Privacy and personal data protection in Africa

Advocacy toolkit

Privacy and personal data protection in Africa: Advocacy toolkit

Coordination team
Koliwe Majama (APC)
Janny Montinat (APC)
Anriette Esterhuysen (APC)

Compiled by
Hlengiwe Dube, University of Pretoria,
Centre for Human Rights
Avani Singh, ALT Advisory

Copy editing and proofreading
Lynne Stuart (Idea in a Forest)
Lori Nordstrom (APC)
Lynn Welburn

Publication production and support
Cathy Chen (APC)

Graphic design
Monocromo

Published by the African Declaration on Internet Rights and Freedoms Coalition
https://africaninternetrights.org
April 2021

ISBN 978-92-95113-39-8
APC-202103-CIPP-T-EN-DIGITAL-329
Supported by the Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH

Table of contents

Overview of the toolkit

This advocacy toolkit provides an overview of the legal standards concerning the right to privacy and personal data protection in Africa and offers a set of practical tools for stakeholders in the formulation and implementation of data protection frameworks.

The toolkit is relevant as a resource for anyone who desires to understand the human rights-based approach to privacy and data protection in Africa. It aims to provide the basis for the development of further advocacy, country specific initiatives and to mobilise support for the reforms and implementation of data protection frameworks. It can also provide a basis to harmonise and strengthen engagement and advocacy across all focus countries, building our collective agency and overall effectiveness. In this regard, this toolkit is a significant step towards further buttressing advocacy on privacy and data protection in Africa.

Furthermore, the toolkit is a guide to engage with, advocate for, and inform policy makers on data protection and privacy in Africa. It can also be used as a manual by trainers in the understanding of data protection and privacy for various actors. The toolkit will also be helpful to human rights practitioners who are not specialists in privacy and data protection, to provide knowledge of this field which is becoming significant in all sectors. Non-governmental organisations, policy makers and legal practitioners will find it useful as a point of reference on data protection and privacy in Africa.

The toolkit is divided into three parts: **Part One** provides an introduction to the international and regional human rights framework; **Part Two** delves into the content of the right to privacy and personal data protection; and **Part Three** deals with duty bearers and rights holders. The toolkit focuses on the following issues:

- Data protection terminology
- Key principles of data protection law
- Frameworks on data protection in Africa
- Rights of data subjects and obligations of duty-bearers
- Potential contributions of various role players in personal data protection and privacy
- Policy guidelines on data protection and privacy.

As issues regarding the right to privacy and personal data protection become increasingly prevalent in our everyday lives, particularly in the digital area, it is envisaged that issues highlighted in this toolkit will evolve and present opportunities of providing further guidance on data protection and privacy in Africa going forward.

Part 1.
Introduction to the international and regional human rights framework

Significance of the right to privacy

The right to privacy and the processing of personal information is not a new phenomenon, but more attention has been paid to it in the past few decades as technological advancements have made an impact. Privacy is an expansive conception involving an individual's autonomy and how he or she relates to society.[1] This right is recognised as a vital enabler of other rights, such as the rights to dignity, freedom of expression, association and assembly.[2]

1 Banisar, D. (2011). *The Right to Information and Privacy: Balancing Rights and Managing Conflicts*. The International Bank for Reconstruction and Development / The World Bank. https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf

2 Ibid.

Due to technological advancements, the collection of personal information is now ubiquitous and generally mundane. The significant increase in access to the internet and other information and communications technologies (ICTs) has resulted in a consequent increase in the quantities of data being generated and collected. Personal information is exchanged among people, institutions and departments, both in the public and private sector. The collection of information can be inescapable, and at the same time the information sharing practices could be intrusive and raise the potential for serious concerns regarding the invasion of the right to privacy.

In the United Nations Resolution on the Right to Privacy in the Digital Age, there is an acknowledgment of both the positive attributes brought by the new technologies and the vulnerabilities that arise. However, reliance on and use of ICTs cannot be overlooked.[3] It is of concern that governments use these technologies to "undertake surveillance, interception and data collection" and that this has had an impact on the states' obligations as to the respect, protection and fulfilment of human rights.[4] The intensified use of technologies facilitates information collection and the dissemination of information, including personal data. Data is being collected, processed, shared and transferred every day, with or without the knowledge of the affected persons, which has serious implications for personal privacy.

The right to privacy has acquired new significance in the digital age. Advancements in technology modify and accelerate the processing, analysis, collection and storage of data, including personal information. For example, technology has augmented surveillance

3 United Nations. (2014, 21 January). The Right to Privacy in the Digital Age. General Assembly resolution 68/167 A/RES/68/167. https://undocs.org/pdf?symbol=en/A/RES/68/167

4 Ibid.

practices, necessitated the establishment of databases, made it possible to anonymise and de-anonymise data – all on a wide scale and all with implications for the right to privacy. The increased interference with this right exists mostly in environments with limited oversight mechanisms and it results in data breaches, misuse of personal data, unlawful and indiscriminate interception of communications and impermissible data retention policies.

Data protection as a cornerstone to realising the right to privacy has gained increasing traction as an important human rights and public interest issue. Africa intensified its interest in the privacy and data protection discourse more recently, a bit later than other continents.[5] This interest stemmed from, among other things, the growth of ICTs, the emergence of digital economies, and the requirement under European data protection law that data transfers to non-European Union member states require adequate data protection safeguards.[6] Recent developments have also resulted in greater civic awareness about the need to protect privacy and personal information, which in turn have led to public demands by civil society for appropriate laws and protections that effectively safeguard this right.

While the right to privacy remains an "elusive concept, resulting in much debate and confusion" in Africa, it is generally agreed that privacy is a fundamental human right.[7] As such, there is seen to be a growing body of legal norms – at the domestic, sub-regional and regional levels – that seek to safeguard the right to privacy. It is therefore apparent that there is an increasing recognition and awareness that privacy and data protection are fundamental elements of democracy and digital economies that Africa needs to rapidly embrace.

5 Makulilo, A. B. (2012). Privacy and data protection in Africa: a state of the art. *International Data Privacy Law, 2*(3), 163-178. https://www.researchgate.net/publication/273026565_Privacy_and_data_protection_in_Africa_a_state_of_the_art

6 Ibid.

7 Gondwe, M. (2011). *The Protection of Privacy in the Workplace: A Comparative Study*. PhD Thesis, Stellenbosch University.

The human rights perspective: International and regional human rights framework

Everyone is entitled to human rights as guaranteed under international, regional and national laws (constitutions, human rights acts and/or other legislation). Human rights are inherent, inalienable, interdependent, indivisible and non-discriminatory and play a significant role in promoting the dignity of the person, freedom, peace, justice and equality. Any limitation of human rights should be clearly justified and grounded in the three-part test for a justifiable limitation as developed under international law, namely that such limitation must be provided by law, pursue a legitimate aim and be necessary and proportionate in pursuance of that aim.

The bedrock of human rights under international law is established by the Universal Declaration of Human Rights (UDHR). Out of this non-binding foundation, two key binding human rights instruments emerged: the International Covenant on Civil and Political Rights (ICCPR), which enshrines civil and political rights;[8] and the International Covenant on Economic, Social and Cultural Rights (ICESCR), which enshrines economic, social and cultural rights that states should realise over time.[9] Since then, there has been a range of other treaties developed that are more specifically subject-matter focused, such as treaties focusing on the elimination of racial discrimination, the rights of women and children, or persons with disabilities.

There are also regional human rights instruments that enshrine human rights, namely the African Charter on Human and Peoples' Rights (African Charter); the European Convention on Human Rights; the American Convention on Human Rights and the

8 This includes the rights to life, liberty, freedom of expression, access to information, privacy and assembly.

9 This includes the rights to health, education, work and to participate in cultural life.

Additional Protocol to the American Convention; and the Arab Charter of Human Rights. There are also regional bodies, such as the African Commission on Human and Peoples' Rights (African Commission), that monitor the compliance with these treaties. The mandate of these bodies includes deciding on complaints regarding human rights violations against member states and human rights monitoring.

To give effect to the rights enshrined under international treaties, states should adopt legislative and other measures in their domestic jurisdictions. The measures could be the adoption of constitutions, laws, or the establishment of institutions in line with international law and standards. These are the expression of the state's compliance with its international obligations. It is not permissible for states to rely on their domestic laws to justify non-compliance with their international obligations.

The nature of human rights

Human rights are fundamental and inherent to all persons. They are enshrined in both national and international laws, and all persons are entitled to enjoy such rights without distinction, by virtue of their humanity. When fully realised, human rights reflect the minimum standards to enable persons to live with dignity, freedom, equality, justice and peace.

As mentioned, human rights are described as being inherent, inalienable, interdependent, indivisible and non-discriminatory. This means that they are the birthright of all persons, and cannot be unlawfully withdrawn without a justifiable basis for doing so. Moreover, each right is closely related to, and often dependent upon, the realisation of other rights. There is no hierarchy of rights, with all rights being of equal importance, and they should be realised without prejudice.

Universal	Human rights belong to all people
Inalienable	Human rights cannot be taken away
Interconnected	Human rights are dependent on one another
Indivisible	Human rights cannot be treated in isolation
Non-discriminatory	Human rights should be respected without prejudice

Source: The Advocates for Human Rights: Human Rights Basics[10]

Responsibilities of the state

Under international law, states are typically recognised as the primary duty bearers for the realisation of human rights. In this regard, states have the duty to respect, protect and fulfil human rights. This entails both positive and negative duties on states. In the first place, states are required to avoid violating the rights of individuals and communities within their territories, as well as to protect those individuals and communities against violations by others. Importantly, the duty to fulfil requires states to take positive steps to enable the full enjoyment of human rights. Additionally, corporations, organisations and individuals are required, at a minimum, to respect the rights of others.

10 http://www.theadvocatesforhumanrights.org/human_rights_basics

Respect	Protect	Fulfill
Governments must not deprive people of a right or interfere with persons exercising their rights.	Governments must prevent private actors from violating the human rights of others.	Governments must take positive action to facilitate the enjoyment of basic human rights.
For example, governments can: • Create constitutional guarantees of human rights. • Provide ways for people who have suffered human rights violations by the government to seek legal remedies from domestic and internactional courts. • Sign international human rights treaties.	For example, governments can: • Prosecute perpetrators of human rights abuses, such as crimes of domestic violence. • Educate people about human rights and the importance of respecting the human rights of others. • Cooperate with the international community in preventing and prosecuting crimes against humanity and other violations.	For example, governments can: • Provide free, high-quality public education. • Create a public defender system so that everyone has access to a lawyer. • Ensure everyone has access to food by funding public assistance programs. • Fund a public education campaign on the right to vote.

Source: The Advocates for Human Rights: Human Rights Basics[11]

Human rights-based approach

A human rights-based approach (HRBA) is grounded on the principles drawn from international and regional treaties, and places human rights as the yardstick in all policy and planning. It is defined by the principles that include participation, accountability and transparency, non-discrimination and equality, empowerment of rights holders and legality. By relying on a HRBA, policy makers perform better at meeting their human rights obligations, and have better outcomes that benefit rights holders.

11 Ibid.

This is done through integrating international human rights system norms, principles and standards, and goals. Some of the elements that define a HRBA include the adoption of programming defined by human rights standards; clearly defining the rights of rights holders and the corresponding obligations of duty bearers; examining reasons for failure to realise some human rights objectives; and assessing the capacity of rights holders to claim their rights from duty bearers and develop strategies to enhance those capacities. A HRBA also entails using human rights standards and principles in monitoring and evaluation of outcomes and processes.

Some of the benefits include empowerment of rights holders; prioritising marginalised groups; enhancing participation and access to information; and promoting accountability. It also identifies duty bearers and rights holders; promotes human rights approaches in problem solving; and promotes optimal resource utilisation.

