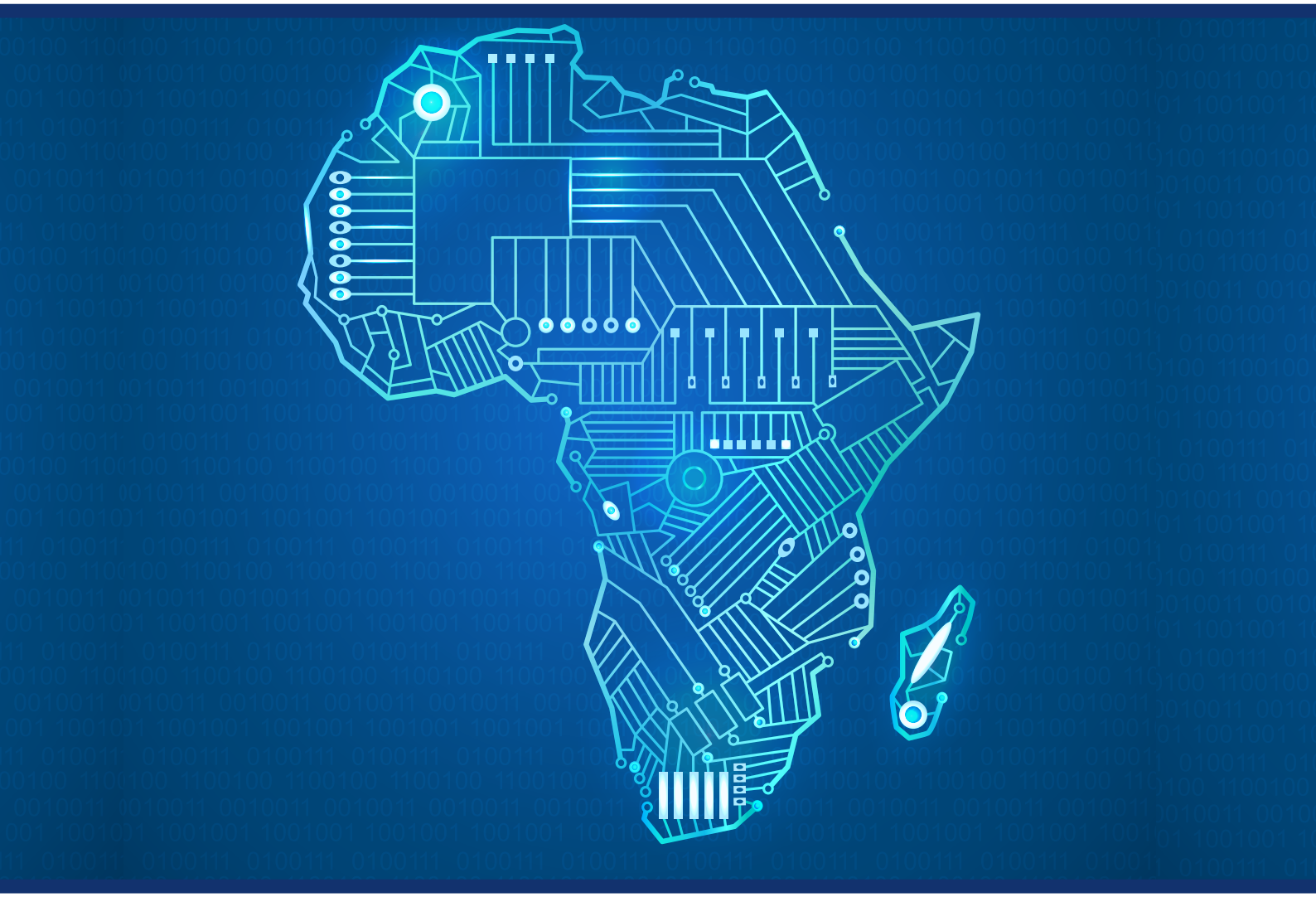
The IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa



The International Bar Association (IBA), established in 1947, is the world's leading international organisation of legal practitioners, bar associations, law societies, law firms and in-house legal teams. The IBA influences the development of international law reform and shapes the future of the legal profession throughout the world. It has a membership of more than 80,000 lawyers, 190 bar associations and law societies and 200 group member law firms, spanning over 170 countries. The IBA is headquartered in London, with offices in São Paulo, Seoul, The Hague and Washington, DC.

International Bar Association
4th Floor, 10 St Bride Street
London EC4A 4AD
United Kingdom
iba@int-bar.org
www.ibanet.org

The IBA African Regional Forum aims to further enhance the objectives of the IBA by means of cooperation, support of bar associations in developing countries, development of laws, and the exchange of information and ideals.

Contents

Acknowledgements

The IBA African Regional Forum would like to express its profound appreciation to the Consultant and all Forum members who contributed in many diverse ways to the development of this Guide. The Forum would especially like to acknowledge and thank:

- Teki Akuetteh Falconer – *Consultant for the Project and Senior Partner, Nsiah Akuetteh & Co, Ghana*
- Ralph T O'Brien – *Principal Consultant, REINBO Consulting, UK*
- Pieter Steyn – *Director, Werksmans, South Africa*
- Anthony Atata – *Partner, Hallblack Law Firm, Nigeria*
- Oyeyemi Aderibigbe – *Senior Associate, Templars, Nigeria*
- Ademola Bidemi – *General Counsel, Unilever, Nigeria*
- Sydney Chisenga – *Managing Partner, Corpus Legal, Zambia*
- Alice Namuli Blazevic – *Partner, Katende, Ssempebwa & Company Advocates, Uganda*
- Mamadou Mbaye – *Mame Adama Gueye & Associates, Senegal*
- Danielle Moukouri Djengue – *Managing Partner, D Moukouri & Partners, Cameroon*
- Osayaba Giwa-Osagie – *Senior Partner, Giwa-Osagie & Co, Nigeria*

Foreword

Africa's data protection landscape has undergone significant changes over the past decade. There has been an increase in the adoption and implementation of data protection laws and frameworks by countries, regional bodies and the continent at large. The implementation of the General Data Protection Regulation of Europe (GDPR) has witnessed calls by data controllers and processors in Europe on their counterparts in Africa for more stringent standards to protect the personal data they process on their behalf. Data protection regulators in Africa have also called on the continent's legal practitioners to comply with their respective data protection laws even though little or no guidance has been provided to help lawyers comply with these directives.

These calls have been met with requests for further guidance and support, as most legal practitioners have little or no capacity to facilitate compliance to data protection obligations due to its complex and technical nature. The Guide facilitates understanding of privacy/data protection by providing practical solutions to manage personal data within a law firm.

The Guide addresses privacy/data protection planning, functionality and management of a legal practice in Africa. The guide will provide lawyers in Africa with sustainable, practical and easy to implement data protection controls/protocols. It has been developed drawing from the basic principles contained in the various laws and frameworks on the continent of Africa as well as global trends such as the General Data Protection Regulations (GDPR) of Europe and other associated international best practices.

It also provides an overview of the data protection landscape in Africa, a checklist for assessment of data protection compliance by legal practitioners, privacy-by-design mechanisms, a step-by-step guide to the implementation of data protection principles and data classification methods for privacy management of a legal practice.

Key definitions

Personal data	Information about an individual or a person (natural person) that can be identified or is identifiable directly or indirectly from an information. Personal data may be as simple as a name or a telephone number or may include other identifiers such as internet protocol (IP) addresses, cookie identifiers, radio frequency identification tags (RFID) or other factors. Under data protection legislation such as the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA), personal data is defined as including data of a legal person.
Special/sensitive category of personal data	This category personal data require greater protection because it is sensitive. It normally includes the following information on a data subject: • race, colour, ethnic or tribal origin; • trade union membership; • political opinions; • religious, philosophical or other beliefs; • health (medical, physical, mental health) information; • genetic information; • biometric information; • sex life and/or sexual orientation.
Data subject	An individual who can be identified, directly or indirectly through an identifier such as a name, ID number, location data, or through factors specific to that person's physical, physiological, genetic, psychological, economic, cultural or social identity. Under data protection legislations such POPIA, data subject is defined to include a legal person.
Data controller	A person, company or body which, either alone, or jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.
Data processor	A person, company or body (other than an employee of the data controller) who processes personal data on behalf of the data controller.

Processing	The means of obtaining, recording or holding information, or carrying out any operation or set of operations on that information. Processing includes: • organisation, adaptation or alteration of the information or data; • retrieval, consultation or use of the information or data; • disclosure of the information or data by transmission, dissemination, or otherwise making it available; • alignment, combination, blocking, erasure or destruction of the information or data.

1. Introduction

The data protection landscape in Africa has undergone significant changes over the past decade. There is an increase in the adoption and implementation of data protection laws and frameworks by countries, regional bodies and the continent at large. International developments such as the coming into effect of the General Data Protection Regulation of Europe (GDPR) also, led to calls by data controllers and processors in Europe on their counterparts in Africa for more stringent standards to protect the personal data they process on their behalf.

Legal practitioners in Africa have also witnessed an increased call by data protection regulators in Africa to comply with their respective data protection laws. However, there continues to be little or no guidance on how lawyers can comply with these directives. All calls for the implementation of privacy and data protection by lawyers in Africa have been met by urgent requests for further guidance and support, as most legal practitioners have little or no capacity to ensure compliance with data protection obligations due to their complex and technical nature.

This Guide provides a template for a model law (in Appendix two), an understanding of privacy/data protection and showcases practical solutions and tools that legal practitioners in Africa can use to manage personal data in their operations. The Guide has been developed taking into consideration the importance of meeting compliance obligations under data protection laws. It aims to help legal practitioners uphold the professional and ethical duties to protect their clients, minimise potential sanctions and avoid reputational damage associated with the mismanagement of personal data.

The Guide addresses privacy/data protection planning, functionality and management of a legal practice in Africa. It provides sustainable, practical and easy to implement data protection controls/protocols for lawyers, taking into consideration the basic principles as contained in the various laws and frameworks across the continent, as well as key global trends such as the European Union's General Data Protection Regulations (GDPR).

The Guide also provides: a checklist for the assessment of data protection compliance by legal practitioners; privacy-by-design mechanisms; a step-by-step guide to the implementation of data protection principles; and, data classification methods for privacy management in a legal practice. It is a useful resource on data protection law in Africa and ensuring compliance within a legal practice for any legal practitioner in Africa.

2. Data protection in Africa

Data protection is the process of safeguarding personal information, in accordance with a set of principles laid down by law. The fundamental purpose of data protection legislation is to guard against the dangers associated with the collection and processing of personal information arising from the use of computers. In principle, it involves two parties an information owner (usually individuals) and an information holder (individual or organisations that collect and process personal information eg, government agencies, hospitals, technology companies, law firms, hotels, banks, etc). Data protection seeks to balance an individual's expectation of privacy of their information and communication with that of the information holder's legitimate use of such information. In different parts of the world data protection is also known as information privacy, data privacy, or digital privacy.

Data protection standards have been developing for over 100 years. Key landmarks include; the first automated business data processing dating back to the 1890 US census; the end of the Second World War; the Universal Declaration of Human Rights in 1948; the establishment of the basic principles of data protection by the Organisation for Economic Co-operation and Development (OECD) in 1980, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (popularly known as 'Convention 108') by the Council of Europe in Strasbourg, France in 1981. Technology has always played and continues to play a key role in the development of data protection laws. As the world of business data processing evolved, so did the methods and practices of data protection. The frameworks and laws have developed mainly in response to technological advances which increase the collection, holding and dissemination of personal information as well as surveillance of people.

Data protection law is derived from fundamental human rights law. As such, data protection law can be considered a balancing act between the needs of the many and the needs of the individual. As a topic, this makes for a highly emotive and argumentative arena, as there can be entirely valid competing arguments, where both parties are acting in good conscience believing they serve the best interests of their clients. Any organisation which manages individuals' personal data will be required to comply with legal obligations; fulfil the moral imperative to protect the data of individuals within their care; and ensure that their partners and suppliers do the same.

Privacy as a fundamental right is referenced in both the Universal Declaration of Human rights and the European Convention on Human Rights.

Universal Declaration of Human Rights 1948 (Article 12)

'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

European Convention of Human Rights 1950

(Article 8 of the Convention - Right to respect for private and family life)

1. 'Everyone has the right to respect for his private and family life, his home and his correspondence.
2. 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

In light of these fundamental rights, a balancing act often applies, as data protection laws include considerations of the needs of two interested parties: the individual's data and a corporate/business/government interest.

There is however a difference between privacy and data protection. While privacy can be awkwardly used as a euphemism for 'secrecy', it also applies to areas which data protection laws cannot reach. Data protection only applies to the communications, correspondence and information on individuals. Privacy stretches further. It reaches into areas such as territorial, bodily privacy and organisational privacy.

As discussed in Chapter 3 on principles, data protection covers a larger area than simply the decision to disclose or keep confidential, and therefore gives organisations obligations where privacy and security are no longer an issue. In fact organisations have data protection obligations throughout the data lifecycle regardless of confidentiality considerations.

Finally, it is worth noting that data protection law as a human right, stands apart from commercial considerations of intellectual property law, and data 'ownership'. The data controllers have obligations, individuals have rights and the regulators have powers.

None of these obligations, powers or rights involve the assignment of intellectual property and ownership rights. In fact to do so often places individuals at a disadvantage, as human rights should be available to everyone for free. Assigning commercial value to data and allowing data rights to be bought and sold should be prohibited, as it leads to data protection and privacy rights afforded only to those with the means to defend them, and often places the disadvantaged in a worse situation, as they are forced to sell or relinquish data rights in their economic interest.

Conventions that operate and been favoured across various African countries include the OECD Guidelines, Directive 95/46/EC of Europe, Council of Europe Convention 108 (and 'Modernised 108+'), the Malabo Convention, ECOWAS Directive, EAC and SADC model laws. These conventions and the existing privacy or data protection laws in Africa have also been taken into consideration in the development of this Guide.

Africa's data protection/privacy environment has been steadily growing since the year 2000. This has been fuelled by the need to leverage on information and communications technologies (ICTs) as a strategic component in the development of many economies. The advantages countries stand to gain by deliberately embracing policies that enable, guarantee trust and the development and growth of ICTs cannot be overemphasised.

Africa's data protection/privacy ecosystem is largely influenced by Europe's uniform approach that looks at an omnibus law which governs both public and private sectors while recognising data protection/privacy as a human right. Although the African continent has witnessed some dynamic and progressive frameworks and laws on data protection/privacy, the ecosystem can still best be described as 'underdeveloped and disparate'. Today,

there are various frameworks and laws across Africa which are at different levels of implementation. Though similar in nature, these frameworks and laws have variations that create challenges around harmonisation, collaboration and coordination. *If African countries want to be important players in the offshoring and outsourcing markets, (apart from its competitive telecoms infrastructure and multilingual workforce) there is the need for a harmonised and adequate data protection environment, especially when it comes to doing business with the rest of the world.*

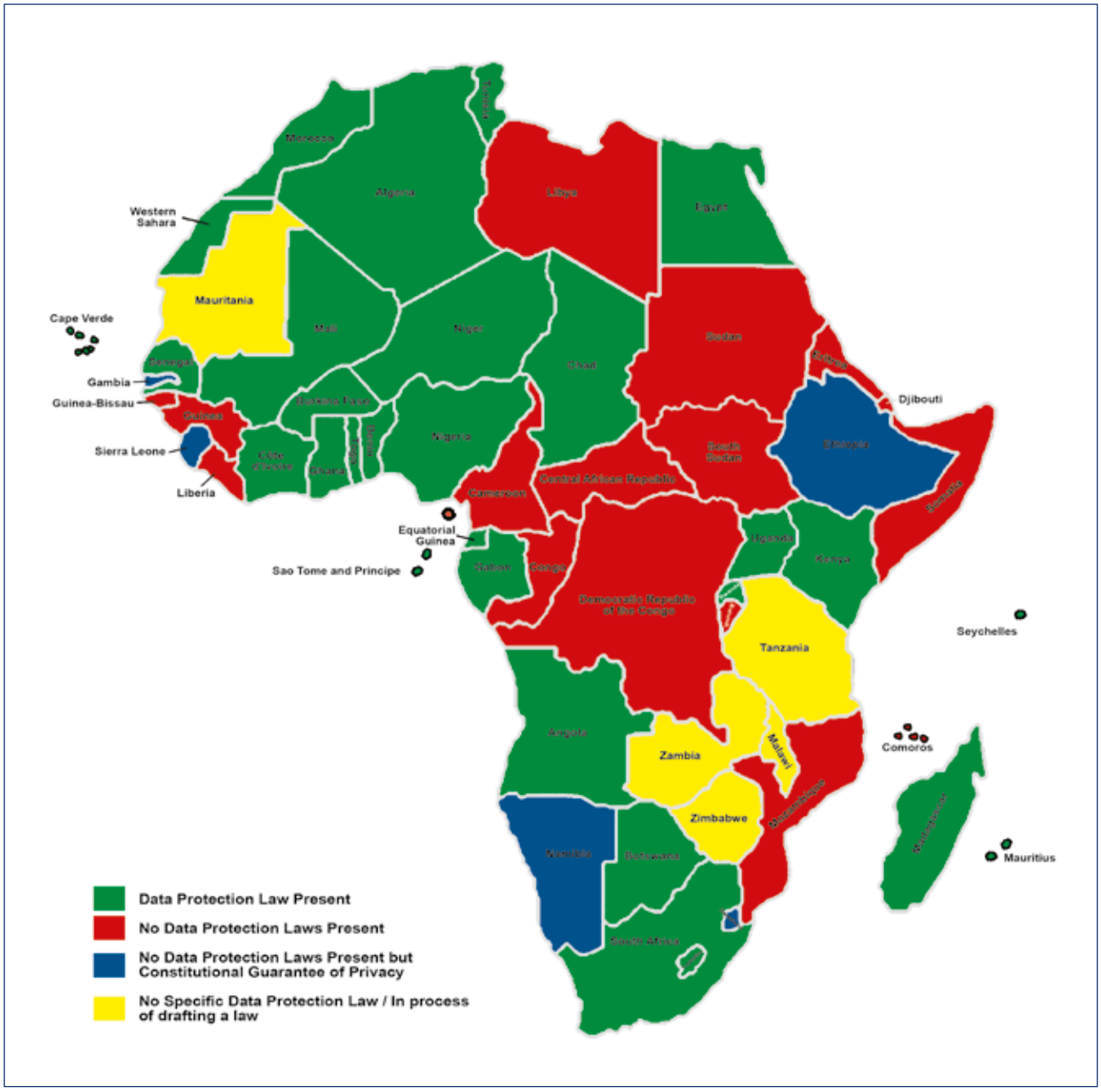


Figure 1: Heat map on the status of data protection in Africa

At continental and regional levels the following frameworks exist.

