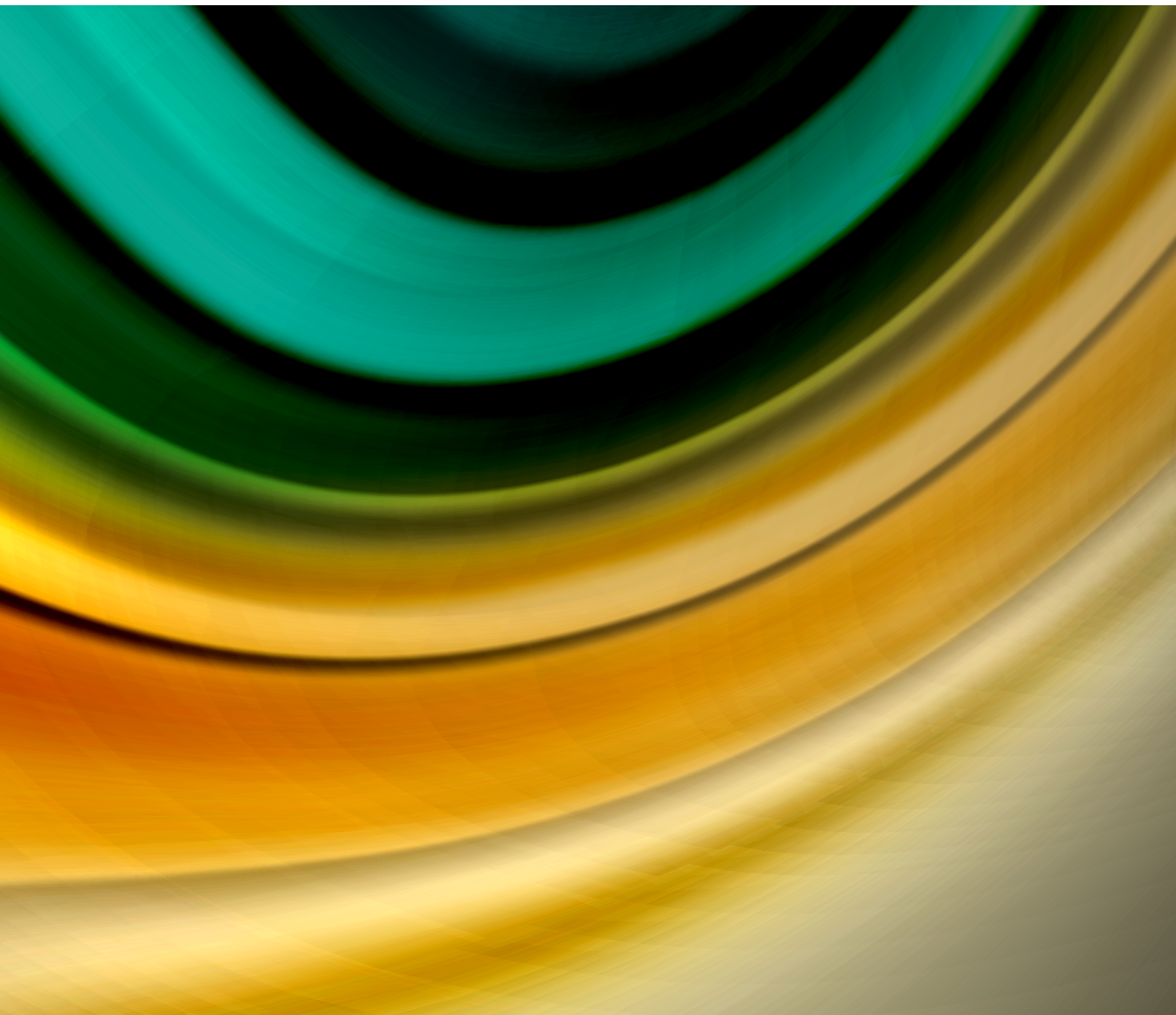
**Right of the data subject to withdraw their consent**

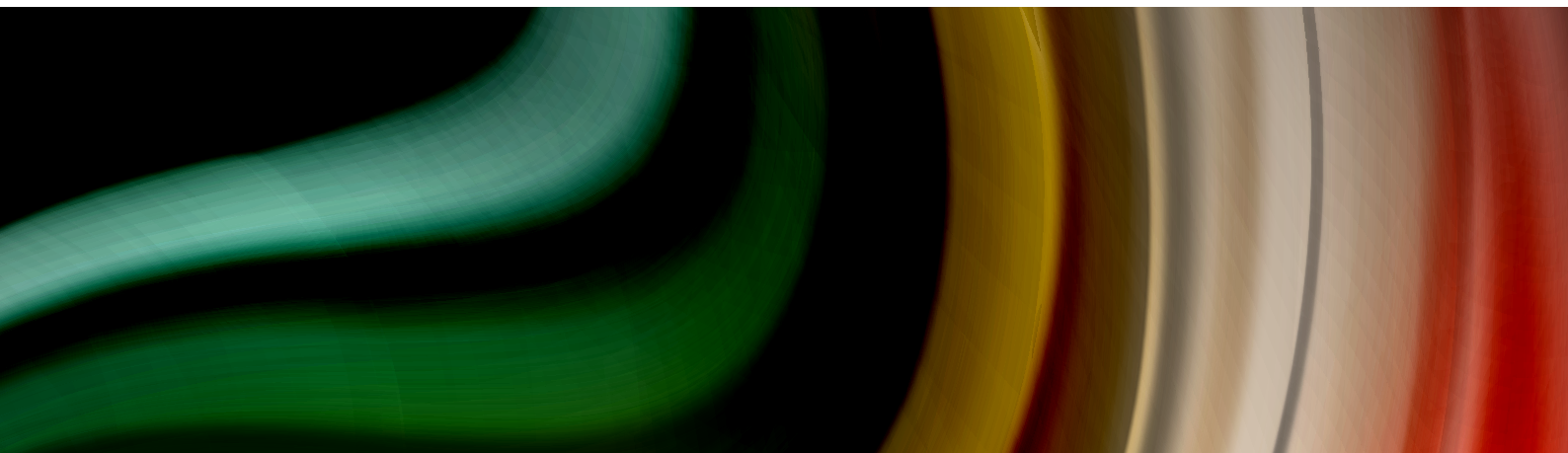
The data subject has the right to withdraw their consent at any time.

The withdrawal of consent by the data subject does not affect the lawfulness of processing of personal data based on consent before its withdrawal.

The withdrawal of consent by the data subject is as easy as expressing it and takes effect as of the date on which the data subject applied for it.

The draft Regulation Governing use of Personal data in Rwanda 2019 under its Chapter VII lists the rights of the data subject to include the right to access personal information, right to prevent processing of personal data, right to data portability, and the right to compensation.





Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

Article 37 of the Law n° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy provides that every controller or processor shall 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 it is processed
- 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 permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in accordance with the rights of data subject.

Article 38 provides that in compliance with the principles of the processing of personal data, the data controller and the data processor discharge the following duties:

- Implementing appropriate technical and organizational measures
- Keeping a record of personal data processing operations
- Carry out personal data protection impact assessments where the processing of personal data is likely to result in a high risk to the rights and freedoms of a natural person
- Perform such other duty as may be assigned to them by the supervisory authority.

The personal data protection impact assessment referred to above is carried out in case of:

- A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing of personal data, including profiling, and on which decisions that produce effects concerning such persons are based
- Processing on a large scale of sensitive personal data
- A systematic monitoring of a publicly accessible area on a large scale
- Processing of personal data identified by the supervisory authority as likely to result in a high risk to the rights and freedoms of natural persons
- New technologies used to process personal data.

What are the penalties for non-compliance with data privacy law in your country?



