Personal Data Protection Guidelines for Africa

A joint initiative of the Internet Society and the Commission of the African Union

9 May 2018

African Union

Introduction

In 2014, African Union (AU) members adopted the African Union Convention on Cyber Security and Personal Data Protection ("the Convention")[1]. AU Ministers in charge of Communication and Information and Communication Technology (CICT) and Postal Services confirmed their commitment to the Convention in the African Union Specialized Technical Committee on Communication and ICT Ministerial Declaration (AU/CCICT-2)[2].

The Declaration set a strong objective of African action on cybersecurity and personal data protection to deliver benefits to Africa. In particular, it called on the African Union Commission (AUC) to develop guidelines on personal data protection (Para. 31).

To facilitate implementation of the Convention, the AUC asked the Internet Society (ISOC) to jointly develop the Privacy and Personal Data Protection Guidelines for Africa ("the Guidelines"). The Guidelines were created with contributions from regional and global privacy experts, including industry privacy specialists, academics and civil society groups.

The Guidelines emphasize the importance of ensuring trust in online services, as a key factor in sustaining a productive and beneficial digital economy. They also offer guidance on how to help individuals take a more active part in the protection of their personal data, while recognising that in many areas, positive outcomes for individuals depend on positive action by other stakeholders.

The Guidelines set out 18 recommendations, grouped under three headings:

- Two foundational principles to create trust, privacy, and responsible use of personal data
- Eight recommendations for action by the following stakeholders:
    - Governments and policymakers
    - Data Protection Authorities (DPAs)
    - Data controllers and data processors
- Eight recommendations on the following themes:
    - Multi-stakeholder solutions
    - Wellbeing of the digital citizen
    - Enabling and sustaining measures

Privacy and personal data protection is a broad and ever-changing domain; the Guidelines are not an end-state—they are a blueprint for an evolving process of developing policy, operational guidance, and best practice, as new circumstances and requirements emerge.

1 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
2 https://au.int/sites/default/files/newsevents/reports/33025-rp-addis_ababa_declaration_of_the_stc-cict-2_en.pdf (Para.31)

Table of Contents

Introduction 2
Table of Contents 3
Executive Summary 4
Acknowledgements 6
The African Context 7
The Policy Context 7
Towards consistency with privacy principles applied in other regions 9
Principles identified in the Malabo Convention 9
Similar sets of principles from other sources 9
Existing regional and national frameworks in Africa 10
Themes by Stakeholder Group 11
Recommendations 19
About the Internet Society 28
About the Commission of the African Union 28

Executive Summary

This section summarises the principal roles and responsibilities of the main stakeholder groups, with respect to personal data protection.

Governments and policymakers

Role: to empower the digital citizen, and ensure the online environment is trusted, safe, and beneficial to all stakeholders.

Responsibilities:

- Increase their understanding of the benefits and hazards of the data-driven economy.
- Understand the economic and social forces at work in the personal data ecosystem.
- Cultivate the long-term social framework for trust in the digital economy, ensuring that the benefits are distributed fairly.

These are the goals of the foundational principles, and the enabling and sustaining measures.

Data protection authorities (DPAs)

Role: to increase legal certainty, by enforcing data protection laws, investigating alleged privacy violations, imposing sanctions where applicable, and working with the stakeholder groups and other DPAs.

Responsibilities:

- Provide expert input to governments on data protection policy and laws.
- Give clear guidance to data controllers and manufacturers/developers of products and services.
- Deliver effective enforcement of data protection regulations, including investigation and sanctions.
- Develop advice and help for data subjects.
- Coordinate with other DPAs, in support of consistent cross-border data protection rules and enforcement.

Data controllers and their partners

Role: to create and apply responsible and sustainable practices for handling personal data, that reflect the data subject's interests as well as those of the data controller and partners.

Responsibilities:

- Maximise trust, as an expectation of the citizen/customer/user, as a benefit delivered by your services and products, and as an economic asset of your organisation. Trust enhances reputation, strengthens consent, and can deliver competitive advantage in a commercial context.
- Tackle the practical problems of personal data protection (consent, data retention periods, data security, etc.), with the right blend of technical and procedural measures.
- Increase the use of Privacy by Design (PbD) and value-based design[3] , as an integrated part of product/service development.

3 Most product design processes focus primarily on aspects such as function, form, aesthetics, and cost. Value-based design recognises that every design choice has an ethical dimension and integrates ethical considerations systematically into the design and development lifecycle.

Citizens and Civil Society

Role: to create effective digital citizens; to become active stakeholders of their own privacy and personal data.

Responsibilities:

- Understand the risks involved in online life.
- Understand and exercise the rights relating to personal data, privacy and autonomy.
- Develop your capabilities to protect their interests online, whether directly, or by using tools and services that help enhance their privacy.
- Develop a collective voice (with consumer and civil society organisations) to shift the consumer market towards better privacy.

Multi-Stakeholder Tasks

Every stakeholder has a role in collectively creating a trusted online ecosystem that operates to the benefit of all.

Privacy is about respecting individuals' expectations as to how their personal information is handled; privacy depends on a relationship of respect, between the individual and the stakeholders who collect and use data about them. Better online privacy happens when everyone who has a stake in it is part of the solution.

Many practical problems of data protection require collaborative action by more than one stakeholder; for example,

- Development of best practice codes of conduct (DPAs, data controllers, industry bodies);
- Creation and operation of certification schemes for data protection (DPAs, consumer organisations, standards and certification bodies); and
- User consent, and respect for privacy contexts[4] (DPAs, data controllers, consumer bodies).

These are the actions recommended under the heading of "Multi-stakeholder solutions".

4 Privacy is often a matter of respecting the context in which information is disclosed, and not sharing or re-using it in other contexts (for example, not taking private medical data and publishing it in a newspaper).