The principles of a HRBA are as follows:

- *Interdependence and interrelatedness:* Human rights are by their nature symbiotic and interrelated. Each right has a contributory effect on other rights, which could be positive or negative. For example, the realisation of the right to privacy can contribute to the enjoyment of freedoms of association and assembly. Similarly, the fulfilment of the right of freedom of expression could be dependent on rights such as the right of access to information and right to privacy.
- *Equality and non-discrimination:* This principle is embedded in international norms and standards that all human beings are equal and dignity is inherent in every person. Discrimination should be prohibited, whether on the grounds of politics,

language, sexual orientation, religion, colour, ethnicity, gender, race, age, opinion, national, social or geographical origin, disability, property, birth or other status, as acknowledged by human rights standards.

- *Participation and inclusion:* The principle of participation underpins the essence of a HRBA. It is based on the notion that each person has the right to participate in the decision-making processes that affect their wellbeing and lives. The participation is also centred on the principle of non-discrimination and equality. For participation to be successful and effective, rights holders require adequate and credible information.

- *Accountability and rule of law:* The state has the obligation to protect human rights as mandated under international law and standards that states sign up to. They are answerable and must comply with human rights obligations. Duty bearers are also answerable in the observance of human rights. Failure to comply should attract sanctions and remedies for rights holders. The public and private sectors, such as the media, community and civil society, are instrumental in holding the government accountable for not upholding their obligations.

The right to privacy has acquired new significance in the digital age. Advancements in technology modify and accelerate the processing, analysis, collection and storage of data, including personal information.

Part 2.
The right to privacy and personal data protection

Privacy is a fundamental human right that is guaranteed in international and regional human rights instruments. It also finds expression in more than 130 national constitutions, including those in Africa. It is enshrined in Article 12 of the UDHR, Article 17 of the ICCPR, Article 16 of the Convention of the Rights of the Child (CRC) and Article 10 of the African Charter on the Rights and Welfare of the Child. The African Charter does not have a provision on the right to privacy,[12] but this right has been acknowledged under the Declaration of Principles on Freedom of Expression and Access to Information in Africa (the declaration).[13]

12 https://privacyinternational.org/news-analysis/2227/privacy-international-62nd-session-african-commission-human-and-peoples-rights

13 African Commission on Human and People's Rights. (2019). Declaration of Principles on Freedom of Expression and Access to Information in Africa. https://www.chr.up.ac.za/images/researchunits/dgdr/documents/ati/Declaration_of_Principles_on_Freedom_of_Expression_ENG_2019.pdf

The acknowledgment of the right to privacy in the declaration stems from the pronouncements of the African Commission that recognise the importance of privacy online, such as the 2016 Resolution on the Right to Freedom of Information and Expression on the Internet.[14] In particular, this resolution emphasised the importance of privacy in the realisation of the right to freedom of expression and to hold opinions without interference, as well as the right to freedom of peaceful assembly and association. In addition, the African Declaration on Internet Rights and Freedoms contains data protection as one of the rights that states should endeavour to implement in the digital age.[15]

The right to privacy is essential for the protection of dignity and autonomy of the person, and forms the basis for the enjoyment of other human rights such as freedom of expression, the right to seek, receive and impart information, and freedoms of association and assembly. In the access to information regime, privacy is recognised as a justifiable limitation or "exemption", as it is a legitimate justification for non-disclosure of information. Privacy is not an absolute right and can be limited under certain circumstances.

An effective data protection framework is crucial to the realisation of the right to privacy. The importance of privacy and data protection is summarised as follows:

To ensure accountability for data misuse	Privacy, being recognised as a fundamental human right, forms the basis for providing remedies in cases of violations and establishing privacy laws that guarantee the protection of the right to privacy.

14 For adopted resolutions of the African Commission on Human and Peoples' Rights see https://www.achpr.org/adoptedresolution

15 https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf

To help build trust	Trust is a significant element of any relationship. In the context of personal information, trust and confidence are established and strengthened when information is safe. "Breaches of confidentiality are breaches of that trust."[16]
To prevent arbitrary surveillance	In terms of international human rights law, the duty to protect human rights lies with the state. It is also the duty of the state to ensure that there is adequate national security. There has to be a balance between the national security obligation and the obligation to protect privacy.
To ensure control over personal data	Individuals should have control over their data: who can use, access, and process data. The absence of such authority over one's information increases vulnerability to the misuse of data.
To establish and maintain social boundaries (physical and informational)	Healthy relationships are also dependent on the ability to create and maintain boundaries and "having control over who knows what gives us peace of mind."[17] For example, social media platforms have privacy and security features for such purposes. "We need places of solitude to retreat to, places where we are free of the gaze of others in order to relax and feel at ease."[18]
To protect freedom of speech and thought	When privacy rights are established, not everything that people do can be monitored. Certain thoughts and expressions, especially those with negative labels, can be tracked. Privacy rights provide protection against arbitrary monitoring. Privacy is therefore a crucial element to the enjoyment of freedom of expression and opinion. The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has explained that "the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas."[19]

16 Solove, D. (2014, 20 January). 10 Reasons Why Privacy Matters. *Teach Privacy*. https://teachprivacy.com/10-reasons-privacy-matters/

17 Soken-Huberty, E. (n/d).10 Reasons Why Privacy Rights are Important. *Human Rights Careers*. https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/

18 Solove, D. (2014, 20 January). Op. cit.

19 La Rue, F. (2013, 17 April). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf Frank La Rue is a former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

To provide the freedom to engage freely in politics	The right to privacy is an enabler in the exercise of political rights. For example, this includes the ability to cast a vote in confidentiality. It also enables people to keep their political opinions private.
To protect reputations, to enable individuals the ability to evolve and to ensure respect for individuals	In terms of the right to privacy, individuals are empowered and protected through the ability to have certain kinds of information about or by them removed. For example, in the EU context, there is the right to be forgotten which enables people to remove information from internet searches in applicable circumstances. "We must have some ability to protect our reputations from being unfairly harmed. Protecting reputation depends on protecting against not only falsehoods but also certain truths."[20] People are constantly changing and growing. The right to privacy should enable one to change and evolve without being reminded about their past mistakes. "Certainly, not all misdeeds should be shielded, but some should be, because we want to encourage and facilitate growth and improvement."[21] Privacy is about respecting a person's desire to keep aspects of their life private. Such wishes should be respected, unless there are compelling reasons for the disclosure, which should generally be in the public interest.
To protect financial assets and guard against cybercrimes	Companies store personal data, and the failure to protect it can have disastrous consequences such as identity theft or the disclosure of credit card numbers. Institutions, such as financial institutions, should establish mechanisms to protect the financial and personal information that they have been entrusted with.
To protect information from manipulation	Technology companies like Facebook, Amazon, Google and others collect and store personal information and are not entitled to use the data as they please. Consent is a fundamental element of the right to privacy and when in the wrong hands, personal information can be wielded as a powerful tool. For example, in the Cambridge Analytica scandal,[22] personal data from Facebook user accounts was used without user consent to influence voters by means of political advertising. This has revealed how the misuse of personal information – including personal preferences and ideological inclinations – can be manipulated to affect the way in which people make key decisions.

20 Solove, D. (2014, 20 January). Op. cit.

21 Ibid.

22 Lapowsky, I. (2019,17 March). How Cambridge Analytica Sparked the Great Privacy Awakening. *Wired*. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

To nurture the ability to control life	Personal data is essential to one's life in general, and is a determinant for many things that affect one's life. However, having the autonomy and control over such lives also entails having a say in how personal data is used, or the ability to object and have legitimate grievances heard when data uses might cause harm. Having the ability to remove, correct and amend is the hallmark of that freedom. Privacy also enables one the freedom to make choices without having to explain or justify such choices.
Limit on power	Knowledge about a person creates a sense of power over them, and respect for the right to privacy creates a limit on power held by government and other institutions over people's information.
For human dignity, freedom of association and other human rights	Privacy is important for the realisation of other human rights such as human dignity and the freedom of association. For example, the African Union (AU) Convention on Cyber Security and Personal Data Protection implores the adoption of data protection laws with requirements to take into account respect for the rights of citizens, guaranteed under the fundamental texts of domestic law, and protected by human rights treaties and conventions, particularly the African Charter. In essence, a determination on whether the right to data privacy takes precedence over other rights is dependent on the facts and circumstances in each particular case, and needs to comply with the three-part test for a justifiable limitation as established under international law.
To protect personal financial information	Individuals are entitled to know if their financial and personal information has been shared to a third party. There is need to control commercial prospecting in the banking sector and regulate transfers of bank data abroad. To avoid any misuse of the files, access to banking details and confidential information should be limited to authorised persons.

To protect sensitive information	Sensitive information requires additional safeguards to provide more protection. Health information falls under such information. There is need to preserve the privacy of patients in order to protect them from any harm related to the disclosure and exploitation of health data. It is also crucial to prevent harms such as the sale of health-related information to third parties (e.g. insurance companies, financial institutions or laboratories) without prior consent. It is also important to protect health data in order to prohibit any use of patient data for commercial purposes; to avoid the risk of the computer hacking of health databases and to protect hospitals, clinics or laboratories against possible complaints/lawsuits from patients whose medical reports were published on social networks (i.e. COVID-19 cases).

Sources: https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important and https://teachprivacy.com/10-reasons-privacy-matters

African constitutions and information privacy

In Africa, some of the constitutions refer to personal data or information privacy, such as those from Algeria, Cape Verde and Mozambique. This is in addition to the provision of the right to privacy. The Constitution of Algeria simply provides that the protection of personal data is a fundamental right without much elaboration, while those of Cape Verde and Mozambique have detailed provisions on the same.

For example, the Constitution of Cape Verde provides for the protection of the right of citizens to access, rectify and update, as well as to be informed of the purpose of, computerised data that affects them; the transfer and storage of computerised personal information by public and private authorities; the prohibition of the allocation of a single national identification number to citizens; and the prohibition of the processing of sensitive data except with the consent of the data subject.[23] It provides that the

23 http://constitutions.unwomen.org/en/countries/africa/~/media/983cd3b8346a4d53b9e116676bff7363.ashx

processing of sensitive data should be authorised by law, and should only be undertaken in a non-discriminatory manner or for non-identifiable statistical purposes.

In Mozambique, the constitution provides for the right of individuals to access and rectify their personal information; the adoption of a law to regulate the processing of personal information and the creation, use and conditions of access to such personal information by public and private entities; the prohibition of the processing of sensitive personal information without any express exception; and the prohibition of access to and transfer of personal information of third parties, except as authorised by law or a court order.[24]

Communication privacy in African constitutions

Most constitutional provisions on the right to communication privacy in Africa simply protect "privacy of correspondence" or communication (such as Eritrea, Equatorial Guinea, Kenya, Morocco, Guinea, South Africa, South Sudan, Sudan, Swaziland, Tanzania, Uganda, Tunisia and Zimbabwe) or the "secrecy of correspondence" (such as Benin, Djibouti, Guinea, Mali and Togo) without any further elaboration. Other provisions, however, explicitly identify the various forms of communication mediums that are prohibited from interference by the state, such as "all forms of telecommunications" (such as in Malawi and the Democratic Republic of Congo); "postal, electronic, telegraphic communication" (such as in the Central African Republic and Gabon); "telephone conversations and telegraphic and electronic communications" (such as in Sierra Leone); "either written, oral, or through any medium of communication" (such as in Seychelles); or "postal letters and communications

24 https://www.constituteproject.org/constitution/Mozambique_2007

made by means of telephones, telecommunications and electronic devices" (such as in Ethiopia).

Some constitutional provisions on privacy go further to include provisions permitting interference with the right to privacy subject to such interference being authorised by law or a court order. These countries include Chad, Central African Republic, Rwanda, Niger and Burkina Faso. Others that include a court order are Cameroon, Liberia and Morocco. Those that include both requirements of law and a court order are Madagascar and São Tomé and Principe. In terms of constitutional provisions permitting interference with the right to privacy only in accordance with law, a few instances exist in which the law is required to be such that is "necessary in a democratic society" (such as in Ghana, the Gambia, Namibia, Nigeria and Guinea Bissau). More generally, however, the interference by law is permitted for specific reasons such as: "the interest of defence, public safety, public order, public morality, public health, the administration of government, town and country planning, nature conservation and the economic development and well-being of the country" (such as in Angola, Central African Republic and Senegal); the "prevention of crime" (such as in Ethiopia and Namibia); or for the "protection of the public order against imminent threats, in particular to fight the risks of epidemic, fires or to protect people in danger" (such as in Mauritius, Seychelles, Sierra Leone and Swaziland).

