REPORT

GLOBAL

RECs: Towards a Continental Approach to Data Protection in Africa

Perspectives from Privacy and Data Protection Harmonization Efforts in Africa

Author: Mercy King'ori
Editor: Bianca Marcu

FUTURE OF PRIVACY FORUM

Acknowledgments

The author thanks Hunter Dorwart, Isabella Perera, and Alexander Thompson for their contributions to this report.

Table of Contents

RECs: Towards a Continental Approach to Data Protection in Africa

Perspectives from Privacy and Data Protection Harmonization Efforts in Africa

Author: Mercy King'ori, FPF

February, 2024

Introduction

On July 28, 2022, the African Union (AU) released its long-awaited African Union Data Policy Framework (DPF), which strives to advance the use of data for development and innovation, while safeguarding the interests of African countries. The DPF's vision is to unlock the potential of data for the benefit of Africans: "improve people's lives, safeguard collective interests, protect (digital) rights and drive equitable socio-economic development." One of the key mechanisms that the DPF seeks to leverage to achieve this vision is through harmonization of member states' digital data governance systems to create a single digital market for Africa through the integration and harmonization of data policies. It identifies a range of focus areas that would greatly benefit from harmonization, including data governance, personal information protection, e-commerce, and cybersecurity.

In order to promote cohesion and harmonization of data-related regulations across Africa, the DPF recommends leveraging existing regional institutions and associations that are already in existence to create unified policy frameworks for their member states. In particular, the framework emphasizes the role of Africa's eight Regional Economic Communities (RECs) to harmonize data policies and serve as a strong pillar for digital development by drafting model laws, supporting capacity building, and engaging in continental policy formulation.

Created through the 1991 Treaty Establishing the African Economic Community (Abuja Treaty), RECs have operated as Africa's flagship regional governmental authorities for economic and social development, including on harmonizing ICT related laws. Since 2005, when the first ICT policy (which already included elements of data protection policy) harmonization efforts began, one key competence of the RECs has been to create model data protection frameworks to prevent fragmentation of national laws and regulations.[1]

In 2008, the Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA) project was launched in Addis Ababa[2] to progress similar harmonization. In early 2010, four RECs—representing West, East,

[1] Harmonizing Cyberlaws and Regulations: The experience of the East African Community https://au.int/sites/default/files/newsevents/workingdocuments/27223-wd-harmonizing_cyberlaws_regulations_the_experience_of_eac1.pdf

[2] HIPSSA Launch Meeting https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/Launching-Meeting-HIPSSA.aspx

Southern, and Central Africa—adopted model data protection frameworks that vary in scope, applicability, and language. These frameworks exist within the larger structure of the AU, the body tasked with developing continental policy initiatives, such as the 2014 Convention on Cyber Security and Personal Data Protection (Malabo Convention), Africa's continental framework for data protection.

The RECs will continue to play a role in digital harmonization efforts in Africa as specified in the AU Data Policy Framework. Their broad similarities in areas including data protection principles, applicability, processing obligations, and data subject rights, indicate a common structure and evolutionary baseline through which further data protection developments have occurred in the continent.

This report aims to provide an overview of these regional and continental initiatives, seeking to better clarify the state of data protection harmonization in Africa and to educate practitioners about future harmonization efforts through the RECs. Section 1 begins by providing a brief history of policy harmonization in Africa before introducing the RECs and explaining their connection to digital regulation. Section 2 dives into the four regional data protection frameworks created by some of the RECs and identifies key similarities and differences between the instruments. Finally, the report analyzes regional developments in the context of the Malabo Convention through a comparative and critical analysis and, lastly, provides a roadmap for understanding future harmonization trends.

1. Harmonization in Africa - Introducing the Regional Economic Communities (RECS)

Harmonization is a key ingredient of policymaking in Africa within numerous sectors, including agriculture, finance, infrastructure, health, and technology. To this end, the AU has created committees in the form of Specialized Technical Committees (STCs) that oversee policy harmonization efforts in different sectors. The STC on Communication and Information Communications Technology oversees ICT policy and regulation harmonization in Africa. Harmonization here refers to the coordination of laws and regulations between African Union (AU) member states to promote uniformity of rules for stakeholders and to provide organizations with more predictability when operating in member states. Since the creation of the AU, which is the largest public body on the continent to emerge from the Organization of African Union (OAU), policymakers have prioritized harmonization of laws across Africa to spur economic integration and social development.