Acknowledgements

We would like to acknowledge the invaluable contributions of Robin Wilton (Internet Society), who worked on the first draft of the guidelines and reviewed the successive drafts based on the input from contributing experts. We would also like to acknowledge the contributions of the following, all of whom participated in the expert workshop to identify and discuss the major themes of these Guidelines and commented on the draft text:

Souhila Amazouz (AUC)
Yaovi Atohoun (ICANN)
Dawit Bekele (ISOC)
Alebachew Berhanu (Bahir Dar University)
Betel Hailu (ISOC)
Verengai Mabika (ISOC)
Evelyn Namara (ISOC)
Marsema Tariku (ISOC)
Wakabi Wairagala (CIPESA)
Auguste Yankey (AUC)
Moctar Yedaly (AUC)
Kinfe Yilma (University of Melbourne)

Other contributions, and/or reviews of successive drafts, were kindly provided by:

Jacques Bus (Digital Enlightenment Forum)
Jemal Hussien (AUC)
Olaf Kolkman (ISOC)
Eve Maler (Forgerock Inc.)
Christine Runnegar (ISOC)
Colin Wallis (Kantara Initiative)
Pat Walshe (Privacy Matters Ltd.)
Sally Wentworth (ISOC)

Internet Society, April 2018
Document Ref.: AUC-PDPG-Apr2018

The African Context

These Guidelines take into account the following characteristics of the African context, as identified by the expert group:

- 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 consentless profiling of citizens, 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:
    - African Union member states' limited ability to influence the behaviour of external service providers.
    - Potentially-increased risk of data misuse where content and services are solely provided by foreign companies (such as "over the top" services or OTTs) and enforcement of local data protection laws may therefore be more difficult.

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

The Policy Context

As the African Union Convention on Cyber Security and Data Protection (2014) and the Addis Ababa Ministerial Declaration (AU/CCICT-2, 2017) illustrate, the Guidelines were developed in the context of rapid change in the scope and availability of online services in Africa, and a backdrop of ambitious African policy goals under Agenda 2063.

The AU has devoted considerable policy focus to harmonization. For example, the Constitutive Act of the African Union[5] (Article 3, Page 6) refers explicitly to coordination and harmonization of policies between the existing and future Regional Economic Communities, in support of (among others) the following goals:

- A united and strong Africa
- Accelerated political and socio-economic integration of the continent
- Establishment of conditions which enable Africa to play its rightful role in the global economy
- Sustainable development at the economic, social and cultural levels.

The AUC is also establishing the "Policy and Regulation Initiative for Digital Africa" (PRIDA), within which tools and methodologies for harmonizing and coordinating policy and regulation will be explored.

As part of an objective of greater regional integration, the Assembly of the Union, in its 27th Ordinary Session (July 2016, Kigali, Rwanda), resolved to implement a protocol for the free movement of persons across the continent.

5 https://au.int/sites/default/files/pages/32020-file-constitutiveact_en.pdf

- This resolution has implications for the standardised, safe and privacy-respecting exchange of citizens' identity data, in the context of border crossings, and the subsequent exchange of personal data across borders, when a citizen is working, residing, or transacting outside their country of origin. The same Session recognised the importance of free movement of goods and services as an element of deeper continental integration and unity.
- The principle of free movement of persons is also reflected in Art.43 of the Treaty Establishing the African Economic Community (1991, Abuja, Nigeria).

The AU has also taken significant steps towards establishing a Continental Free Trade Area (CFTA) in support of the principles of free movement of persons, goods and services, as reflected in the Decisions, Declarations and Resolution of its 25th Ordinary Session (June 2015, Johannesburg, South Africa). This has implications for the corresponding cross-border transfer of personal data, in the context of online transactions (trade), and of individuals living and working in member states other than their country of origin.

AU member states also have obligations relating to fundamental freedoms and human rights, as set out in declarations and conventions of the AU and the United Nations. This includes the commitment to respect, protect and promote the right to privacy, and personal data protection. In a number of instances, the right to privacy is already established in member states' constitutions (for example, Botswana, Democratic Republic of Congo, Egypt, Ghana, Kenya, Nigeria, Sierra Leone, South Africa, Tanzania, Uganda, Zambia and Zimbabwe recognise the right to individual privacy in their national constitutions as a fundamental human right).

All these policies and obligations have implications in terms of the safe, transparent, robust and privacy-respecting exchange of personal data across borders and between jurisdictions. This, in turn, imposes a burden on AU member states to ensure that progress towards regional integration, free trade and development is not hindered or made more risky, by an inability to exchange personal data securely, reliably and with appropriate respect for individuals' rights.

In parallel, safe, robust and privacy-respecting use of personal data is an essential enabler of AU member states' ability to do the following:

- Maintain their own self-determination in the information society, and keep abreast of rapid change
- Capitalise on technological innovation
- Create and sustain trust in a data-driven economy

To sustain trust in the data-driven economy, AU members must acknowledge the role personal data plays, and the economic forces it generates. When successful, the data-driven economy can create economic growth, deliver compelling and innovative services, and improve the quality of life.

However, the data-driven economy can also have a dark side, where personal data is handled in exploitative or abusive ways, and where the interests of the data subject are damaged. The cost and risk inherent in these cases sometimes only becomes apparent when things go wrong—when there is a data breach, or fraud is exposed. This can have a profound effect on trust and confidence in online services, and a corresponding impact on the data-driven economy. The Guidelines recommend steps to reduce the risk of these latter, unwelcome outcomes.

The expert group was mindful that, for some AU member states and policymakers, personal data protection may be a relatively unfamiliar domain, which can be a barrier to effective policymaking. The Guidelines aim to help empower member states in developing policy and laws on personal data protection. The recommendations are, therefore, accompanied by a number of enabling and sustaining measures, such as focused programmes of awareness-raising and education, for policymakers and individuals.

Finally, there is the risk of significant impact (on their citizens and economies) if AU member states do nothing. Accordingly, the Guidelines propose actions aimed at mitigating this risk.

Towards consistency with privacy principles applied in other regions

Principles identified in the Malabo Convention

Article 13 of the Convention identifies the following six principles relating to data protection:

- Consent and legitimacy
- Lawful and fair processing
- Purpose, relevance and retention of data
- Accuracy of data over its lifespan
- Transparency of processing
- Confidentiality and security of personal data

Similar sets of principles from other sources

A number of national and international privacy frameworks have largely converged to form a set of core, baseline data protection principles. These are implemented in national privacy frameworks in over 100 countries. Perhaps the three most prominent are the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines (non-binding, and last amended in 2013), the Council of Europe's Convention 108, which is binding to its 51 signatories[6] and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and last updated in 2015. These documents express similar privacy principles and are widely recognized as providing a solid foundation for online privacy policies and practices.

With minor variations, they form the basis of guidelines adopted by the United Nations General Assembly and the Commonwealth of Nations, and are broadly aligned with the European Union's General Data Protection Regulation 2016.