- African Union Convention on Cyber Security and Personal Data Protection (2014)[1] (also known as the Malabo Convention)
- SADC Model Law on Data Protection (2010),[2] ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010); and
- the EAC Framework for Cyberlaws (2008).

The Malabo Convention has only been signed by 14 out of the 55 AU member countries of which only eight countries have ratified and deposited after more than six years of its adoption. The Convention will come into force 30 days after the 15th ratification and deposit. Although the AU Convention can be a useful starting point to harmonisation, it has been argued that the data protection framework it provides may have outlived its usefulness as bridge for collaboration (especially with Europe) because it was predominantly modelled after the EU Data Protection Directive 95/46/EC that has now been repealed and replaced by the General Data Protection Regulations (GDPR).[3]

Nevertheless, the Malabo Convention does provide a personal data protection framework which African countries may potentially transpose into their national legislation and encourages African countries to recognise the need for protecting personal data and promoting the free flow of such personal data, taking global digitalisation and trade into account. The Convention and guidelines are strategic frameworks for harmonisation which is essential to facilitate cross-border data transfers within Africa as well as that with the rest of the world. A harmonised data protection environment is critical for the socio-economic development in the fourth industrial revolution. The ability to move seamlessly and transfer such data including personal data will influence growth and development.

As of July 2020 there were 29 African countries with legislation which regulates data protection/privacy,[4] out of which about 11 have data protection authorities. Of the countries that have data protection laws there are significant differences in their structures and approaches to implementation. These differences in the various country laws have been influenced by their legal, political, economic and cultural differences.

The disparate and underdeveloped nature of data protection and privacy laws in Africa poses several challenges to industry players, regulators and all stakeholders within Africa and the rest of the world. It not only makes it difficult for industry players but weakens the opportunity for a united front and the ability of the continent to negotiate bridges for collaboration and cooperation.

Data protection and privacy continue to face many changes in Africa some of which stem from the lack of resources (human and financial) to build the necessary capacity to develop the data protection/privacy ecosystem. Most data protection authorities in Africa are poorly resourced and therefore lack the ability to attract the high-calibre staff needed to drive their agenda. The lack of resources also weakens regulators' enforcement capabilities.

---

1 African Union, 'African Union Convention on Cyber Security and Personal Data Protection', 27 June 2014, available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

2 Establishment of Harmonized Policies for the ICT Market in the ACP Countries, 'Data Protection: Southern African Development Community (SADC) Model Law', 2013, available at: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

3 Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), available at: https://gdpr-info.eu.

4 Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Egypt, Equatorial Guinea, Gabon, Ghana, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Niger, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Seychelles, South Africa, Togo, Tunisia, Uganda and Western Sahara.

Data protection and privacy expertise on the African continent is also sparse. There are few experts that are sparsely scattered, minimising their impact in the environment. An efficient data protection ecosystem can only be driven in a well-informed environment. Unfortunately for Africa, little has been done in the way of awareness creation and capacity building to support this developing industry. This challenge has also fuelled the general lack of knowledge and understanding on issues of data protection and privacy.

Due the unconsolidated nature of the laws across Africa, there are also challenges around the cross-border data transfers within Africa as well as between Africa and the rest of the world. The existing laws on cross-border transfers are varied, with countries that have restrictions on transfers and others that do not. These restrictions usually come by way of prior authorisations/approvals and data residency/localisation laws. With predominantly limited financial resource and staff constraints as well as existing bureaucratic systems the prior authorisations/approvals are expensive and have been known not only to burden the authorities but also discourage growth and innovation.

These challenges are not insurmountable but can be addressed by painstakingly working out frameworks for harmonisation, issuing guidance, cooperation and collaboration as well as exploring mechanisms to improve cross-border data flows. As an emerging economic region, Africa is growing at a rapid pace, it is therefore important to create an environment that facilitates the effective conduct of business within Africa and with other international markets. While the need to understand the African data protection/privacy regulatory landscape is key, efforts to address the challenges identified will be crucial for sustained socio-economic development in Africa.

3. Data protection principles

Data protection in Africa is usually based on a law which lays down the general principles applicable to the processing of personal information in any given situation. This is due to the omnibus nature of the continent's data protection laws. While some countries, such as the US, have had various laws that focus on specific sectors or issues, an omnibus law seeks to address the collection and use of all personal information, regardless of industry or sector.

Data protection legislation in Africa can also be said to be principle-based. Such laws do not contain hard and fast rules but instead rely on a context-specific focus for entities to determine their own compliance. Most of the principles in data protection laws and frameworks in Africa have similarities with the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 OECD Guidelines) as well as the EU Data Protection Directive 95/46/EC and the more recent GDPR. The 1980 OECD Guidelines are an internationally accepted set of rules for processing personal information and have been the fundamental bedrock of most data protection laws across Africa. The OECD Guidelines provided the following as basic principles of national application.[5] These can also be found in many data protection laws across Africa:

- Collection limitation principle
- Data quality principle
- Purpose specification principle
- Use limitation principle
- Security safeguards principle
- Openness principle
- Individual participation principle
- Accountability principle

The Overview of data protection laws in Africa (see Appendix one) provides a detailed list of the various principles which can be found under data protection laws across the continent. The data protection principles stated in article 13 of the Malabo Convention are also as follows:

- Principle 1 – Legitimacy of personal data processing
- Principle 2 – Lawfulness and fairness of personal data processing
- Principle 3 – Purpose, relevance and storage of personal data processing
- Principle 4 – Accuracy of personal data processing
- Principle 5 – Transparency of personal data processing
- Principle 6 – Confidentiality and security of personal data processing

As a result of their principle-based nature, for several decades data protection laws and frameworks have adapted to changes in behaviour and technology. The principle-based approach gives room to self-assess and determine responses to changes in society using the principles as a guiding tool. Under data protection laws, all entities which collect and use personal information are therefore expected to manage their own privacy risks by

5 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

applying the principles to each personal data processing purpose/context and data lifecycle.

For this purposes of this Guide, the data protection principles that have similarities with most of the principles listed in the laws and frameworks across Africa have been used to explain what they mean and how they can be implemented.

Principle of transparency (openness)

This principle key to a data controller's ability to demonstrate compliance. It places obligations on data controllers to be transparent and honest about the way they collect, hold, use or share information about individuals. To achieve openness, the data controller must adhere to all other data protection principles and provide accessible information to the data subject on how their information is processed, what information is stored, where it is stored and why it is stored.[6] The principle of transparency (openness) is based on the legal tenet that 'there should be no covert surveillance without lawful authority'.

Transparency must be achieved both internally and externally through:

- *Data protection policies* which clearly describe how a data controller collects, holds and uses personal information as well as how it intends to achieve the principles.
- A designated *independent data protection officer/team* that monitors and ensures accountability to policies throughout an organisation.
- *Codes of conduct* that provide common rules on how data protection will be implemented within an organisation.
- *Privacy notices* that provide simple and clearly understood information on how their information will be processed at the point of collection.
- *Guidelines* developed and published by the regulator for data controllers to follow.
- *Breach notification mechanisms* based on the risk profile of the data being processed.
- *Procedures and processes* which allow for regular external review of processes and policies by third parties to ensure that the data controller is living up to its own standards.

Privacy notices

Privacy notices are one of the key methods to ensure transparency. Individuals must be provided with a range of privacy notices regardless of the legal basis which justifies their use. Privacy notices are not contractual but must be given at the point of collection to educate an individual. They can be given at the point when an individual is taking a service, or as a 'catch all' corporate high-profile privacy FAQ linked to other information.

An organisation will need different privacy notices, which may be provided on the basis of the information that is being collected at any point in time. Privacy notices can be given in many formats including verbal, recorded messages, 'pop up' windows, videos, as part of call centre scripts, text at the beginning or end of forms, internet pages, etc. The most important point is to ensure the information is communicated succinctly without using legal language and jargon, delivered in clear and simple language, bearing in mind the audience (data subjects) which the data controller serves.

---

6 Teki Akuetteh Falconer, 'Principles of data protection', a series of articles in *The Daily Graphic of Ghana*.

When data is collected directly from the data subject, privacy notices must include the following information:

- the identity and the contact details of the data controller;
- the contact details of the data protection officer, or privacy team;
- the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- where the processing is based on legitimate interests, what those interests are;
- where consent is relied on, how to withdraw consent;
- where the processing is based on a contract, what the contract is;
- where the processing is based on a legal obligation, what it is;
- the recipients or categories of recipients of the personal data, if any;
- any international transfers and how the data is protected in the other jurisdiction and any justification for transfer;
- the period for which the personal data will be stored, or the criteria used to determine that period;
- the existence of the rights the data subject may have;
- the right to lodge a complaint with a supervisory authority (the regulator);
- if data subject is required to provide the personal data, the possible consequences of failure to provide such data; and
- the existence of any automated decision-making, including profiling, meaningful information about the logic involved, as well as the consequences for the data subject.

In instances where the personal data has been given or passed on to a new data controller (and not collected from the data subject), the new data controller also has a responsibility to reach out proactively to the data subject and inform them that they now have their personal data in their possession, if possible. This does not extend to processors, who should be covered by the scope of the original privacy notice.

Again, this is to prevent situations where third-party organisations are in receipt of the personal data from other sources without the knowledge of the data subject. In this case the new controller should state in addition to the above, where/who they have received the personal data from. A typical example of such indirect collection is the buying and selling of marketing lists or collection of data from social media platforms.

Principle of legitimacy of personal data processing (legal basis)

The principle of the legitimacy of processing personal (also known in as use justification) is essentially prohibition on the use of personal data without good cause or legal basis. It requires that personal data must be processed fairly and lawfully. It means that, just because one can find data or have access to it, does not mean one can

legally collect it and use it. It puts an obligation on data controllers not to process personal data without a legal justification.

The main purpose is to protect the interests of the individuals whose personal data is being processed. It applies to everything one does with the personal data, except where an exemption has been given under law. It is important to emphasise that processing of personal data which has an adverse effect on an individual may not necessarily be unreasonable or unlawful. The key is whether the negative effect is justifiable under the law. In practice, therefore it means that a data controller/processor must:

- have legitimate grounds for collecting and using the personal data;
- not use the information or data in ways that have unjustifiable adverse effects on the individuals concerned;
- handle personal data only in ways individuals will reasonably expect; and
- make sure they do not do anything unlawful with the personal data.

This principle of legitimacy can vary from jurisdiction to jurisdiction, and national laws can create their own, specific legal basis and exemption. Generally, the principle has the following characteristics.

- *Power favouring the data controller:*
  - necessary for meeting a legal obligation placed on the data controller;
  - necessary for the implementation of a contract, or in order to enter into a contract with the data controller.
- *Power balancing test between the data subject and data controller:*
  - necessary for the legitimate interests of the data controller, balanced against the rights and freedoms of the individual;
  - necessary in the public interest, balanced against the rights and freedoms of the individual; and
  - necessary in the individuals vital interest, where they are incapable of giving consent.
- *Power in favour of the data subject:*
  - consent, which shall be –
    - easy to withdraw as to give;
    - an action taken by the individual (not an opt-out);
    - informed (see transparency);
    - freely given (no imbalance of power);
    - specific (limited to a situation or format, rather than wide or generalised).

Often the individual will have fewer rights if the data is required for contract. In this case, they have the option to terminate the contract through its normal severance provisions. In situations where a national law requires the data collection, such as for income tax, or for public registers the individual has no such rights.

A law firm may have a contract to provide legal services for a data subject and therefore must collect the minimum necessary personal information for that contract in order to perform the services and collect its fees. But the firm may also wish to use of the information for direct marketing its other services (such as training programmes) to the Individual. The data is the same in each case, but as the purpose changes, so does the legal basis. All the purposes must therefore be clearly documented in the privacy notice.

The three 'balancing test' legal basis (legitimate interests, public interest and vital interests) must be documented by the data controller if relied on. There needs to be an assessment of the organisation's interests versus the individual's expectation of privacy. Relying on such basis opens up the right to an objection, and an individual may challenge the decision taken.

There is often misconception that consent should be used as a preference. Generally, this is not so, as it is the worst legal basis for data controllers to rely on. It is easily withdrawn, and hard to prove that the consent is valid. A society run on consent, for example, would not function, as an individual could for example, withdraw consent for data use for taxation or criminal investigation, which would rapidly move the world into anarchy. Furthermore, consent between employers and employees will almost never be valid, as the individual wants a job, which makes it impossible for the consent to be truly and freely given in an equitable situation.

Also, many jurisdictions require additional protection of special category (sensitive) data by asking the data controller to provide a second legal basis in order to justify such processing. This operates as a ban on the processing of the special category (sensitive) data unless the data controller can provide both justifications. Typically, the justification for the processing of special category data includes the following:

- Processing necessary for employment, social security and social protection law.
- Processing necessary for the vital interests of the data subject or of another natural person where the data subject is incapable of giving consent.
- Processing carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body such as political, philosophical, religious or trade union.
- Processing of personal data which is manifestly made public by the data subject.
- Processing necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing necessary for reasons of substantial public interest, with appropriate safeguards.
- Processing necessary for the purposes of preventive or occupational medicine, or healthcare.
- Processing necessary in the public interest for public health and safety.
- Processing necessary for archiving purposes in the public interest.
- Processing necessary for scientific, historic, research or statistical purposes.
- Where the data subject has given explicit consent to the processing for a specific purpose.

Organisations will have to spend time understanding the data they process and the purpose for which they use it, in order to document the relevant legal basis. If they cannot find a valid legal basis, it could be that they are

breaking the associated data protection law. It is worth noting that because data processors do not determine purposes of use, they are presumed to operate *intra vires* under the legal basis set by the data controller.

Principle of purpose limitation

This principle involves only using the data collected for the specified purpose, and not for any other purpose that has not been notified to the individual or justified by a legal basis. For example, data collected for the provision of a contract between the data controller and data subject, should not subsequently be used for direct marketing without establishing this in a relevant privacy notice and the legal basis to do so.

The principle aims to ensure that data controllers or processors are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned. In practice it means that data controllers must be clear from the outset about why they are collecting personal data and how they intend to use it; and ensure that if they wish to use or disclose personal data for any purpose, which is additional to or different from the originally-specified purpose, the new use or disclosure is fair.

Secondary or future uses, which may not be obvious to the data subjects, must also be brought to their attention at the time their personal data is being collected. They must be given the option of saying whether they want their information to be used in other ways apart from the primary purpose. If a data controller has information about a data subject and wishes to use it for a new purpose (which was not disclosed or perhaps not even contemplated at the time the information was collected), the data controller is required to inform the data subject of the new purpose. This provision also helps the data controller achieve transparency in the processing of personal data.