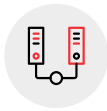
Law N° 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes

- Article 16 provides that any person who intentionally and unlawfully gets access to computer or computer system data and (a) does not have consent from any person who is so entitled; (b) is not entitled to control and access to the computer or computer system data; and (c) accesses another person's computer system without authorization, in order to know recorded or transmitted data, by all means and regardless of the location; commits an offence.
- Upon conviction of one of the offences referred to above, the individual is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).
- Article 17 provides that any person who, with intent to commit an offence, causes a computer system or a computer to perform any function for the purpose of securing access to any program or data held in any computer system commits an offence. Upon conviction, they are liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).
- Article 26 states that it is an offence:
 - To receive, use or provide access to any program or data held in a computer or computer system without authorization
 - For anyone that is authorized to receive or to have access to any program or data held in a computer or computer system, to receive and use them from another person knowing that the other person has obtained that program or data through unauthorized means
 - For anyone that has obtained any program or data held in a computer or computer system through authorized means and gives that program or data to another person who is not authorized to receive or have access to that program or data; commits an offence.
- When convicted of any of the offences above, the person is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).
- Article 44 provides that any service provider who does not exercise due care and skill to prevent the disclosure of computer data made available to third party, commits an offence. Upon conviction, they are liable to a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).



The Law n° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy imposes the following penalties:

- Imposes a sentence of imprisonment of not less than one (1) year but not more than three (3) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties on a person who accesses, collects, uses, offers, shares, transfers or discloses personal data in a way that is contrary to this Law, commits an offence.
- Imposes a sentence imprisonment of not less than one (1) year but not exceeding three (3) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties on any person who knowingly, intentionally or recklessly: 1° re-identifies personal data which have been de-identified by a data controller or a data processor ;2° re-identifies and processes personal data, without consent of the data controller.
- Imposes on a person who unlawfully destroys, deletes, conceals or alters personal data, a sentence of imprisonment of not less than three (3) years but not more than five (5) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties on a person who destroys, erases, conceals or alters personal data in a way that is contrary to this Law, commits an offence.
- Imposes a sentence of imprisonment of not less than five (5) years but not more than seven (7) years and a fine of not less than twelve million Rwandan francs (RWF 12,000,000) but not more than fifteen million Rwandan francs (RWF 15,000,000) or one of these penalties to any person who unlawfully sells or offers data.
- Imposes a sentence of imprisonment of not less than seven (7) years but not more than ten (10) years and a fine of not less than twenty million Rwandan francs (RWF 20,000,000) but not more than twenty-five million Rwandan francs (RWF 25,000,000) or one of these penalties on a person who collects or processes sensitive personal data in a way that is contrary to this Law, commits an offence.
- Imposes a sentence of imprisonment of not less than one (1) year but not more than three (3) years and a fine of not less than three million Rwandan francs (RWF 3,000,000) but not more than five million Rwandan francs (RWF 5,000,000) or one of these penalties on a person who provides false information during and after registration, commits an offence.
- The Law n° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy states that a corporate body or a legal entity that commits one of the offences referred to above commits an offence. Upon conviction, it is liable to a fine of Rwandan francs amounting to five percent (5%) of its annual turnover of the previous financial year.
- The Law n° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy additionally imposes steep penalties by providing that aside from the penalties provided for in this Law, the court, in all cases, may order the confiscation of property and belongings used in the commission of any of the offences provided for in this Law and the proceeds gained.
- The court may also order the closure, permanently or temporarily for the period that it considers appropriate, of the premise or of a legal entity in which any of the offences provided for in this Law has been committed.



The Draft Regulation Governing use of Personal data in Rwanda 2019 imposes the following penalties:

- Imposes on any data controller or data processor that contravenes an enforcement notice of the Regulatory Authority issued under provisions of this Regulation an administrative fine of between five hundred thousand Rwandan francs (RWF 500,000) and fifteen million Rwandan francs (RWF 15,000,000) Rwanda francs for each day of its non-compliance to the requirements, as of the day of confirmed notification.
- Imposes a fine between five million (5,000,000) and ten million (10,000,000) Rwandan Francs on any data controller or data processor that processes data without consent.
- Imposes a fine of between five million (5,000,000) and ten million (10,000,000) Rwandan Francs on any data controller or data processor that collects data from a third party.
- Imposes a fine of between ten million (10,000,000) and fifteen million (15,000,000) Rwandan Francs on any data controller or data processor that processes particularly sensitive data contrary to the provisions of this Regulation.
- Imposes a daily fine of between one million (1,000,000) and five million (5,000,000) Rwandan Francs, for each day calculated from the day the breach occurred on any data controller or data processor who intentionally fails to notify the regulatory authority of the data breach.
- Imposes a daily fine of between ten million (10,000,000) and twenty million (20,000,000) Rwandan Francs, for each day calculated from the day the processing or storage of data started on any data controller or data processor who processes or stores personal data outside Rwanda without authorization

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The agency responsible to enforce compliance is the National Cyber Security Authority (NCSA) as mandated by Law no 26/2017 of 31/05/2017 establishing the National Cyber Security Authority and determining its mission, organisation and functioning.

Does your country's data privacy law follow the framework of the EU's GDPR?

Both the Law N° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy and the draft Regulation Governing use of Personal data in Rwanda 2019 follows the same framework as the GDPR.

These legislations have some highlighted similarities, including principles relating to processing of personal data, obligations on the companies and organizations in order to ensure the privacy and protection of personal data, providing data subjects with certain rights, and assigning powers to regulators to ask for demonstrations of accountability or even impose fines in cases of non-compliance.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

In an increasingly digitalized world, businesses and organizations are embracing online platforms to conduct socio-economic activities. Data is increasingly becoming an important asset, and collecting and sharing data can serve as big business in the present day's digital economy. In addition, citizens are also increasingly becoming aware of the importance of protecting one's personal data.

African countries, therefore, cannot afford to be left behind. They have to ensure that they put in place legislation to secure the protection of data and privacy in order to prevent issues stemming from unprotected data, such as unauthorized use of one's personal data without their knowledge, as well as the negative impact on a company or organization's reputation should it face sanctions among other factors.

Emmanuel Muragijimana – Principal Associate
emmanuel@ksolutions-law.com
+250 727 000 973

K-Solutions & Partners
Kigali, Rwanda

South Africa



South Africa

What laws currently exist in your country to protect and ensure the privacy of data?

- The Constitution of the Republic of South Africa – section 14 of the Constitution stipulates that everyone has the right to privacy, which includes the right not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed.
- The Protection of Personal Information Act, 2013 (POPIA) – in force since July 2021, POPIA promotes the protection of personal information processed by public and private bodies, introduces minimum requirements for the processing of personal information, outlines the rights of data subjects, regulates the cross-border flow of personal information, introduces mandatory obligations to report and notify data breach incidents, and imposes statutory penalties for violations of the law.
- The Cybercrimes and Cybersecurity Act, 2020 – was signed into law in June 2021 and came into force on 1 December 2021. It brings the country's cybersecurity legislation in line with global standards. The Act compels electronic communications service providers and financial institutions to act when they become aware that their computer systems have been involved in a cybersecurity breach, as defined under the Act. They must report such offences to the South African Police Service within 72 hours of becoming aware of the offence, and preserve any information which may be of assistance in the investigation. Non-compliance with this provision is a criminal offence and massive fines can be imposed. The Act further criminalises harmful data messages, such as those that invite or threaten violence or damage to property, as well as those that contain intimate images. Data is broadly defined in the Act as "electronic representations of information in any form." The Act also criminalises cyber fraud, extortion, forgery and the theft of incorporeal property. Also listed as an offence is the unlawful accessing of a computer system, data storage medium or personal data. Those found guilty of a cybersecurity offence face hefty fines and lengthy prison sentences of up to 15 years.
- The National Credit Act, 2005 (NCA) – requires that any person who receives, compiles, retains or reports any confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information, and in particular, must use that information only for a purpose permitted or required in terms of the NCA or other national or provincial legislation; and report or release that information only to the consumer or prospective consumer, or to another person only (a) to the extent permitted or required by the NCA or other national or provincial legislation, or (b) as directed by the consumer or prospective consumer or an order of a court or the National Consumer Tribunal.
- The Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 – also governs the monitoring and interception of communications. The default position in terms of this Act is that all workplace monitoring and interception is prohibited, unless it falls within one of the exceptions in Chapter 2 of the Act. Thus, employee monitoring is permitted:
 - Where the employee consents or where their consent can be reasonably implied
 - Where the interception occurs in connection with carrying on of business (the business exception)
 - Where interception is carried out by a person who is a party to the same communication.
- The Promotion of Access to Information Act 2 of 2000 (PAIA) – allows access to any information held by the State, and any information held by private bodies that is required for the exercise and protection of any rights.