These are the focus areas of those privacy principles:

- **Collection limitation.** Personal data must be obtained and processed lawfully, fairly, and, to the extent possible, transparently.
- **Data quality.** Personal data must be accurate at the point of collection, and reasonable steps must be taken to ensure its accuracy is maintained over the period of retention.
- **Purpose specification.** Personal data must be collected only for specified, explicit, and legitimate purposes. Personal data should only be used for such other purposes as are compatible with applicable laws, such as archiving data that is in the public interest, or for scientific research.
- **Use limitation.** Personal data must not be disclosed, made available, or used for other purposes except with the consent of the individual or where authorised by law.
- **Security safeguards.** Personal data should be protected by reasonable security safeguards to maintain its integrity and confidentiality.
- **Openness.** There should be a general policy of openness about developments, practices, and policies with respect to personal data.

6 As at the date of publication of these Guidelines.

- **Individual participation.** Individuals must have the right to obtain information about their personal data held by others. This data must be provided within a reasonable period of time, in a form that is readily intelligible, and at a cost that is not excessive. Data subjects have the right to challenge their data and to have it amended if it is inaccurate, or erased if that is appropriate.
- **Accountability**. Those who collect and process personal data must be able to demonstrate their compliance with these principles.

The alignment with the six principles set out in Article 13 of the Convention is not exact, but there is a lot of commonality. Two areas of difference are, as follows:

- Article 13 of the Malabo Convention lists "Consent" as a separate principle, whereas in the OECD and Council of Europe frameworks, consent is included as a criterion of lawful processing.
- Articles 7 and 10 of the Council of Europe's Convention 108, Principle 14 of the OECD Privacy Guidelines and Paragraph 32 of the APEC Privacy Framework, express requirements relating to accountability of the data controller. Accountability is not explicit in the Malabo Convention's principles (Article 13) or in the Obligations of the Personal Data Controller (Articles 20-23). However, Articles 16-19 imply accountability on the part of the data controller, by expressing certain rights on the part of the data subject (accuracy of data, correction, deletion, etc.).

These variations are relatively minor, and they should not obscure the fact that there is far more commonality and alignment than divergence. Nevertheless, we suggest that AU member states give particular attention to accountability mechanisms for data controllers in their respective data protection frameworks, so that this important topic does not go unaddressed.

Existing regional and national frameworks in Africa

Research conducted by CIPESA for these guidelines identified the following African frameworks that reflect privacy and data protection principles similar to those listed above:

- SADC Model Law on Data Protection (2010)
- ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010)
- EAC Framework for Cyberlaws (2008)

According to the same research, the following countries have current or proposed legislation (at the time of writing of these Guidelines) that incorporates similar principles regarding the rights of data subjects and the establishment of data protection authorities: Angola (2016), Equatorial Guinea (2016), Mauritania (2017), South Africa (2013), Burkina Faso (2004), Mali (2013), Gabon (2011), Benin (2009), Ghana (2012), Ivory Coast (2013), Lesotho (2012), Madagascar (2014), Morocco (2009), Senegal (2008), Tunisia (2004), Zimbabwe (2003). The data privacy and protection bills of Kenya, Niger, Nigeria, Tanzania and Uganda also have similar provisions.

Themes by Stakeholder Group

This section of the Guidelines reflects the topics and issues raised during the consultation process and expert workshop.

They are grouped by stakeholder type, and within each stakeholder section, the themes are ordered according to the corresponding articles of the Convention. The aim of this section is to provide context and background information for the Recommendations given in the subsequent section.

Governments and Policymakers

Theme	Observations
Cross-border data flows and frameworks	Regulation that is commensurate with that in other jurisdictions contributes to mutual trust and lays a foundation for the trusted exchange of data, including (but not limited to) personal data. Personal data protection, therefore, an enabler of improved trust in the cross-border movement of persons, goods and services.
Harmonization (Malabo Convention, Preamble, Para. 20)	The Convention's Preamble refers to the desirability of harmonized cyber legislation. On the same principle, steps to increase consistency in data protection legislation among AU member states will help to reduce or mitigate asymmetries in privacy protection. Personal Data Protection strategies, policies and laws should seek to encompass the following areas: • Increased awareness of personal data protection obligations and rights • Policy goals and frameworks • Laws and data protection authorities; enforcement and penalties AU Member states will need to collaborate to achieve such consistency. The AUC's PRIDA initiative is expected to be an important enabler of such efforts.
Citizens' rights, and prerogatives of the State (Malabo Convention, Preamble and Art. 8)	The Convention reaffirms AU member states' commitment to respect for fundamental freedoms and human rights, and for the African Charter on Human and People's Rights. An important principle is to ensure that individuals enjoy equivalent rights both online and offline. Moreover, the Convention also refers to the prerogatives of the State, by which it is understood that the right to privacy is a qualified one, legitimately overridden, in some instances, in the interests of national security, law enforcement and public safety. This poses a governance challenge in terms of: • Setting consistent and workable conditions under which such exceptions from data protection law may be allowed; • Constructing a robust and reliable oversight regime to monitor the use of such exceptions, particularly in national security contexts, where access to relevant governance information may be constrained (for understandable reasons).

Asymmetry and reciprocity between the levels of protection provided by AU member states, and between African Union members and other entities (Malabo Convention, Art. 10.6.k)	It is likely that asymmetries in the level of data protection provided by AU members will exist, but their effects can be mitigated and/or reduced, by appropriate attention to governance, regulatory and enforcement measures, and economic factors. Article 10.6.k of the Convention mentions reciprocity arrangements for transfers of data outside the AU. Reciprocity is a key factor in reducing asymmetry in personal data protection. Consistent adequacy criteria (among member states) for the processing of personal data are an important mechanism for ensuring practical reciprocity in legal and enforcement measures. (However, this is just one approach. In the Asia-Pacific region, for example, rather than pursue adequacy decisions as the basis for cross-border transfers, APEC developed a voluntary accountability-based mechanism, known as the APEC Cross Border Privacy Rules system (CBPR system) and the APEC Privacy Recognition for Processors (PRP system.)