Another exception allowing limitations to the right to privacy by law is "for the purpose of protecting the rights and freedoms of other persons" (such as in Lesotho and Mauritius). This clearly indicates the realisation that the right to privacy often requires the balancing of this right with other competing rights of individuals, such as the right to freedom of expression, access to information and freedom of assembly.

Scope of data protection laws and personal information

The original focus of data privacy laws was to address e-commerce and consumer protection issues and, increasingly today, the impact of ICT on innovation. Data protection is also referred to as information privacy or data privacy in legal frameworks that protect individuals against the negative impact of the processing of their personal information. It combines the protection of personal data and the recognition of the right to privacy.

Instruments such as the EU General Data Protection Regulation (GDPR) and the AU Convention on Cybersecurity and Personal Data Protection ground the protection of personal data on the protection of human rights in general, and data privacy in particular. Technology advancements increase the amount of information that is collected, shared, processed and stored. This also increases the significance of data protection.

Data protection frameworks typically focus on the processing of personal information or data. Specifically, this refers to information that identifies an individual, who is referred to as the data subject. For example, this has been defined as follows:

- In terms of the GDPR, personal data is any information relating to an identified or identifiable natural person. This includes a person's name, date of birth, address, phone number, email address, membership number, IP address and photographs. Sensitive information is also included such as one's religion, ethnicity, sexual orientation, trade union membership, medical information, criminal data and children's data.
- In terms of Article 1 of the AU Convention, personal data is "any information relating to an identified or identifiable

natural person by which this person can be identified directly or indirectly in particular by reference to by an identification number or to one or more factors specific to his/her physical, psychological, mental, economic, cultural or social identity".

- In terms of the ECOWAS Supplementary Act, it is defined as "any information relating to an identified individual or who may be directly or indirectly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, economic, or social identity."

- In South Africa, for example, in terms of the Protection of Personal Information Act 4 of 2013 (POPIA), the definition of personal information sets out a non-exhaustive list of the types of information that this might include, such as information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; the biometric information of the person; the personal opinions, views or preferences of the person; and the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.[25]

Most data protection frameworks also define certain types of personal information as "special" or "sensitive", which are afforded heightened protections. For example, the AU Convention defines the term "sensitive personal data" as "all personal data relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions."

25 https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

European frameworks relating to data protection

Europe has typically been the world leader in the field of data protection and has been highly influential in the development of regional and domestic frameworks on data protection in other parts of the world, including Africa. For example, the data protection laws in many African states are based on the 1995 EU Directive on the Processing of Personal Data,[26] which is the predecessor to the GDPR. It is therefore relevant to the context and understanding of the present discussion to explore the European frameworks relating to data protection.

Convention for the Protection of Individuals with Regard to the Processing of Personal Data

The Convention for the Protection of Individuals with Regard to the Processing of Personal Data – commonly referred to as Convention 108 – is an instrument of the Council of Europe (COE).[27] Convention 108 opened for signature on 28 January 1981 and was the first legally binding instrument in the data protection field. The purpose of Convention 108 is to "protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy." Furthermore, it provides for the free flow of personal data between states party thereto.

26 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

27 Council of Europe. (2018). *Convention 108+ Convention for the protection of individuals with regard to the processing of personal data*. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1h

In May 2018, the COE published Convention 108+ in an effort to update and modernise the framework. It was noted at the time that:

> [W]ith new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that the Convention should be modernised in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism.

A key feature of Convention 108 is that, in addition to the members of the COE, it also provides that non-European states may accede to it. For example, in the African context, Cape Verde, Mauritius and Senegal have acceded to it. This is of relevance for several reasons: it is a recognition of the adequacy of their data protection frameworks; it adds an additional bulwark of protection of persons within those states; and it can serve to facilitate cross-border data transfers between those African states and Europe. Convention 108 remains open for accession by other African states that may meet the necessary requirements.

General Data Protection Regulation (GDPR)

The GPDR is the EU data protection legislation.[28] It came into effect on 25 May 2018 and applies to every EU member state and sets out the framework for the protection of privacy rights and the framework for the use of personal data. The application of the GDPR is intended to harmonise the collection, storage, use and sharing and processing of personal information

28 https://gdpr-info.eu

across Europe.[29] Harmonisation of data protection frameworks reinforces the protection of the right to privacy of individuals even in contexts where information crosses borders. The GDPR also clarifies rights, responsibilities, principles and sanctions within the ambit of data protection. It places an obligation on data controllers and data processors to adhere to the GDPR requirements whenever processing personal information.[30]

The rights of data subjects including the right of access to personal data, the right to data portability, the right to the restriction of processing and the right to rectification, are provided for under the GDPR.[31] Under this regulation, processing of personal information should be based on the following principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.[32] The regulation also defines the conditions for transfers of personal data to third countries or international organisations, which is only permissible if the conditions in the GDPR are complied with, including in respect of whether there is adequate protection.[33]

Independent supervisory authorities are provided for under Chapter 6.[34] This provision encapsulates the powers, competence, tasks, rules of establishment, membership and independence of the authority. Remedies, liability and penalties are captured in Articles 77 to 84,[35] while implementation procedures are written up in Chapter 10 (Articles 92 to 93). The

29 Ibid.

30 Ibid., Chapter 4, Art 24-43.

31 Ibid., Art 12-23.

32 Ibid., Art 5. See also United Nations guidelines concerning computerised personal data files adopted by the General Assembly on 14 December 1990; OECD guidelines. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

33 Ibid., Art 44-50.

34 Ibid., Art 51-59.

35 Ibid., Art 77-84.

failure to comply with the GDPR carries significant penalties, including administrative fines of up to EUR 20,000 (USD 24,285) or 4% of the total worldwide annual turnover of the preceding year, whichever is higher.[36]

A noteworthy feature of the GDPR is that it seeks to apply extraterritorially to countries outside Europe, in circumstances where non-EU entities collect and process personal data of EU data subjects. In terms of Article 3(2), such extraterritorial application arises where the processing activities are related to the offering of goods or services to data subjects in the EU, or the monitoring of their behaviour as far as such behaviour takes place within the EU. Recital 23 to the GDPR explains that the purpose of this provision is to ensure that natural persons are not deprived of the protection to which they are entitled under the GDPR.

African frameworks on data protection

Within both the global and regional international human rights frameworks, concerted efforts are now being made to strengthen the protection of personal data through the elaboration of normative standards on data privacy. In Africa, although the African Charter does not contain the right to privacy, there is an existing framework for privacy and data protection at regional and sub-regional level, the most recent being through Principles 40 to 43 of the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa.

The need to harmonise laws and policies has also led to the adoption of the data protection frameworks in the Economic Community of West African States (ECOWAS), the Southern African Development Community (SADC) and the East African Community

36 Ibid., Art 83.

(EAC). A continental treaty (the AU Convention) is also in place, although it has not yet received the required number of ratifications for it to enter into force. While there is growing momentum around privacy and data protection through the adoption of data protection legislation, more countries are also gravitating towards national security-oriented legislation and focusing more on cybercrime and cybersecurity legislation,[37] as well as resorting to different forms of communications surveillance.[38]

In Africa, there are several unique contextual factors that have influenced the development and implementation of the applicable data protection frameworks. As identified in the Personal Data Protection Guidelines for Africa – a joint initiative of the Internet Society and the Commission of the African Union, published in May 2018 – the following are seen to be characteristics of the African context:[39]

- Significant cultural and legal diversity across the continent, with different privacy expectations.
- Variations in access to technology and online services among member states.
- Sensitivities regarding ethnicity and profiling of citizens without consent, in the context of a nation state.
- Different levels of capability in areas such as technology and technology-related law and governance.
- Risks arising from high dependency on non-African manufacturers and service providers, including AU member states' limited ability to influence the behaviour of external

37 Sutherland, E. (2017). Governance of cybersecurity - The case of South Africa. *African Journal of Information and Communication (AJIC)*, 20, 83-112. http://wiredspace.wits.ac.za/handle/10539/23574

38 Makulilo, A. B. (2016). A Person Is a Person through Other Persons: A Critical Analysis of Privacy and Culture in Africa. *Beijing Law Review, 7,* 192-204. https://www.scirp.org/journal/paperinformation.aspx?paperid=69939

39 https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

service providers and the potentially-increased risks of data misuse where content and services are solely provided by foreign companies.

These factors can increase the difficulty of formulating and enforcing consistent policy among – and sometimes even within – African states.

National laws on data protection

Cape Verde was the first African state to adopt data protection legislation in 2001. Since then and by the end of 2019, 18 other countries have adopted data protection laws. These are: Angola,[40] Benin,[41] Botswana,[42] Burkina Faso,[43] Cote d'Ivoire,[44] Gabon,[45] Ghana,[46] Egypt,[47] Kenya,[48] Lesotho, Madagascar,[49] Mali,[50] Mauritius,[51] Morocco,[52] Senegal,[53] Seychelles,[54] South Africa,[55] Tunisia[56] and Uganda.[57] A number of other African countries have also drafted bills on data protection which are at various stages

40 https://www.lexology.com/library/detail.aspx?g=429baa59-8d93-4048-b3e7-342a52e4eb31

41 https://apdp.bj/wp-content/uploads/2016/08/Loi-No-2009-du-22Mai-2009-Version-Anglaise.pdf

42 https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf

43 https://dataprotection.africa/wp-content/uploads/2019/10/Burkina-Faso-Factsheet.pdf

44 https://dataprotection.africa/wp-content/uploads/2019/10/Ivory-Coast-Factsheet-1.pdf

45 https://dataprotection.africa/gabon/

46 https://media.mofo.com/files/PrivacyLibrary/3981/GHANAbill.pdf

47 Mohammed, B. (2019, 22 June). Egypt's legislators pass country's first data protection regulation law. *Daily News Egypt*.https://www.zawya.com/mena/en/legal/story/Egypts_legislators_pass_countrys_first_data_protection_regulation_law-SNG_147402777/

48 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

49 https://dataprotection.africa/madagascar/

50 https://dataprotection.africa/mali/

51 https://dataprotection.africa/mauritius/

52 Chenaoui, H. (2018, 11 September). Moroccan data protection law: Moving to align with EU data protection? *iapp*. https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/

53 http://www.wipo.int/edocs/lexdocs/laws/fr/sn/sn009fr.pdf

54 https://seylii.org/sc/legislation/act/2002/9

55 https://popia.co.za/

56 http://desiderando.com/Docs/UNPAN042957.pdf

57 https://ulii.org/ug/legislation/act/2019/1

of the legislative process. These are Burundi, Cameroon, Central African Republic, Chad, Equatorial Guinea, Ethiopia, Eritrea, Guinea, Guinea Bissau, Kenya, Liberia, Malawi, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sierra Leone, Swaziland, Tanzania, Togo, Zambia and Zimbabwe.

AU Convention on Cyber Security and Personal Data Protection

The AU adopted the Convention on Cyber Security and Personal Data Protection (also known as the Malabo Convention) in 2014.[58] As of September 2020, the convention had been ratified by only eight states.[59] It requires 15 ratifications to enter into force. The AU Convention should be read together with the Personal Data Protection Guidelines for Africa, which are intended to provide guidance on the implementation of the convention.[60]

The convention seeks to introduce a normative standard for cybersecurity, e-commerce, cybercrime and personal data protection and also advances the need for harmonised cyber legislation on the continent. The adoption of the AU Convention has been spurred on by considerations of the "massive data collection" in Africa, the recognition that privacy has become a widely recognised fundamental human right in the digital age, and the importance of the role of the AU in data protection.[61] Unlike the GDPR, the AU Convention will only have legal force in a particular jurisdiction when it is transposed into the legislative framework.

58 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

59 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION.pdf

60 https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/

61 Abdulrauf, L.A., & Fombad, C. M. (2016). The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa. *Journal of Media Law 8* (1), 67-97.