Are these laws in force?

Yes, all of the laws are in force.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

In October 2021, the Information Regulator requested that public comments be submitted on the Amendment of the Regulations Relating to the Protection of Personal Information, 2018 ("Draft Regulations").

The Draft Regulations outline the procedure to be followed in certain circumstances contemplated in POPIA, including:

- Guidance for data subjects on how to object to the processing of their personal information
- Guidance on how data subjects can request the correction, destruction or deletion of their personal information
- Guidance on how responsible parties can request a person's consent to process their personal information for unsolicited electronic direct marketing
- How data subjects can go about submitting a complaint to the Information Regulator.



If your country has privacy laws, what constitutes the definition of personal data according to the law?

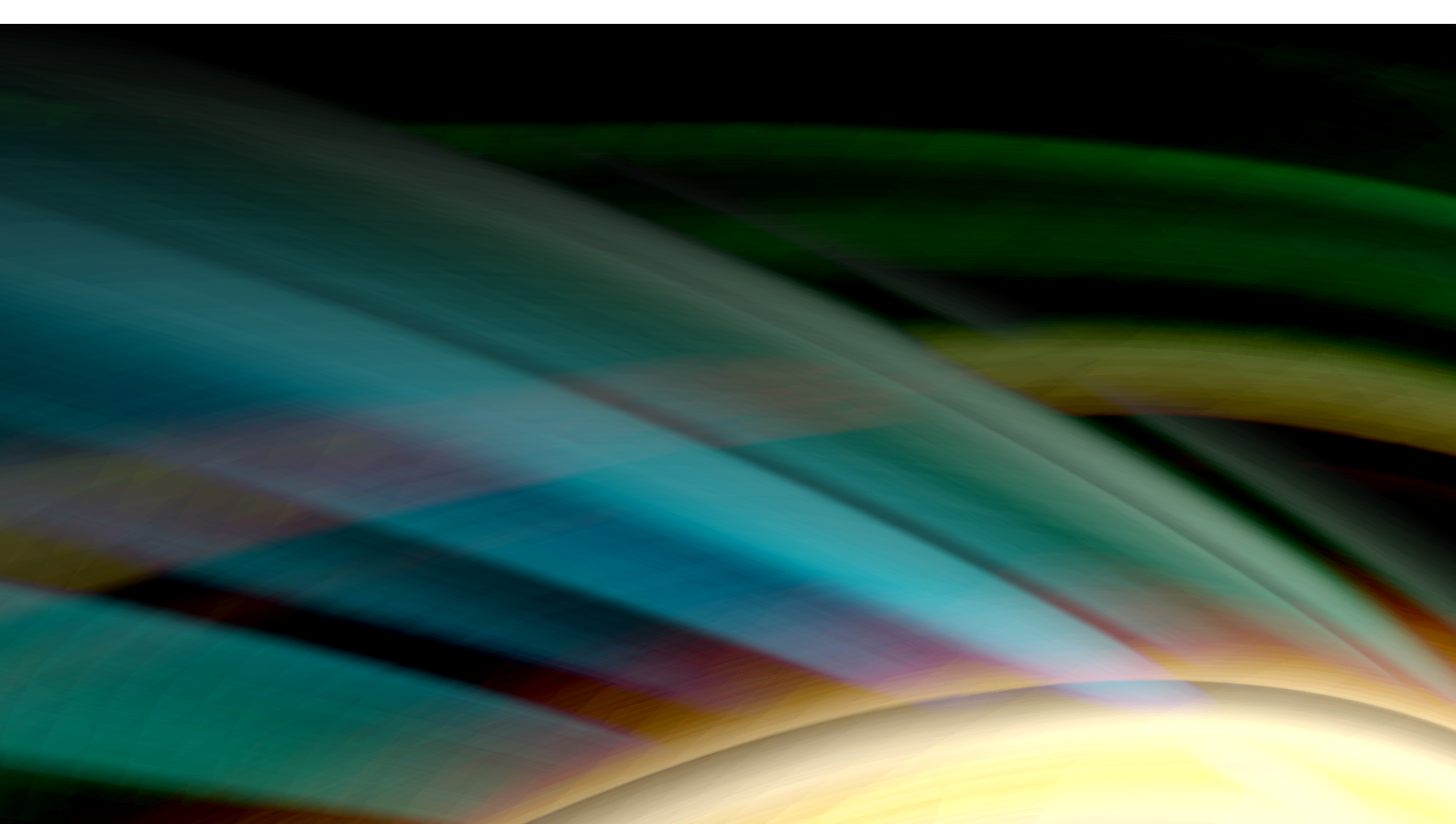
"Personal information" is broadly defined in POPIA to include information that relates to both an identifiable, living, natural person, and where applicable, an identifiable juristic person or legal entity.

Personal information 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, wellbeing, disability, religion, conscience, belief, culture, language, and birth
- Information relating to the education, medical, financial, criminal, or employment history of the person
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person
- The biometric information of the person
- The personal opinions, views, or preferences of the person
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence
- The views or opinions of another individual about the person
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

There is a separate category in POPIA for "special personal information". This includes information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behaviour.

The personal information of a child is specifically regulated by POPIA.



What are the rights of data subjects according to any data privacy law in your country?

A data subject has the right to have their personal information processed in accordance with the conditions for the lawful processing of personal information referred to in POPIA. These rights include, among others:

- The right to be notified that personal information is being collected, accessed or acquired by an unauthorised person
- The right to establish whether a responsible party holds personal information of that data subject and to request access to this personal information
- The right to request the correction, destruction or deletion of personal information
- The right to object, on reasonable grounds, to the processing of personal information
- The right to object to the processing of personal information at any time for purposes of direct marketing
- The right not to have personal information processed for the purposes of direct marketing by means of unsolicited electronic communications
- The right not to be subject to the automated processing of information
- The right to complain to the Information Regulator
- The right to institute civil proceedings regarding interference with personal information.

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

Broadly, POPIA sets out the essential parameters for the lawful processing of personal information, including:

- Eight core information protection principles
- A number of substantive issues concerning the processing, collecting, transferring and maintaining of personal information
- Exemptions from the information protection principles
- The rights of data subjects regarding unsolicited electronic communications and automated decision making
- The establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of POPIA and PAIA
- The regulation of trans-border information flows
- Enforcement mechanisms



Responsible parties

Responsible parties processing personal information must ensure that personal information is only processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the organization, and the organization must take steps to make affected data subjects aware of the purposes for which the personal information will be processed.

Subject to certain exceptions, personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected.

A responsible party is required to:

- Be accountable for complying with all aspects of POPIA and for ensuring that any appointed operators who process personal information on their behalf are also compliant
- Appoint an information officer (optional but not mandatory) to ensure compliance with the conditions set out in POPIA and deal with complaints from data subjects who seek to enforce POPIA
- Unless exempt, prepare a manual in terms of section 51 of PAIA and make the same publicly available
- Obtain prior authorisations from the Information Regulator, if required in respect of the processing of certain types of personal information
- Notify the Information Regulator and affected data subjects of a security breach
- Maintain documentation of all processing
- Secure the integrity and confidentiality of personal information in its possession or under its control and ensure that it is appropriately safeguarded against loss, destruction or unlawful access.