Data Controllers

Theme	Observations
Roles and obligations	Data controllers' behaviour is motivated by diverse factors (such as profitability, efficiency, social or community benefit) often depending primarily on whether the data controller operates in the commercial, public or non-profit sector, for instance. Their behaviour will also be constrained, in principle, by applicable law —but only if that law is effectively enforced. In this context, the law can usually only set a minimum threshold for acceptable data controller behaviour. Truly effective protection of privacy is likely to require data controllers to exceed the purely legal threshold and adopt best practices for data handling, such as participating in a certification scheme for personal data protection. This might be considered, under the Convention, as a data protection equivalent to the request (in Article 32) to develop harmonized codes of conduct in the cybersecurity domain.
Relationship of data controllers and data processors	In relation to personal data: • Data controller means a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed. • Data processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. As a general principle, the data controller does not lose any obligations when they pass personal data to a data processor to process on their behalf. The data processor also "inherits" the responsibilities of the data controller with respect to protecting the data passed to them, and the privacy of the data subject. However, for example, a data processor would not be responsible for responding to subject access requests (SARs) relating to the personal data passed to them: the data processor can legitimately refer such a request to the data controller. (SARs will be mentioned in more detail below, from the perspectives of the data controller and the data protection authority).

Consent (Article 13, Principle 1)	Getting consent for personal data processing presents ethical, legal and practical challenges. Well-meaning legislation can give data controllers a perverse incentive for solutions that undermine trust instead of reinforcing it. For example, the European Union introduced a "cookie law" that was intended to prevent websites from tracking users without their knowledge or consent, using small pieces of identifiable data (cookies) stored in the user's browser. Some websites responded by presenting a "take it or leave it" consent option that did not give users a meaningful choice. This may have obeyed the letter of the law, but failed to implement it in spirit. By and large, users did not get better privacy outcomes as a result. Solving the difficult problem of consent is likely to require a combination of legal and technical measures and, in some cases, a counter to the strong economic incentives service providers may have to "get around" the law. Personal data protection laws should be developed through a process that balances what is legally required with what is technically possible, and what best represents the interests of the individual being asked to give consent. In some data protection regulations, such as the Council of Europe's Convention 108, the requirement for consent is further constrained (for example, requiring that consent be informed, specific, revocable, and so on), each of these conditions will have implications that may require legal, technical and procedural measures to put into practice by the data controller. This problem, largely, still lacks definitive solutions, and member states are encouraged to stimulate multi-disciplinary investigation into better ways of addressing it.
Personal data flows between contexts, and its impact on privacy (Art. 13, Principle 2 - Fairness of processing)	Contextual integrity is important.[7] Personal data that is collected in one context and later used in another context without the awareness and consent of the individual breaches an individual's privacy (for example, personal data that is shared by a user to complete an online retail transaction, but is sold to an advertiser without the individual's knowledge). This notion of contextual integrity implies a duty on the data controller to be aware of the context in which data was collected, and to respect the integrity of that context. This is related to the privacy principle of "purpose of collection". As there are often powerful incentives for data controllers to transfer data from one context to another (for instance, to take customers' transactional data and sell it so that it can be used for targeted advertising), data protection policies must either ensure that this is never to the detriment of the data subject, or ensure that the data subject has the opportunity to express and enforce preferences about whether, when, or how this should happen. The transfer of data between different contexts is especially an issue when users are unaware that it is happening. For example, a child who is given a "connected" teddy bear may not understand that the bear links the private "home" context with a third party commercial context. Users of the Strava fitness tracker seem not to have realised that the device was making it possible to take location data from one context (such as an active military base) and make it public in another (searchable maps online). Since users often have little control over the subsequent use of data they disclose, much of the responsibility for appropriate use of data must fall on the data controller. Governments should encourage a culture of ethical or value-based design[8], ensuring that service providers are aware of the design choices that embed privacy and other ethical principles in the products and services that process personal data.
Data subject access requests (Malabo Convention, Articles 16-19), and their relation to accountability and transparency	Most current data protection laws also incorporate a principle of accountability, as defined, for example, in the OECD Privacy Guidelines. The OECD Guidelines also cite transparency as a key element of accountability. For data controllers, this implies (among others) an obligation to respond to requests from the data subject about what data is held about them. This, in turn, implies a requirement on policymakers to ensure that data subject access requests are addressed in a legal framework that ensures they are handled in a way that serves the data subject's legitimate interests, and does not impose obstacles on the data subject or undue burdens on the data controller.

7 "Privacy As Contextual Integrity" (Helen Nissenbaum, Washington Law Review, 2004)
8 See, for example, "Ethical IT Innovation" (Sarah Spiekermann, 2016)

Confidentiality of data processing, and appropriate measures to secure data (Articles 20-21, and Article 15 concerning linkability)	The Convention obliges data controllers to take appropriate measures to secure personal data, ensuring its confidentiality and integrity. "Appropriate measures" will include a range of technical, procedural and physical options. For example, paper records locked in a filing cabinet are protected by one form of access control; digital records behind strong authentication and authorization measures[9] have another form of protection; files that are encrypted yet another, and so on. Data controllers should be encouraged to apply industry-accepted best practice standards for data security. In that regard, many countries have adopted a risk-based approach, where the measures considered appropriate are evaluated in terms of the risk, likelihood and potential impact of a failure to protect the personal data in question. The three "classic" factors of security are all relevant in this context: confidentiality, integrity and availability. Data must be protected against unwanted disclosure, unwanted modification, and unwanted destruction/inaccessibility. Member states should refer to the corresponding cybersecurity guidance on these topics. Also under the cybersecurity heading, data controllers and, where necessary, data protection authorities should seek guidance concerning reliable security mechanisms (algorithms, key lengths and key management disciplines), at the national and international level. Examples of sources of such guidance, in other regions, are: • ENISA (European Union Agency for Network and Information Security) • NIST (United States, but widely referred to by other countries) • CESG (UK-specific guidance, for instance, to UK industry) Such guidance will help national authorities gauge, for example, the period for which a particular form of encryption should be considered a reliable protective mechanism for the purposes of Articles 20-21. Similarly, where pseudonymization and/or anonymization techniques are used as a means of protecting personal data against unwanted disclosure or use, their effectiveness should be monitored in light of advances in techniques for "re-identifying" supposedly anonymized or pseudonymized data. In addition to re-identification, two other threats to privacy should be considered in this context: inferences, and linkability. • Inference refers to the possibility of taking non-personal data and using it to derive personal assumptions or predictions, or of taking personal data and using it to derive sensitive personal data about someone. In other words, data that might not appear to be personal may in fact be, or may be used to infer data that is personal. Similarly, "normal" personal data might be the starting point for inferring sensitive personal data. Member states should review their data protection legislation to check that individuals or groups are protected against being singled out, or discriminated against, through the use of such derived or inferred data. • Linkability refers to the ability of data controllers or third parties to establish that personal data from different sources relates to the same individual. For example, that the call records for this telephone number relate to the same individual as the posts on that social media site. Data linkage of this kind can seriously erode the privacy and autonomy of the individual, by preventing them from maintaining discrete contexts in their online life. These are difficult areas in which to legislate successfully, particularly when technology relating to inference (artificial intelligence, algorithmic decision-making, and machine learning) is evolving so rapidly, and when it is so easy for data to be mined for the kinds of linkage described above. Accordingly, we recommend a multi-party approach to the problem, and a search for solutions based on the ability to combine regulatory, procedural, technical and educational measures as required. A risk-based approach is likely to deliver the best results.