Creation of the RECs

In part, this prioritization emerged as the AU shifted its focus from supporting liberation from colonization and apartheid to spearheading Africa's development. African countries made significant strides toward this objective when they adopted the Abuja Treaty in 1991 and Agenda 2063 in 2015, a

50 year roadmap for achieving inclusive economic development across the continent. Both instruments call for the harmonization of policies in all areas of economic activity.

To accomplish this goal, the Abuja Treaty created eight Regional Economic Communities (RECs), which form the larger African Economic Community (AEC), and each involves member states that correspond to a particular region in Africa. These include the:

- Arab Maghreb Union (UMA)
- Common Market for Eastern and Southern Africa (COMESA)
- Community of Sahel–Saharan States (CEN–SAD)
- East African Community (EAC)
- Economic Community of Central African States (ECCAS)
- Economic Community of West African States (ECOWAS)
- Intergovernmental Authority on Development (IGAD)
- Southern African Development Community (SADC).

The RECs operate as regional, intergovernmental platforms to coordinate policy and promote uniformity of rules across participating member states. They also serve as fora through which countries may engage with each other. Within the RECs, the Abuja Treaty places *individual* and *collective* responsibility on member states to oversee the harmonization and eventual implementation of existing and new sectoral policies in their individual jurisdictions. This means that while the RECs operate as separate regional, inter-governmental institutions, national authorities must still transpose and enforce policy through their own administrative bodies.

Notably, the Abuja Treaty envisions harmonization through the RECs as the first step towards larger continental integration, which includes establishing an inter-REC Free Trade Area and Customs Union, eliminating tariff and non-tariff barriers, and eventually creating a Continental Customs Union, an African Common Market, and a Pan-African Monetary and Economic Union.

Harmonization in the Digital Economy

Traditionally, the RECs have predominantly cooperated in areas such as peace, security, development, and governance, as these are common areas where most member states face challenges. With the advent of information technologies and their increasing use in society, the scope of cooperation has expanded to include new areas. One such new area concerns how countries collectively navigate policy challenges brought on by technological advancement, spurring harmonization efforts around the

regulation of information and communication technologies (ICTs), telecommunications, electronic commerce, digital services, intellectual property, and cybersecurity.

With the support of entities such as the United Nations Conference on Trade and Development (UNCTAD), International Telecommunication Union (ITU), and the European Commission,[3] policymakers in four RECs created **regional data protection frameworks that aimed to guide member states in their adoption of national laws**. These frameworks include:

- The SADC Model Law (2012),[4]
- The EAC Cyberlaw Legal Framework (2008),[5]
- The ECCAS Model Law and the Economic and Monetary Community of Central Africa (CEMAC) Consumer Protection Directive (2013),[6] and
- The ECOWAS Supplementary Act on Personal Data Protection (2010).[7]

Owing to the absence of a formal right to privacy and data protection in the African Charter of Human and People's Rights, these four regional frameworks represent the earliest comprehensive push for regional data protection harmonization across the continent. Modeled heavily from the European Union (EU) Data Protection Directive 95/46/EC, the creation of the frameworks in part culminated in the AU's Convention on Cyber Security and Personal Data Protection (Malabo Convention) in 2014[8] and the Privacy and Personal Data Protection Guidelines for Africa,[9] both of which operate on the continental level and in theory offer a unified roadmap for data protection.

---

[3] Support for harmonization of the ICT Policies in Sub-Saharan Africa https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

[4] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[5] https://au.int/sites/default/files/newsevents/workingdocuments/27223-wd-harmonizing_cyberlaws_regulations_the_experience_of_eac1.pdf

[6] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/REGIONAL%20documents/projets_des_lois_types-directives_cybersecurite_CEEAC_CEMAC.pdf

[7] https://cyrilla.org/pt/entity/828sabbytwn?searchTerm=Protection%20from%20Online%20Falsehoodsand%20Manipulation%20Bill&page=2

[8] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

[9] https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

Additionally, as part of the continuum of policy harmonization, the AU created the Africa Continental Free Trade Agreement (AfCFTA) (the Agreement) in 2018 to promote intra-African trade through the elimination of tariff and non-tariff barriers. From a data perspective, trade in goods and services under AfCFTA is expected to be accompanied by an increase in cross-border data flows. To ensure effective implementation of the Agreement, one of the mandates of AfCFTA is to promote harmonization of appropriate policies.[10] One of the proposed protocols in the Agreement concerns digital services, which was adopted during the 37th AU Heads of State Summit in February, 2024. The Protocol continues to call for greater harmonization of digital services policies, including data protection. The RECs therefore provide an important window into the landscape of African data protection and the possibility of larger continental harmonization.