The eight core conditions

There are eight conditions responsible parties must meet for the lawful processing of personal information according to POPIA:

- Accountability - responsible parties are responsible for ensuring the conditions for lawful processing are met.
- Processing limitation - responsible parties must process personal information lawfully, minimally, in accordance with the consent, justification and objection provisions, and with the data subject's consent, unless certain exceptions apply.
- Purpose specification - responsible parties must process personal information for a specific purpose and adhere to the retention and restriction of records provisions in POPIA.
- Further processing limitation - further processing of information must be compatible with the purpose of collection.
- Information quality - responsible parties must take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated.
- Openness - responsible parties must maintain the documentation of all processing operations under its responsibility and take reasonably practicable steps to ensure that the data subject is aware of certain information.
- Security safeguards – responsible parties must:
 - Secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures
 - In terms of a written contract, ensure that an operator, which processes personal information on its behalf, establishes and maintains security measures
 - As soon as reasonably possible after the discovery of a security compromise, notify the Information Regulator and the data subject.
- Data subject participation - responsible parties must allow a data subject to access and correct its personal information. The responsible party may also be required to correct, delete or destroy personal information.



Data protection impact assessment

Regulation 4(b) of the Regulations made by the Information Regulator relating to the Protection of Personal Information, 2018 requires that a responsible party must undertake a Personal Information Impact Assessment (PIIA) to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information. A PIIA must:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to data subjects
- Identify any additional measures to mitigate those risks and ensure compliance with the eight conditions for lawful processing.



Direct Marketing

POPIA requires an “opt-in” system for direct marketing. Businesses are prohibited from approaching consumers, for the purposes of direct marketing, unless: the business has obtained consent, or the consumer is an existing customer of the business.

Businesses may approach a data subject who is not an existing customer only once to request the data subject’s consent for direct marketing purposes in the prescribed Form 4, and provided consent was not previously withheld.

Businesses may process the personal information of a data subject who is a customer of the business under any of these circumstances:

- If the business obtained the contact details of the data subject in the context of the sale of a product or service
- For purposes of direct marketing of the business’ own similar products or services
- If the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality.



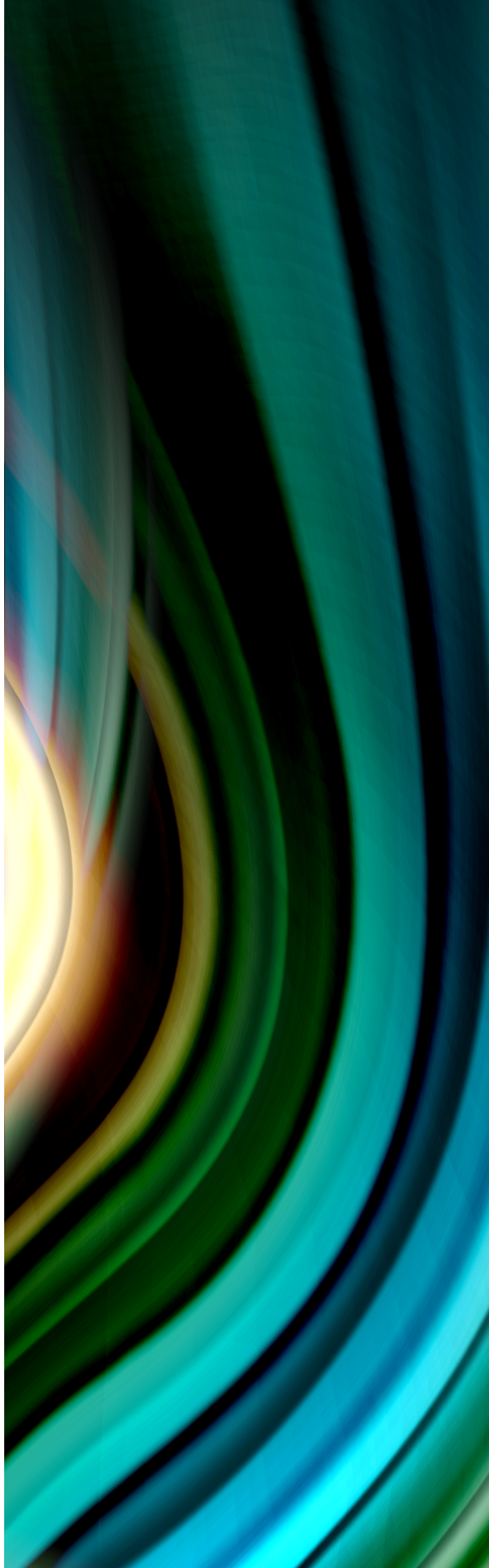
Security breach notification under POPIA

Businesses experiencing a data breach must notify the Information Regulator and the data subject, where there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorized person. This notification must be made as soon as reasonably possible after the discovery of the compromise. Notification may be delayed if certain exceptions apply. Businesses must report every breach, regardless of whether it could cause or caused significant harm.

In terms of the obligations of operators (i.e. data processors), any person who processes personal information on behalf of another business (i.e. the responsible party), in terms of a contract or mandate, must notify that business immediately where there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorised person.

What are the penalties for non-compliance with data privacy law in your country?

- **Criminal Sanctions:** POPIA provides for a number of criminal offences. Criminal offences under POPIA attract fines and imprisonment not exceeding 12 months or ten years.
- **Administrative Fines:** If a responsible party is alleged to have committed an offence in terms of POPIA then the Information Regulator may impose an administrative fine on such responsible party. The administrative fine payable in relation to any offence must not exceed ZAR 10 million (approximately USD 649,469).
- **Civil Sanctions:** A data subject or, at the request of the data subject, the Information Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of POPIA whether or not there is intent or negligence on the part of the responsible party. A court hearing the proceedings is entitled to award an amount that is just and equitable and is further entitled to award damages for patrimonial loss (i.e. special damages that aim to redress to the extent that money can, the actual or probable reduction of a person's patrimony) and non-patrimonial damages (i.e. damages for pain and suffering or an infringement of personality rights).



What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?



The Information Regulator

POPIA provides for the establishment of an independent supervisory authority – the Information Regulator. The Information Regulator is an independent body that is subject only to the law and the Constitution and is accountable to the National Assembly. The Information Regulator is, among other things, empowered to monitor and enforce compliance by public and private bodies with the provisions of PAIA and POPIA.



The Information Officer

The Information Regulator has published a guidance note in respect of the appointment of information officers and deputy information officers.

Although, POPIA does not require that an information officer must be a local person, the guidance note provides that in order to ensure accessibility, the information officer of a multinational entity based outside the country must authorise any person within the Republic of South Africa as an information officer.

POPIA also provides for the appointment of deputy information officers. With regard to the appointment of deputy information officers, the guidance note provides that the information officer of a multinational entity based outside South Africa must designate any person within South Africa as a deputy information officer. A person designated as a deputy information officer should be afforded sufficient time, adequate resources and the financial means to devote to matters concerning POPIA and PAIA. In addition, the guidance note provides that an information officer or a deputy information officer should report to the highest management office within the private body. This means that only an employee at the level of management and above should ideally be considered for designation as an information officer or as a deputy information officer.

A deputy information officer should be accessible to everyone, particularly to a data subject in respect of POPIA or a requester in terms of PAIA. Deputy information officers are required to have a reasonable understanding of POPIA and of the business operations and processes of the private body. In addition, only employees of a South African company can be appointed as a deputy information officer. In this regard, the guidance note specifically provides that a deputy information officer must be based in South Africa.

Depending on the circumstances, any obligation or liability incurred as a result of any delegation of any powers, duties and responsibilities to a deputy information officer will be imposed on either the information officer or responsible party.

The person authorising any person as the information officer of a juristic person retains the accountability and responsibility for any power or the functions authorised to that person.

The information officer may be any one of the following: (i) the chief executive officer (CEO), (ii) the managing director (MD), (iii) an equivalent officer to the CEO or MD, or (iv) anyone duly authorised by that officer.

The information officer must be registered with the Information Regulator in order to perform their duties and responsibilities under POPIA. The person authorising any person as the information officer of a juristic person retains the accountability and responsibility for any power or the functions authorised to that person. The names and contact details of a company's information officer and deputy information officer will be made available on the Information Regulator's website.