9 Authentication is the process of validating that someone is who they claim to be, at the point where they try to access a service or resource. Authorization is the process of establishing that an authenticated user has the right to access the service or resource in question. Access control is the process of enforcing that right.

Retention periods (Malabo Convention, Art. 22)	Most current data protection laws incorporate a principle of setting limits on data retention. However, few data controllers put the principle into practice, and consequently much data is held for longer than required (sometimes indefinitely), putting data controllers at increased risk of a breach of personal data, and data subjects at risk of privacy violation. The regulatory and supervisory regime should not be based on the assumption that data will be deleted by default, so should include measures to encourage data minimisation and deletion, and ensure adherence to that principle.
Sustainability of access to data (Malabo Convention, Art. 23)	The data controller is obliged, under the Convention, to ensure that personal data remains technically accessible. In privacy terms, this will have a bearing on the data controller's ability to comply with the various requirements of Articles 16-19 of the Convention (rights to notification, access, correction, erasure, etc.). It may also be a factor in complying with Data Subject Access Requests (Article 17): Article 17 will fail to serve the interests of the data subject if data controllers are able to respond to data subject access requests in a manner or format which the data subject cannot use.

Data Protection Authorities

Theme	Observations
Elements of a governance regime (Articles 10-12)	Where stakeholders have a statutory role under privacy and personal data protection laws, compliance with statutory requirements must be subject to monitoring and enforcement; this relates directly to the Accountability data protection principle. Where stakeholders have contractual or standards-based obligations, it must be possible to audit their compliance, which implies the presence of qualified and capable assessors and auditors. These entities should therefore be added to the list of stakeholders, as follows: • Data Subjects, • Data Controllers of various kinds (identity provider, attribute provider, service provider), • Data Protection Authorities, • Conformance Assessors, • Compliance Auditors, and • Accreditation bodies for Assessors and Auditors. This also implies that data protection authorities have the power to investigate the processes for accreditation, assessment and audit, and penalise failures. Such a regime can form the basis for a certification scheme, to standardise and implement the data protection principles. A certification scheme could also cover related functions such as information security disciplines, which are vital to establishing what constitute "appropriate measures" under Articles 20-21 (and relevant to Articles 15 and 23). In the context of each member state, a certification scheme for these disciplines would allow regulations and guidance to be developed for: • Confidentiality, integrity and availability services for data processing. • Evaluation and selection of cryptographic algorithms, key lengths and key management procedures. • Gauging the relative strengths of different authentication mechanisms. • Protection of personal data through anonymization and pseudonymization. • Risk assessment criteria for re-identification of anonymized/pseudonymized data. • Risk assessment criteria relating to inference data and linkability. Certification can then form the basis for awarding a trustmark to stakeholders that meet the specified criteria, which, in turn, can help to inform and guide individuals about the trust decisions they make online.

Role and independence of DPAs (Article 11)	A data protection authority (DPA) may fail to meet its intended purpose if it can be subjected to undue political, administrative or commercial pressure. For example, if its staff are subject to arbitrary appointment/dismissal, if it is starved of the appropriate enforcement powers or resources, or if it is subjected to commercial lobbying or vexatious litigation.
Adequacy decisions (Article 12.2.k)	Effective DPAs are a key element of ensuring that cross-border data transfers happen in a framework of mutual trust and consistent standards (see also the Observations above, under Governments and Policymakers, relating to reciprocity).
Rights of data subjects (Articles 13, 16-19)	DPAs will have a key role to play in clarifying, communicating, monitoring and enforcing the rights of data subjects, as outlined in multiple articles/provisions of the Convention. Article 18: the right to object to processing. DPAs will bear some responsibility for agreeing on the legitimate grounds for such objections, and considerable responsibility for determining when it is practical and reasonable to exercise such a right (for example, at what point can it be assumed that a data subject has implicitly agreed to processing, and under what circumstances should an explicit request for consent be sought?). Article 19: the right to rectification/erasure. DPAs may be required to give guidance, for example, on the circumstances under which personal data can/may/must be deleted at the data subject's request, even if the data in question is true and accurate. For example, at what point might a data subject ask for personal data to be deleted on the grounds that the data controller no longer needs it—and if the data subject and data controller disagree on this point, who should resolve the disagreement? The right to erasure should be distinguished from the right to de-indexing (sometimes misleadingly referred to as the "right to be forgotten"[10]). De-indexing web content, in the privacy context, is a way to make certain data less readily accessible online. Under EU law[11], it has been used to require search engines to suppress the results of certain searches indexed on the name of the data subject. This does not prevent information from being published on the Web, nor does it guarantee that the information cannot be found. Among others, the ECOWAS Supplementary Act on Data Protection[12] contains broad provisions, which could be used to introduce a similar right.