Article 25(3) places an obligation on states to:

> [E]nsure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

In terms of Article 8, states are obliged to establish legal frameworks to strengthen the protection of rights related to physical data and sanction violations of the right to privacy and to ensure that data processing respects the rights of natural persons, while protecting the "prerogatives of States, rights of local communities and purposes for which businesses were established." Furthermore, under Articles 11 and 12, there is a requirement for the establishment of a national data protection authority (DPA) in each jurisdiction.

The AU Convention calls on states to establish legal frameworks for the protection of personal data and privacy. The scope of data that falls under the convention includes:

- Any collection, processing, transmission, storage or use of personal data by a natural person, the state, local communities, and public or private corporate bodies.
- Any automated or non-automated processing of data contained in or meant to be part of a file, with the exception of the processing defined in Article 9.2 of this convention.
- Any processing of data undertaken in the territory of a state party of the African Union.
- Any processing of data relating to public security, defence, research, criminal prosecution, or state security, subject to the exceptions defined by specific provisions of other extant laws.

Under Articles 13 to 16, it provides for the principles and rights of data subjects. Specifically, Article 13 sets out the following principles: the principle of consent and legitimacy of personal data processing; the principle of lawfulness and fairness of personal data processing; the principle of purpose, relevance and storage of processed personal data; the principle of accuracy of personal data; the principle of transparency of personal data processing; and the principle of confidentiality and security of personal data processing. Furthermore, the rights of data subjects include the right to information; the right of access; the right to object; and the right of rectification and erasure. The obligations of data controllers, which include storage, sustainability, confidentiality and storage, are provided for under Articles 20 to 23 of the AU Convention.

However, the human rights concerns of the convention are well documented. These include the lack of clear definitions, the bundling of data protection and cybersecurity, judicial overreach and communications surveillance concerns. The convention has been criticised for its emphasis on the African Charter, yet the charter does not have a provision for privacy.[62] The other deficiency with the convention is that it fails to provide a minimum threshold for compliance and robust judicial oversight.[63]

SADC Model Law on Data Protection

It was adopted in 2013 under the Harmonisation of the ICT Policies in Sub-Saharan Africa project (HIPSSA) project. The aim of the Model Law is to give effect to the right to privacy through protection of personal information based on the accountability

62 Gwagwa, A. (2014). The African Union Convention on Cybersecurity and Personal Data Protection. *Zimbabwe Human Rights International Office Bulletin.* https://www.academia.edu/11328759/The_African_Union_Convention_on_Cybersecurity_and_Personal_Data_Protection

63 Ibid.

and transparency. It is also intended to harmonise data protection legislation in the sub-region. Essentially, it provides guidance on data protection, including the collection, storage, processing and sharing of personal information, the establishment of national data protection authorities, and limitations on the processing of personal information.

The Model Law provides guidance on the establishment of an independent, resourced DPA to facilitate compliance with the law and protection of privacy in general. In terms of the Model Law, the DPA should have regulatory and investigative powers to investigate data breaches and administrative justice for data subjects. On data transfer, the Model Law states that personal data will be freely transferred to jurisdictions that offer adequate data protection. The Model Law does not include privacy or data protection by design or default to ensure prioritisation of data protection during collection, processing and storage and sharing of personal data.[64]

Articles 22 and 25 of the Model Law deal with the security of data. To ensure the security of personal data, data controllers have the responsibility to:

> [T]ake the appropriate technical and organisational measures that are necessary to protect the personal data from negligent or unauthorised destruction, negligent loss, as well as from unauthorised alteration or access and any other unauthorised processing of the personal data.

In the case of a security breach, the data controller has an obligation to notify the DPA, without any undue delay, although there is no clarity on what entails a security breach or undue delay.

64 The principle of privacy or data protection "by default" refers to the concept that companies or organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, with a short storage period and limited accessibility) so that by default personal data is not made accessible to an indefinite number of persons.

Also, there is no indication in the Model Law that the data subject will be notified of security breaches that involve their personal data. These gaps could potentially compromise the principle of transparency and accountability that is aptly referenced in the preamble.

The ECOWAS Supplementary Act on Personal Data Protection

The ECOWAS Supplementary Act on Personal Data Protection[65] (the Supplementary Act) was adopted in February 2010 by the heads of state and governments of ECOWAS to supplement the revised ECOWAS treaty. It is binding on ECOWAS member states. The supplementary act establishes a legal framework for the collection, processing, transmission, storage and use of personal data. The provisions of the act mirror the 1995 EU Directive and some of the provisions are like the provisions of the AU Convention.

To give effect to the provisions of this treaty, the member states are expected to establish data protection frameworks through the adoption of legislative and other measures. Only Gabon (2011), Ghana (2012), Cote d'Ivoire (2013) and Mali (2013) passed their data protection laws after the adoption of the Supplementary Act. In total, 11 countries in ECOWAS have data protection laws.

The EAC frameworks for cyber law

The EAC[66] has adopted the frameworks for cyber law. It is intended to provide guidance on the adoption of cyber laws which contain aspects of expositions, legislative guidelines, reference materials and recommendations. The 2008 framework was

65 http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf

66 https://www.eac.int/

developed under the EAC Council of Ministers, and the 2010 framework was developed with the support of the United Nations Conference on Trade and Development (UNCTAD). In terms of the frameworks, they recommend that member states shall adopt international best practice on data protection,[67] with scant detail on the content of this. Specifically, the 2008 framework only identifies the following as a minimum obligation: to comply with certain "principles of good practice" in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security; and to supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended.

It doesn't provide specific guidance on the exact frameworks that member states are expected to adapt to their domestic contexts. It is not intended to be a model law, but instead intended to assist states by providing overarching principles to inform their own legal development. The 2008 framework concludes on the topic of data protection that:

> The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area.

67 Greenleaf, G., & Georges, M. (2014). African Regional Privacy Instruments: Their Effect on Harmonisation. *Privacy Laws and Business International Report, 132*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566724

Content and principles of data protection laws in Africa

As of 2020, approximately half of the African countries have data protection laws,[68] although this number is constantly changing as countries seek to adopt new data protection laws. While these laws typically capture the essential data protection principles and requirements, they differ in some aspects, such as restrictions on cross-border data transfers, data security, data breach notification and the appointment of a data protection officer (DPO). For instance:

- All the adopted laws require data subjects to be notified that their personal data is being processed.[69]
- With regards consent, approaches differ. While it is a general requirement in most laws, there are some variations. For example:
  - Benin: Consent is mandatory for the processing of sensitive personal data but not required for data that is not sensitive.
  - Mali: There are no explicit rules regarding consent, but a data subject has the right to object to the processing of their data.
- On the security of data, the requirement to take organisational and technical measures to protect data from loss, misuse, unauthorised access, disclosure, alteration and destruction is generally recognised, although with varying levels of detail.[70] For example, the Côte d'Ivoire law provides for detailed security requirements.

68 The countries are: Algeria, Niger, Mauritania, Togo, Equatorial Guinea, Chad, Comoros, Madagascar, South Africa, Cote d'Ivoire, Lesotho, Mali, Angola, Gabon, Ghana, Benin, Morocco, Senegal, Burkina Faso, Mauritius, Tunisia, Zimbabwe, Cape Verde, Seychelles, Botswana, Egypt, Kenya, Uganda. https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

69 Rich, C. (2017). A Look at New Trends in 2017: Privacy Laws in Africa and the Near East. *Bloomberg Law*, *16* (4).

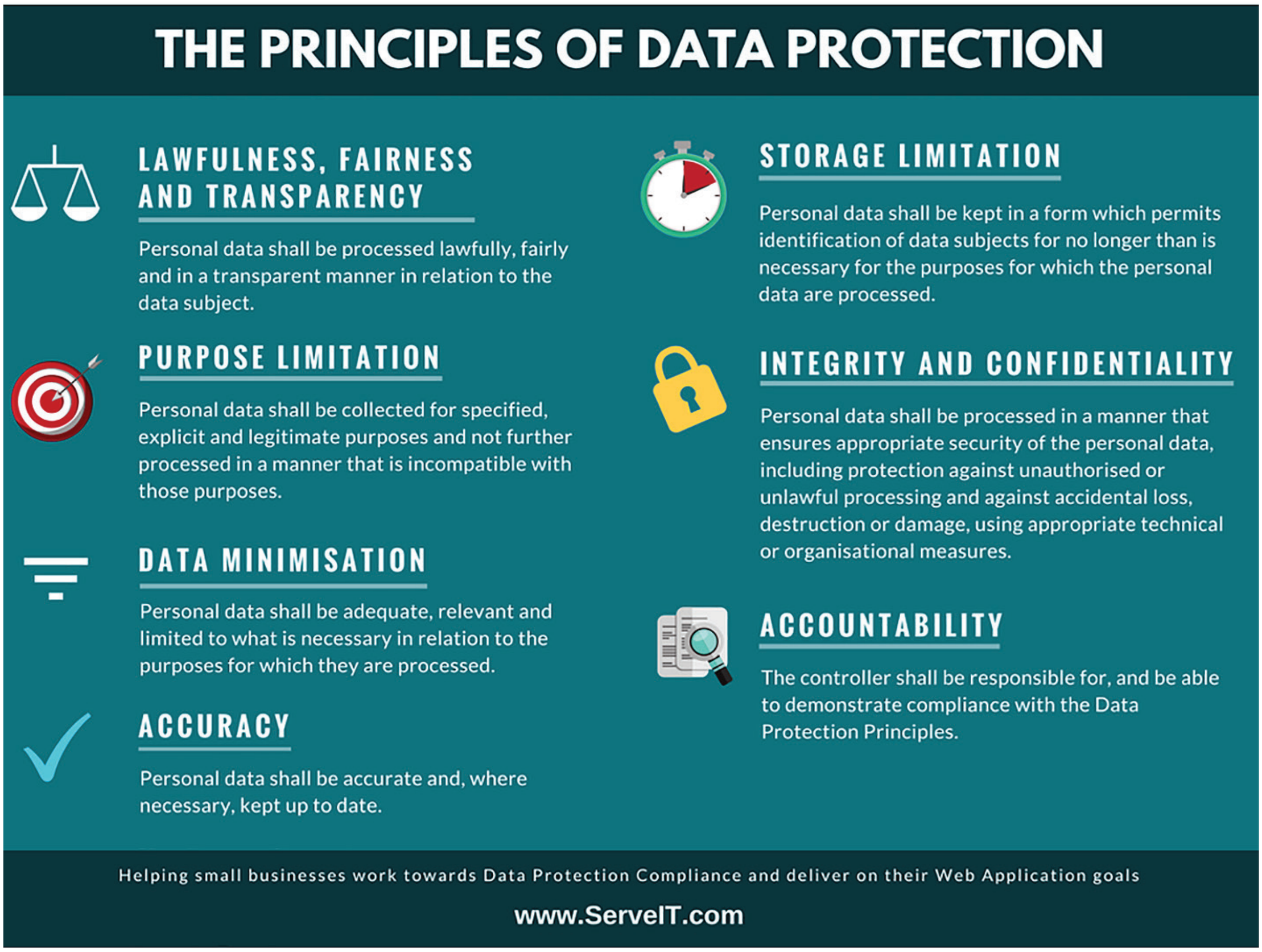
70 Ibid.

- On a data subject's right to access and correct their data, these core principles of data protection are also found in African frameworks; however, not all laws are specific regarding timeframes for responding to such requests.[71]
- All the laws have a requirement for data to be kept accurate, complete and up to date. This is referred to as data integrity. Data should be processed only for the intended purpose.
- Data retention is also a common feature in African data protection laws, in which organisations or institutions are required to retain personal data only for the period of time required to achieve the purpose of the processing.

Principles of data protection

In the AU Convention, Article 13 contains six principles which are also found in other international, regional and national data protection frameworks. The only omission is the principle of accountability. These principles exist in various combinations but are generally present in all frameworks on data protection. In a few instances, these principles are not in a section or part of these laws, but have been combined with other provisions, such as the obligations of data processors or controllers, as is the case in the law of Gabon. It should be noted that the data minimisation principle in the EU Directive of 1995, as replicated in the GDPR, is reflected as the "purpose, relevance and storage" principle of the AU Convention.