The Manual

Unless exempt, a manual in terms of section 51 of PAIA is also required. The manual must be made publicly available at the company's offices and on the company's website.

Does your country's data privacy law follow the framework of the EU's GDPR?

POPIA was first prepared as a draft bill in 2009, and was based on the regulations of the EU's first data privacy legislation – the EU Data Protection Directive (1995), which was replaced by the GDPR in 2018. There are similarities and major differences between POPIA and the GDPR.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

Rapid digitization, boosted by the pandemic, means that it is now critical to implement policy, legislative and regulatory frameworks that are intended to guide and enforce the protection and security of personal data, not just in Africa but around the world. Failure to do so will lead to business failure, massive financial loss, loss of investment and a devastating rise in criminality.

Janet MacKenzie – Partner
janet.mackenzie@bakermckenzie.com
+27 11 911 4300

Baker McKenzie
Johannesburg, South Africa

Togo



Togo

What laws currently exist in your country to protect and ensure the privacy of data?

To protect and ensure privacy of data, Togo has adopted, since 29 October 2019, the law N°2019-014 relating to Personal Data Protection.

Are these laws in force?

Yes, these laws are in force

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

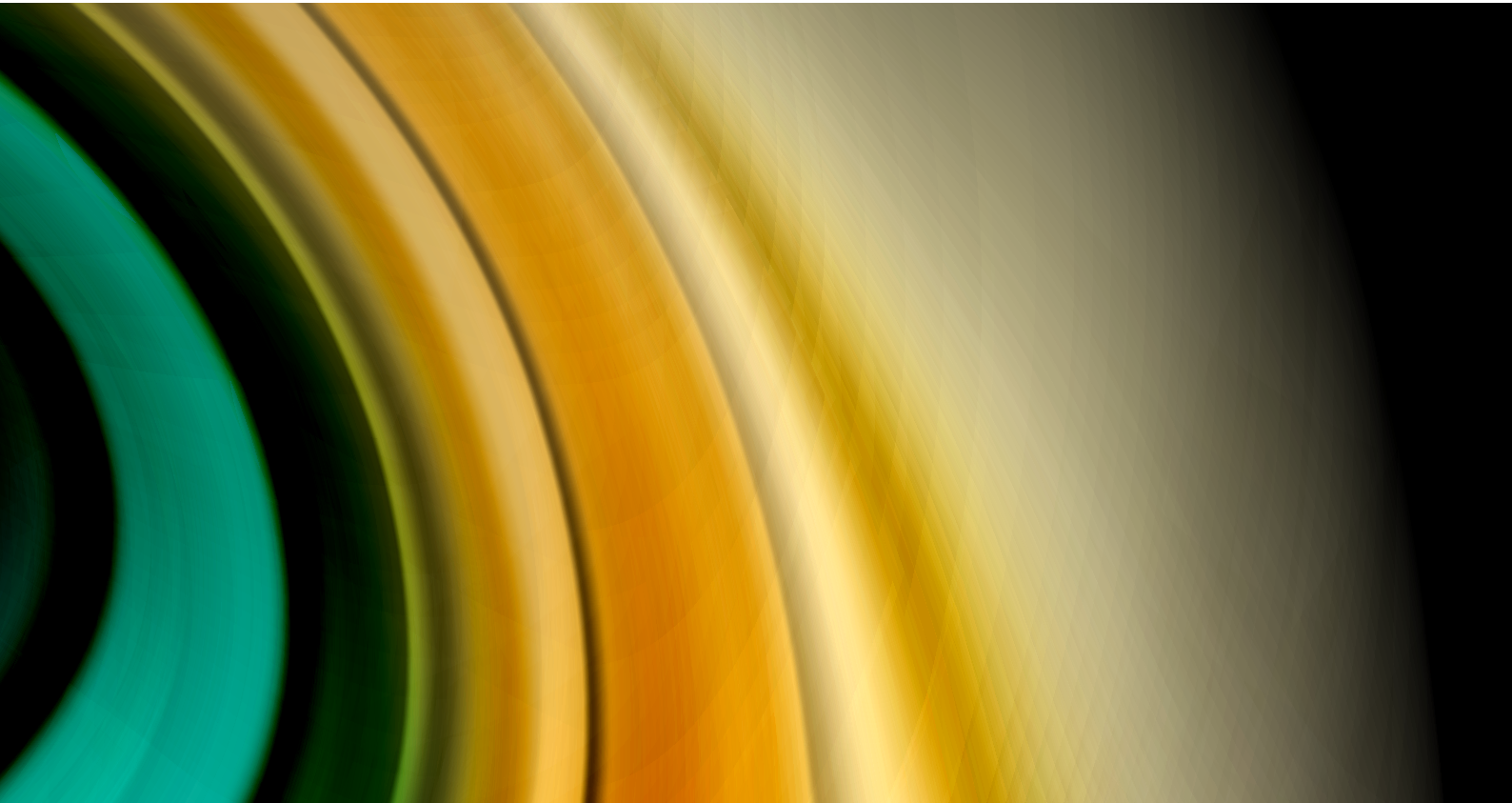
On 30 July 2021, the national Assembly adopted a bill authorising the ratification of the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention).

If your country has privacy laws, what constitutes the definition of personal data according to the law?

According to the law, personal data is any information relating to an identified or identifiable natural person, directly or indirectly, by reference to a number identification or to one or more elements specific to their physical, psychological, genetic, cultural, psychic, social or economic identity.

What are the rights of data subjects according to any data privacy law in your country?

The rights of data subjects according to data privacy law in Togo are the right to information, the right of access, the right to object, the right of rectification and deletion, the right to erasure and data backup after death.



Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

The obligations of data controllers and processors according to data privacy in Togo are the confidentiality obligation, the security obligation, the retention obligation and the obligation of sustainability.

What are the penalties for non-compliance with data privacy law in your country?

The penalties for non-compliance with data privacy in Togo depend on the offense committed. For this purpose, the legislator provides for the penalties of imprisonment conditional on the payment of a fine or one of these two penalties.

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The data protection regulator in Togo is the Personal Data Protection Authority, "Instance de Protection des Données à Caractère Personnel - IPDCP", an independent statutory body created under the Data Protection Act to enforce the law.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

The penetration rate of internet in Africa is constantly increasing, because Africa has realized the importance of the internet as a vector of development. With a population of more than a billion inhabitants, Africa is potentially a huge mine of personal data, which explains the proliferation of GAFAM projects to better connect the continent. It is therefore important, already at the primary stage, to regulate data privacy and protection.

Does your country's data privacy law follow the framework of the EU's GDPR?