10 "Hiding In Plain Sight" (Garstka, Erdos, University of Cambridge 2017) gives a thorough explanation of de-indexing vs. "right to be forgotten": https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043870

11 The "Google v Spain" Judgment, 2014 http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

12 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010)

Citizens and Civil Society (articles 8.1, 8.2)

Theme	Observations
Rights and corresponding responsibilities to learn and be informed	The bulk of practical responsibility to protect privacy can be seen to fall on data controllers and data protection authorities. This reflects the inherent asymmetry in the relationship between data subjects and the companies and public sector bodies that process their data. Data subjects have very little practical or technical ability to protect their personal data once it has been collected. However, individuals are stakeholders too, and not only in the sense of having things done to them or their personal data. Individuals cannot exercise rights of which they are unaware, and consumers cannot influence the market through their behaviour if they are insufficiently informed about the consumer choices they make. Individuals need to be empowered to be informed digital citizens/consumers, and to be aware, for example, of the bargain they enter into when they sign up for "free" services, or participate in social media platforms that monetize their data. Moreover, citizens also have a legitimate expectation that they can safely go about their normal business online—so legislators and supervisory authorities have a corresponding duty to ensure that citizens are not put at undue risk of harm by the use of ICTs and the digital economy. Asymmetries of power and information can represent a significant barrier in this regard, as they can: • Prevent consumer behaviour from exercising due influence on the market. • Mask the effects of exploitative or predatory business models. • Undermine trust in e-commerce and other online services. • Hinder Africa from reaping the benefits of digital transformation. The same kinds of asymmetry can also erode trust in the relationship between the citizen and public services. When such erosions of trust become systemic, whether in the commercial or public sectors, the hoped-for benefits of the digital economy cannot be realised. The kinds of trustmark and certification scheme described above, under "Elements of a governance regime", are an important part of creating and maintaining the trust relationship between individuals and online services.
Independent advice and capacity-building	Individuals need help and encouragement in their efforts to be better informed about personal data protection and its relevance to privacy. Civil society has a role to play in helping ensure that independent research, analysis, reports and advocacy are available, and that individuals are motivated to learn about, and protect their online privacy.
Representing stakeholder interests	Civil society organisations (CSOs) and the academic community have an important role to play, in the African context, in helping to ensure that privacy and data protection efforts are not hampered by the continent's size and diversity. In this regard, we encourage civil society organisations to convene at national and regional levels, taking advantage of existing regional groupings in the AU. Other groupings may also be of value, so as to represent more effectively the interests of particular stakeholder groups such as women and children, people with disabilities, those at particular risk of cyberbullying, and so on.

Independent advocacy	CSOs can perform a valuable service in providing independent assessments of the current state of data protection laws and privacy, including comparative analysis with other member states and other regions/continents. They also have a potential role in providing input to established processes such as the UN's Universal Peer Review. For civil society to be effective in this role, governments must also do their part to ensure that CSOs have a safe and constructive environment in which to work, with appropriate protection against harassment and interference.

Recommendations

Foundations: Privacy, Trust and Responsible Use

Privacy as a foundation for trust in the digital environment

Recommendation: We encourage AU member states, in their policy measures to ratify and implement the Malabo Convention provisions, to be explicit that the protection of online privacy and personal data is not only a fundamental right, but also a vital long-term process aimed at cultivating and sustaining trust in the use of ICTs, as a pre-requisite for the continued development of the Information Society in Africa. This is particularly important with regard to social factors such as ethnicity, vulnerability, disability and disadvantage.

Sustainable and responsible use of personal data in the data-driven economy

Recommendation: Governments and data protection authorities should monitor the data-driven economy for potentially damaging practices with regard to personal data, such as the following:

- Data collection and monetization practices that distort the market and result in lack of consumer choice.
- Data usage practices that give rise to unmanaged risk (for example, a small entrepreneurial company that accumulates far more data than it has the resources or skills to manage; or a large enterprise that consolidates mass quantities of data into a single, irresistible target).
- Predatory or exploitative business models that lack transparency and accountability about the collection and use of personal data.

Where possible, governments and data protection authorities should act to correct practices such as those described, while having due regard to the benefits of sustainable innovation, competition and business models. Effective enforcement of preventive measures is likely to require a mutually-agreed set of principles and rules to govern cross-border transfers of personal data.

Stakeholders: Governments and Policymakers

Greater consistency in personal data protection across Africa

Recommendation:

- Develop a consistent approach to: personal data protection policy and law; the establishment of regulatory authorities; and enforcement measures (this is described further below, under DATA PROTECTION AUTHORITIES).
- Develop common and consistent criteria for assessing adequacy in the level of personal data protection to enable cross-border transfers in the AU.

These are important factors in ensuring that there is reciprocity among member states in:

- The terms and conditions under which data controllers operate.
- The rights and conditions enjoyed by individuals with regard to the collection and use of personal data.
- The enforcement measures and legal remedies available to data subjects.

Member states should also take particular note of the AUC's PRIDA initiative as it evolves, ensuring they are well placed to take advantage of the opportunities it presents for collaborative work to harmonize policy and regulation in this area. [MC - Preamble p.3, and Article 10.6]

Respect for privacy online and offline

Recommendation: Member states must respect and protect individuals' rights to privacy online as well as offline. They should review their laws, procedures and practices, including those related to communications surveillance or interception, to ensure effective fulfilment of those obligations.

Exceptions to data protection and privacy laws

Recommendation: Member states should only permit exceptions to the application of privacy and personal data protection laws for matters of national sovereignty, national security or public safety, where it satisfies a legitimate aim, is necessary, proportionate and not arbitrary. Members should ensure any powers that are exempt from the application of privacy and personal data protection laws are subject to a robust, reliable and independent judicial supervisory regime that provides transparency and accountability. [MC - Preamble p.2, p.3]

Stakeholders: Data Controllers and Data Processors

Subject Access Requests (SARs) - Data Controller perspective

Recommendation: Data controllers must be obliged to respond to SARs in a manner or format that the data subject can process. Otherwise there is a risk that Article 17 will not serve the interests of the data subject.

Contribute to multi-party solutions

Recommendation: Where data protection problems require multi-party or coordinated solutions, data controllers should play their part in the processes of problem definition, consensus on available options, and implementation of solutions. This applies particularly to the areas described in more detail in the section below, on multi-stakeholder solutions:

- Best practice, codes of conduct and certification,
- Consent,
- Respect for contextual integrity,
- SARs responses,
- Confidentiality and integrity of personal data, and
- Retention periods.

Data Controllers should pay particular attention to advances in best practice—such as privacy by design and privacy by default. These are, among others, important factors in determining when not to collect or retain data.

The decisions to collect, process, or retain data typically follow on from a series of other design and implementation choices, which have been made throughout the product development process. Data Controllers should take advantage of the increasing amount of guidance on ethical or value-based system design to embed privacy-enhancing principles into their products from the earliest stages. This will reduce the subsequent cost of achieving compliance with data protection requirements, and give rise to a trust dividend from users.