Principle of collection limitation (data minimisation)

According to the OECD Guidelines, *'there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject'*. The principle of collection limitation requires the data controller to ensure that the personal data collected is sufficient and fit for the purpose.

The data collection should therefore be limited to only what is strictly necessary to allow the processing purpose to be carried out. Equally, it should also be adequate and enough to allow the purpose to be achieved. Any data that is excessive for the purpose should be removed, deleted or anonymised. It is important to note that valid justifications for collection do not include *'off-chance'* or *'just in case'*, although data can be held to guard against likely risks to the data controller or the individual on a case-by-case basis.

- *Identify the minimum* amount of personal data that would be sufficient to fulfil the purpose for which you are processing the information.
- *Obtain, process and store* only *that amount of personal data – no more or less.*
- Do not collect or hold *any personal data on the 'off chance' or 'just in case' it may be useful in future.*
- *Where* sensitive personal data *is concerned, it is particularly important to make sure to collect or retain only the minimum amount of information needed.*
- Techniques designed to eliminate the connection between personal data and specific individuals, such as *de-identification and pseudonymisation, are encouraged*. The data controller would be able to use the information for other purposes under the minimality principle when data no longer permits identification. An example is the use of anonymised call data records from a telecoms company for statistical purposes.

Excessive data collection is a modern phenomenon, and organisations often create and combine data sets into large 'data lakes' running algorithms against it to try to identify data insights. This can be extremely dangerous from a data protection point of view, as it often places individuals at risk, and has the potential to do great harm, as these algorithms are designed to discriminate by picking out certain groups or outcomes. Where this is necessary, data should be collected with a specific aim in mind, and only used to achieve that aim. This also means that data input forms should be designed to minimise collections. For example: *Do you need to know full date of birth as opposed to an age range such as 'over 18'? Do you need to know gender or ethnicity? Do you need data input fields to allow free text options, or would limiting responses to a few pre-specified options minimise the data?*

Quick tips

- Personal data must be sufficient for the purpose it is being collected and held.
- Do not collect more information than needed for the said purpose.
- Minimise personal data through de-identification and pseudonymisation techniques. Such techniques are designed to eliminate linkability to data subjects and are compatible with the purpose of minimality if the data no longer permits identification.

Other issues for consideration

What is necessary, relevant and not excessive?

The words 'necessary', 'relevant' and 'not excessive' can be found in most laws. Their meanings may be inferred from the reason why the data controller is collecting or holding the personal data in the first place. What is 'necessary', 'relevant' and 'not excessive' must also be looked at on an individual basis or from the perspective of each group of individuals where the individuals in the group share relevant characteristics. An example is a bank collecting information on its customers and other third parties such as children of its customers. The purpose

for the customer is different from that of the third party. The bank cannot therefore collect the same amount of information on the third party. In order to consider whether the data controller is holding the right amount of personal data, they must be clear as to why they are collecting, holding and using such information. Reasons may differ from one individual to another.

What would constitute excessive information?

Where personal data is not needed for the reason for which it was sought, it will be categorised as an excessive collection. If one needs to hold information about certain individuals only, the information should be collected solely from those individuals, as the information is likely to be excessive and irrelevant in relation to other people. An example is where an employer holds details of the blood groups of all its employees but only needs that information for those who do hazardous work in case of a workplace accident. For the rest of the workforce, blood group details are likely to be irrelevant and excessive.

Personal data should not be processed if insufficient for its intended purpose

The principle also recognises that there may be situations where the data controller may need to collect more personal data than needed, so as to have enough information for an intended purpose. An example is where a group of individuals set up a club and at the outset the club had only a handful of members, who all know each other, and the club's activities are administered using only basic information about the members' names and email addresses. Over time, if the club's membership increases, it may become necessary to collect additional information about members so that the club can properly identify them, and keep track of their membership status, subscription payments, etc.

What can be considered necessary and relevant opinion?

Generally, data protection laws do not give individuals the right to demand that the data controller delete an opinion about them from their records because they believe it is based on irrelevant information, or has not taken account of information they think is important. However, the record of such an opinion (or of the context it is held in) should contain enough information to enable a reader to interpret it correctly. For example, it should state the date, the author's name and position. If an opinion is likely to be controversial or particularly sensitive, or if it were to have a significant impact when used or disclosed, it is important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, this should be made clear. For instance, a doctor's record may hold only a letter from a consultant and it will be the hospital file which contains greater detail. In this case, the record of the consultant's opinion should contain enough information to enable the more detailed records to be traced.

Principle of data quality (accuracy)

This principle is based on the fact that for personal data to be relevant for the purposes for which they are to be used: *be accurate, complete and kept up-to-date.*

Compliance with this provision is always dependent on the personal data processed as well as the purpose of collection. For instance, where the accuracy of the personal data is vital to meet the purpose of collection, greater effort is required to ensure that such information is accurate. This may impose a burden on data controllers to get an independent confirmation of the accuracy of the data. There will therefore be a greater burden, for instance, on a data controller collecting information for the purpose of providing identification or healthcare than there will be on one collecting data to provide a free email service.

Where an individual sends an email to the law firm, she has engaged requesting that it changes its records about her willingness to receive marketing information, the firm may amend its records without necessarily making any further checks. However, if the same client emails again asking the firm to send her case files/dockets to a new address, the firm must carry out additional security/ verification checks before granting the request.

It is the data controller's responsibility to make sure the information source is credible. It is important to distinguish between situations where updating the information may misrepresent or mislead because of the purpose of the collection. Most data protection laws do not define the word 'accurate', but an inference can be drawn from the provisions and best practice to say that personal data will be inaccurate if it is incorrect or misleading taking into consideration the facts as they exist, or the purpose for which the personal data was processed.

Where a journalist with a reputable outlet writes up the profile of a particular public figure and it includes information derived from rumours circulating on the internet that the said individual was once arrested, then the journalist is asserting the rumour as an accurate fact. As a data controller the news outlet is responsible for verifying or qualifying the information before publication.

There is often confusion on how to deal with records which contain mistakes. People understandably do not want their records to be tarnished by, for example, a disciplinary action that was later cancelled. However, data controllers may have legitimate and sometimes legal obligations to keep records that accurately reflect what happened in the past. Holding such records may also be in the interest of the data subject. It is therefore acceptable to keep records of events that happened in error, provided those records are not misleading. In such circumstances it is advisable to add a note to the record to clarify the mistake.

A misdiagnosis of a medical condition must be held as part of a patient's medical records even after the diagnosis because it is relevant for the purpose of explaining treatment given to the patient, or to additional health problems.

Whether or not personal data must be up to date, depends on the purpose for which the information is used. If the information is used for a purpose which depends on it remaining current, then it must be kept up to date.

Employee payroll records should be updated when there is a pay rise. Similarly, records should be updated for customers' changes of address so that goods can be delivered to the correct locations. However, where information is held only for statistical, historic or other research reasons, updating the information might even defeat the purpose of holding it.

Quick tips

- Take reasonable steps to ensure the accuracy of any personal data obtained.
- Ensure that the source of any personal data is clear.
- Carefully consider any challenges to the accuracy of information.
- Consider how to update the information where necessary.

Data input forms must therefore be designed to ensure data is accurate, and up to date where it is not a transactional/historic/point-in-time record. For example, picking a date from a pre-defined calendar rather than allowing manual input, selecting from a pre-defined list of options can be useful in improving accuracy. Data validation can also be a useful tool in ensuring greater rates of accuracy. For instance, ensuring that invalid responses such as '32' is not entered in a day field or '13' in a month field, or using regularly updated official sources to verify addresses, post codes, or other databases to match data. Encryption techniques such as hashing data can also increase the data integrity, helping ensure it is effectively managed.

In some cases, it may be necessary to share data with third parties, carry out audits, ask the data subject themselves to validate the data, or to compare data with other sources in order to gauge accuracy. This should be undertaken with great care to ensure disclosure is notified and securely handled.

Individuals have the right to have their data amended or corrected, or to have compensation for damage or distress if inaccurate data causes harm. Amputating the wrong leg, denying employment due to a criminal record an individual mistaken identity or discrimination are all potential consequences of inaccurate data. Data can be objectively accurate ('the person is lazy'), or subjectively accurate (their manager thinks the person is lazy). In the second case, the data can be inaccurate (the staff member is not lazy), but there could be an accurately recorded manager's opinion to the contrary. Where data accuracy is in dispute, it should be clearly marked, and its use carefully limited.

Retention limitation

Most laws do not specify the length of time which a data controller must retain personal data, but set out considerations that should be taken in account when defining how long for and what information can be retained. The general rule is that a data controller can retain personal data for as long as is necessary to achieve the purpose for which the data was collected. Organisations should therefore draft data retention schedules and plan for the deletion or anonymisation of personal data when it has outlived its defined retention period. Retention periods should be based on:

- laws or legal obligations that define specific retention periods;
- industry codes of practice and guidance;
- the length of time needed to achieve the purpose of collection, such as the contractual period or when the product or service has been delivered;
- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information;
- the ease or difficulty of making sure it remains accurate and up to date; and

- any secondary purposes for which retention of the data may be required, such as defending legal rights or the case of a complaint.

It is often a challenge for organisations to manage data at the end of its lifecycle. Ensure that personal data is deleted when no longer required. Data lifecycles should be mapped, and personal data archived and deleted where appropriate. For example, rather than deletion of a whole record it is possible to delete some of the data which is no longer required or irrelevant to achieve the purpose.

In deciding the length of time which a data controller must keep personal data, clarity of the purpose for which the information is being collected is essential. Where a data controller wants to retain outside the general rule, it must be: authorised by law; or reasonably necessary for circumstances that relate to the function of the data controller; or as a result of a contract; or with the data subject's consent.

A bank holds personal data on its customers such as address, date of birth and mother's maiden name, etc, as part of its know-your-customer or security requirements. In this scenario it will be appropriate for the bank to retain the data for as long as the customer has an account as well as long after the account has been closed, since the bank may need to continue holding this information for legal or operational reasons.

When personal data is no longer required for its specified purpose the data controller must ensure that information is deleted or disposed of in a secure manner. Where personal data is still required for the specified purpose, but is not accessed regularly, it is advised that such information be archived and securely stored. A data controller must regularly review the personal data they hold and delete or archive where appropriate.

Personal data may be retained for longer periods of time in some cases than in others. A retention period is dependant the nature and type of personal data processed, the business needs and the data classifications according to specific policies within an organisation. Typical instances could include:

- Images from a CCTV system installed to prevent fraud at an ATM machine must be retained for a long period, since a suspicious transaction may not come to light until the victim reads their bank statement.
- CCTV images from a pub may only need to be retained for a short length of time as incidents will come to light very quickly. However, where a crime is reported to the police, the images must be retained until the police obtain them for investigation.
- An employer who receives applications for a job vacancy should not keep recruitment records of unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought unless there is a clear business reason for doing so.

The storage of large amounts of data over a long period of time will require a large storage capacity (whether electronic or physical) which may also have financial implications for the data controller. Apart from the cost of data storage, there may be other cost implications to meeting obligations such as data quality, subject access requests and security safeguard obligations under the law. All these pose considerable risk to retaining personal data over a long period of time.

Quick tips

- Review the length of time personal data is kept.
- Consider the specified purpose for the information before deciding whether (and for how long) to retain personal data.
- Securely delete information that is no longer needed for specified purposes.
- Update, archive or securely delete information if it goes out of date.

At the end of the retention period or the life of a personal data record, the data should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can help with flagging such records for review or deletion after a pre-determined period. This may be particularly useful where many records of the same type are held.

The retention provision will however not apply to personal data held for historic, statistical or research purposes. A data controller retaining personal data for these reasons must ensure that the records containing the personal data are adequately protected against unauthorised access or use.

Principle of data security (confidentiality, integrity and availability)

The law requires the controller and processor to take 'appropriate technical and organisational measures' to prevent a 'breach of security'. Security involves the preservation of the confidentiality, integrity and availability of information assets. It is sometimes tempting to focus on simple prevention of disclosure to unauthorised parties. However, security must also looks at the loss or damage to the data which makes it inaccurate or unreliable; as well as the harm that may be caused by not having access to the data should it become unavailable.

There is no set requirement in law for specific security controls, meaning it is up to the organisation to understand its own risks and perform a documented assessment to produce the appropriate controls that manage those risks. While 'appropriate' is not defined in most laws, what is appropriate must take into consideration technological developments, industry practice and associated financial capabilities and/or costs. That is not to say that the data controller must have state-of-the-art security technology to protect personal data, but that one regularly reviews its safeguards to address any gaps as far as technology is concerned. There is no 'one size fits all' as far as this principle is concerned and the level of security depends on one's risks. In determining whether the level of security is adequate, regulators normally look at the organisation's size, scope and scale of processing, as well as what is state of the art. Obviously, a different level of security would be expected from a top secret installation, compared to a company producing boxes, to an organisation making manual wheelchairs, to a social media platform, to a payroll company. Data controllers should also enforce the determined security controls and level of security through contracts data with processors.

A hospital which holds a highly sensitive or confidential personal data (such as individual health or credit card records) on an IT system must invest heavily in IT security to prevent any potential threat to such information. Similarly, if another hospital holds such sensitive information on manual records, the safeguards must focus on the protection of the manual records.

The lack of security measures by a data controller may cause real harm and distress to the individuals whose

personal data they process. Examples of harm may include identity theft, risk of physical harm or intimidation, fake credit card transactions, mortgage fraud, impersonation, etc. Not all security breaches have such grave consequences, but the majority may lead to embarrassment or inconvenience to those concerned and data controllers are required to protect such individuals. Apart from compromising the safety of individuals, if personal information is not adequately protected, it can also damage a data controller's reputation.

Quick tips

- *Appropriate:* Perform a risk assessment to determine security control levels proactively.
- *Organisational:* Controls should include physical, human and administrative security.
- *Technical:* Controls should also include the online and computerised environment.
- *Controls:* Measures should be introduced to manage risk, such as passwords, policies, firewalls, encryption, etc.
- *Data breach:* A lapse of security, leading to the accidental or malicious loss, damage, access to or disclosure of the personal data.

The level of protection required depends on the nature of the personal data in question, as well as the risk of harm that might result from its improper use, or from its accidental loss or destruction. Most laws do not define the security measures. However, whatever security requirements may be adequate will also depend on the sector in which the data controller operates and the applicable industry standards. Physical and technological safeguards are essential but must be implemented alongside other management and organisational security measures. Training, data protection impact assessments, policies and assigning of data protection responsibility are all recognised as management and organisational safeguards.

Notwithstanding the security measures in place, there may be circumstances under which security is compromised or breached. In which case, the data controller is required to deal with the security breach effectively. A compromise or breach may arise from a theft, a deliberate attack on systems, from the unauthorised use of or access to personal data, as well as from accidental loss or equipment failure. When there is a breach, the data controller must respond to and manage the incident appropriately. In the case of a breach, as soon as possible after becoming aware of the breach, the data controller is required to notify the regulator and the individuals affected or likely to be affected. The data controller must also take steps to ensure the restoration of the integrity of the information system.

Where third-party processors are contractually or legally limited in their ability to investigate the attributes and characteristics of the relevant data to identify a security compromise (for instance, to verify whether personal data is implicated), the notification obligation of such processors is limited to notifying relevant data controllers of incidents that may constitute security compromises. Upon such notification from a third-party processor, it is the relevant data controller's responsibility to investigate the data, confirm whether a security compromise has occurred and notify the regulator and data subjects.

Common International Organization for Standardization (ISO) standards look at a wide security stance identifying a wide range of security controls, varying from preventive, detective, and administrative to corrective control types. Controls should encompass the full range of security management areas, deployed in appropriate strength to counter any appropriate threat. For example in some areas a wooden door with a lock will suffice, in others armed guards, surveillance, metal doors with biometric controls will be a more appropriate solution.

The ISO 27001 and ISO 27002 standards group controls into different security domains, which include:

- information security policies;
- organisation of information security;
- human resources security;
- asset management;
- access control;
- cryptography;
- physical and environmental security;
- IT operational security;
- IT communications security;
- systems acquisition, development and maintenance;
- supplier relationships;
- information security incident management;
- information security aspects of business continuity management; and
- legal and regulatory compliance.

See organisational obligations (Chapter 6) for more on data breach management and notification.

Principle of individual participation

This principle ensures that data controllers enable the recognition of individuals' rights as appropriate. In order to comply with this principle, the data controller may be required to observe obligations under data protection laws such as the ones on notification of security compromises; access to personal information; correction of personal information; as well as the recognition and guarantee of the rights of access, rights to be forgotten, prevention of processing and the rights relating to automated decision-making, etc. In practice, data controllers must have processes in place to respond to and address those rights. These may include manual processes or automated tools, such as self-service portals to allow individuals to perform tasks such as withdrawals of consent, access to records, corrections, etc.