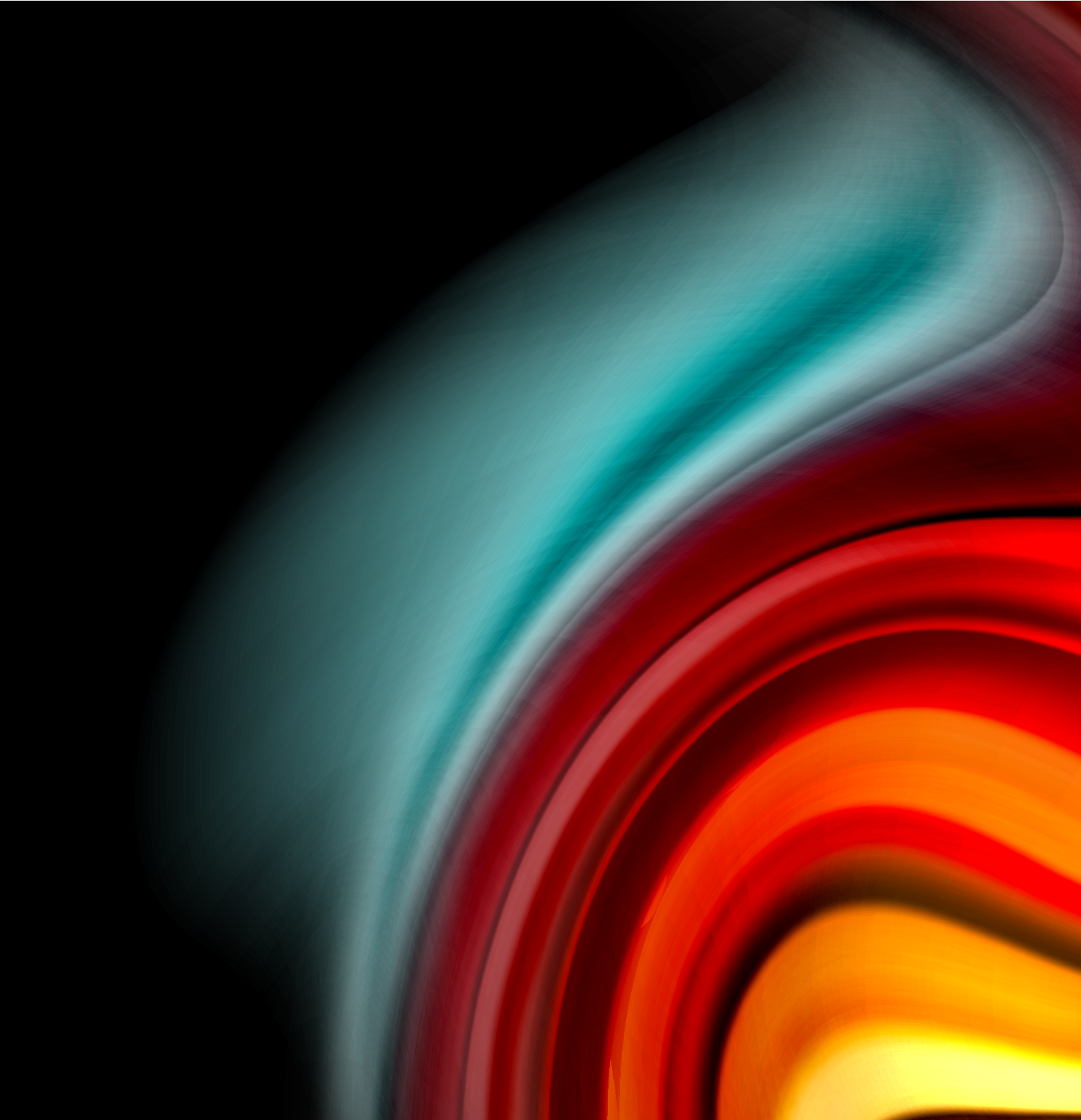
Yes, the data privacy law follow the framework of the GDPR.

Kafui Achille AMEKOU DI – Avocat
kafui.amekoudi@amkalegal.com
contact@amkalegal.com
amekoudi.lawfirm@gmail.com
+228 90 96 01 85/ 99 99 55 00

AMKA Law Firm
Lomé – Togo



Uganda



Uganda

What laws currently exist in your country to protect and ensure the privacy of data?

The following laws and regulations govern data privacy and security in Uganda:

- The Constitution of Uganda, 1995 as amended
- The Data Protection and Privacy Act, No. 9 of 2019
- The Data Protection and Privacy Regulations, 2021.

Are these laws in force?

Yes. The Data Protection and Privacy Act was enacted in 2019 (Act), guarantees the protection of privacy of the individual and of personal data by regulating the collection and processing of personal information. The Act focuses on the protection of privacy and personal data through regulation of its collection, processing and storage. The Data Protection and Privacy Regulations, 2021 (Regulations) were published and gazetted in March 2021 by the Minister of Information Communication Technology and National Guidance.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

The recent passing of enabling Regulations on 12 March 2021 are intended to implement the Act by prescribing for the necessary procedural requirements.

If your country has privacy laws, what constitutes the definition of personal data according to the law?

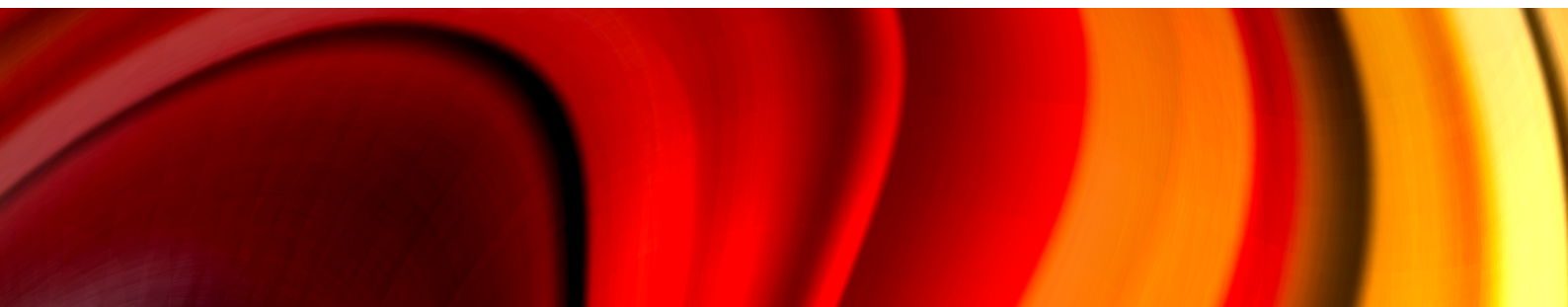
According to section 2 of the Act, personal data is defined as information about a person from which the person can be identified, that is recorded in any form and includes data that relates to:

- The nationality, age or marital status of the person
- The educational level, or occupation of the person
- An identification number, symbol or other particulars assigned to a person
- Identity data
- Other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual.

What are the rights of data subjects according to any data privacy law in your country?

Data subject rights are set out through sections 24 to 28 of the Act. These rights are:

- The right to access personal information
- The right to know the purpose for which the information is collected
- The right to prevent processing of personal data
- The right to prevent processing of personal data for direct marketing purposes
- The right not to be subjected to a decision affecting the data subject which is solely based on processing by automatic means.



Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

Data controllers and processors in Uganda have the following obligations:



Data processing notification

Every person, institution or public body collecting or processing personal data is mandated to register with the National Information Technology Authority – Uganda (NITA-U) for inclusion on the Data Protection Register. In addition, the Register can be accessed by the public for purposes of inspection.



Data processing transfer

The Act does not bar the processing or storage of personal data outside Uganda, as long as the jurisdiction receiving the data has adequate protection measures at least equivalent to the protection under the Act or the data subject has consented to such transfer.⁵⁴



Data processing records

The Act mandates a data collector or processor not to retain the personal data of a data subject for a period longer than necessary to achieve the purpose for which the data is collected and processed.⁵⁵



Data Protection Impact Assessment

Where the collection or processing of personal data poses a high risk to the rights and freedoms of natural persons, the data collector, processor or controller shall prior to the processing and/or collection carry out an assessment of the impact of the envisaged collection or processing operations on the protection of personal data.⁵⁶



Data Protection Officer appointment

Section 6 of the Act stipulates that, insofar as the Act applies to an institution, the institution is required to appoint a data protection officer (DPO).



Data breach notification

Under Section 23 of the Act, it is mandatory to notify NITA-U of any unauthorised access or acquisition of data, in addition to the remedial action taken.

⁵⁴ Section 19, Data Protection and Privacy Act 2019

⁵⁵ Section 18, Data Protection and Privacy Act 2019

⁵⁶ Regulation 12, Data Protection and Privacy Regulations, 2021



Data breach retention

As a general rule, the Act does not set a duration for the retention of data. However, it stipulates that personal data should not be retained for a period longer than is necessary to achieve the purpose for collection or processing of the data, unless: ⁵⁷

- The retention of data is required or authorised by law (e.g. the Anti Money Laundering Act, 2013 sets 10 years as the duration for retention of records)
- The retention is necessary for a lawful purpose related to the function or activity for which the data is collected or processed
- The retention is required by a contract between parties
- The data subject consents to the retention of the data.