Stakeholders: Data Protection Authorities

Role and independence of data protection authorities

An independent national data protection authority (DPA) is a vital element of the legal and institutional framework for building trust online, as envisaged by the Malabo Convention (Articles 10-12).

Recommendations: The post of DPA commissioner should be filled by appointment, have a limited term of appointment, and be subject to oversight by an advisory board representing stakeholders, including representatives of citizens (civil society), consumers (consumer organisations), commercial data controllers (chambers of commerce), academia and government, and where available, operators of personal data protection certification schemes (see Recommendation 9, below).

Member states should establish an independent DPA to ensure their national privacy and personal data protection laws are being observed. The DPA should have a clear mandate, powers and resources to be able to:

- Monitor compliance with, and enforce, applicable law on privacy and data protection.
- Facilitate the development of voluntary industry codes of conduct.
- Receive and address claims, petitions and complaints regarding the processing of personal data, and inform the authors of findings.
- Impose sanctions and remedies for contraventions of the law.
- Provide interpretation and, where necessary, authoritative administrative rulings on the application of laws.
- Assess the adequacy of protection for cross-border data transfers.
- Collaborate and exchange information, guidance and best practice experience with counterpart DPAs.
- Engage with other stakeholders (such as governments, data controllers, civil society) to develop regulatory guidance, trust frameworks, and enabling measures such as stakeholder education.
- Inform people and data controllers about their rights and obligations.
- Develop proposals to improve the legislative and regulatory framework for personal data processing.

In the interests of trust and transparency, member states should encourage or require DPAs, and other bodies with responsibility for monitoring privacy and personal data protection, to report publicly on their activities where appropriate.

Subject Access Requests (SARs) - DPA perspective

Recommendation: Member states should ensure that data protection authorities have the appropriate powers relating to Subject Access Requests (SARs), to complement the obligations described in Article 12(2) of the Convention.

- Where data subjects have a right to request copies of personal data from a data controller, data protection authorities (DPAs) must be capable of monitoring the outcomes of related legislation. DPAs must have powers to ensure that SARs are handled in a way that serves the data subject's legitimate interests, does not impose obstacles on the data subject (such as excessive fees, burdensome procedures, etc.), and does not result in undue burdens on the data controller.

Theme: Multi-Stakeholder Solutions

This section gives Recommendations in several areas where successful outcomes will depend on coordinated effort between stakeholders.

Best practice, codes of conduct and certification schemes

Recommendations:

- In pursuit of the multi-party goals described in this section, member states should convene multi-stakeholder forums including data protection authorities, data controllers and other stakeholders, to supplement the legal baseline with voluntary codes of conduct that implement best practices in privacy and personal data protection.
- Governments, industry and consumer bodies should consider introducing certification schemes to indicate that a product or service meets specific data protection criteria. For example, certification might signify that a data controller has been audited against best practice criteria for privacy by design, data security, or transparency in its terms and conditions.

Formation of an Africa-wide personal data protection committee

Recommendation: Establish an Africa-Wide committee, focused specifically on the theme of privacy and personal data protection, to facilitate coordination and information sharing among stakeholders, help identify privacy areas where resources are needed, and advise African Union policymakers on regional strategies and capacity building.

The Committee would be an evolving, compact, and trusted network of experts formed by the AUC in collaboration with the African Internet community. The Committee's leadership should be multi-stakeholder. It should draw on expertise from Africa-wide and national level organisations, and institutions such as the Regional Economic Communities (RECs), and include DPAs, business, representatives from academia, the technical community, and civil society. By structuring itself as a flexible, multi-stakeholder network, the Committee could ensure it is positioned to address emerging and future privacy challenges facing Africa.

The Committee could be tasked to advise and support the AUC in its privacy activities by:

- Advising the AUC on privacy and personal data protection issues and policies, such as capacity building initiatives;
- Being the long-term repository for best practice recommendations on privacy and personal data protection;
- Identifying areas of research needed for the formulation of general or sector-specific policies and guidelines, as new circumstances and requirements emerge;
- Identifying ways to support DPAs build capacity and share information at the regional and African Union level;
- Providing a trusted stakeholder forum for responsible and coordinated disclosure of data breaches;
- Proposing ways to increase the skills of privacy professionals in Africa (for example, as part of a certification program); and
- Helping the AUC formulate co-operative cross-border strategies for privacy and capacity building.

The work of the Committee should be coordinated with the Communication and Information Communications Technology (ICT) Specialized Technical Committee of the AU, through the auspices of the AUC. Details regarding its name, mission, vision, objectives, and detailed activities could be developed by the AUC in collaboration with the African Internet community.

In particular, we recommend this as a route to build trust through a certification system for personal data protection, based on the concepts outlined above, under "Elements of a governance regime". A concrete goal for such a Committee could be to create the trust

framework to put such a governance regime into practice. The framework would define roles for conformance assessors, compliance auditors and accreditation bodies. Those bodies, in turn, would be responsible for codifying criteria corresponding to each role in the governance regime.

- In the case of data controllers and data protection authorities, much of that codification will already be suggested by applicable legislation.
- In the case of accreditation bodies, or guidance concerning information security mechanisms, it may be necessary to identify or develop the relevant assessment criteria.
- In the case of the information security disciplines, member states should seek sources of qualified guidance, nationally, regionally and internationally if necessary.

Consent

Recommendations:

- Data protection authorities should engage with data controllers (for instance, through industry bodies) for a collaborative, multi-stakeholder approach to the problem of consent, so as to agree to a balance between technical measures (such as consent receipts), regulatory measures (such as cookie notices), and product design measures (such as user experience and controls).
- Where consent is legally qualified (for example, legal constraints specifying that consent should be informed, specific, freely-given, revocable, etc.), data protection authorities should convene a multi-stakeholder group including service providers, lawyers, civil society, designers and academia, to decide whether the legal requirements are best met by technical, regulatory or user-oriented measures, or combinations of these.