Subject access requests

The right of access to personal data (also known as subject access) mandates the data controller when required to by an individual (whose information they are holding), to provide them with a copy of such information. Depending on the laws in question an individual will usually be entitled to be:

- told whether their personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be or has been given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work, except where this information is a trade secret. Data protection laws will usually specify the period within which to provide such response.

Can a data controller require individuals to use specially designed forms when making subject access requests?

Data protection laws do not require individuals to use specially designed forms when requesting access to their personal information. Any requests in writing may be considered as a valid request, whatever the format. Many organisations however produce subject access request forms and most data protection laws will allow the data controller to use such form as long as it is in a reasonable manner and format. Standard forms can make it easier for a subject access request to be recognised, as well as making it easier for an individual to include all the details which may be needed by the data controller to locate the information they want.

Can subject access requests be made on behalf of others?

Data protection laws do not prevent an individual from making a subject access request through a third party. Often, this will be a lawyer acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, the data controller must be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or a more general power of attorney.

Handling requests for information about children

Despite the fact a child may be too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, for example, to a parent or guardian. It is therefore the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental or legal responsibilities for them. Before responding to a subject access request for information held about a child, it should be considered whether the child is mature enough to understand their rights. If the data controller is confident that the child can understand their rights, then they should respond to the child rather than to a parent or guardian. What matters is that the child is able to understand in broad terms what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following are among the considerations that should be taken into account:

- the child's level of maturity and their ability to make decisions such as this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility which may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information – this is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information;
- any views the child or young person has on whether their parents should have access to information about them.

What a data controller should do if a data subject's data includes information on other people

Responding to a subject access request may involve providing information that relates to the individual making the request and another person. Under such circumstance, data protection laws may allow a data controller to refuse the request where doing so may also mean disclosing the information about another individual. There are however exceptions to this rule where the other individual has consented to the disclosure, or it is reasonable in all the circumstances to comply with the request without that individual's consent.

Principle of transfer limitation

This principle limits the transfer of personal data to only countries that ensure an adequate level of protection for the rights and freedoms of data subjects. Most data protection laws equate adequate level of protection to that which is the same as the '*home country of the data*' or higher. In some jurisdictions, there is also a requirement for authorisation prior to transfer.

Many national laws require that the personal data does not leave the country or region unless the data controller can prove that the data is adequately protected to the national law by the country or organisation receiving it. Normally this means providing legal options to allow data transfer. These can include:

- Country-by-country adequacy decisions – the regulator or government of a country has assessed another country's law as adequate to your own.
    - Company-by-company appropriate safeguards – acceptable standards recognised by law and may include
        - approved codes of conduct and certifications;
        - approved contract clauses;
        - approved binding corporate rules;
        - international agreements and government treaties.
- Case-by-case legal derogations – these vary and depend on the specific national legislation, but may include consent, law enforcement requests and legal functions.

Derogations are intended to be a one off exception and should not be relied up on for bulk data transfers. In contrast to this, other laws including that on national security may also require the retention or localisation of data to a given jurisdiction. In such cases, some laws may require data to be held locally for a given period, for access by law enforcement where required.

Increasingly legislation is trying to counteract or reverse the effects of global technologies. The advent of the internet and cloud-based computing has made data access effectively global, giving great utility to individuals who can gain access to data from any location at any time. However, as a response this increases access to data from jurisdictions with variations in legal protections for individuals. As a result, some privacy laws restrict movement of data across international borders where the rights and freedoms of individuals cannot be guaranteed. It is therefore important to pay close attention to the requirement of particular data protection laws.

4. Common exemptions

Most laws contain a number of limited exemptions to the general rules or may have specific laws covering the processing of data for other purposes. It is therefore important to note such exemptions that define the data management rules for the specific purposes. The exemptions are not absolute, and data protection laws define the extent of the limitations. Generally, the exemptions only relieve a data controller of their obligations relating to:

- the right to be informed;
- the right of access;
- dealing with other individual rights;
- reporting personal data breaches; or
- complying with some (but not all) of the principles.

The application of an exemption depends on the purpose for which personal information is to be processed and must therefore be looked at on a case-by-case basis. In ensuring compliance, a data controller must justify and document reasons for relying on an exemption. The exemptions are not absolute, and their application may in some cases be subject to some other obligations or laws, such as legislation relating to employment, healthcare, law enforcement or national security. In determining whether an exemption is applicable, it is important to ascertain the extent to which the exemption will apply under data protection laws. The following provides information about some of the exemptions and how they work under data protection laws.

A valid exemption is limited and can be justified under the following circumstances, if it:

- is necessary and proportionate in a democratic society;
- is clearly defined and prescribed by law;
- respects the fundamental rights and freedoms of persons; or
- is only applicable because the failure to do so will prejudice a legitimate aim.

Social and domestic purposes (home/personal use) exemption

This exemption is absolute and allows processing of personal information outside the scope of data protection laws. It applies to personal information that is processed during social or domestic (household/personal) activity. This means that if you only use personal data for such things as writing to friends and family or taking pictures of family/friends for your own enjoyment, you are not subject to the data protection laws. Such activities must however have no connection to a professional or commercial activity.

Legal professional privilege exemption

This exemption applies when the data controller processes information under a legal professional privilege (or confidentiality of communications) to which legal action may be maintained against the data controller in case of a breach. Under these provisions the legal professional is exempt from third-party subject access request obligations in respect of information to which a claim of breach of such legal professional privilege may stand.

The legal professional, barring any such circumstances is therefore required to comply with the data protection obligations.

Law enforcement exemption

This exemption applies to the processing of personal information by competent authorities for law enforcement purposes only. The exemption relieves the competent authorities from obligations under data protection laws that relate to provisions on:

- all the principles (except that of security and accountability);
- the conditions for processing special categories of personal data and data about criminal convictions and offences;
- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- the communication of personal data breaches to individuals;
- consultation with the regulator for high risk processing; and
- international transfers of personal data.

National security exemption

This exemption relates to the processing of personal information for the purposes of safeguarding national security or defence only. It relieves the competent authorities from obligations under data protection laws that relate to provisions on:

- all the principles (except that of security and accountability);
- the conditions for processing special categories of personal data and data about criminal convictions and offences;
- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- the communication of personal data breaches to individuals; and
- consultation with the regulator for high risk processing.

Self-incrimination exemption

This exemption applies when complying with the provisions of the data protection law will disclose evidence of ones commission of an offence. It is meant to protect such individuals in accordance with other rights that they may have from incriminating themselves. The exemption relates to complying with obligations on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

Regulatory functions exemption

This exemption applies to the processing of personal information in the exercise of regulatory/statutory functions. It only applies where compliance with the data protection law obligations are likely to prejudice the proper discharge of the regulatory/statutory function. The provisions whose compliance may affect the proper discharge of such functions include:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only to the extent that they relate to the right to be informed and the other individual rights.

Research and statistics

This exemption applies when the data controller processes personal data for scientific or historical research or statistical purposes. The exemption does not apply to the processing of personal data for commercial research purposes such as market research or customer satisfaction surveys, unless it can be demonstrated that the research uses rigorous scientific methods and furthers a general public interest. This exemption relieves a data controller from obligations under data protection laws that relate to provisions on:

- the right of access;
- the right to rectification;
- the right to restrict processing; and
- the right to object.

Journalism, academia, art and literature

This exemption applies to the processing of personal information for journalistic, academic, artistic or literary purposes also known as 'special purposes'. This exemption relieves a data controller from obligations under data protection laws that relate to provisions on:

- all the principles (except that of security and accountability);
- the conditions for consent;
- the conditions for processing special categories of personal data and data about criminal convictions and offences;
- processing not requiring identification;
- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- the communication of personal data breaches to individuals; and
- consultation with the regulator for high risk processing.

This exemption will only apply under the following circumstances:

- Where the data controller reasonably believes that compliance with the provisions will be incompatible with the special purposes.
- Where the processing is being carried out with a view to the publication of some journalistic, academic, artistic or literary material.
- Where the data controller reasonably believes that the publication of the material will be in the public interest, taking into account the special importance of the general public interest in freedom of expression, any specific public interest in the particular subject, and the potential to harm individuals.

5. Individual rights

Individual rights under data protection laws vary by country across Africa, however these rights may fall within the groupings below. In order to guarantee such rights, data controllers must put in place systems to facilitate recognition of such rights as earlier stated under the principles. A data controller can employ the use of electronic systems to help manage the requirements of such rights. Such interventions my include self-service models. To reduce manual resource investment, often a self-service model can be employed, with the individual being provided options via automated solutions, rather than via manual processes. However, manual options should also exist, to facilitate rights for those without access to technology. Ethically rights should be provided for free to enable them to be accessed by disadvantaged individuals, although some regimes might allow a small nominal costing, or charges for example, for multiple copies of data. There are limited exemptions in play here, such as to protect others' rights, or to refuse requests that are irritating, unfounded or repetitive in nature.

Please note that some of these rights will only apply in certain situations. For example, the right of erasure is linked to consent, objection to 'the interests' legal basis, and portability to contract.

Access

After transparency, the most important right is to gain a copy of the data. This is fundamental, to review the personal data an organisation holds in order to facilitate the other rights stated below. This includes having a secure method to authenticate the individual requesting the information, and to send the information via an appropriate secure channel to the individual requesting it. Legal rights may specify a deadline for response, and nominal costs that can be charged, while other jurisdictions allow this right for free. Answering these requests promptly will involve a sound knowledge of where individual's data is held, and a documented process to answer these efficiently. The law may also include a right to other information surrounding the data (similar to that found on a privacy notice), such as disclosures, recipients, purposes of use, retention periods, international transfers, etc. This right is essential, because without understanding the data held, it is unlikely that the individual will be able to pursue the additional rights below.

Erasure

Erasure is often misunderstood, as it is a much more limited right than publicised. It only applies in limited situations, such as where the controller does not have the legal basis to retain data (such as where relying on a consent that has been withdrawn), or where the organisation has broken or failed against the privacy principles (eg, retaining information past its retention period, or holding excessive or unnecessary data).

In reality erasure is frequently linked to situations such as email marketing campaigns, where on many occasions, the requestor does not actually want erasure at all, rather to be added to a suppression list so the organisation knowns not to email them again.

Objection

Where data uses are optional or an organisation has taken a balancing test for legal basis, this opens up the right for the individual to object to the processing. This includes objection to purposes that are not mandatory, such as data uses for marketing, research, statistics, public interest or anything based on a balancing test surrounding individuals' rights. Organisations should have processes and arguments in place to deal with objections raised and be prepared for their processing to have to change depending on the outcome of these objections.

Rectification/completion

Where information is incorrect, individuals should be in a position to correct it. However, this should not happen without proof of the accuracy of an individual's claim. Equally, where an individual has asked for data to be corrected or changed but has then been unable or unwilling to comply due to a disagreement, this should be noted and logged. Such instances should be read in conjunction with the accuracy principle above, as this right will come into play mainly where that principle has been broken.

Finally it is worth mentioning that sometimes organisations can take incorrect decisions because they do not have all the facts about an individual. Rectification can also include individuals voluntarily giving more information to complete or add to their record.

Restriction

Following on from any inaccurate or incomplete data, while the disagreement exists between the controller and the individual, it may be that continued use of the data may place the individual at risk. The individual should therefore have the right to request that data is set aside and marked 'do not use' for the duration of the disagreement, or until the risk to the individual has passed. This is difficult to manage in systems that do not have the capability of marking data in this way.

Portability

Where the legal basis is consent or contractual necessity, some jurisdictions allow individuals to ask to transfer the data they have submitted (not any data the controller has added to it) to a new provider. This is realistically to allow individuals to shift their accounts between companies, such as changing banks or electricity suppliers. This information should be made with interoperability in mind in order that common formats can be used to transmit the data to other providers in formats that are easy for them to use.

Automated decision making

An automated decision is where a computer or technology makes a decision about or regarding an individual human being that has some sort of impact on the individual's life. This includes very basic decisions such as searching a stack of CVs for skills to decide on shortlists for interview, decisions about online loan applications, or online car insurance, to more complex decisions such as algorithms applied to data sets to decide on policing distribution, or the likelihood of criminals reoffending. Modern computing is moving increasingly towards discriminatory algorithmic decision making and increased automation.

Rights in relation to automated decision making include: being aware it is happening through the privacy notice; describing the logic involved within the algorithm (not to the extent of giving away trade secrets); and to have a human being involved in, or reviewing the decision. These rights have yet to see much use, but it is envisaged as computers increasingly make algorithm-based decisions, this is an area in which individuals will be increasingly striving to assert their rights.

Other rights

The following rights are tied up with the ability of an individual to enforce their rights alongside the regulator.

Complaint

Individuals should be given the capacity to raise any concerns they have with the controller, and effective dealings with the individual's complaints at this time can prevent an individual from escalating their complaint to a regulator or court of law. Dealing with individuals fairly and efficiently and giving them transparent access and swift remediation to problems with their data should be a key line of defence in allowing the organisation to gain an early warning of future problems and deal with them before they become more severe and more 'official'. Dealing with an individual's complaints effectively in the first place can stop more negative press and reputational harm further down the line.

The individual has a right to complain to the national regulator, but in most cases the regulator will require the complaint to have been first taken up and exhausted with the controller in order to give them the opportunity to rectify the issue before formal action is taken.

Legal remedy/compensation

In addition to actions via the regulator, the individual may also have rights to take an action in a court of law in order to receive compensation for damage or distress caused to the individual by a breach of the law or if failure of the principles causes harm to the data subject. This can create a situation of 'double jeopardy' for the organisation, as in some jurisdictions it is possible to receive both a penalty from the regulator and the courts.

Representation

Finally, some national laws allow for representative actions, where organisations can act on behalf of an individual or group of data subjects and take actions on their behalf. This sort of 'collective' or 'class' action is difficult to operate in some jurisdictions, especially where classes are large – in some cases involving global audiences.

6. Data controller/data processor obligations

Data protection officers are a legally mandated role in some jurisdictions. The role of the data protection officer is however, not to set up and implement a privacy programme within an organisation, as that is what a privacy manager or officer does. Instead, the data protection officer is more of an audit and oversight role, to advise the management of the controller in their level of legal compliance, and to act as a representative of the views of the data subject in reminding the organisation of its duties and obligations in implementing the principles of data protection and its obligations under the law. The further into implementing the programme the DPO gets, the less independent they can be in this role, as that would mean they would effectively end up auditing their own work.

The data controller/data processor's obligations vary from country to country, in general the obligations may be grouped in the following manner.

Transparency

This has been discussed as an obligation with the data protection principles (in Chapter 3), but as before this is about ensuring that 'no covert surveillance without a lawful authority' takes place, by providing individuals with privacy notices to inform them of the facts surrounding your processing of their data, and ensure it is made known to them that you have collected/are using the personal data that relates to them. This is irrespective of whether you are in contact with the individual, or have collected it indirectly from another source, as discussed above.

Accountability

Accountability is essentially being able to address data protection issues proactively as part of a structured and documented management system (see the privacy management duties of the data protection officer, outlined below).

Data protection and privacy is a programme, not a project, and requires continued management focus, resources and attention to ensure appropriate controls have been planned, established, implemented, measured, monitored and improved, as the laws and case law change, and as the products, services, cultural norms and technology of the world change around us.

This means that the data protection management regime needs to be continually reviewed and updated, and the organisation has the ability to 'show their homework' to any interested parties, proving their effective management of privacy risks, such as to data subjects, regulators, management, partners etc.

Organisations should identify areas where the privacy risks and controls can be monitored and measured in operation, to ensure a level of control appropriate to the risks. This may and should include external and internal independent audit to identify areas of non-compliance and improvement opportunity within the operation of the scheme, and the controller should take and document appropriate corrective and preventive actions to ensure these identified actions are carried out and are effective.

Accountability is perhaps the most essential part of managing data protection going forwards and requires a high level of management commitment, resourcing and support.

Representatives

If doing business in EU or EEA countries, or the UK, using the personal data of persons in the EEA, or targeting goods and services at those locations, their laws have a requirement to establish either a business establishment within the EEA, or to nominate a representative organisation within the EEA to act as a contract point for both the local data subjects and supervisory authorities. This is due to the extra-territorial extent provisions of the EU's GDPR.

Organisations are encouraged to establish local representatives if doing business in these areas, and identify if other local country privacy laws require the same across the world.