However, while there are similarities between the regional data protection frameworks, each of the RECs has proposed its own model law with key differences and nuances (see Section 2) and has done so for differing reasons. Some of the model laws explicitly recognize the need to protect privacy and fundamental rights in the digital age and ground their provisions in holding organizations accountable to individuals, while other models emphasize the role of a harmonized legal ecosystem to catalyze trade and innovation.

The differences in the regional data protection frameworks have also been compounded by the Malabo Convention, which shares broad similarities with the RECs but also varies in key ways (see Section 3). As a result of these differences between the RECs themselves and the Malabo Convention, member states have had multiple frameworks to choose from when fashioning their own data protection laws. This, in part, has contributed to a fragmentation of data protection frameworks across the continent, hampering regional and continental harmonization. The next sections delve more deeply into this by providing an analysis of the contents of the RECs model laws and the Malabo Convention as they pertain to regional harmonization.

2. Data Protection Harmonization through the RECs

Each of the REC data protection frameworks has its own history, with a combination of internal and external factors driving harmonization. Internally, efforts in some of the RECs, such as ECOWAS, began in 2008, when its members agreed to adopt data privacy laws. Externally, in the same year, the ITU adopted the Reference Framework for Harmonization of the Telecommunication and ICT Policies and

[10] Article 11(3)(e), AfCFTA

Regulation in Africa,[11] with funding from the EU, initiating a regulatory unification project - Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA). The project aimed to harmonize regulatory frameworks in sub-Saharan Africa across a range of sectors, centering data protection as one of three prongs in a "cybersecurity" package, which included electronic transactions and cybercrime.

HIPSSA involved participation from four RECs that would go on to create their own data protection frameworks (SADC, EAC, ECCAS, and ECOWAS). Deliberations through HIPSSA resulted in the drafting of model laws in the SADC and the ECCAS, which broadly overlap, save for some key differences in wording. Similarly, the creation of ECOWAS' data protection framework was directly influenced by the ITU and the EU's 2005 precursor to HIPSSA.[12] Conversely, developments in the EAC preceded HIPSSA. While the EAC REC participated in HIPSSA, its data protection framework differs in some aspects from the other model laws. The creation of EAC's data protection framework was led by UNCTAD, as discussed below. IGAD and UMA did not yet create harmonized data protection frameworks due to a nascent ICT industry at the time.[13] As a result, data protection frameworks in all four of the RECs differ in the type and scope of the instruments, their level of prescription, and their applicability.

- ECOWAS, the SADC, and the ECCAS have issued **model data protection laws.** The first is **mandatory** in theory while the latter two are **voluntary**. These model laws overlap in scope, principles, processing obligations, and data subject rights. In practice, ECOWAS has struggled to enforce its Supplementary Act across member states.

- The EAC, by contrast, has created a draft Bill of Rights enshrining the right to privacy and a **voluntary cyberlaw legal framework** that proposes recommendations for Internet regulation. The legal framework is not a model law and contains chapters that extend beyond the field of data protection.

- There is some, albeit little, consistency in how member states should **implement or enforce** data protection laws. Some instruments (like the Supplementary Act of ECOWAS) explicitly call for member states to establish data protection authorities, while others like the EAC Legal Framework call for governments to determine the structure of an authority that is suitable to

11 https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/presentations/AUC%20-%20Z.%20Bonkoungou%20-%20Reference%20Framework%20for%20Harmonization%20of%20ICT%20Policies%20EN.pdf

12 https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

13 See the SWOT Analysis done on these other regions https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/ICT%20Regulatory%20Harmonization.pdf

each country's conditions. Both the SADC and the ECCAS model laws contain a chapter on enforcement that broadly overlaps and shares commonalities with ECOWAS' law.

- Each of the instruments recognizes **common data protection principles,** such as lawful and fair processing, purpose limitation, and necessity. The model laws of ECOWAS, the SADC, and the ECCAS were inspired directly from HIPSSA and the EU Data Protection Directive. The EAC cyber framework, developed under a different initiative, also adopts similar principles.

- While the instruments broadly **overlap in definitions**, some add more detail and concepts than others. For instance, the SADC's model law defines personal data simply as any data related to a data subject, while those in ECOWAS and the ECCAS adopt a more detailed definition that includes the concept of direct or indirect identifiability. Likewise, ECOWAS' model law does not define "genetic data" or "child," while both the SADC and the ECCAS law contain such a definition.