What are the penalties for non-compliance with data privacy law in your country?

The Act creates a number of offences which are aimed at ensuring compliance with the law. Such offences include: ⁵⁸

- Unlawfully obtaining or disclosing personal data
- Unlawful destruction, deletion, concealment or alteration of personal data
- Sale of personal data.

The penalties imposed against corporations for these offences range from the imprisonment of the corporation's officers for a term not exceeding ten years, payment of a fine of UGX 4.9 million (approximately EUR 1,160), or 2% of the corporation's gross income in the event the offence is committed by a corporation.

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

Yes. The National Information Technology Authority – Uganda (NITA-U) is designated as the national data protection authority and also maintains the Data Protection Register, which lists every institution, person or public body collecting or processing personal data.

The Personal Data Protection Office is Uganda's independent data protection authority established under NITA-U and it is responsible for overseeing the implementation of and enforcement of the Data Protection and Privacy Act.

⁵⁷ Section 18, Data Protection and Privacy Act 2019

⁵⁸ Part VIII, Data Protection and Privacy Act 2019

Does your country's data privacy law follow the framework of the EU's GDPR?

Partially. The Act aims to protect the privacy of the individual and of personal data and is, in some limited aspects, inspired by the GDPR. The Act also mirrors the UK Data Protection Act, 1998, which revolves around several principles concerning data protection and collection.

The Act created the personal data protection office in NITA-U, also an independent body synonymous to the UK's Information Commissioner's Office, set up under Chapter 6 of the GDPR.

One of the main contrasts with GDPR is the absence of legitimate interest as a legal basis for processing in the Ugandan Act.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

Recently, there has been an upsurge in the data processing industry in respect of the data mining and data analytics areas. The COVID-19 pandemic has also led to an increase in remote access to information and data globally. It is therefore imperative that African countries raise awareness, invest in training and set up relevant infrastructure to enable the implementation of data privacy and protection.

There is a vast need for autonomous data protection and privacy regulatory bodies which can independently impose and collect fines so that funds are not lost in corruption and embezzlement, and so that personal data is lawfully collected and processed, and breaches are managed throughout the continent, to promote economic and social development.

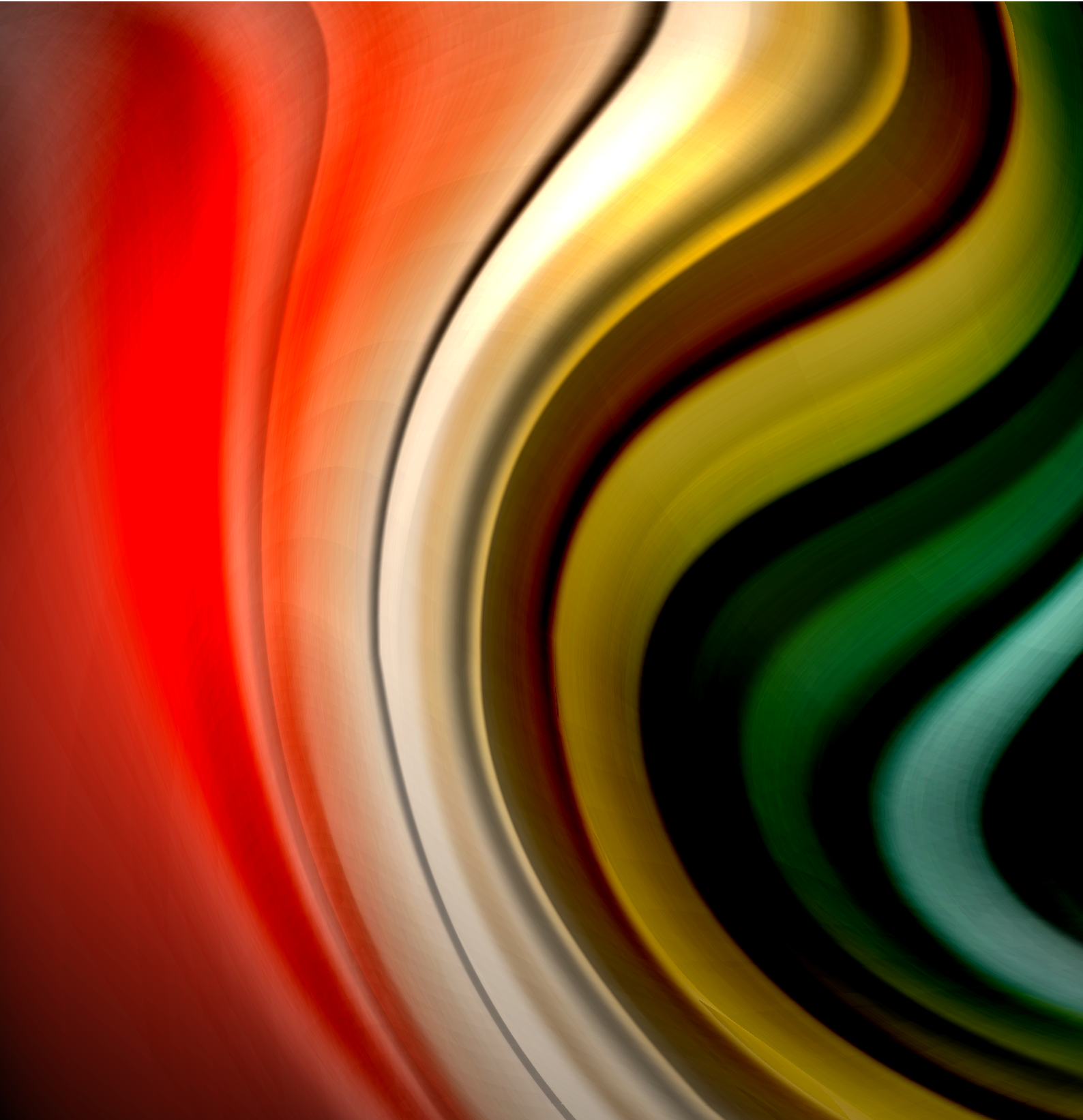
Following the adoption of the African Union Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention), it is also imperative for African countries to use this mechanism in the establishment and implementation of regulatory frameworks on cyber security and personal data protection in the new electronic and technology era where, a lot of personal data and information may easily be accessed remotely.

Arnold Lule Sekiwano – Partner
lule@engorumutebi.co.ug

Ritah Nakalema – Senior Associate
+256 (0) 393 - 216- 520
+256 (0) 414 - 231- 393/4

Engoru, Mutebi Advocates
Kampala, Uganda

Zimbabwe



Zimbabwe

What laws currently exist in your country to protect and ensure the privacy of data?

The following laws provide for the privacy of data:

- **Section 57 of the Constitution** of Zimbabwe, which provides for the right to privacy
- **Section 62 of the Constitution**, which provides for the right of access to information
- **Data Protection Act**,⁵⁹ which provides for data protection in compliance with section 57 of the Constitution
- **The Freedom of Information Act**⁶⁰
- **The Courts and Adjudicating Authorities (Publicity Restrictions) Act**,⁶¹ which regulates and restricts court attendance and publication of proceedings in certain instances
- **Section 17(1) of the Census & Statistics Act**,⁶² which restricts the disclosure of information obtained for the purposes of the Act
- **Section 8 of the National Registration Act**,⁶³ which directs the persons working in the Registrar General's office to keep in secret all information coming to their knowledge in the exercise of their duties
- **Section 48 of the Consumer Protection Act**,⁶⁴ which provides for the consumer's right to confidentiality and privacy
- **Section 11 (b) of the Postal and Telecommunications Act and Subscriber Registration Regulations**,⁶⁵ which obliges service providers to obtain subscribers' consent before transferring data to a foreign host.

Are these laws in force?

Yes.

What are the most recent legal developments, or pending developments, in your country around data privacy and protection?

Zimbabwe has made significant progress in the past five years in promulgating laws which deal with data privacy and protection. The Data Protection Act was promulgated on 3 December 2021 in an effort to address the challenges that have arisen due to technological advancements.