Processors

This relationship is normally managed by a contract between the data controller and processor. The contract should ensure that the processor:

- processes the personal data only on documented instructions solely from the controller;
- ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- follows all information security measures defined by the data controller;
- informs and allows the controller to object if engaging another sub-processor;
- assists the controller in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;
- assists the controller in ensuring compliance with the obligations pursuant to data protection impact assessments, security measures and data breaches;
- deletes or returns all the personal data to the controller (at the choice of the controller), after the end of the provision of services relating to processing, and deletes existing copies unless retention is required by law;
- makes available to the controller all information necessary to demonstrate compliance with the obligations and the contract;
- contributes and submits to audits, including inspections, conducted by the controller or other auditors authorised by the controller.

The controller should perform due diligence before taking on a new processor, ensure that there are the relevant contract provisions, and manage the relationship going forwards, monitoring that the processor complies with the contract, and has not simply signed it without taking action to improve their privacy management for the individual. Finally there should also be ensured adequate provision for making certain that on contract termination, adequate safeguards are in place to ensure recovery or deletion of the personal data from that processor and/or any sub-processors.

Records of processing

In order to comply with most obligations, it is important that data controllers track and control where the personal data is that they have custody of, and to record the metadata (data about data) necessary to manage their privacy risks. This includes elements such as collection sources, disclosures, purposes, legal basis,

compliance to the principles, security measures, assessments, international transfer data movements, retention periods, disposal mechanisms etc.

This record of processing activities should be kept up to date throughout the operation of the scheme, and any alteration to the processing activities of the scheme should be reviewed for privacy risks. This is a significant project in itself, and examination of the processing of the organisation or 'data audit' should be the first step in any organisation's data protection legal requirements and compliance. Keeping this up to date is a difficult task, but organisations should at least produce a high profile summary of their processing purposes and the associated summary of a data lifecycle for review by a regulator if required.

Cooperating with regulators

The law places a responsibility on both data controllers and processors to cooperate with and comply to requests from the regulators.

Security

Security management is both a controller and processor responsibility (see the Principle of data security in Chapter 3 for more information).

Breach notification

An organisation can never be 100 per cent secure. Therefore, inevitably a breach may occur, and some jurisdictions legally require notification to individuals and regulators. Processors have responsibilities to notify controllers, and controllers have responsibility to notify the regulators and data subjects themselves in some instances.

Furthermore, the effective management of a security breach can determine an organisation's survivability in such times and reflects on the reputational harm that can result. Reacting swiftly to introduce further controls to minimise harm to individuals is key to ensuring effective crisis management of any breach. Information minimisation principles delivered above (such as anonymisation, or separation or minimisation) can certainly assist in reducing the impact of any breach.

Breach notifications should include:

- the nature of the breach, including the type and number of individuals affected, and the number of records affected;
- the timeline and circumstances of the breach, including the window in which the breach may have occurred, or individuals' data exposed;
- the name and contact details of individuals who can give further information about all parties involved in the breach;
- any consequences to individuals that may occur as a result;
- any security measures and protections taken both before and after the breach, including those to alleviate any harmful effects.

Security breach notification is required by some jurisdictions, not only to the privacy regulator, but also to local industry regulators (such as financial or medical regulators). Penalties may be levied by regulators other than data protection supervisors in respect to data breaches, and case law in the area of vicarious liability is constantly evolving.

Data protection impact assessments

Controllers are required to consider the risk of their processing operations on the individual. In some cases this may be legally required under circumstances, where the processing involves new and innovative technologies, large-scale processing of special category data, or large-scale monitoring and surveillance.

Organisations should be conducting data protection impact assessments to ensure impact on individuals' privacy is considered proactively, and relevant controls put in place that can provide the appropriate protections. This is the concept of 'privacy by design'. Outcomes should include documentation of the assessment, and a set of actions to introduce controls that reduce the risk to the individual.

The data protection impact assessment should include a description of:

- the data to be processed;
- the individuals whose data will be processed;
- the processing, including a timeline of the data from collection to disposal;
- the risks the processing causes to the individuals;
- the measures applied to manage the risks;
- the legal requirements that apply;
- the advice given during consultation with regulators;
- advice given by privacy expertise and regulators;
- the consultation carried out with individuals, and the views gathered;
- the measures applied to comply with the advice given; and
- any residual risks, or measures that could not be managed or implemented and the justification and acceptance of management for these.

Data protection officer

No organisation should attempt to create and maintain privacy management without appropriate access to privacy advisory resources. This could be employed, or sourced from external resources. There are several roles and responsibilities that can be assigned for the purposes of managing privacy.

These roles may include:

- Senior accountable officer – individual responsible for privacy management, should be a senior management role;
- Data protection officer – audit and review role, and 'voice' of the individual within the organisation;
- Privacy risk manager – individuals responsible for managing risk to the individuals and reporting on how these risks are managed;
- Privacy programme manager – individuals responsible for establishing and implementing an organisation's privacy programme;
- Privacy manager – person responsible for day-to-day running and maintenance of the privacy programme, such as providing advice to the business, and managing documentation and records, possibly responding

to individual requests;

- Privacy audit and review – individuals responsible for identifying improvement opportunity and assessing the privacy programme against identified requirements;
- Privacy legal expertise – individuals who advise on legal requirements and national law compliance;
- Privacy engineer – individuals who have privacy by design expertise, normally within software development and solution design; and
- Privacy consultancy – individuals with extensive experience (normally greater than ten years) who advise organisations on building privacy programmes.

Codes of conduct and certifications

Controllers should identify relevant standards and codes of practice which may be relevant to their processing activities. These codes of practice act as an aid in identifying relevant controls in order to protect the individuals their schemes serve.

In addition, they should review available independent accredited certification schemes for applicability and hold and maintain relevant independent accredited certification in order to provide assurance of their compliance to them. Some certifications available include BS 10012-2 and ISO 27701.

7. Regulator powers

Regulators' powers vary in structure, scope and authority. Naturally there is a good reason for data controllers to be concerned about the enforcement actions of national regulators but the powers of the regulators can be divided into three: advisory, authorisation, or enforcement.

Enforcement actions can, in turn, be split into three sections: the serving of notices; the power to issue fines against data controllers or processors; and personal liability offences that may place individuals at risk of committing a crime.

Voluntary undertakings

Although this may not be an official standing, voluntary undertaking is often a way for data controllers to avoid more formal enforcement by signing a public document promising to introduce changes and alter practices. This will be reviewed by the regulator with the intention of proving that the organisation is doing as it says, and if they break their voluntary agreement, then enforcement action is certain to follow.

Audit

Some regulators have the power to audit an organisation or to make the organisation submit to compulsory audits over a period of time as a way of increasing the organisation's accountability, expose its shortcomings and to improve the organisation's privacy regime.

Entry and inspection

Some regulators have powers of entry and inspection such as warrants, or can obtain these from a court to enter a property and/or seize records.

Information notice

An information notice is normally the first formal power used by an organisation on non-cooperative organisations. This compels the organisation to release documents and evidence required for the regulator to investigate.

Enforcement notice

An enforcement notice can be levied to try to force an organisation to change its practices in order to 'force' compliance on them. This normally involves mandating a change to ensure the adoption of data protection principles or privacy management obligations.

Stop notice

Perhaps the most difficult for an organisation to handle, is an ability to serve a notice telling an organisation to 'stop processing personal data'. Clearly, this could shut down a business overnight, but is normally limited to the processing for a specific purpose, such as marketing.

Fines and penalties

Fines and penalties vary across Africa, and can broadly be divided into: non-compliance with an individual's right;

non-compliance with an obligation; or failing to uphold the data protection principles. In some jurisdictions regulators can serve fines as administrative authorities themselves, while in others they must go through the courts.

Publicity

Perhaps the greatest weapon in the regulator's toolbox is the ability to 'name and shame' organisations which do not comply.

Personal liability offences

Although personal liability and criminal liability varies from national law to national law, again these can be divided into two types: offences anyone is capable of triggering; and offences triggered by employees or management of data controllers and/or processors.

This could include:

- Anyone;
- Unlawful obtaining of personal data;
- Unlawful selling of personal data;
- Unlawful procurement of personal data;
- Altering records in order to prevent access/disclosure;
- Trying to re-identify individuals from anonymised data without permission of controller;
- Employee/management;
- Non-compliance with a regulator notice;
- Non registration with the regulator (where required);
- Making access requests a precondition of employment (enforced subject access).

8. How the GDPR affects your practice

Data protection law is derived from fundamental human rights law. As such, data protection law can be considered a balancing act between the needs of the many and the needs of the individual. As a topic, this makes for a highly emotive and argumentative arena, as there can be entirely valid competing arguments, where both parties are acting in good conscience believing they serve the best interests of their clients. Any organisation which manages individuals' personal data will be required to comply with legal obligations and fulfil the moral imperative to protect the data of individuals within their care, ensuring that their partners and suppliers do the same.

Privacy as a fundamental right is referenced in both the Universal Declaration of Human rights and the European Convention on Human Rights.

Universal Declaration of Human Rights 1948 (Article 12)

'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

European Convention of Human Rights 1950

(Article 8 of the Convention - Right to respect for private and family life)

1. 'Everyone has the right to respect for his private and family life, his home and his correspondence.'
2. 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

In light of these fundamental rights, a balancing act often applies, as data protection laws include considerations of the needs of two interested parties: the individual's data and a corporate/business/government interest.

There is however a difference between privacy and data protection. While privacy can be awkwardly used as a euphemism for 'secrecy', it also applies to areas which data protection laws cannot reach. Data protection only applies to the communications, correspondence and information on individuals. Privacy stretches further. It reaches into areas such as territorial, bodily privacy and organisational privacy.

As discussed in Chapter 3 on principles, data protection covers a larger area than simply the decision to disclose or keep confidential, and therefore gives organisations obligations where privacy and security are no longer an issue. In fact organisations have data protection obligations throughout the data lifecycle regardless of confidentiality considerations.

Finally, it is worth noting that data protection law as a human right stands apart from commercial considerations of intellectual property law, and data 'ownership'. The data controllers have obligations, individuals have rights and the regulators have powers.

None of these obligations, powers or rights involve the assignment of intellectual property and ownership rights.

In fact to do so often places individuals at a disadvantage, as human rights should be available to everyone for free. Assigning commercial value to data and allowing data rights to be bought and sold should be prohibited, as it leads to data protection and privacy rights afforded only to those with the means to defend them, and often places the disadvantaged in a worse situation, as they are forced to sell or relinquish data rights in their economic interest.

GDPR working definitions

Although individual countries' laws may vary in their own legal definitions, and they vary across the continent, generally laws are based on either the 1995 European Union Data Protection Directive 95/46/EC or the more recent 2016 European Union Data Protection Regulation 96/617 (The General Data Protection Regulation or GDPR).

While the Directive-based laws occur more frequently across Africa, data controllers should be looking at adopting standards based on the later Regulation, as these laws adopt a higher standard of protection for individuals. Using the GDPR as a data protection standard will therefore create a compliance regime that will be more global and allow interoperability within a number of other countries. Some key working definitions under the GDPR are provided below.

Anonymous data

Data that is incapable of identifying a living individual. To be truly anonymous, it is important that the data is no longer capable of identifying any individual. Only truly anonymised data therefore lies out of the scope of data protection law. It is worth noting that the more data points there are within a smaller parent population, the more capable it is to identify data subjects.

Pseudonymous data

Pseudonymised data does not exempt data from the law, as it is still capable of potential re-identification of the individual. It is nevertheless a useful risk reduction mechanism to be employed by organisations seeking to protect individuals, or to make use of data with less risk. Pseudonymisation techniques normally remove obvious identifiers such as name and address, and replace with unique reference numbers to allow re-identification later.

Personal data

Any information relating to identified or identifiable natural persons. In greater detail:

- 'any information' – regardless of format, nonetheless limited exemptions may exist for unstructured manual data;
- 'relating to' – more 'about' the individual at its focus rather than some transaction or event they may have been involved in;
- 'identified or identifiable' – the data must be able to identify an individual, or have the possibility of them becoming identified, such as by name, image, location, description etc;
- 'natural person' – a living individual, not a 'legal person', such as a business.

Special category data

Sometimes called 'sensitive data', this varies from jurisdiction to jurisdiction. In general this tends to focus on areas which would endanger equal treatment of individuals, and can be considered data that must be given extra protection, and also data which often requires a higher justification to hold and use (see 'use justification/ legal basis' below).

Special category data often includes:

- data revealing:
  - racial or ethnic origin;
  - political opinions;
  - religious, or other beliefs of a similar nature;
  - trade union membership;
- data used to identify individuals based on
  - genetic data;
  - biometrics (fingerprints, facial recognition, retinal scans etc);
- data concerning:
  - physical or mental health or condition;
  - sex life or sexual orientation;
  - criminal or civil offences, alleged commission of those offences and their disposal (result) in a court or administrative process.

Data subject

The living individual who is capable of being identified by the personal data. Note that records and data sets can often refer to multiple data subjects, but care must also be taken to the context of the record in terms of who it 'relates to' and in what capacity the individual is acting. For example, the individual's right to privacy can vary depending on how 'public' they make themselves. An individual acting as a private citizen has more right to privacy than when they are at work, and then more than if they are in public office, and then more than if they deliberately make their lives private as a celebrity figure. That is not to say that celebrities do not have a right to privacy, but will have to look at if they are acting in a public or private capacity when evaluating their privacy rights. Similarly when an individual uses their rights to request access to their data (such as emails they may have sent at work), the employer should have due regard to releasing only emails 'about' the individual in the personal capacity, as emails they have sent regarding the corporate customers might be considered 'relating to' the customer rather than the employee as the focus is on the customer. In this example it meets the definition of personal data excepting the 'relates to' test.

Supervisory authority/regulator

The national body set up to regulate privacy law (see local regulatory bodies for more information), granted powers by legislation that may include advisory, authorisation and enforcement powers and duties.

Controller

Defined as an entity (an individual or organisation) that determines the means and purposes of processing. In practice, this is normally the organisation taking the decisions on how, where and why the data is processed.

They then have to meet their obligations under the law and to the individuals and can be liable for damage/distress caused to individuals and regulatory penalties.

Processor

A processor acts on the instruction of the controller. This is normally a vendor or service provider to the controller (eg, outsourced payroll provider), that collects or receives personal data on behalf of the controller. This relationship is normally managed by a contract between controller and processor. What such a contract should typically ensure is detailed under 'Processors' in Chapter 6 'Data controller/processor obligations'.

It should be remembered that if the processor does any sort of processing that is not set out in the contract, or under the specific instruction of the controller, they will have become a controller themselves, as they are now determining means and purpose themselves. Often processors unwittingly use data for other supplementary reasons not captured in the contract and become controllers legally by accident. This is especially the case with internet services that provide platforms such as social media or social networking providers, and 'cloud computing' platforms, where the legal contract states that they are simple processors, but often are in actuality acting as a controller in fact due to their data use outside of that specified in the contract and the ability to do more with the data than the original controller.

Joint controllers

If organisations jointly determine the means and purposes of processing along with another controller, they can be considered joint controllers. This is often misinterpreted, as joint controllership is often groups of companies acting as a single brand (such as a large bank or multinational), even though legally separate entities, or setting up a joint concern (such as police and council setting up a CCTV partnership). There are a number of indicators that makes joint controllership more likely, including;

- joint branding;
- shared management responsibilities and policies;
- shared access to single databases;
- common/shared purposes of data use;
- single relationship with data subject;
- single privacy notice; or
- single contract with the individual.

The fewer of these that are in place (ie, processing data in separate databases, under separate brands for separate purposes under separate privacy notices and contracts), the more likely it is that the two or more entities are in fact separate controllers, each with their own relationship with the data subject and obligations to meet. Organisations often nominate joint controllership by mistake when there is more than one controller involved in the transfer of personal data.

How will the GDPR affect my law firm?

An understanding of the impact of the new General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is crucial for any lawyer wishing to expand their law firm.

The GDPR came into effect on 25 May 2018, replacing the Data Protection Directive of 1995 (officially Directive 95/46/EC). GDPR aims to give control back to citizens and residents over their personal data, and simplify the regulatory environment for international business by unifying the regulation within the EU.

When it comes to confidential and highly personal data, law firms store a considerable amount of information. As such, they have a greater responsibility to keep data safe and take accountability for how data is collected, stored and used. It will be important for law firms to understand how they collect, store and use clients and employees' personal data in order to ensure compliance.

- If your practice collects, stores or uses the personal data of EU citizens, you are subject to the GDPR.
- Fines for non-compliance can be up to four per cent of annual worldwide turnover or €20m, whichever is greater.
- The GDPR defines parties as either 'controllers' or 'processors'. A data controller states how and why personal data is processed, whereas a processor is the party doing the actual processing of the data. For example, a controller could be any law firm, while a processor could be an IT firm undertaking the actual data processing.
- It is important to note that even if your firm is based outside of the EU, the GDPR will still apply so long as you deal with personal data belonging to individuals residing within the EU.