- The instruments **differ in the obligations** they impose on data controllers, as well as the **scope of data subject rights**. The three model laws impose a broader panoply of processing and notification obligations and data subject rights, while the EAC legal framework contains minimum obligations for controllers to comply with principles of data protection, to provide data subjects with information held about them, and to provide mechanisms for correcting their personal data. The EAC proposes that member states rely on international best practices for further guidance. These model laws also contain requirements and exceptions for processing of **sensitive data**. Notably, ECOWAS prohibits the use of personal data for **direct marketing** without consent, while the SADC and ECCAS frameworks only give the data subject a right to object to direct marketing. EAC Framework is silent on direct marketing.

- Three model laws (ECOWAS, the SADC, and the ECCAS) explicitly impose **restrictions on transferring personal data** to countries that have not adopted an **adequate level of protection**. The SADC model law is broader than ECOWAS's Supplementary Act and the ECCAS's model law. The former's restriction applies also to SADC members, while ECOWAS and ECCAS restrictions **only apply to states outside** of the respective regional community. The EAC Framework does not have provisions on data transfers. In practice, member states and REC institutions have struggled to enforce these restrictions due to several reasons, such as not specifying legal processes for such transfers in detail.

The Economic Community of West African States (ECOWAS)

Image Source:

Established by the Treaty of Lagos in 1975, ECOWAS contains 15 members and aims to promote cooperation and economic integration in West Africa.[14] It adopted the **Supplementary Act A/SA.1/01/10 on Personal Data Protection** (Supplementary Act) in 2010, which subsequently became a core feature of the ECOWAS Treaty system, making violations of the Act enforceable against member states through the ECOWAS Court of Justice. The impetus of the Supplementary Act emerged in parallel with HIPSSA, but diverges from that process in that its data protection framework is binding, while the HIPSSA model laws are voluntary.

Influenced strongly by the EU Directive, the Supplementary Act contains 49 articles divided into eight chapters. The Act sets forth key objectives, data protection principles, obligations of processing, data subject rights, and provisions on cross-border data transfers.

[14] The member states include Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

- **Objectives** - The Act aims to protect privacy and promote the free flow of data, particularly in the context of the Internet, which the Act treats as a new technology that raises numerous challenges for regulators (Recitals 10 & 11). Notably, the Act identifies increased risks of online profiling and tracing of individuals, signaling the need for African states to align their data protection frameworks with the African Charter.
- **Scope** - The Act applies to any processing of personal data carried out in the REC and adopts the terminology of the EU Directive. Processing may occur through automated or non-automated means by individuals, government bodies, and private legal entities (Article 3(1)(2)).
    - The Act does not apply to household processing (Article 4);
    - Broad exceptions exist in the Act for processing carried out for public security, defense, investigation and prosecution of criminal offenses, or state security reasons (Article 3(4));
    - Additionally, the Act recognizes other exclusions for processing of personal data for journalistic, research, artistic, or literary purposes (Article 32).
- **Data Protection Principles** - The Act sets forth data protection principles commonly found in other data protection laws, including: legality and fairness of process, purpose limitation and necessity, accuracy, transparency, confidentiality, and accountability of processing.
- **Processing Obligations** - Processing is presumed lawful unless the controller violates an obligation or a principle defined under the law. The Act identifies specific processing activities that warrant additional scrutiny, such as the processing of sensitive personal data (Article 30), a prohibition against direct marketing (Article 34), and principles related to automated decision making (Article 35).
- **Data Subject Rights** - The Act recognizes the right to information, access, objection, rectification, and destruction. In relation to data subject rights, controllers must follow confidentiality, security, preservation, and durability when processing personal information (Article 38-41).
- **Enforcement** - The Act calls on each member state to establish its own data protection authority. Explicit powers of the authority include determining complaints, issuing codes of conduct, and imposing monetary sanctions and administrative penalties (Article 14).
- **Cross-Border Transfers** - The Act establishes an adequacy requirement for transfers of personal data to non-ECOWAS members (unless specific conditions are met) and an obligation for controllers to notify the DPA of such transfers (Article 36).