71 Ibid.



Source: Principles of Data Protection[72]

Bearing in mind that there may be some variations across different jurisdictions, the principles of data protection may be summarised as follows:

Lawfulness, fairness and transparency

All processing of personal data must be carried out lawfully, fairly and in a transparent manner, taking into consideration the legal basis, which includes compliance with all legal

72 Kean, J. (2018, 24 May). GDPR Advice for Retail and Hospitality Businesses. *TUCR.io*. https://tucr.io/gdpr-advice-for-retail-and-hospitality-businesses/#.X4CLii8RqYU
Data Protection Principles. *Privacy International* . https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf

obligations as stipulated in the data protection legislation. The data controller must disclose information regarding the personal data it holds to the data subject. Also, processing of data is deemed legitimate where the data subject gives consent. In terms of Article 13 of the AU Convention, the need for consent may be waived where the processing is required for compliance with a legal obligation of the data subject; performance of a task in the public interest or performance of the official duty of the data controller or a third party; performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract; and for the protection of the "vital interest" or fundamental rights of the data subject.

Purpose limitation

For all personal information that is collected and processed, the purpose should be explicitly stated, legitimate and limited to that purpose only. Any subsequent processing must be compatible with the purpose for which it was initially collected. The initial and subsequent data processing must be for a purpose which is specific, explicit and legitimate; adequate, relevant and not excessive; and kept only as long as is necessary, unless an exception applies, such as in relation to data processed lawfully for historical, statistical or research purposes.

Data minimisation

The processing, including the collection and storage, of data is limited to what is adequate, relevant and necessary. It has been noted that "the possibility to collect personal data about others should be minimised. Next within the remaining possibilities, collecting personal data should be minimised.

Finally, the time how long collected personal data is stored should be minimised."[73]

Accuracy

Personal data should be accurate, up to date, complete and relevant to the stated purposes. In this regard, the AU Convention provides that every reasonable step must be taken to ensure that data which is inaccurate or incomplete is erased or rectified, having regard to the purposes for which it was collected or further processed.

Storage

Personal data should only be retained for the period of time that is necessary for the stated purpose(s). It can be kept longer in form, but there should be adequate safeguards to ensure that there is no re-identification.

Integrity and confidentiality

Appropriate and adequate organisational and technical measures should be adopted to safeguard the security of personal data. The confidentiality of personal data must be protected, especially where it involves the transmission of data over a network. Where the processing is undertaken by a third party on behalf of the data controller, the latter must ensure that that processor is chosen based on a sufficient guarantee to ensure compliance with security requirements.

73 Pfitzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf

Accountability

Those entrusted with processing personal data should demonstrate compliance with data protection legislation and remain responsible and accountable for the protection of personal data throughout the lifecycle of processing activities while such data is in their possession or under their control.

Key elements of data protection laws[74]

Consent

Consent is one of the grounds of justification that may be relied on for the processing of personal information. In terms of the AU Convention, consent of a data subject "means any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing." Principle 42(2)(a) of the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa provides that the processing of personal information must by law be with the consent of the individual concerned.

Registration prior to processing of personal data

Except where exemptions apply, some laws require organisations to register with the data protection authority before processing personal data, especially sensitive information, genetic and biometric data, and national identity numbers. In Angola, the requirement for registration to process personal data also includes registration for processing sensitive information and personal credit video surveillance data, as well as transfers to

74 The following examples are extracted from Rich, C. (2017). Op. cit.

countries that do not provide an adequate level of protection. In Benin, the exemption for registration applies when an institution appoints a person to maintain a registry for the processing activities. Burkina Faso, Chad and Cape Verde have similar requirements. In the case of Ghana, failure to register is an offence and, in a situation which involves the transfer of data, “the recipients and countries to which personal information is intended to be transferred must be listed in the organisation’s database registration.” Tunisia has a similar requirement with regards to cross-border data transfers. South Africa has a specific provision that requires organisations to seek authorisation prior to processing children’s data before transferring it to a third party in a foreign country that does not offer an adequate level of protection for the processing of personal information.

Video surveillance

Limit privacy breach/data breaches.

Limit the systematisation of video surveillance of individuals.

Limit conflicts or issues related to the infringement of individual liberties.

Cloud storage

Ascertain the legal status of the service providers and the applicable law in the event of a legal challenge.

Ensure data security in the cloud.

Ascertain the data controller’s obligations.

Find the places where data is being stored abroad.

Limit the risks of sovereignty loss over processed data.

Data protection authority

The laws provide for the establishment of a national data protection authority, mostly to oversee the implementation of and compliance with the country's data protection framework. Such provisions exist in the data protection laws of Morocco (national supervisory authority), Senegal (commission for the protection of personal), Tunisia (the National Authority for Protection of Personal Data), South Africa (the information regulator), Madagascar (the Malagasy Commission on Informatics and Liberty), Ghana (the Data Protection Commission) and Equatorial Guinea (the Personal Data Protection Governing Authority). Many of these institutions are yet to be established except in countries like Tunisia, Ghana, Senegal and South Africa.

It also bears mention that the African network of personal data protection authorities (RAPDP) is a regional network that organises cooperation between members, supports the drafting of data protection legislation, and comments on data protection matters on the continent including promoting African data protection frameworks.[75]

Cross-border transfers

Provisions regarding the cross-border transfer of personal data form one of the characteristics of data protection laws. They are meant to ensure that data subjects receive an adequate level of protection, as they do in their countries, when their personal data

75 Rich, C. (2017). Op. cit.

is transferred to another jurisdiction. The general rules should be that when personal data is transferred to another country, the recipient country should have adequate protections, unless another justification for such a transfer exists. In countries such as Benin, authorisation from the DPA is required prior to such transfers. In Burkina Faso, specific authorisation is not required, but initial registration with the DPA should include information regarding data transfers. In the laws of Cote D'Ivoire such requirements apply to countries that are outside ECOWAS. In Madagascar, where a third party is involved, transfers may be permitted only when the organisation that originally processed the data approves. In Morocco, if the transfer is to a country that does not have adequate protection, such transfers can be authorised by the DPA. This applies in exceptional circumstances, for example, where the DPA can authorise contractual clauses or binding corporate rules. Morocco also recognises all EU approved jurisdictions. In Senegal, transfers that are considered not massive, or which have the consent of the data subject, or have other exceptions can be made to jurisdictions with less adequate protections, if this is done out of contractual necessity or vital interests, for example. It is also possible where the recipient organisation proves that there are sufficient guarantees in place. The following aspects are also important when considering transfer of genetic and biometric data:

- The principle of proportionality must be respected.
- The transfer/sharing of sensitive data should be supervised.
- Creation of centralised biometric databases should be supervised.
- Cloud storage of biometric data abroad should be avoided.
- Processing and access to biometric databases by foreign companies should be prohibited.

Data security

Data protection laws in Africa provide for data security to guarantee the safety of personal data. Some of the data that is processed is classified as sensitive information and specific organisational and technical measures have to be activated for safety purposes. Angolan law has specific requirements for sensitive information, including coding. In Gabon, the law on data security is more detailed, and has requirements such as the need for organisations to prevent unauthorised access to premises, protection of storage media, protection of data from unauthorised access and backing up the data where necessary. In Burkina Faso, coding is mandatory for data that is disclosed by health care professionals.

Data security breach notification

Notification in the event of a data security breach is one of the principles of data protection which also finds expression in certain data protection laws. In Ghana, data controllers and data processors are mandated to notify the DPA and the affected data subjects in the case of a data breach and also to take steps to rectify the damage and restore data security. In South Africa, the data breach notification requirement is mandatory. In Angola, the data protection law does not contain such a requirement, but the Law on Electronic Communications and Information Society Services has provisions requiring the DPA and the regulatory authority for electronic communications (INACOM) to be notified without undue delay. In countries such as Benin, Burkina Faso, Cape Verde, Mali and Madagascar, there is no obligation to give notice in the event of a data security breach.

The right to privacy is essential for the protection of dignity and autonomy of the person, and forms the basis for the enjoyment of other human rights such as freedom of expression, the right to seek, receive and impart information, and freedoms of association and assembly.

Part 3.
Duty bearers and rights holders[76]

Rights holders: The data subject

Data subject	Any person whose personal data is protected under a data privacy framework. This may be defined as follows: • AU Convention: "Any natural person that is the subject of personal data processing." • SADC Model Law: "Any individual who is the subject of the processing of personal data and who is identified or identifiable."
Rights of data subject	Different laws contain different rights for data subjects. These rights may include: • The right to be informed • The right of access • The right to rectification • The right to erasure • The right to restrict processing • The right to data portability • The right to object • Rights in relation to automated decision making and profiling.

76 See AU Convention, GDRP, SADC Model law on Data Protection, The ECOWAS Supplementary Act on Personal Data Protection.

Duty bearers

Data controller	Anyone (individual or entity) that is involved in the processing of personal data. A data controller is responsible for determining the purpose for the processing of personal data. This may be defined as follows: • AU Convention: "Any natural or legal person, public or private, any other organisation or association which alone or jointly with others, decided to collect and process personal data and determines the purposes." • ECOWAS Supplementary Act: "Any public or private individual or legal entity, body or association, who alone or jointly with others, decides to collect and process personal data and determines the purposes for which such data are processed." • SADC Model Law on Data Protection: "Any natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data. Where the purpose and means of processing are determined by or by virtue of an act, decree or ordinance, the controller is the natural person, legal person or public body has been designated as such by or by virtue of that act, decree or ordinance."
Data processors	Any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This may be defined as follows: • SADC Model Law on Data Protection: "A natural person, legal person, or public body which processes personal data for and on behalf of the controller and under the data controller's instruction, except for the persons who, under the direct authority of the controller, are authorised to process the data." • Data processing activities are increasingly being outsourced by states and private entities to third parties (data processors). Ensuring that data processors have defined responsibilities safeguards the protection of information from the negative impact of data processing.

Obligations of data controllers and processors	Data controllers and processors facilitate the exercise of the rights of data subjects, in accordance with the principles of data protection as prescribed in law. Data subjects also have a right to challenge or lodge a complaint regarding such processing to the national data protection authority, and are entitled to pursue legal remedies with the relevant judicial authorities. Data controllers have an obligation to implement data protection policies, to implement technical and organisational measures on data protection and to adhere to any relevant codes of conduct. Duties with regards to records and processing of data include to maintain a record of processing activities; determine the purpose of the processing; provide the name and contact details of the controller; provide a description of categories of data subjects and categories of personal data, international transfers of personal data and the documentation of the appropriate safeguards; and provide information regarding the envisaged limits of erasure of the different categories of data and the general description of the technical and organisational security measures implemented. It is also the duty of the data controller to notify the national data protection authority when necessary, for example in the case of a data breach. In that regard, a description of the data breach should be provided. Any failure to report within the time prescribed by the law should be explained. The data controller should communicate the occurrence of a data breach to data subjects using simple language. Data processors should only process personal information according to the instructions given by the data controller. In processing personal data, data processors must take appropriate security measures; observe confidentiality; and demonstrate compliance with the relevant laws.

National data protection authority

Data protection authorities have different names and approaches in different jurisdictions, but their function is similar. They oversee the application of data protection laws in their independent capacity. Others also have a role in access to information framework (such as the South African Information Regulator, for example).

South Africa	Information Regulator
Ghana	Data Protection Commission
Mauritius	Data Protection Office (Prime Minister's Office)
Morocco	Commission nationale de contrôle de la protection des données à caractère personnel

The role of the data protection authority includes:

- Responding to requests for opinions or providing clarification regarding personal data processing
- Informing data subjects of their rights
- Authorising processing of data files (sensitive data)
- Auditing processed personal data
- Imposing sanctions or warnings on data controllers
- Providing advice on data processing
- Informing a relevant judicial authority of data protection offences
- Authorising cross-border transfers
- Providing guidance on the regulatory frameworks
- Processing data protection queries.

In South Africa, the DPA has a dual mandate, both in promoting access to information and protecting the right to privacy. This dual existence is important in providing guidance on achieving the delicate balance between the two fundamental rights.