What lawyers need to know

Here are just a few of the new obligations that law firms will need to consider:

- The GDPR places greater emphasis on accountability. This means you must have an accurate record of the data you hold, demonstrate how data is collected, and whether the collection is 'lawful'.
- You must be able to demonstrate that you are managing personal data in a way that complies with the Regulations. Firms must be able to supply, on request, information on the data they hold and how it has been used.
- Consent under the GDPR must be a freely given, specific, informed and an unambiguous indication of the data subject's wishes. Law firms will need to review how they collect personal data and record consent.
- For processing of personal data to be lawful under the GDPR, a lawful basis needs to have been identified before personal data is processed. It is important that law firms determine their lawful basis for processing personal data and document this.
- The GDPR creates some new rights for individuals and strengthens some existing rights under data protection laws. Law firms will need to ensure they allow individuals to exercise a range of individual rights, including the right to be forgotten, right of data portability and right of access.
- Under the GDPR, data protection is no longer the responsibility of IT. The protection of personal data must be considered and embedded in a law firm's processes, from marketing to HR and business development.

Bibliography

Communication from the Commission to the European Parliament and the Council, 'Exchanging and Protecting Personal Data in a Globalised World', EU, Brussels, 10.1.2017 COM (2017) 7 Final.

Andrew Chambers and Graham Rand, *The Operational Auditing Handbook: Auditing Business and IT Processes*, (2nd edn, John Wiley & Sons 2010), Appendix 3, International Data Protection Legislation, see https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3 accessed 26 November 2020.

CIPESA, 'Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa', (July 2018), *CIPESA ICT Policy Briefing Series,* see https://cipesa.org/?wpfb_dl=272 accessed 26 November 2020.

'Data Protection Africa', (ALT Advisory, Johannesburg), see https://dataprotection.africa accessed 26 November 2020.

'Data Protection Laws of the World, (DLA Piper), see https://www.dlapiperdataprotection.com accessed 26 November 2020.

DPAS Newsletter – 2018 (1st Edition); Data Protection & Privacy Challenges in Africa by Teki Akuetteh Falconer.

Teki Akuetteh Falconer, 'Principles of data protection', a series of articles in *The Daily Graphic of Ghana*

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 (2018).

Graham Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 Privacy Laws & Business International Report, 14-18, see https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593 accessed 26 November 2020.

ICO Guide to Data Protection, see https://ico.org.uk/for-organisations/guide-to-data-protection accessed 26 November 2020.

Verengai Mabika, 'Privacy and Personal Data Protection Guidelines for Africa', (Internet Society 2018), see https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf accessed 26 November 2020.

Marianne Lesigne, Data protection developments in Africa (Research World, 13 August 2019), see https://www.researchworld.com/data-protection-developments-in-africa accessed 26 November 2020.

Malabo Convention – African Union Convention on Cyber Security and Personal Data Protection, African Union (2014).

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, see https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm accessed 26 November 2020.

'Personal Data Protection Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union', (9 May 2018), see https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf accessed 26 November 2020.

Privacy International, 'Keys to Data Protection: A Guide for Policy Engagement on Data Protection', London, August 2018.

'Privacy is Paramount: Personal Data Protection in Africa', (Deloitte, Johannesburg 2017), see https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf accessed 26 November 2020.

Cynthia Rich, 'A Look at New Trends in 2017: Privacy Laws in Africa and the Near East', Privacy and Security Report, (9 November 2017), *Bloomberg Law*, see https://media2.mofo.com/documents/170911-privacy-africa.pdf accessed 26 November 2020.

SADC Model Law on Data Protection (2013).

'The state of data protection rules around the world: A briefing for Consumer Organisations, (Consumers International 2018), see: https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf accessed 26 November 2020.

Supplementary Act on Personal Data Protection within ECOWAS, Economic Community of West African States (2010).

Appendix one

Overview of data protection laws in Africa

The table below provides a brief overview of data protection/privacy laws across Africa as of July 2020. The table identifies the respective countries and their data protection/privacy laws (where available). It also summarily looks at the legal regimes in place, the data protection principles under the respective laws, whether or not there is an existing regulator, registration/authorisation regimes and cross-border transfer requirements among others.

The table can be read in conjunction with Figure 1, the colour-coded heat map on page 12.

OVERVIEW OF DATA PROTECTION/PRIVACY LAWS IN AFRICA

The table below provides a brief overview of data protection/privacy laws across Africa as at March 2020. The table identifies the respective countries and their data protection/privacy laws (where available). It also summarily looks at the legal regimes in place, the data protection principles under the respective laws, whether or not there is an existing regulator, registration/authorization regimes and cross border transfer requirements among others.

Country	Laws Identified	Status of Data Protection Law	Legal Regime Applied *(Constitutional Recognition, Acts of Parliament, Subsidiary Legislation, and Administrative Fiat)*	Data Protection Principles Identified	Regulator	Registration / Authorization Requirement	Enforcement Level & Regime	Cross Border Transfer Restrictions	Breach Notification	Data Localization & Portability	Others	References
Algeria	Law No. 18-07 (Law 18-07) of June 10, 2018	Data protection law present	1. Constitutional Recognition (Article 39 of the Constitution of Algeria (Privacy, Secrecy of Communication): "(1) The private life and the honour of the citizen are inviolable and protected by the law. (2) The secrecy of private correspondence and communication, in any form, is guaranteed.") 2. Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Autorité National de Protection des Données à Caractère Personnel	Yes	- No Significant level of enforcement - Monetary fine and two (2) to five (5) years of jail term	Applicable	Required	Localization: No Portability: No	1. Express consent 2. Children's data protection 3. Researchers are allowed to contact a data subject without consent through automatic call, e-mail or similar technology. 4. Data Subject rights provided for	Article 39, Constitution of Algeria https://oxfordbusinessgroup.com/overview/legal-landscape-summary-laws-and-regulations-investors-algeria https://www.researchworld.com/data-protection-developments-in-africa/ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593 https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3
Angola	Lei No. 22/11 da Protecção de Dados Pessoais de 17 de Junho (in Portuguese)	Data protection law present	Act of Parliament	Specific principles followed according to Lei No. 22/11 law: 1. Transparency 2. Legality 3. Good Faith 4. Proportionality 5. Truthfulness 6. Respect to private life and legal and constitutional guarantees.	Agência de Proteção de Dados (APD) created in October 2019	Yes	- No Significant level of enforcement - Monetary fines and Jail terms	Applicable The Regulator requires prior notice for any international transfers of personal data to countries deemed to have an adequate level of protection. The ADP must authorize transfer to jurisdictions considered as not having an adequate level of protection.	The law on data protection does not mandate the reporting of data breaches. However the Electronic Communication and Information Society Services Law requires companies that offer electronic communications services to the public to notify the APD and the Instituto Angolano das Comunicações, (INACOM) of any breach that adversely	-	1. No requirement by law to appoint data protection officers 2. Data Subject rights provided for	https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf https://dataprotection.africa/angola/

									affects personal data.			
Benin	Book V of the 2017 Digital Code of the Republic of Benin: Protection of Personal Data Loi No 2009-09 du 22 mai 2009 portant organisation de la protection des données à caractère personnel (in French) [Law No 2009-09: Dealing with the Protection of Personally Identifiable Information (PII)]	Data protection law present	Acts of Parliament	Specific principles followed according to Section 5, Loi No. 2009-09: : 1. Loyal and permissible collection. 2. Specification of Purpose 3. Compatibility with further processing. 4. Use limitation 5. Individual participation 6. Accountability 7. Security safeguards	Autorité de protection des données à caractère personnel (APDP) NB: Independent administrative body with full autonomy	Yes	- Significant level of enforcement - Administrative and criminal sanctions with penalty five (5) to ten (10) year prison sentence and/or Ten Million (Frcs CFA 10,000,000) to Fifty Million (Frcs CFA 50,00,.000)	Applicable Transfer of personal data to another country is allowed only when that country provides a level of protection equivalent to that put in place by the provisions of Book V of the 2017 Digital Code of the Republic of Benin. Transfer of personal data to another country or an international organization, requires prior authorization from the Regulator. (Refer section 43, Loi No. 2009-09)	Required	Localization: No Portability: Yes	1. Data Controllers are required to file annual reports with the Regulator. 2. Data Subject rights provided for. 3. Provisions similar to the GDPR include extra-territorial application, privacy by design, direct liability of processors, data breach notification to the DPA and to the data subject, data protection impact assessment, mandatory data protection officers, meaningful information required about the logic involved in automated data decisions, and a right to be forgotten.	https://apdp.bj/wp-content/uploads/2016/08/Loi-No-2009-du-22Mai-2009-Version-Anglaise.pdf https://dataprotection.africa/benin/ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593
Botswana	Data Protection Act 2018(DPA)	Data protection law present	1. Constitutional Recognition ([Ch0000s3] 3(c) CONSTITUTION OF BOTSWANA 1966, provides for "...protection for the privacy of his home and other property and from deprivation of property without compensation, the provisions of this Chapter shall have effect for the purpose of affording protection to those rights and freedoms subject to such limitations of that protection as are contained in those provisions...") 2. Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Information and Data Protection Commission (Commission) not created. NB: Not an independent body. It is under the direction of the Minister, to whom the members of the Commission must swear an oath of secrecy.	Yes	- Not currently enforced - Monetary fine of up to P100,000 and up to three (3) years of jail term (Refer Section 31, Data Protection Act 2018)	Applicable Transfer of personal data to another country is prohibited unless that country provides an adequate level of protection, which will be determined by the Commissioner. (Refer Section 47, Data Protection Act 2018)	Required	-	1. Data subject rights provided for. 2. Data controllers may appoint a data protection representative to ensure compliance with the DPA and good processing practices. The Commissioner should be notified of such an appointment, which will exempt a data controller from notifying the	Chapter II, Botswana Constitution 1996 Data Protection Act 2018 (DPA) https://dataprotection.africa/botswana/

											Commissioner before processing personal data except in special circumstances.	
Burkina Faso	Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel (in French) passed in 2007	Data protection law present	1. Constitutional Recognition (Article 6 of the Constitution of Burkina Faso 1991: "The residence, the domicile, private and family life, secrecy of correspondence of every person are inviolable. It can only be affected according to the forms and in the cases specified by the law.") 2. Act of Parliament	Specific principles followed according to Loi N°010-2004/AN: 1. Consent and legitimacy 2. Purpose of collection 3. Proportionality and relevance 4. Data retention 5. Security and confidentiality 6. Preliminary formalities (obtain approval in the absence of an exception or exemption)	Commission de l'Informatique et des Libertés (CIL) NB: Independent body with membership from various sections of society	No	- Significant level of enforcement - Administrative sanctions via enforcement notices and criminal sanctions	Applicable The Regulator allows international data transfers by legal or contractual means. The legal process necessitates that the host country either has comprehensive personal data protection legislation or its legal system otherwise provides adequate protection. The contractual process, in case of the absence of data protection legislation, requires two companies to abide by a contract of the personal data transfer in accordance with the protection legislation. The Regulator recognises the binding corporate rules (BCR) of the Association francophone des autorités de protection des données (AFAPDP) as an alternative to the contractual process.	Not Required	-	1. Data subject rights provided for. 2. The Regulator has been working for over a decade and over the period had discovered certain flaws in the law and in its implementatio. There has been an attempt to reform and therefore a revision of the law has been drafted, but not yet passed.	https://dataprotection.africa/burkina-faso/ https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3
Burundi		No data protection laws Despite not having a comprehensive data protection law, Burundi has been a party to meetings of the East African Community (EAC) to consider the status of cyber laws and highlight areas for reform. A few sectoral laws and regulations contain data protection provisions or impose confidentiality obligations on specific types of personal information. Employment, banking, telecommunications, and healthcare are among the sectors covered.										https://dataprotection.africa/burundi/
Cameroon		No data protection laws										
Cape Verde	Lei No 133/V/2001 of 22 January 2001 (in Portuguese)	Data protection law present	1. Constitutional Recognition	General principles followed: 1. Collection limitation 2. Data quality	Comissão Nacional de Proteção de Dados Pessoais (CNPD)	No	- Significant level of enforcement	Applicable Transfer of personal data	Not Required	-	1. Data subject rights provided for.	https://dataprotection.africa/cape-verde/

	Law No. 133, passed in 2001, was Cape Verde's original data protection law. It closely mirrored European data protection laws at the time, as Cape Verde's legal system largely draws from that of the Portuguese. Law No. 41 was passed in 2013 to supplement and update Law No. 133, and Law No. 42 was subsequently passed.		(Articles 42 and 43 of the Constitution of Cape Verde (1992) state: Article 42 (Utilization of computerized means) 1. The utilization of computerized means for registration and treatment of data that are individually identifiable, relative to political, philosophical and ideological convictions or to religious faith, party or trade union affiliation and private life, shall be prohibited. 2. The law will regulate the protection of personal data stored in the computerized record, the conditions of access to the data banks, as well as the establishment and the use, by public or private authorities, of such data banks or computerized software. 3. The access to the archives file, computerized records and databases for information on personal data relative to third parties or the transfer of personal data from one computerized file to another belonging to different services or institutions shall not be allowed, except in cases laid out by law or by judicial decision. 4. In no circumstance shall there be a sole national number ascribed to Capeverdean citizens. Article 43 (Habeas data) 1. Habeas data shall be granted to every citizen to secure his knowledge of information stored in files, archive or computerized records concerning him, as well as to inform him of the objective of such information and to demand a	3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	NB: It is an independent administrative authority responsible for enforcing the data protection laws of Cape Verde.		Administrative sanctions via enforcement notices & bans and criminal sanctions	outside of Cape Verde can be done with respect to the provisions of applicable domestic data protection law and is only permissible if the foreign country ensures an adequate level of protection. The transfer of personal data to a country which does not ensure an adequate level of protection may be permitted by CNPD if the data subject has given consent to the transfer or under limited exemptions provided for by the law.			2. It is required that the data controller appoint a data protection officer responsible for managing compliance with the law.	https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3

			correction or update of the data. 2. The law will regulate the habeas data procedure.) 2. Acts of Parliament									
Central African Republic		No data protection laws										
Chad	Law 007/PR/2015 on the Protection of Personal Data of 10 February 2015	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Agence Nationale de Sécurité Informatique et de Certification Electronique (ANSICE)	Yes NB: *if a DPO is appointed, then the organization may be exempt from registration.*	- Administrative and criminal sanctions (including fines and imprisonment)	Applicable Transfer of data is prohibited outside Central African Economic and Monetary Community (CEMAC) and the Economic Community of Central African States (CEEAC), it is required that cross border transfer outside the regional jurisdiction must comply with adequate level of data protection and with approval.	Required	-	1. Data subject rights provided for. 2. Appointment of data protection officer is voluntary	https://www.alwihdainfo.com/Tchad-nominations-a-l-Agence-nationale-de-securite-informatique-et-de-certification-electronique_a81338.html https://juriafrique.com/eng/2016/11/16/chad-sets-up-a-personal-data-protection-device/ https://media2.mofo.com/documents/170911-privacy-africa.pdf
Comoros		No data protection laws Comoros is already a signatory to the African Union Convention on Cybercrime and Data protection.										https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf
Congo		No data protection laws										
Côte d'Ivoire	Loi No 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (in French)	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Autorité de Régulation des Télécommunicatios /TIC de Cote d'Ivoire (ARTCI) NB: It is an independent administrative authority.	Yes	- Significant level of enforcement - Administrative sanctions via enforcement notices and criminal sanctions	Applicable Organizations may only transfer personal information to a "third country" that provides an equivalent level of protection. Prior DPA authorization is required for such transfers. The Cote D'Ivoire Law defines a "third country" as any country outside the Economic Community of West African States (ECOWAS). There are no limitations on the transfer of personal information to	Not Required	-	1. Data subject rights provided for. 2. Personal data processing of sensitive data requires prior authorisation from ARTCI 3. Establishes the right to be forgotten.	https://dataprotection.africa/cote-divoire/ https://media2.mofo.com/documents/170911-privacy-africa.pdf https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3

								other ECOWAS member states.				
Democratic Republic of the Congo		No data protection laws										
Djibouti		No data protection laws										
Egypt	Data Protection Law no. 151 of 2020	Data protection law present On February 24, 2020, Egypt's Parliament passed the Personal Data Protection Law ("PDPL"). Presidential assent was given on 15 July 2020.	Constitutional Recognition (Article 57 of Egypt's Constitution) Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Personal Data Protection Centre (Centre) established under the authority of the Competent Minister Yet to begin work.	Yes (Licensing & permits)	- Law was recently given Presidential assent and will come into force 3 months after Gazette.	Applicable. Transferring or sharing personal data abroad requires a permit from the Centre, provided that the recipient country of the transfer has equal or greater data protection regulations.	Required within 24 hours when the law is finally in force.	-	1. The data subject rights are guaranteed under the law 2. Any electronic communication for the purpose of direct marketing to the Data Subject shall be prohibited. Save under strict and prescribed conditions under the law. 3. The provisions of the law are excluded where personal data is held by the Central Bank of Egypt and entities subject to its control and supervision.	Data Protection Law No. 151 of 2020 https://dataprotection.africa/egypt/ https://www.researchworld.com/data-protection-developments-in-africa/
Equatorial Guinea	Law 1/2016 (Data Protection Law) enacted in 2016	Data protection law present	Constitutional Recognition (Item 13 of the Constitution of Equatorial Guinea includes: "Item 13: Every citizen shall enjoy the following rights and freedoms: g)—The inviolability of the home and the privacy of all correspondence.") Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Personal Data Protection Governing Authority (DPA)	Yes	- Significant level of enforcement - Administrative sanctions via enforcement notices and criminal sanctions	Applicable Organizations may not transfer any processed personal information to countries that fail to provide a legally equivalent level of protection, unless the transfer has been previously authorized by the DPA or an exception such as consent or contractual necessity applies.	Not Required	-	1. No requirement to appoint Data Protection Officer	https://media2.mofo.com/documents/170911-privacy-africa.pdf
Eritrea		No data protection laws										
Ethiopia	Freedom of the Mass Media and Access to Information Proclamation No. 590/2008	Constitutional protection present	Constitutional recognition Acts of Parliament	Personal data must be collected and processed with due care and only for an intended lawful purpose.	Not existent	No	Although the right to privacy is enshrined in the Ethiopian constitution, the current laws do not provide full	Generally applicable for lawful intent.	Required under the Computer Crime Proclamation No. 958/2016. Notice must be	-	1. Personal data must be collected and processed with due care and only for an	https://dataprotection.africa/ethiopia/