On 21 September 2021, Cabinet also approved the principles of the Electronic Transaction and Commerce Bill. We have not had sight of the principles and are unable to provide further details. However, in making the announcement, the Minister of Information Publicity and Broadcasting Services stated that:

"The nation is being informed that the development of information communication technologies in cyberspace requires that the legal and policy environment be adapted to take into account the relevant changes. In particular, there is need for a holistic electronic transaction regulation regime in the face of the opening up of markets and movement of goods and services across borders, and growing incidences of scams and unfair practices, which leave the end-user at risk".

59 Chapter 11:22

60 Chapter 10:34

61 Chapter 7:04

62 Chapter 10:05

63 Chapter 10:17

64 Chapter 14:14

65 Statutory Instrument 95 of 2014

If your country has privacy laws, what constitutes the definition of personal data according to the law?

The term “personal data” is not defined. The term “personal information” is defined in the Freedom of Information Act ⁶⁶ as information about an identifiable individual, which includes:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual
- Information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
- Any identifying number, symbol or other particular assigned to the individual
- The address, fingerprints or blood type of the individual
- The personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual
- Correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence
- The views or opinions of another individual about the individual
- The views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual
- The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual
- But excludes information about an individual who has been dead for more than twenty years.

The Data Protection Act defines “personal information” as information relating to a data subject, ⁶⁷ and includes:

- A person's name, address or telephone number
- A person's race, national or ethnic origin, colour, religious or political beliefs or associations
- A person's age, sex, sexual orientation, marital status or family status
- An identifying number, symbol or other particulars assigned to a person
- Fingerprints, blood type or inheritable characteristics
- Information about health care history, including a physical or mental disability
- Information about educational, financial, criminal or employment history
- Opinions expressed about an identifiable person
- The individual's personal views or opinions, except if they are about someone else
- Personal correspondence pertaining to home and family life.

⁶⁶ Section 2 Freedom of Information Act

⁶⁷ Section 3 Data Protection Act

What are the rights of data subjects according to any data privacy law in your country?

The rights that accrue to data subjects under existing laws are:

In terms of the Freedom of Information Act:

- The data subject has a right to be informed of a request for information made in respect of them. The notification is done by the information officer who must advise the data subject of the request and the protection granted in terms of the Act with respect to the information concerned.⁶⁸
- The data subject also has a right to make written representations to the information officer why the request for access should be refused or give written consent for the disclosure of the information requested.⁶⁹

In terms of the Consumer Protection Act:

- Any confidential information pertaining to a consumer or prospective consumer received, compiled, retained or reported in terms of the Act is confidential and should be used only for the purpose permitted or required in terms of the Act, or other national legislation.⁷⁰
- The consumer's right to confidentiality and privacy includes the right to refuse to accept, or require another person to discontinue, or in the case of an approach other than in person, to pre-emptively block, any approach or communication to that person; if the approach or communication is primarily for the purpose of direct marketing.⁷¹

In terms of the Data Protection Act, a data subject has a right to:

- Be informed of the use to which their personal information is to be put
- Access their personal information that is in custody of the data controller or data processor
- Object to the processing of all or part of their personal information
- Correct false or misleading personal information
- Delete false or misleading data about them⁷²
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them unless the data subject has consented to same.⁷³

In terms of the Postal and Telecommunications Act Subscriber Registration Regulations, section 11(b) directs service providers to seek subscribers' consent to the transfer of their personal data when the provider intends to transfer information relating to the subscribers to a foreign host.

⁶⁸ Section 32 Freedom of Information Act

⁶⁹ Section 33 Freedom of Information Act

⁷⁰ Section 48 (1) Consumer Protection Act

⁷¹ Section 49 Consumer Protection Act

⁷² Section 14 Data Protection Act

⁷³ Section 25 Data Protection Act

Briefly, what are the obligations of data controllers and processors according to data privacy in your country?

The obligations of data controllers and data processors as set out in the Data Protection Act are as follows:

- To ensure that data processed is:
 - Adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed ⁷⁴
 - Accurate and, where necessary, kept up to date ⁷⁵
 - Retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed ⁷⁶
 - Accessible regardless of the technology used and ensure that the evolution of technology shall not be an obstacle to the access or processing of such data. ⁷⁷
- To ensure that data is collected for specified, explicit and legitimate purposes and that the data is not further processed in a way incompatible with such purposes. ⁷⁸
- To make certain disclosures when collecting data directly from data subject or from a third party. ⁷⁹
- To ensure that personal information is processed in accordance with the right to privacy of the data subject. ⁸⁰
- To process data only as instructed by the controller, without prejudice to any duty imposed by law. ⁸¹
- To take the appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data. ⁸²
- To appoint a data processor who will provide sufficient guarantees regarding the technical and organisational security measures employed to protect the data associated with the processing undertaken and ensure strict adherence to such measures. ⁸³
- To notify the Data Protection Authority, without any undue delay of any security breach affecting data he or she processes, in the prescribed manner. ⁸⁴
- To take all the necessary measures to comply with the principles and obligations set out in the Act and have the necessary internal mechanisms in place for demonstrating such compliance to both the data subjects and the Authority in the exercise of its powers. ⁸⁵
- Not to transfer personal information of a data subject to a third party who is in a foreign country, unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out. ⁸⁶

74 Section 7(1) (a) Data Protection Act

75 Section 7(1)(b) Data Protection Act

76 Section 7(1) (c) Data Protection Act

77 Section 7(2), Data Protection Act

78 Section 9, Data Protection Act

79 Sections 15 and 16, Data Protection Act

80 Section 13 Data Protection Act

81 Section 17, Data Protection Act

82 Section 18, Data Protection Act

83 Section 18(4), Data Protection Act

84 Section 19, Data Protection Act

85 Section 24, Data Protection Act

86 Section 28, Data Protection Act

What are the penalties for non-compliance with data privacy law in your country?

In terms of section 78 (3) of the Consumer Protection Act, the disclosure of any person's confidential information obtained in carrying out any function in terms of the Act attracts a fine not exceeding level 14 (currently ZWD 500,000.00) or imprisonment for a period not exceeding two years or to both.

In terms of section 8 of the Courts and Adjudicating Authorities (Publicity Restriction) Act [Chapter 07:04], the disclosure of any information, fact, matter, document, recording or part thereof which is prohibited shall attract a fine not exceeding level ten (currently ZWD 70,000.00) or imprisonment for a period not exceeding two years or both.

Contravention of sections 11, 13, 18(4), 24 and 28 of the Data Protection Act is an offence which attracts a fine not exceeding level eleven (ZWD 100,000.00) or imprisonment for a period not exceeding seven years or to both.

It is important to note that the Data Protection Act also introduces consequential amendments to the Criminal Law (Codification and Reform) Act [Chapter 9:23] and it seeks to expand the scope of the latter Act to deal with offences such as unlawful acquisition of data, hacking, cyber bullying and harassment, sending spam, transmission of data with intimate images without consent of the person concerned, pornography involving a child or exposing pornography to children, etc.

What is the structure of governance around data protection laws – has an agency been introduced to enforce compliance?

The Postal and Telecommunications Regulatory Authority is the designated Data Protection Authority ⁸⁷

87 Section 5 Data Protection Act



Does your country's data privacy law follow the framework of the EU's GDPR?

Zimbabwe does not have a comprehensive data privacy law and the legislative provisions in place do not follow the framework of the GDPR.

How imperative do you think it is for African countries to implement data privacy and protection, and why?

It is crucial for African countries to put in place laws regulating the protection of data in light of global technological advancements. Several jurisdictions are lagging behind in so far as regulation of this area is concerned.




Amalia Manuel – Partner
amalia@praetor.co.zw
+263 242 704244 – 6

Atherstone & Cook
Harare, Zimbabwe



ATHERSTONE & COOK



Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

bakermckenzie.com

© 2021 Baker McKenzie. All rights reserved. Baker & McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.