Data protection compliance checklist

These are some of the minimum requirements in protection of personal information. They are in the form of questions and are derived from privacy and data protection frameworks. The purpose of the checklist is to provide guidance in complying with some of the important aspects of a data protection framework. This is a general checklist and not directed to any specific sector.

Data protection standards

- Is there data protection legislation?
- Are there any sectoral laws on data protection?
- Is the law comprehensive?
- Is the data protection law being adequately implemented?
- Does the data protection law deal with marginalised and vulnerable groups (women, children, persons with disabilities and sexual minorities)?
- Does the legislation define its interaction with other laws permitting the state to process personal information?
- Does the law define and regulate the relationship between privacy and other rights such as freedom of expression and access to information?
- What additional safeguards are in place for the processing of sensitive data?
- Does the law include digital identifiers and location data as personal information?
- How does the law address the obligation to conduct data protection impact assessments in instances of high risk processing?

National data protection authority

- Does the law provide for the establishment of an independent national data protection authority with the powers to enforce the legislation?
- Has the independent DPA been established in terms of the law?
- Does the law guarantee the independence of the DPA?
- What is the role of the DPA?
- What powers does the DPA have?
- Can the DPA appoint its own staff?
- Can the DPA act independently in the implementation of the law and meting out sanctions in cases of data breaches?
- Does the national law require appointment of data protection officials?
- Is the contract of the DPA publicly available?
- Is the DPA adequately resourced?
- What efforts is the DPA making in raising awareness on privacy and data protection?
- Has the DPA developed sector specific guidelines for the use of personal information?

Personal data being processed[77]

- What are the categories of personal data being processed?
- What "sensitive personal data" is being collected?[78]
- What safeguards are in place to ensure enhanced protection of sensitive data?
- Is the processing voluntary or mandatory?

Purpose

- For what purpose is personal data being collected?
- Is the purpose explicit and legitimate?
- Has the original purpose of collection been maintained?[79]
- Does the law provide for the secondary use of personal data?
- What are the safeguards for the secondary use of personal data?
- Does the law provide for the proportionality principle? The processing of personal data must not be excessive vis-à-vis the purposes of its collection or any identified further processing.

77 In this case "processed" refers to "collected, stored, analysed, transferred, deleted."

78 Data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or regarding sex life.

79 Personal data must not be further processed for any other purpose other than the original purpose of collection.

Data controller[80]

- Who is the data controller? (The name and address of the organisation).
- Who is the representative of the data controller? (Who will be in charge of processing data and handling queries and requests?)
- Does the data controller take an oath of secrecy to protect information (even after they stop working)?
- Are there any data processors?

Data retention

- How is data stored before and after it is processed?
- What is the necessary time frame for keeping personal data for the purpose that it has been collected for?
- What happens to the data after the designated period elapses?
- Will the data be anonymised or erased?
- Is personal data kept in an identifiable form for no longer than is necessary for the purposes for which the data was collected or for which it was further processed?
- Does the national law provide exceptions for data retention? Are the purposes specified for prolonged data retention? For example, for historical, statistical or scientific purposes?
- What safeguards are in place to guarantee enhanced protection in the storage of sensitive data?
- What kind of data should be retained?

Quality of personal data

- Is the data that is being processed complete, accurate and up to date (where necessary)?
- Does the law provide for the quality of personal data?
- How is the quality of data ensured during collection, storage, sharing or transfer?
- What measures are in place to erase and/or rectify inaccurate or obsolete data?

80 The data controller determines the purposes and means of the processing of personal data. Identification of the data controller is to identify who bears the compliance responsibilities.

Consent

- Are privacy practices explained to enable meaningful consent?
- Is meaningful consent well articulated?
- Has consent by the data subject been freely given for the collection, use and disclosure of personal information?
- Is the consent explicit?
- Is the consent specific to the particular purpose of the processing of their personal data?
- Is the consent informed?
- How does the national law provide for consent to the processing of personal data?
- Are risk of harm and other consequences clearly articulated to facilitate informed consent so that data subjects fully understand the consequences of the processing of their personal data?
- Does the law provide for opt-out options?
- What are the sanctions for not respecting explicit consent?
- Are the rights holders aware of the consent provisions?
- What measures are in place to ensure that there is awareness on consent in the context of privacy and data protection?

Rights of data subjects

- Has the data subject been informed about processing of their personal data?
- Was adequate information provided to the data subject prior to obtaining their consent?
- Was the identity of the data controller revealed?
- Was the intended purpose of the processing of data revealed?
- Was the recipient(s) of the data revealed?
- Has the data subject been informed of their right of access to and the right to rectify personal data?
- How are data subjects informed about the processing of their personal data?
- Are there any data processing situations that present specific risks to the rights and freedoms of data subjects? What organisational and technical safeguards have been put in place for such situations?
- Has the national DPA been informed of the potential risks? What prior checks have been conducted?
- Is the data subject informed about all third parties that have had access to their personal data?

Confidentiality[81]

- Does the national law contain provisions for confidentiality?
- How is the principle of confidentiality guaranteed?
- What are the sanctions for breach of confidentiality?

Data security[82]

- What are the possible privacy risks?
- How is personal data kept secure?
- What organisational and technical measures exist to ensure that personal data is protected from unauthorised processing, destruction, alteration, disclosure or loss?
- Are the existing data security measures up to standard?
- Is there a law for data security? What are its provisions?
- What is the level of awareness with regards to data security?

Notification obligation

- Has the data controller notified the national data protection authority of any processing of personal data?
- Does the law provide for the notification obligation?
- What is the notification procedure?
- Are there any exemptions?
- Does the law provide for data breach notification?

Cross-border data transfers

- What do the laws provide regarding cross-border data transfers?
- What are the restrictions regarding cross-border data transfers?
- Is there awareness of cross-border data transfers?

81 Any person who has access to personal data must not access or provide access to, delete or otherwise process this personal data "except on the instructions of the controller" when the law requires otherwise (e.g. for law enforcement purposes).

82 In measuring compliance on data security, it is important to consider the principles of data protection by design and by default including implementation. Data protection should be at the core of any activity or engagement that deals with personal data. Organisational measures include adoption of data protection policies and technical measures include use of privacy enhancing mechanisms such as encryption.

Direct marketing

- What organisational and technical measures have been adopted to strike the balance between meeting customers' expectations and complying with privacy and data protection legislation?
- How is adequate prior consent obtained?
- What measures have been adopted to widen the scope of consent and to ensure that consent is freely given, specific, informed and unambiguous to strengthen the need for transparency in the collection of consent from individuals?
- Is the system designed for individuals to "opt in" to direct marketing as opposed to "opting out"?
- Where an individual has provided their email address as part of a sale or service, is there a clear opt out option in each marketing communication?
- What technical measures have been adopted to ensure that all opt outs are processed "without undue delay" and to ensure that no "opt out" requests slip through the cracks?
- How are opt outs managed?
- In cases of profiling or analytics to tailor marketing campaigns specifically to individuals, are there options for individuals to exercise their right to request not to be profiled?
- Has the privacy by design approach been adopted?
- Are privacy impact assessments carried out on any large-scale processing of personal or sensitive personal data?
- Are adequate due-diligence processes in place prior to engaging with marketing affiliates?
- Does the organisation conduct training and awareness programmes to enable the organisation's marketing teams to ensure compliance with the privacy and data protection frameworks in direct marketing?
- What measures are in place for individuals to complain regarding invasions of privacy in marketing?
- What are the privacy expectations with regards to contracts with third parties?

Sanctions

- What are the sanctions for failure to comply with the data protection law?
- Does the law provide for an appeal against the decisions of the national data protection authority?

Vulnerable data subjects

- Does the law recognise the existing inequalities between different data subjects?
- Who are considered vulnerable data subjects?
- What are the determinants for vulnerability?
- How does the law protect the rights of vulnerable data subjects?
- Is there clarity on what the restrictions entail?

Guidelines for policy makers and duty bearers on the HRBA to data protection and privacy policy and regulation

Policy makers and other duty bearers have an important role to play in contributing to the protection of the right to privacy and the promotion of data protection. A HRBA identifies rights holders and the freedoms that they are entitled to in accordance with international human rights standards. It also outlines the obligations of duty bearers. Essentially, policy responses, when a HRBA is the guiding framework, should promote accountability from duty bearers whose mandate is to respect, protect and fulfil rights and empower rights holders to claim and enjoy their rights.

Data protection is a human rights issue

Policy makers should acknowledge that privacy is a fundamental right. Data protection cannot be viewed separately from other rights that the state has already signed up to under its obligations to upholding international human rights law. Data protection is inextricably linked to the right to privacy and contributes to other human rights, such as the right to dignity. Data protection is now an established right in some jurisdictions.[83]

83 Article 8 of the Charter of Fundamental Rights of the European Union, provides that "everyone has the right to the protection of personal data concerning him or her."

Putting a data protection framework in place represents an opportunity for the state to demonstrate its commitment to uphold human rights through the protection of personal data. The responsibility of policymakers lies in the ability to support the public and address causes of human rights violation, as well as to empower rights holders to claim and exercise their rights.

Balancing privacy and data protection with other rights and interests (the balancing act)

With regards to balancing privacy and data protection with other rights, data protection connects with other rights such as access to information, freedom of expression, the right to dignity and others. One of the exemptions under an access to information framework is the protection of personal information.[84] Yet overly restrictive protection of personal information could potentially infringe on the ability of the public to access information that could be in the public interest. Again, data minimisation and the right of erasure under data protection could impact rights such as access to information and freedom of expression. The essence of protecting personal data, while essential to the realisation of the right to privacy, could impact on the right "to seek, receive and impart information and ideas of all kinds"[85] because the information may be personal and interfere with the right to privacy.

Processing of sensitive or other personal information could also potentially lead to discrimination. All these rights are fundamental in a democracy and human rights are universal, indivisible, interdependent, and interrelated. Policy makers should balance

84 Model Law on Access to Information for Africa, Sec 27.

85 African Charter on Human and Peoples' Rights, ICCPR, UDHR.

these rights in a manner that does not compromise the objective of human rights realisation.[86]

The right to privacy and data protection rights must be proportionate and balanced against other human rights such as the right to dignity, freedom of expression, the right of access to information and other fundamental rights. Also, business considerations, law enforcement and national security have to be taken into consideration.

Justifiable limitations

Privacy is a fundamental right as provided for under international law but it is not an absolute right. There are legitimate reasons under which the right to privacy can be limited. Interference with the right to privacy can only take place in cases that are envisaged by the law.[87] The law that articulates the interference on the right to privacy should be in compliance with international human rights law and standards, for example, the ICCPR. Interference, as provided for by the law, should be reasonable, serve a legitimate purpose and be necessary in a democratic society. The law should be clear on the practices and circumstances under which the right to privacy can be limited.

In light of these restrictions, the law should be clear on the competent authorities/institutions and officials that are authorised to perform activities that might interfere with the right to privacy. The laws should also provide for adequate remedies in cases of unlawful interference with the right to privacy.

86 South Africa has the Information Regulator to oversee the implementation of access to information legislation and data protection: striking the balance.

87 Human Rights Committee. (1988). General Comment No 16 on the Right to Privacy, para 3.

Reasons for limiting the right to privacy could include:

- National security
- Public safety
- Economic well-being of the country
- Prevention of disorder or crime
- Protection of health or morals
- Protection of the rights and freedoms of others.

In the context of national security, privacy infringing activities such as surveillance should be conducted within the confines of the law. Surveillance should be regulated by the appropriate legal framework, which in some case could be included under the data protection law. There is a need to establish an appropriate balance between data protection and surveillance. Appropriate limits and conditions for surveillance should be established within the law and ensure that the level of surveillance is necessary, appropriate and proportionate to the purpose of the surveillance and also ensure the availability of effective remedies. The basis for limitations to the right to privacy should be the public interest notion and should be clearly defined in law. The public interest approach is thus applicable, also in instances where consent or anonymisation are impracticable. However, there should be adequate safeguards when identifiable data is handled so that individuals whose data has been processed in this manner are not harmed and also to hinder the identification of such individuals, for example, in reports or publications.