	Computer Crime Proclamation No. 958/2016						protection to this right, especially in the realm of personal data.		made to the Network Security Agency & the Police		intended lawful purpose. 2. Ethiopia has circulated a draft Data Protection Bill 2009 for consideration.	
Gabon	Loi n°001/2011 relative à la protection des données à caractère personnel (in French)	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Commission Nationale de Protection des Données à Caractère Personnel (CNPDCP). National Commission for the Protection of Personal Data (DPA) NB: An independent administrative authority established in November 2012	Yes NB: The appointment of a DPO may relieve the organization of some, but not all, of its registration obligations.	- Significant level of enforcement - Administrative sanctions, via enforcement notices, panelties and criminal sanctions	Applicable Transfer of personal data to another country is allowed only when that country provides a sufficient level of protection for privacy, freedoms and fundamental rights of individuals regarding the processing of personal data. The transfer of personal data to a country which does not ensure an adequate level of protection may be permitted if the data subject has given consent to the transfer or under limited exceptions.	Not Required	-	1. The appointment of a DPO is not required. 2. The processing of sensitive data is prohibited barring certain exceptions. 3. Health professionals may transfer personal information they use within the framework of the authorized processing of personal information. Where such data permit the identification of individuals, they must be encrypted before they are transmitted, unless the data are associated with pharmacovigi la- nce studies or research protocols carried out in the context of cooperative national or international studies or where necessitated by the specificity of the research.	https://dataprotection.africa/gabon/ https://media2.mofo.com/documents/170911-privacy-africa.pdf
Gambia	Information and Communications Act No. 2 of 2009 (in English)	Constitutional Protection present	Constitutional Recognition (Section 23 of the Constitution of Gambia (2001) states: "Privacy (1) No person shall be subject to interference	Personal data must be collected and processed with due care and only for an intended lawful purpose.	Not existent	No	Enforcement as constitutional rights	Not Required	-	-	-	https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3 https://media2.mofo.com/documents/170911-privacy-africa.pdf

			with the privacy of his or her home, correspondence or communications save as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights and freedoms of others.'')									
Ghana	Data Protection Act (Act No. 843) 2012 - DPA (in English)	Data protection law present	Constitutional Recognition (Article 18 of the Constitution of Ghana (1992) states: ''(2) No person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.'') Act of Parliament	Specific principles followed according to Section 17, Act 843: 1. Accountability 2. Lawfulness of processing 3. Specification of purpose 4. Compatibility of further processing with purpose of collection 5. Quality of information 6. Openness 7. Data security safeguards 8. Data subject participation	Data Protection Commission of Ghana (DPC) was set up in 2015	Yes (Renewable for a 2-yr cycle) It is a punishable offence not to register with the DPC.	- Significant level of enforcement - Administrative sanctions, via enforcement notices, penalties and criminal sanctions with fines up to GHC6000 and imprisonment of up to five (5) years	Not Applicable - Under Section 18 of Act 843, data of foreign data subjects shall be processed in compliance with data protection legislation of the foreign jurisdiction when data of that data subject is sent to Ghana for processing.	Required	Localization: No Portability: No	1. Data subject rights are provided for. 2. Personal data selling or offering to sell the personal data of another person anywhere constitutes a punishable offence.	1992 Constitution of Ghana Data Protection Act 2012 (Act 843) https://www.dataprotection.org.gh https://dataprotection.africa/ghana/ https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3 https://media2.mofo.com/documents/170911-privacy-africa.pdf
Guinea		No data protection laws										
Guinea-Bissau		No data protection laws										
Kenya	Data Protection Act No. 24 of 2019 (the Act) was signed into law in November 2019	Data protection law present	Act of Parliament	Section 25 of Act No. 24 stated the following principles: (a) processed in accordance with the right to privacy of the data subject; (b) processed lawfully, fairly and in a transparent manner in relation to any data subject; (c) collected for explicit, specified and legitimate purposes and not further processed in a manner	Office of the Data Protection Commissioner (Commissioner) currently undergoing setup. The position for the Commissioner role was recently advertised.	Yes	- Yet to commence enforcement	Applicable Personal data shall not be transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject. (Refer Section 25(h))	Required Must notify the Commissioner without delay within 72 hours The communication of the breach to the data subject shall not be required where the data controller or	-	1. Data subject rights are provided for. 2. It is not mandatory to appoint a Data Protection Officer 3. Data protection impact assessment is required the	Data Protection Act No. 24 of 2019 (the Act) https://dataprotection.africa/kenya/ http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.pdf https://qz.com/africa/1746202/kenya-has-

				incompatible with those purposes; (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required; (f) 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; (g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and (h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.					data processor has implemented appropriate security safeguards which may include encryption of affected personal data.		law (Refer section 32)	passed-new-data-protection-laws-in-compliance-with-gdpr/
Lesotho	Data Protection Act, 2011 (Act No. 05 of 2012) came into force in 2013. Published in the Lesotho Government Gazette as Act, No. 5 of 2012	Data protection law present	Constitutional Recognition Lesotho 1993 Constitution as amended provides under Chapter II that "Every person shall be entitled to respect for his private and family life and his home." Acts of Parliament	Specific principles followed according to Part III of the Data Protection Act, 2011: 1. Purpose specification and further processing limitation 2. Minimality 3. Data retention 4. Information security 5. Quality of information 6. Automated processing control	Lesotho's Data Protection Commission (LDPC) Not setup yet	Yes	- Yet to commence enforcement The LDPC will have considerably less enforcement power than analogous bodies in other jurisdictions given that it's stipulated powers in the Act (such as its lack of ability to impose fines on entities that violate the Act).	Applicable The Act allows personal information to be transferred to recipients in a member state that has adopted the SADC data protection requirements the recipient demonstrates that the data is necessary for a task carried out in the public interest or pursuant to the lawful functions of a data controller; or recipient demonstrates a need for the transfer and there is no reason to assume that the data subject's interests would be prejudiced by the transfer or processing in the member state.	Not Required	-	1. Data subject rights are provided for. 2. It is not mandatory to appoint a Data Protection Officer	Data Protection Act, 2011 (Act No. 05 of 2012) https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3 https://media2.mofo.com/documents/170911-privacy-africa.pdf https://dataprotection.africa/lesotho/
Liberia		No data protection laws										
Libyan Arab Jamahiriya		No data protection laws										
Madagascar	Loi No. 2014-38 (in French)	Data protection law present	Constitutional Recognition. (Madagascar's 2010 Constitution grants	General principles followed: 1. Collection limitation 2. Data quality	Commission Malagasy sur l'Informatique et des Libertés	Yes (known in the law as prior declaration)	- Yet to commence enforcement	Applicable A data subject's personal data may	Not Required	-	1. Data subject rights are provided for.	https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3

	came into force upon publication in the Madagascan Official Gazette on 20 July 2015		individuals the inviolability of their persons, domiciles, and of the secrecy of their correspondence) Act of Parliament	3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	(CMIL), has not yet been established. (Malagasy Commission on Informatics and Liberty) NB: Designated as an independent data protection authority.	Data controllers who appoint a data protection officer are not required to issue prior declarations except in special circumstances (e.g., an extraterritorial transfer to a country that does not provide an adequate level of personal data protection).	1. warnings and notices to comply with the obligations defined in the DP Law; 2. notice of withdrawal of the authorisation; and / or 3. a fine of up to 5% of the last financial year pre-tax turnover (not deducted from tax turnover). 4. criminal sanctions (jail term of up to two (2) years)	only be transferred out of Madagascar if the country provides an adequate level of protection for privacy and fundamental rights and liberties or under strict conditions where adequacy doesnt exist. The data recipient in the receiving country cannot transfer personal data to another country without the authorisation of the original data controller and CMIL.			2. A DPO must be appointed. 3. The Madagascar Law also prohibits subsequent transfers except with the approval of the organization responsible for the original processing and the DPA.	https://dataprotection.africa/madagascar/ https://media2.mofo.com/documents/170911-privacy-africa.pdf
Malawi	Electronic Transactions and Cybersecurity Act Act No. 33 of 2016	No dedicated and specific law for Data Protection Inferred from current Act No. 33 of 2019.	Act of Parliament	General principles followed (inferred from Act No. 33): 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	No Authority currently for Data Protection compliance The Malawi Communications Regulatory Authority is responsible for the implementation of Act No. 33 of 2016.	No	- Partial enforcement May impose administrative penalties of up to K5,000,000 for violations.	Not Applicable	Not Required	-	1. Data subject rights are provided for.	https://dataprotection.africa/malawi/
Mali	Loi No 2013-015 du 21 mai 2013 (in French) Law no. 2013/015 on the Protection of Personal Data (Mali Law) was adopted in May 2013.	Data protection law present	Constitution Recognition (The right to privacy is protected under the Constitution of Mali) Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Autorité de protection des données à caractère personnel (APDP) and was launched in March 2016.	Yes	- Significant level of enforcement Administrative sanctions via enforcement notices and criminal sanctions	Applicable Transfer of personal data to another country is allowed only when that country provides sufficient legal protection for privacy, freedoms, and fundamental rights of individuals regarding the processing of personal data.	Not Required	-	1. Data subject rights are provided for. 2. On 31 March every year, the Supreme Court reviews the law, and makes revisions, if necessary	https://media2.mofo.com/documents/170911-privacy-africa.pdf https://dataprotection.africa/mali/
Mauritania	Proposed Data Protection Legislation as at 2017	In progress	Proposed Act of Parliament	It has been noted that the proposed legislation adopts the OECD guidelines which emphasizes on eight (8) principles including limitation in data collection, data quality control, data collection purpose, user limitation, establishment of security safeguards, openness, the individual's right especially regarding participation and accountability for compliance with measures undertaken.	No Authority	-	-	-	-	-	Mauritania is one of the Signatories to the Convention on Cyber Security and Personal Data protection adopted by the African Union in 2014.	https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf https://cipesa.org/?wpfb_dl=272

Mauritius	Data Protection Act 2004 (DPA 2004) (in English) Data Protection Act 2017 (DPA 2017) Repealed DPA 2004 so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR).	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Office of the Data Protection Commissioner	Yes Registration is valid for three years	- Significant level of enforcement Administrative sanctions via enforcement notices and criminal sanctions (Rs200,000 or imprisonment for a term not exceeding five years) .	Applicable A controller or processor may transfer personal data to another country if the Commissioner is given proof of appropriate safeguards with respect to the protection of the personal data or the data subject has explicitly consented to the proposed transfer albeit the the risk, and where the transfer is necessary under specific requirements of the law.	Required Notifying the data subject is not required if: 1. the controller has applied appropriate technical and organisational protection measures to the personal data affected by the breach; 2. the controller has mitigated the high risk to the rights and freedoms of the data subject; or 3. it would involve disproportionate effort and the controller has made a public communication or similar measure whereby the data subject is informed just as effectively.	-	1. Data subject rights are provided for. 2. If the Commissioner has reasonable grounds to believe that data is vulnerable to loss or modification, he, she or they may ask a judge for an order for the expeditious preservation of such data. The Commissioner may also carry out periodic audits of the systems and security measures used by data controllers and processors.	https://dataprotection.africa/mauritius/ https://media2.mofo.com/documents/170911-privacy-africa.pdf
Morocco	Law No. 09-08/2009 on the protection of people toward data protection of a personal nature In 2009, Morocco enacted Law No. 09-08 relating to protection of individuals with regard to the processing of personal data and its corresponding implementation decree, Decree No 2-09-165 (referred to collectively as DP Law).	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Commission Nationale de Protection des Données Personnelles (CNDP) NB: an independent data regulator	Yes Organizations must register all partially or wholly automatic processing of personal information with the DPA prior to the commencement of processing, unless an exception applies.	- Significant level of enforcement CNDP has power to levy sanctions on data controllers that violate the DP Law.	Applicable Personal data is transfers outside Morocco require prior authorisation from the CNDP.	Not Required	-	1. Data subject rights are provided for. 2. There is no obligation to appoint a DPO 3. In addition to registration, prior authorization must be obtained for certain types of processing, such as the processing of sensitive information including genetic, health, and criminal data.	https://dataprotection.africa/morocco/ https://media2.mofo.com/documents/170911-privacy-africa.pdf
Mozambique		No data protection laws The Republic of Mozambique Constitution entitles all citizens to the protection of their private life and grants them the right to honour, good name, reputation, protection of their public image, and privacy. The Constitution also acknowledges the need to legislate on access, generation, protection, and use of computerised personal data, but such legislation has not yet been enacted. It further provides that all individuals shall have the right to access data collected on them and have it rectified, but this right has not yet been defined. Nonetheless, a data subject is entitled to demand the correction and the update of any inaccurate, incomplete, or wrong personal information related to them.										https://dataprotection.africa/mozambique/
Namibia	Namibian Constitution 1990 (GG 2)	Constitutional protection provided	Constitutional recognition	Namibia recognises the right to privacy as a fundamental human right in its	Not existent	No	Enforcement as constitutional rights	-	-	-	The Ministry of Information and	Namibian Constitution (GG2) 1990

	Namibian Constitution First Amendment Act 34 of 1998 (GG 2014) Namibian Constitution Second Amendment Act 7 of 2010 (GG 4480) Namibian Constitution Third Amendment Act 8 of 2014 (GG 5589)	Article 13, Namibian Constitution (GG2) 1990 Provides for the right to privacy for all citizens.		Constitution, and the government is currently drafting a Data Protection Policy to protect citizens against abuse of their personal data and to regulate extraterritorial data transfers.							Communication Technology (MICT) is expected to finalise a draft Data Protection Bill to be published in either 2019 or 2020.	https://dataprotection.africa/namibia/
Niger	Law No. 2017-28	Data Protection Law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Haute Autorité de Protection des Données à caractère personnel (HAPD). NB: an independent administrative authority	Yes The processing of personal data is subject to prior notification to the HAPD. If a data controller appoints a data protection officer, notification is unnecessary unless personal data is being transferred across national borders.	- No significant level of enforcement	Applicable Transfer of personal data to another country is allowed only when that country provides a superior or equivalent level of protection for privacy, freedoms and fundamental rights of individuals regarding the processing of personal data.	Not Required	-	1. Data subject rights are provided for.	https://dataprotection.africa/niger/
Nigeria	Data Protection Bill 2019, was not assented to by the President. Nigeria Data Protection Regulation (NDPR) 2019.) Created under the National Information Technology Development Agency (NITDA) Act.	Data protection law present	Constitutional Recognition (Section 37 of the 1999 Constitution of the Federal Republic of Nigeria, provides for the right to privacy. Subsidiary Legislation	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	National Information Technology Development Agency (NITDA) NB: an executive agency, NDPR provisions can be superseded by any act of Parliament	Yes	- Enforcement just started The NDPR states that any entity found to be in breach of the privacy rights of any data subject will be liable, in addition to any other criminal liability, for the following: • for data controllers "dealing with more than 10,000 data subjects," a fine of 2% of annual gross revenue of the preceding year or 10 million Naira, whichever is greater; or • for data controllers "dealing with less than 10,000 data subjects," a fine of 1% or 2 million Naira, whichever is greater.	Applicable For an extra-territorial transfer of personal data to occur, NITDA must decide that the jurisdiction, sector, or the organisation in question grants an adequate level of protection, and the Attorney-General must also perform an analysis of the legal system of the jurisdiction taking numerous considerations into account.	Not Required	-	1. Data subject rights are provided for. 2. As of April 25, 2019, all public and private organisations that process personal data must publicise their NDPR compliant data protection policies and as of July 25, 2019, organisations must conduct an initial audit or their privacy and data protection practices.	https://dataprotection.africa/nigeria/
Rwanda	Information and Communication Technologies Law No. 24/2016 contains a few provisions related to personal data processing.	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation	National Information and Communication Technologies Regulatory Authority	No	- Not significantly enforced The Regulatory Authority is given the power to conduct technical inspections and impose administrative	No provision stipulated	Partly required Licensed electronic communications service providers must inform users about any	-	It is reported that Rwanda is currently drafting a law for personal data protection, which is set to be submitted	https://dataprotection.africa/rwanda/