Purpose of collection

Recommendations:

- Data protection authorities must have the powers and resources needed to enforce the privacy principle of "purpose of collection", as stipulated in Article 13 of the Convention. However, effective implementation of the principle requires a collaborative solution and therefore a multi-party approach. That multi-party approach can and should draw on established principles of privacy by design and privacy by default— specifically in areas such as fairness of design decisions, data minimization, and respect for contextual integrity.
- Governments should ensure that data protection authorities have the resources to monitor and enforce the principle of "purpose of collection". Data protection authorities should issue guidance to vendors and service providers about the need for transparency and accountability with respect to this principle, as a foundation for consumer trust. If necessary, consumer protection legislation should be engaged to reinforce the data subject's rights in the digital environment.

Data retention periods

Recommendations:

- Data protection authorities should engage with data controllers (for instance, through industry bodies) together to agree how to put the principle of retention periods into practice. This is likely to require a combination of technical measures (such as the definition of metadata to record when personal data was collected and the period after which it should be deleted) and regulatory measures, such as an audit of data controllers' practice. [MC - Article 22]
- Such audit measures also imply that there is a resourced and capable body responsible for carrying out audits. The Convention calls for this to be the data protection authority. Governments may need to decide, in the context of the nation state, whether such audits are carried out on a statutory basis, a risk management- based approach, or under codes of conduct in specific regulated sectors (such as health care, financial services, etc.). [MC - Article 12(2)(g)] [MC - Article 17]

Theme: Wellbeing Of The Digital Citizen

Citizens' expectations and governments' duty of care

Recommendations:

- As noted above, under "citizens and civil society", individuals forfeit a good deal of control over their personal data once it has been disclosed. Data controllers therefore bear the bulk of responsibility for ensuring good practice and privacy-preserving outcomes.
- However, citizens should take advantage of the Internet and other sources of guidance to ensure they are properly informed about the risks and benefits of their activities in the digital economy and the connected environment, whether at home, at work or in public spaces.
- There is a corresponding role for governments, whether directly or indirectly, to empower individuals to exercise their rights to privacy, by helping to ensure citizens are informed and educated about how to exercise their rights under privacy and personal data protection law.
- Supervisory authorities and governments should take steps to ensure that online service providers and product vendors are sufficiently transparent about their business models and product capabilities, that individuals are in a position to make an informed choice about the privacy implications of products and services presented to them.

Civil Society Organisations (CSOs)

Recommendations:

- Member states should recognise and support the role of CSOs in:
  - Developing informative research, analysis, reports, tutorials and advocacy materials on privacy and personal data protection to help citizens understand and exercise their rights;
  - Researching the privacy and data security features of online applications and services to identify good and bad practices; and
  - Producing independent, objective and evidence-based reviews of the "state of privacy and data protection", as a monitoring function to protect and represent the interests of individuals.
- Member states are encouraged to see CSOs as partners in creating a safe, knowledgeable and capable population of 'digital citizens', and should ensure that CSOs have the appropriate framework and legal protections within which to contribute to this partnership.

Theme: Enabling and Sustaining Measures

Article 31 of the Ministerial Declaration (Addis Ababa, November 2017) calls on the AUC "to ensure the follow up of the signing and ratification by Member States" of the Malabo Convention.

Accordingly, we encourage member states to adopt the following approach, with a view to increasing the speed and confidence with which members are able to adopt and implement the measures called for by the Convention.

Recommendations: Policymakers should engage collaboratively with civil society, privacy advocates, business, academia and other stakeholders, to produce a range of accessible explanatory and training materials on the following topics. The goal of these materials would be to overcome the barriers represented by lack of awareness, knowledge and understanding.

- Fundamentals of digital privacy, and its risks and benefits
- Common and/or dominant business models for online services
- Advertising and data monetization in the data-driven economy

- Awareness of different cultures and expectations of privacy, in and beyond the African context
- Privacy by Design and the prospects for privacy-enhancing technologies
- Digital inclusion/exclusion and marginalised stakeholders
- Risks and harms that can arise from online activities and data-driven business models
- Implications of emerging technologies (data mining, machine learning and Artificial Intelligence; autonomous systems; Internet of Things, etc.)
- . . . And such other topics as they become relevant from time to time

These materials should form the basis of a programme of stakeholder round-table meetings—including policymaker participation—the purpose of which is to capitalise on the knowledge and awareness gained, and put it to immediate practical use in the form of renewed stakeholder engagement. The programme should have the following goals:

- Exchange information and build trust among policy, technical, legal, commercial, academic and civil society stakeholders;
- Increase policymakers' knowledge, awareness and confidence in new topics;
- Ensure that policymakers have the opportunity to put that knowledge to practical use with their stakeholder communities; and
- Give informed and interested stakeholders a voice in shaping the online future of their countries, regions and continent.

Members may wish to consider modelling such a program on the cybersecurity-related approach called for in Article 31 of the Addis Ababa Declaration (AU/CCICT-2), which envisages an annual cybersecurity conference and a continent-wide cybersecurity month.

For example, it may be productive to institute a regular schedule of:

- Publication of one of the training materials listed above,
- A period for reading and reflection, and
- A stakeholder round-table workshop to discuss the topic and agree on resulting actions.

These activities could culminate in an annual conference and a month of focus on data protection and online privacy.

About the Internet Society

The Internet Society (ISOC) supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that enable universal access.

Together, we focus on:

- Building and supporting the communities that make the Internet work;
- Advancing the development and application of Internet infrastructure, technologies, and open standards;
- Advocating for policy that is consistent with our view of the Internet.

About the Commission of the African Union

The African Union (AU) was officially launched in July 2002, following a decision in September 1999 by its predecessor, the Organisation of African Unity (OAU), which was formed in 1963, to create a new continental organisation to build on its work. A total of 54 countries joined the new organisation, whose headquarters remained in Addis Ababa, Ethiopia.

The Commission of the African Union (AUC) is the secretariat of the AU, entrusted with executive functions. It is composed of ten officials, a Chairperson, a Deputy Chairperson and eight Commissioners. This structure represents the AU and protects its interests under the auspices of the Assembly of Heads of States and Governments as well as the Executive Committee.

The AUC is responsible for the following portfolios: Peace and Security, Political Affairs, Trade and Industry, Infrastructure and Energy, Social Affairs, Rural Economy and Agriculture, Human Resources, Science and Technology, and Economic Affairs.

The guiding vision for Agenda 2063 is the AU Vision of: "An integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in the global arena". The mission of the AU Commission is "to become an efficient and value adding institution driving the Africa integration and development process in close collaboration with African Union Member States, the regional economic communities, and African citizens".