Participation

Participation in the context of data protection is crucial in the formulation of the law and at the implementation phase. Those

who are not able to participate should be empowered to do so and given the necessary support. An essential element of participation is access to information in accessible formats. This facilitates informed participation. These programmes should clearly indicate where data breaches could arise and how to seek redress where necessary. Facilitating public participation in policy helps the state to meet its human rights obligations and can ensure that policies are targeted at meeting public needs. Civil society participation is crucial in the development and implementation of data protection laws. Participation should also include educating the public about privacy and data protection and why it is essential.

Empowerment, transparency and access to information

Transparency is an indispensable principle in a data protection regime. Individuals have the right to know about the processing of their personal information. Such processing should be conducted in a transparent manner, providing access to information. Information that should be disclosed to individuals includes information about the duty bearers, data collection, data storage, sharing or transfer of personal information, access to personal information for the purposes of rectification or erasure where necessary and also to enable or withdraw consent. To facilitate transparency in data protection, all relevant information should be easily accessible and easy to understand in plain language. The information should be available in different formats and various languages that are also accessible to persons with disabilities and linguistic minorities.

Empowerment is necessary to enhance active citizenry and general awareness. If there are laws, whether sectoral or comprehensive data protection law, then policy makers have an obligation to ensure that the public is aware of the law, its provisions and how it affects them. For example, where data

protection legislation provides for the rights of data subjects, policy makers can raise awareness about such legislation and empower the public to claim their rights. Without education and awareness, the effectiveness of the law cannot be measured as it will not be used. Beyond their rights, the public also needs to be empowered about how to seek redress and demand accountability. Raising awareness around privacy and data protection enhances public participation and improves accountability levels.

The relevant authorities should develop programmes and guides to engage and empower the public to understand the data protection framework and their rights on the basis of the data protection principles; and empower and train relevant officials to be able to work with the public on privacy and data protection. This process also includes clarifying the various duty bearers and their corresponding obligations.

All policy makers and duty bearers have to receive adequate training about their roles and tasks, so that they understand the expectations with regard to formulating and implementing a data protection framework. This may be done by reflecting on the obligations of human rights legislation in professional standards and in their requirements for undergraduate training.

It is also important to raise awareness on privacy breaches and what such breaches entail.

Legality

Policy makers and duty bearers must be sure that practices and procedures on privacy and data protection are grounded in international human rights law. Any measures should reflect

compliance with internationally set standards. International law provides for the right to privacy.[88] In addition, there are standards for data protection that are also framed in international law.[89] Any adopted framework should seek to advance human rights and be representative of the available standards. Data protection laws and frameworks can only be viable and effective when they are based on legal norms and operate under the rule of law.

Access to effective remedies

Access to an effective remedy is a fundamental element of human rights. The question of remedies and reparations for victims of violations of the right to privacy is important and data protection violations should be remedied in a manner that is effective and lawful. Any individual whose right to privacy has been violated following a data breach deserves access to an appropriate remedy, including the possibility of reparation. Effective avenues for complaints should be established to allow the public to report without fear of reprisal. Responsible bodies have to respond within a reasonable timeframe. It is essential to ensure that complaints are dealt with within a reasonable time frame, and to establish a whistle-blower protection framework. Information about data protection and mechanisms for accessing remedies should be proactively disclosed and easily accessible. The application of the right to remedy should be consistent with international human rights law and standards and practised without any discrimination. Victims of unlawful infringement of the right to privacy should receive adequate, effective and prompt reparations consistent with the law. In accessing the appropriate remedies, individuals should have access to the relevant information regarding violations and

88 SFLC.IN. (2017, 24 October). Right to Privacy under UDHR and ICCPR. *Privacy Bytes*. https://privacy.sflc.in/universal/

89 See GDPR, AU Convention, ECOWAS Supplementary Act, SADC Model Law of Data Protection.

reparation mechanisms. Effective mechanisms should be established to ensure general access to credible information.

Individuals or data subjects who are affected by non-compliance with data protection laws and other privacy obligations should be enabled to lodge complaints with the relevant mechanisms dealing with non-compliance and access the necessary remedies. Organisations should put in place mechanisms to remedy any forms of non-compliance with the regulations around protection of personal information. In this regard, a number of possibilities to enforce privacy rights and lodge complaints regarding non-compliance should be established. The law should provide for representative actions where civil society organisations can lodge complaints on behalf of aggrieved data subjects.

Effective framework on privacy and data protection

It is essential to update laws and align them with the international human rights and standards. In this regard, an assessment or audit of the existing data protection framework in consultation with human rights and data protection experts to assess compliance with international human rights standards is necessary to inform the law reform process. The adoption of data protection strategies through public participation-based human rights standards and data protection principles is also an essential element in the development of effective frameworks on privacy and data protection.

The accountability obligation

Accountability is a fundamental data protection principle and a demonstration of compliance. It is the responsibility of the state to respect, protect, promote and fulfil the rights. Non-state actors

also have human rights obligations in the data protection regime. The accountability obligation requires the adoption of appropriate technical and organisational measures to give effect to the right to privacy. In their reports to human rights bodies, states should indicate the legal and other measures that have been adopted to give effect to the right to privacy, including the limitations to the right to privacy as well as complaints which have been lodged in respect of arbitrary or unlawful interference and the remedies provided in such cases.

The appointment of a data protection officer to conduct activities such as monitoring and evaluation through recording and maintaining documentation and, where necessary, reporting personal data breaches and carrying out data protection impact assessments is an integral part of a data protection regime, which policy makers should be cognisant of. Data collectors should provide periodic transparency reports indicating the number and nature of data requests received and show that the data was granted. Data processors should indicate technical and organisational measures that are in place to protect data. The impact assessment report should include aspects such as privacy by design and privacy by default and the issue of internal (boards) and external oversight of data controllers and processors.

Adequate resources

The commitment to human rights is demonstrated by the adoption of human rights frameworks and the realisation of those fundamental rights requiring the state to allocate resources (including human and financial). Resources are necessary for the implementation and enforcement of the data protection frameworks. An adequately resourced national data protection authority can effectively monitor the implementation of regulatory and policy frameworks.

For countries with data protection laws, adequate resources should be put in place to support the implementation efforts while countries that do not have data protection laws should provide adequate resources for the development of the necessary legal, policy and institutional framework.

New technologies

With emerging and innovative technologies, regulating privacy and data protection is becoming difficult in that technologies are constantly changing and, in most instances, faster than the laws are amended. The dynamic technologies of the digital age such as cloud computing, the internet of things and data analytics continuously present challenges for data protection while posing risks for personal data. Appropriate frameworks should be established to provide guidance in processing personal data in the context of emerging technologies that have capabilities of micro-targeting and other profiling such as artificial intelligence and facial recognition. Rigorous analysis is essential in ascertaining the extent and capabilities of the technologies to affect the right to privacy and formulating the appropriate regulations.

As a case in point, artificial intelligence relies on the mass collection of data to operate. This collection is a challenge to privacy and to personal data protection. On the other hand, facial recognition technology, which identifies individuals using biometric data, is used by law enforcement offices in some jurisdictions. The internet of things generates massive amounts of data that can be transmitted between connected devices and machines without human intervention. Measures should be adopted to ensure that the automated mass collection of data does not infringe on the privacy of individuals.

Enforcement

Enforcement is an integral component of a privacy and data protection regime. Enforcement powers should be broadened to provide greater protection and enhanced chances of compliance with the data protection standards. Occurrences of data breaches are becoming more prominent, which calls for greater enforcement measures in line with the scope of the data protection challenges being faced. Where necessary, adjustments should be made to powers and sanctions. These standards can be incorporated into the development of a new law or amendments can be made to existing laws. In this regard, legislation should empower state attorneys general and private citizens to pursue legal remedies and adequate resources should be given to institutions that are responsible for the enforcement.

Strategic litigation

Strategic litigation is a tool for responding to unlawful restrictions on rights to privacy and data protection. It is another way of advancing the human rights-based approach to privacy and data protection. Through strategic litigation, laws can be changed and new precedents can be set. However, the challenge with strategic litigation is that it is costly, shrouded with uncertainty, and if unsuccessful, may have negative repercussions for the applicant and the reputation of their organisation. If successful, strategic litigation can place the issue under consideration in the public spotlight. For example the *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*[90] brought attention to the privacy concerns about the South African communication interception

90 http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html

law and the surveillance practice and also facilitated the move towards surveillance reform. Collaboration between lawyers, human rights activists, academia, civil society organisations and other experts is crucial for the success of strategic litigation.

Recommendations for different role players

African Union Commission (AUC) and human rights bodies

The African Union (AU) is a continental body with a membership of 55 countries. The AU consists of political and administrative bodies which develop and implement the decisions and commitments of the assembly of the AU. In 2014, the assembly adopted the Convention on Cyber Security and Personal Data Protection. This convention is aimed at providing a continental framework for cybersecurity and data protection and to provide a basis for harmonising such legislation. The AU should encourage states to ratify the AU Convention on Cyber Security and Personal Data Protection.

The AU has human rights bodies including the African Commission on Human and People's Rights, the African Court on Human and Peoples' Rights and the Committee of Experts on the Rights and Welfare of the Child. Although the African Charter is the main human rights instrument that is monitored by the African Commission and the African Court, it does not have a provision on the right to privacy. However, the African Commission has adopted soft law instruments that contain provisions regarding the right to privacy and also incorporating data protection. The 2019 Declaration of Principles on Freedom of Expression and Access to Information has such provisions (Principles 40-42). Guided by this significant development the African Commission can:

- Incorporate the right to privacy in the work of other special mechanisms of the African Commission, beyond the Special Rapporteur on Freedom of Expression and Access to Information. The right to privacy is a cross-cutting issue which can be tackled by all the special mechanisms.
- Provide guidance on the right to privacy.
- Monitor the right to privacy on the continent.
- Collaborate with the AUC on development of human rights-based privacy and data protection frameworks for example, developing a continental Model Law on Privacy and Data Protection.[91]
- Assess the impact of violations on the right to privacy on other rights and develop Guidelines to states on its protection.
- Appoint a Special Rapporteur on the Right to Privacy and Data Protection.

The Committee of Experts on the Rights and Welfare of the Child could:

- Elaborate on Article 10 of the African Charter on the Rights and Welfare of the Child which provides for the right to privacy through adoption of general comments, declarations or guidelines.
- Actively monitor the children's right to privacy particularly in the digital sphere.

The Pan African Parliament (PAP) is the legislative body of the African Union. With regards to data protection and privacy, PAP could:

- Develop programmes on privacy, data protection, consumer protection, electronic commerce, cybercrime, the fourth industrial revolution and the implications of technology on

91 The African Commission has developed a Model Law on Access to Information.

privacy and data protection. Most countries on the continent are developing legislation on privacy and data protection. It is imperative to have well informed legislators.

- Lead a campaign for the ratification of the African Convention on Cyber Security and Personal Data Protection.
- Contribute to shaping of the fundamental data protection standards.

Sub-regional bodies

These are the East African Community (EAC), Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS). The EAC adopted a framework for cyber law which includes provisions on data protection and privacy. The SADC adopted a Model Law on Data Protection, and the ECOWAS adopted a supplementary law on data protection that specifies principles and practices for data protection legislation.

Policy makers

They could:

- Develop data protection frameworks in line with international human rights law and standards.
- Reform outdated data protection legislation.
- Work with the DPA in formulating sector-specific data protection laws and guidelines.
- Mainstream data protection in sector-specific legislation.
- Monitor the implementation of data protection legislation.
- Organise hearings with industry stakeholders and experts on data protection issues.

- Adapt data protection frameworks to emerging technologies such as artificial intelligence, facial recognition technology and the internet of things.
- Facilitate public awareness on the right to privacy and data protection.
- Monitor data protection matters in international agreements.
- Make the protection of the right to privacy and data protection political priorities.
- Supervise international arrangements on data transfer.
- Develop guidelines for using surveillance technology in line with the data protection laws for the purposes of law enforcement.