				8. Accountability			sanctions on ICT operators. It may suspend access to electronic communications networks and services for certain operators, resolve disputes, and refer matters to courts.		security risks which may occur as a result of a breach of network security measures or protocols, and the necessary remedies available to address the breach of network security.		to the Rwandan Parliament for approval in 2020.	
Sao Tome and Principe	Law No.3/2016 of 10 May 2016 (Data Protection Law 2016)	Data protection law present	Act of Parliament	Follows the general principles set out in the Data Protection Directive (Directive 95/46/EC), and, more particularly, the wording of the Law is very similar to the Portuguese Data Protection Act 1998	National Agency for the Protection of Personal Data (ANPDP) fully operational since 2018 ANPDP's decisions are binding, but may be challenged and appealed against before the Courts.	Yes Under Article 21 of the Law, notification must be given to the ANPDP within a period of eights prior to the processing of the any personal data. Under Article 22, a prior authorisation of the ANPDP must be sought for processing personal data which establishes a data subject's creditworthiness.	- Enforcement efforts are yet to begin Under Article 31, the ANDP has enforcement powers in respect of data controllers and processors that fail in their notification obligations or provide false information. More specifically the ANPDP can impose a fine of up to STD 500 million (approx. €20,850) for violations.	Applicable The ANPDP must be notified before any data transfer outside the jurisdiction can take place.	Not stipulated by the law	-	Sao Tome and Principe is one of the Signatories to the Convention on Cyber Security and Personal Data protection adopted by the African Union in 2014.	https://platform.dataguidance.com/opinion/s%C3%A3o-tom%C3%A9-and-pr%C3%ADncipe-anpdp-starts-its-operations-very-challenging-context https://www.vda.pt/xms/files/v1/Newsletters/2017/Flash_VdA_Legal_Partners_-_Sao_Tome_and_Principe_-_Law_7-2017.pdf https://cipesa.org/?wpfb_dl=272
Senegal	Loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel (in French) Law No. 2008-12 Enacted in 2008 and entered into force in 2014	Data protection law present	Constitutional Recognition Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Commission des Données Personnelles (CDP) Commission for the Protection of Personal Data NB: an independent administrative authority	Yes Submit a declaration to the CDP in advance	- Significant level of enforcement If the controller fails to comply with the enforcement notice, the CDP can sanction the entity through: • a temporary withdrawal of the authorisation for a period of three months at the end of which period, if compliance is not satisfied, becomes final; and • a fine of one million to one hundred million CFA francs. In case of emergency, when implementing processing of personal data has constituted a violation of rights and freedoms, the CDP, after adversarial procedure, can decide:	Applicable Transfer of personal data to another country is allowed only when that country provides sufficient legal protection for privacy, freedoms and fundamental rights of individuals to the processing of personal data. And where these protections are not provided for is possible when the data subject has expressly consented to the transfer, or to protect the data subject's life, to safeguard the public interest, in exercise or defence of a legal claim, and in execution of a contract in the data subject's interest.	Not Required	-	1. Data subject rights are provided for. 2. No obligation to appoint a Data Protection Officer. 3. There has been no strict adherence to data processing principles with data breaches such as surveillance, interception by state security agencies and private entities remaining rampant	https://dataprotection.africa/senegal/ https://cipesa.org/?wpfb_dl=272

							• to delay processing for a maximum of three months; • to lock certain personal data processed for a maximum of three months; or • to temporarily or permanently prohibit the controller from processing against the provisions of the law.					
Seychelles	Data Protection Act 2003 (in English) Based on the 1984 UK Data Protection Act.	Data protection law present	Act of Parliament	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Data Protection Commissioner (DPA)	Yes	- No enforced Administrative sanctions via enforcement & de-registration notices.	Applicable The DPA has the power to prohibit cross-border transfers if it believes such transfers will violate the data protection principles under the act.	-	-	There is virtually no enforced legal protection for personal data in Seychelles today.	https://dataprotection.africa/seychelles/ https://media2.mofo.com/documents/170911-privacy-africa.pdf
Sierra Leone		Constitutional protection provided	Constitutional recognition	-	-	-	-	-	-	-	Sao Tome and Principe is one of the Signatories to the Convention on Cyber Security and Personal Data protection adopted by the African Union in 2014	https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf https://cipesa.org/?wpfb_dl=272
Somalia		No data protection laws										
South Africa	The Protection of Personal Information Act 4 of 2013 (POPIA) was signed in 2013. POPIA in its entirety, was expected to come into force in 2019, but this may be delayed.	Data protection law present	Constitutional Recognition (Section 14 of the Constitution of South Africa establishes privacy as a fundamental human right and the right to privacy is protected under the common law.) Act of Parliament	Specific principles followed according to Protection of Personal Information Act (POPIA) 2013: 1. Accountability 2. Processing limitation 3. Purpose specification 4. Further processing limitation 5. Information quality 6. Openness 7. Security safeguards 8. Data subject participation	Office of the Information Regulator (Information Regulator) Information Regulator have been appointed, with effect from December 1, 2016.	Yes (Refer Sections 57, 58 and 114 of POPIA)	- Partial enforcement The Information Regulator will announce the date at which the law will take effect and enforce the relevant provisions thereafter. Maximum fine under sections 107 and 109 of POPIA is R10 million although this may change once the regulations are promulgated.	Applicable Transferring the personal information of a data subject outside of South Africa to a third party located in a foreign country is prohibited unless under limited exceptions per the POPIA.	Required	-	1. Data subject rights are provided for. 2. During November 2019 the Regulator published a draft set of guidelines to assist public and private bodies with the development of codes of conduct in terms of chapter 7 of POPIA.	The Protection of Personal Information Act 4 of 2013 (POPIA) Data Protection Laws Of The World - South Africa, DLA PIPER (Downloaded 3 April 2020) https://dataprotection.africa/south-africa/
Sudan		No data protection laws										
South Sudan		No data protection laws										
Swaziland	Data Protection Bill	Constitutional protection provided	Constitutional recognition	Chapter IV (c) of the Constitution of the Kingdom of Swaziland provides for the right to privacy of person and property.	-	-	-	-	-	-		https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-

												Personal_Data_Protection_in_Africa.pdf https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3
Republic of Togo	Law No. 2019-014 (in French)	Data protection law present	Act of Parliament	The DPA Law sets out basic principles that govern treatment of personal data: 1. The principle of consent and legitimacy 2. The principle of lawfulness and loyalty 3. The principle of purpose, relevance and conservation 4. The principle of accuracy 5. The principle of confidentiality and security 6. The principle of transparency 7. The principle of choosing the subcontractor 8. The principle of prohibition	Personal Data Protection Authority (PDPA) NB: an independent administrative authority	Yes Before they can collect or process any data, all data controllers and processors must file requests for opinions, declarations and requests for authorisation with the PDPA.	- Enforcement yet to start. Sanctions includes: A temporary withdrawal of authorization granted for a period of 3 months at the end of which if corrective measures are not taken, the withdrawal becomes final or a fine not exceeding one hundred million CFA francs.	Applicable The controller cannot transfer personal data to a third country unless that state ensures an adequate level of protection of life, privacy, fundamental rights and freedoms of individuals with regard to the processing of the data. Before any transfer of personal data to a third country is undertaken the controller must first inform the PDPA.	Not Required	-	1. Data subject rights are provider for.	https://dataprotection.africa/togolese-republic/
Tunisia	(Loi portant sur la Protection des Donn´ees `a Caract`ere Personnel) Law 63/2004 (in French) passed in 2004. Organic Act No. 2004-63	Data protection law present	Constitution Recognition (The 1959 Constitution to include the right to personal data protection in 2002.) Act of Parliament	Tunisia has signed the Council of Europe's Convention 108, the updated Tunisian data protection law will likely reflect the principles therein.	Tunisian Data Protection Authority, Instance Nationale de Protection des Données à caractère Personnel (INPDP)	Yes Any processing of personal data shall be subject to a prior declaration filed at the INPDP headquarters, or by any other means leaving a written record.	- Significantly enforced.	Applicable The transfer of personal data is generally prohibited or subject to strict measures, including prior authorisation from the INPDP, and the explicit consent of the person in question, which is mandatory.	Not Required	-	1. Data subject rights are provided for. 2. Organizations must list on the registration/notification forms the name of the DPO. The DPO must have Tunisian nationality, reside in Tunisia, and have a clean criminal record. 3. It is important to note that organisations with a "public personality" (such as police) are not bound by the obligations that generally apply to personal data processors in Tunisia.	https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119991083.app3 https://media2.mofo.com/documents/170911-privacy-africa.pdf https://dataprotection.africa/tunisia/

Uganda	The Data Protection Act, 2019 (in English) not yet in effect	Data protection law present	Constitutional Recognition Privacy protections are already guaranteed to Ugandans under the Constitution Act of Parliament Data Protection and Privacy Act, 2019	General principles followed: 1. Collection limitation 2. Data quality 3. Purposes specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	Personal Data Protection Office (PDPO) is housed within the National Information Technology Authority (NITA) and comes under the direct control of any person or Authority.	Not stipulated by the provisions of the law	- Not enforced.	Applicable Processing or storage of personal data outside Uganda may occur if adequate data protection measures exist in the country where the data is processed or stored, or with data subject consent.	Required Notification must be made to the NITA	-	1. Data subject rights are provided for. 2. Appointment of a Data Protection Officer (DPO) is required. 3. The Minister of Information and Communications Technology will announce implementation regulations at some point in the future.	https://dataprotection.africa/uganda/
United Republic of Tanzania	Electronic and Postal Communications Act (EPOCA)2010 Data Protection Bill 2013	In progress EPOCA guards against the violation of any person's entitlement to respect and protection of person, the privacy of their own person, their family and matrimonial life, and respect and protection of their residence and private communications.	Constitutional Recognition (Constitution of the United Republic of Tanzania guarantees the right to privacy) Act of Parliament	-	-	No law currently applies	- Not Enforced	Not Applicable	Note Required	-	1. The Cybercrimes Act prohibits operators and other service providers from monitoring activities or data being transmitted in their system, and as such, these providers are shielded from being held liable for illegal activity that takes place within their networks or systems through the actions of third parties. It is, however, lawful for officers, employees, or agents of these providers to intercept, disclose, or use communications transmitted while engaged in any activity necessary to the performance of services or to protect the rights or property of the provider.	https://cipesa.org/?wpfb_dl=272 https://dataprotection.africa/tanzania/

Western Sahara	Not identified	Data protection law present	-	-	-	-	-	Applicable	Required	-	Even though some literature does mention that there is DP Law, this research did not find any evidence beyond the references that says it does exist.	https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf
Zambia	The Electronic Communications and Transactions Act, Act Number 21 of 2009 - the Electronic Communications Act provides some related data protection provisions	In progress Cabinet has approved the introduction of the Data Protection (Repeal) Bill, 2018 to Parliament, with the goal of repealing and replacing the ECTA. This bill has yet to become law.	Act of Parliament	No data protection principles	Zambia Information and Communication Technology Authority (ZICTA) is responsible for enforcing the ECTA	Not Required by the ECTA	- Partially enforced	Not Applicable	Not Required	-	1. No requirement under the ECTA for data protection officers to be appointed 2. Zambia is one of the Signatories to the Convention on Cyber Security and Personal Data protection adopted by the African Union in 2014.	https://dataprotection.africa/zambia/ https://cipesa.org/?wpfb_dl=272
Zimbabwe	Draft Data Protection Bill 2003 Draft Data Protection Bill 2016	In progress	Constitutional Recognition (Zimbabwe's constitution acknowledges the right to privacy) Act of Parliament (Various sectoral laws address the right to privacy and protection of personal information for specific types of data and activities.)	No strict adherence to data processing principles	-	-	- Partially enforced	Not Applicable	Not Required	-	1. The Revised ICT Policy states that a law on data protection and privacy will be passed, and currently a draft Data Protection Bill is circulating online for comments from stakeholders. 2. Zambia is one of the Signatories to the Convention on Cyber Security and Personal Data protection adopted by the African Union in 2014.	https://dataprotection.africa/zimbabwe/ https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593 https://cipesa.org/?wpfb_dl=272

Appendix two

Template for a model data protection law

Preamble

SHORT TITLE

OBJECTIVE

Chapter 1. Interpretation

- Interpretation

Chapter 2. Scope of application

- Scope of application

Chapter 3. Data protection authority/commission/regulator

- Establishment of regulator
- Object of the regulator
- Functions of the regulator
- Governing body of the regulator
- Tenure of office of member
- Meetings of the regulator
- Disclosure of interest
- Establishment of committees
- Allowances
- Ministerial directives
- Appointment of commissioner
- Removal from office of the commissioner
- Functions of the commissioner
- Appointment of other staff
- Funds of the regulator
- Accounts and audit
- Annual report and other reports

Chapter 4. Data protection principles

- Fair, lawful, and transparent
- Purpose limitation
- Minimisation
- Accuracy
- Storage limitation
- Adequate security safeguards

- Accountability

Chapter 5. General grounds for the processing of personal data

- Consent
- Public interest
- Legitimate interest
- Quality of the data
- Processing of special or sensitive data

Chapter 6. Obligation of the data controllers and data processors

- Accountability
- Authority to process
- Integrity and confidentiality
- Openness of the processing
- Recording processing activities
- Processing by third parties
- Privacy by design and by default
- Impact assessments
- Appointment of data protection officers
- Notification of breach
- Content of the breach notification

Chapter 7. Registration of data controllers and data processors

- Establishment of data protection register
- Registration of data controllers and data processors
- Application for registration
- Duration of the registration
- Right to refuse registration
- Cancellation or variation of the registration
- Designation of the data protection officer
- Grant of registration
- Renewal of registration
- Removal from register
- Processing of personal data without registration prohibited
- Access to the register by the public
- Obligation to notify of changes
- Failure to register
- Compliance and audit
- Fees

Chapter 8. International transfer

- Rule as to data centres and servers
- Conditions for transfer out of country
- Safeguards prior to transfer out of country
- Authorisation process

Chapter 9. Rights of the data subjects

- Right to information
- Right to access
- Rights to rectify, block and erasure
- Right to object
- Right to data portability
- Rights related to profiling and automated decision making
- Right to an effective remedy
- Right to compensation and liability
- Exceptions

Chapter 10. Recourse to the judicial authority

- Recourse to the judicial authority

Chapter 11. Enforcement and sanctions (administrative and criminal)

- Enforcement notice
- Cancellation of enforcement notice
- Determination by the commission
- Restriction on enforcement in case of processing for special purposes
- Failure to comply with enforcement notice
- Sanctions

Chapter 12. Limitations/exceptions

- National security
- Prevention, investigation, detection or prosecution of criminal offences
- Public interest and safety
- Public health and security
- Immigration
- Economic or financial interests, including budgetary and taxation matters
- Protection of judicial independence and proceedings
- Exercise of official authority and regulatory functions
- Protection of the individual or the rights and freedoms of others
- Enforcement of civil law matters
- Social and domestic use

- Journalism, academia, art & literature
- Scientific, historical, or statistical purposes
- Professional privilege

Chapter 13. Miscellaneous and general provisions

- General duties of the regulator
- Authorised officers
- Request for assessment
- Procedures for the issue of codes, guidelines and certification
- Training
- Regional/international co-operation
- Disclosure of information
- Confidentiality of information
- Prohibition to purchase, obtain or disclose personal data
- Prohibition of sale of personal data
- Application to the state
- Transmission of notices by electronic or other means
- Service of notices by the regulator
- Regulations
- General penalties
- Transitional provisions
- Repeal and savings
- Commencement

Schedule(s)