DPAs

Their powers, tasks and responsibilities should be clearly articulated in the law. They are responsible for:

- Supervising and monitoring the application of data protection laws.
- Meting out sanctions in cases of non-compliance.
- Informing the general public on the rights and obligations related to data protection.
- Raising public awareness of the right to privacy and data protection.
- Handling complaints regarding the use of personal information and investigating data breaches.
- Providing expert advice on data protection.

- Developing sector-specific guidelines and other tools to for processing personal information and assisting various sectors in understanding their obligations under the data protection framework. For example, developing a framework for the use of personal data in political campaigning.
- Establishing and making public a list of processing operations that require a data protection impact assessment.
- Monitoring data protection impact assessment.
- Working with stakeholders in regulating the use of personal information in marketing.
- Facilitating training on privacy and data protection for various sectors.

National human rights institutions

National human rights institutions (NHRIs) are state institutions that are part of the state apparatus and conferred the mandate to protect and promote human rights.[92] They are established in terms of national laws, and ideally should be governed by the Paris Principles[93] and operate independently from the government. They monitor and investigate human rights violations. They vary in form and name depending on jurisdictions and on the region, legal tradition and common usage, for instance: civil rights protector, commissioner, human rights commission, human rights institute or centre, ombudsman, parliamentary ombudsman or commissioner for human rights and public defender/protector or parliamentary advocate.[94]

92 United Nations. (2010). *National Human Rights Institutions: History, Principles, Roles and Responsibilities.* United Nations. https://www.ohchr.org/Documents/Publications/PTS-4Rev1-NHRI_en.pdf

93 The Paris Principles define minimum standards for NHRIs. See https://www.un.org/ruleoflaw/files/PRINCI~5.PDF

94 United Nations. (2010). Op.cit.

Privacy and data protection are human rights issues, and as such should be seen as human rights concerns which fall within the scope of the mandate of NHRIs. Although data protection is not stated, at least in explicit terms in most constitutions, it is linked to and a fundamental component of the right to privacy, which almost all African constitutions have in their constitutions.

In the context of privacy and data protection, a NHRI should:

- Monitor and enforce government's compliance with the international and regional standards on privacy and data protection.
- Conduct civic education and raise awareness on the right to privacy and data protection.
- Include a section on the right to privacy and data protection in all human rights reports.
- Bridge the divide between privacy issues and other fundamental rights.
- Promote synergy between NHRIs and data protection authorities where these are separate entities.

Law and order

Law enforcement offices and the entire criminal justice system also have a role to play in the data protection regime. It is crucial to understand data processing for law enforcement.

The role of law enforcement officials is to:

- Work with the DPA in developing guidelines for the processing of personal information.
- Process personal information in a lawful, fair and transparent manner.

- Train law enforcement officers on privacy and data protection.
- Adopt organisational and technical measures for processing personal information such as data protection policies, staff training, internal audits of personal information processing, and reviews of internal data protection policies.
- Cooperate with the DPA for guidance on data protection and privacy.

Judiciary

Data protection is also crucial in the administration of justice by the judiciary. In this administration, personal information is exchanged, particularly with the adoption of e-justice initiatives. Data protection is also a tool that facilitates successful interaction and mutual trust between judiciary, law enforcement and other relevant actors in the justice system. The judiciary should:

- Ensure that the right to privacy is upheld.
- Adopt organisational and technical measures to reinforce the management of data within the judiciary.
- Facilitate training on the right to privacy and data protection within the judiciary.
- Establish activities for processing data.

Electoral management bodies

The electoral environment is constantly changing because of technology developments and the entire democratic space is also being transformed by these developments. Political campaigns on social media platforms, biometric voter registration, e-voting, application of facial recognition by police in monitoring of political

activities such as rallies and demonstrations and the use of surveillance for monitoring purposes are some of the ways in which technological transformations also contribute to collection and storage of personal information. ICTs are also expanding the many ways of sharing information in electoral processes. In this electoral information ecosystem, electoral management bodies process personal information and the manner in which this is handled affects the democratic process, particularly the electoral landscape. In the privacy and data protection landscape, the role of the electoral management bodies is to ensure that there is no exploitation of personal information and to:

- Ensure that the voters' register only contains information that is necessary for the electoral process.
- Define the conditions and limits of access to the voters' register.
- Regulate use and access to the voter's register. The law should be clear on access and purpose of processing information in the voter's register.
- Ensure that personal data that is shared in polling stations should be limited to identification of the voter and the voting process.
- Provide cybersecurity training for personnel.
- Put in place mechanisms for monitoring, detecting and responding to cybersecurity attacks.
- Put in place organisational and technical safeguards to curb unauthorised access to personal data.
- Dedicate resources for information security.
- Conduct risk assessments regarding information security.
- Ensure inclusion of cybersecurity of election data in the national cybersecurity strategy.

- Enhance expertise on data protection and cybersecurity.
- Cooperate with authorities and actors such as DPAs, media regulators and cybersecurity authorities.
- Cooperate with the data protection authority in dealing with complaints related to data protection and the regulation of processing of personal information.
- Apply data protection laws to the processing of personal data by political parties and other political actors.

Political parties

Political parties collect personal data to create profiles on voters including sensitive information such as religion, political opinions and income for political profiling. Where a data protection law does not exist, political parties might exploit this grey area. Information is usually obtained from the electoral register and other sources. It is important for political parties to adhere to data protection principles in their processing of personal information during campaigns. In order to demonstrate a commitment to protecting personal information, political parties should:

- Be transparent about their data processing activities, including identifying the mechanisms they use to engage with voters (e.g. social media, websites, direct messaging through platforms like WhatsApp), how personal data is processed and providing access to data.
- Adopt and publish data protection policies.
- Carry out data protection audits and impact assessments.
- Establish a legal basis for each use of personal data (including any sensitive data).

- Ensure that use by third parties also complies with data protection laws.
- In cases of digital political marketing, information should be clear to voters on why they are receiving particular messages including explanations regarding the individual exercise of their rights.

Consumer protection organisations

These groups should:

- Educate consumers on how best to familiarise themselves with and use privacy tools to improve the privacy of their data.
- Educate consumers on data protection to instil an understanding of data protection, particularly collection, sharing and storage of personal information, including sensitive data.
- Work with business entities and advocate for the adoption of measures to protect data (adoption and implementation of appropriate data protection frameworks).

Business sector

Businesses should work to:

- Integrate data protection into all activities and business practices, from the design stage right through the lifecycle.
- Adopt organisational and technical measures to safeguard consumer data.
- Conduct regular training of employees on data protection.
- Regularly monitor and update data security systems to detect attacks.

- Adopt privacy-enhancing technologies to reduce vulnerability of data.
- Notify DPAs and data controllers of any data breaches within the time stipulated in the law.
- Cooperate with the DPA in the implementation of the data protection framework.

Civil society organisations

These have an instrumental role in the development and advancement of the right to privacy and promotion of data protection.

Civil society can contribute to this advancement by continuing to:

- Raise awareness on the right to privacy and data protection, clearly highlighting its enabling capabilities in the realisation of other human rights.
- Continuously engage their governments in matters relating to the right to privacy and data protection.
- Monitor data processors and controllers and notify national DPAs of any violations of the data protection legislation.
- Where relevant, submit requests for advisory opinion on matters of privacy and data protection.
- Where violations have occurred, take legal action before the relevant domestic, regional or international forums.
- Incorporate privacy and data protection matters on the agenda of the sessions of bodies such as the African Commission, the Committee of Experts on the Rights of the Child and the Pan African Parliament, including by submitting shadow reports.

- Actively participate in legal reforms that seek to amend or introduce comprehensive privacy and data protection legislation.
- Advocate for the enforcement of data protection legislation.
- Engage regional bodies like Pan African Parliament on the ratification of the African Convention on Cyber Security and Personal Data Protection.
- Collaborate with PAP on capacity building of parliamentarians on privacy and data protection to enhance their understanding of the matter so that that they contribute to the adoption of human-rights grounded laws on data protection and privacy.
- Conduct parliamentary briefings on privacy, data protection, consumer protection, electronic commerce and cybercrime.
- In the shadow reports, consider bringing issues on privacy and data protection to the attention of the African human rights bodies.

Internet service providers (ISPs)

The significance of ICTs and the use of the internet comes with unique challenges associated with increased frequency in processing of personal data for economic, social and other activities. These developments expedite the processing and exchange of personal data as well as increasing the risk and possibility of personal data being collected, processed and used without the data subject's consent or knowledge.[95]

95 https://rm.coe.int/16805a39d5

ISPs, in the context of data protection, should do the following:

- Make privacy part of the business model.
- Produce periodic transparency reports.
- Provide guidance to customers about potential privacy risks.
- Inform users about security measures to enhance privacy.
- Ensure data integrity and confidentiality.
- Process personal data only when necessary and explicitly state the purpose.
- Transfer data only within the confines of the law.
- Ensure that publishing of data does not infringe on the right to privacy.
- Provide accurate and up to date information to users.
- Ensure security of data.
- Inform users about who they are, what data they collect, process and store, in what way, for what purpose and for how long. If necessary, ask for user's consent.
- Store data only for as long as is necessary to achieve the intended purpose.
- Only use data for promotional or marketing purposes after obtaining explicit consent.
- Address developments and expectations of corporations to ensure that users are appropriately informed of how their data will be processed.
- Consider recent developments such as processing of personal information for AI purposes.

- Publish transparency reports as a means of accountability and assessing the government's consumption of personal data possessed by private entities.
- Use access to information requests as a tool of seeking and obtaining this information.

Academia

Academic institutions play an important role in advancing the right to privacy and data protection in Africa. They provide a platform for undertaking research and debate on the subject. This role of academics helps in generating more knowledge and understanding about the right to privacy and data protection. In this regard, academia should:

- Incorporate studies on the right to privacy and data protection into the curriculum across various disciplines.
- Support the publication of literature that seeks to advance the right to privacy and data protection.
- Organise and create platforms for discussing and debating privacy and data protection.
- Conduct research on privacy and data protection in Africa.

Gender justice advocates

The link between data and gender is not always acknowledged. Gender issues are often sidelined in the discussion on data protection.[96] Gendered dynamics should be taken into account and gender justice advocates should amplify gendered perspectives. Additionally, gender justice advocates should:

96 Brandusescu, A. (2018 9 February). Gender must be central to the data protection conversation, not a side note. *World Wide Web Foundation.* https://webfoundation.org/2018/02/gender-must-be-central-to-the-data-protection-conversation-not-a-side-note/

- Contribute to gender responsive interventions in data protection.
- Contribute to more advocacy on the intersection of gender and data.
- Work with relevant bodies to develop or maintain preventive measures and remedies for violations and abuses regarding the right to privacy, where particular gendered effects are evident.
- Promote good practices in law and service delivery models that address gender-based differences in the enjoyment of the right to privacy.
- Monitor the gendered impacts of privacy invasions on women, men and individuals of diverse sexual orientations, gender identities, gender expressions and sexual characteristics, arising from the loss of the right to privacy.

Children's rights activists[97]

The processing of children's data requires particular protection and processing as they may be unaware or not fully knowledgeable of the risks associated with processing of their personal information. Any processing of children's personal information should be underpinned by the need to protect them. Protecting children should be the default position that everyone should adopt. In this regard, child rights activists should:

- Monitor compliance with the data protection legislation particularly the integration of the best interests of the child, as provided for by the United Nations Convention on the

97 According to Recital 38 of the GDPR, "Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

Rights of the Child,[98] the African Charter on the Rights and Welfare of the Child and other frameworks that protect the rights of the child.

- Advocate for a lawful basis for processing a child's personal data in cases where there is none.
- Ensure that there is specific protection whenever children's personal data could be used for marketing purposes or creating personality or user profiles.
- Ensure that all frameworks on children's privacy are presented in a clear manner using plain, age-appropriate language. Formats should include diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.
- Raise awareness on children's right to privacy.

98 See Article 3 of the United Nations Convention on the Rights of the Child, "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

Essentially, policy responses, when a human rights-based approach is the guiding framework, should promote accountability from duty bearers whose mandate is to respect, protect and fulfil rights and empower rights holders to claim and enjoy their rights.