The Supplementary Act represents an attempt to promote regional harmonization by mandating the adoption of a consistent framework for data protection across ECOWAS member states. The Act closely resembles the EU Directive and explicitly recognizes the need to preserve privacy online and regulate the Internet. However, as an institution, ECOWAS has struggled to enforce its acts across all member states and has not updated the Act since its initial adoption in 2010. More than half of the member

states in ECOWAS have since passed their own national data protection laws with Nigeria being the latest country and reserved authority outside of the regional framework, which has hampered regional harmonization in West Africa.[15]

The Southern Africa Development Community (SADC)

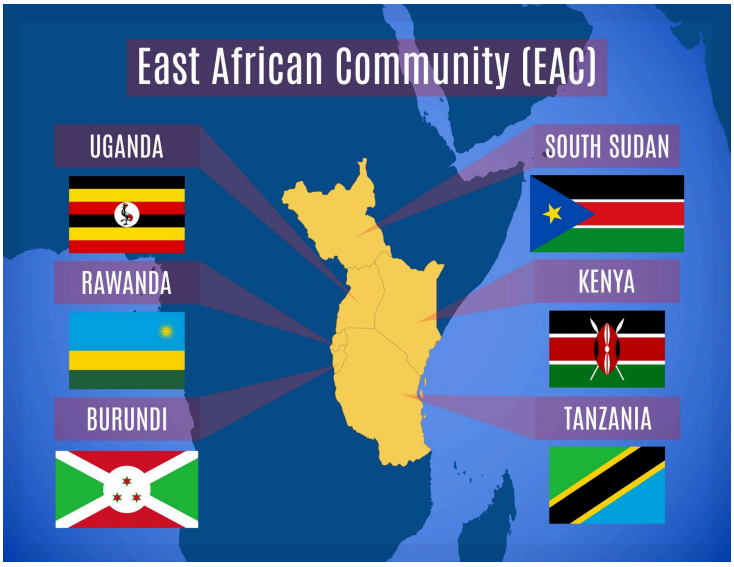
The Southern Africa Development Community (SADC) consists of fifteen countries and emerged from the Southern African Development Coordination Conference (SADCC) in 1992. The SADC initially strove to liberate Southern African countries but has since focused on promoting economic development, alleviating poverty, strengthening regional integration, and harmonizing political values and institutions. In 2012, the body proposed a **Data Protection Model Law** that was developed under HIPSSA, which strives to harmonize data protection policies among member states.

[15] West African countries with data protection laws: Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, Ghana, Guinea, Mali, Niger, Nigeria, Senegal and Togo

- **Scope** - The Model Law applies to both automatic and non-automatic processing of personal data by private and public data controllers permanently established in a member state. If the controllers are not permanently established, the Law applies when the means of processing are not solely for the purpose of transmitting the data through a given country (Article 2).
- **Exceptions** - The Model Law recognizes the right of member states to limit the obligations of the law in certain circumstances. These include where necessary to preserve state security, defense, public safety, and investigation or prosecution. Additionally, exceptions exist for processing in matters of literary, artistic, or journalistic expression (Article 42).
- **Data Protection Principles** - Controllers must follow the principles of fair and lawful processing, purpose limitation, legitimacy, sensitivity, data quality, security, openness, and accountability (Articles 12-15, 24, 29-30). However, the SADC model law does not contain a standalone chapter or section outlining these principles.
- **Obligations** - The Model Law imposes numerous obligations on controllers for processing, such as notifying data subjects of the conditions of processing (Article 21), maintaining confidentiality and security (Article 24), and obtaining authorization from the data protection authority for key processing activities (Article 28). Additionally, controllers must designate a representative in a SADC member state in certain circumstances (Article 2(3)).
- **Data Subject Rights** - The Model Law proposes the following data subject rights: access, rectification, deletion, temporary limitation of access, and right of objection (Part VII).
- **Cross-Border Transfers** - The Model Law prohibits the transfer of personal data to both non-SADC and SADC members that have not adopted the Model Law, unless specific conditions are met.

Like with ECOWAS, the SADC has struggled to ensure that member states implement consistent and similar frameworks, although some states, such as South Africa, looked to the model law when formulating their own data protection regulations.

The East African Community (EAC)



The East African Community (EAC) came into force in 1999 under the EAC Treaty with the aim to, among other issues, foster development among its member states.[16] During a regional e-government framework consultative meeting in 2005, stakeholders decided that regional e-government and e-commerce initiatives would be necessary to aid development in the region.

To this end, the EAC Council of Ministers adopted the EAC Regional E-government program in 2006. One of the identified prerequisites of successful regional e-government and e-commerce initiatives was harmonized legal and regulatory frameworks at national and regional levels. The EAC Taskforce on Cyber Laws was subsequently created in December 2007 to oversee the legal reform process at a time when member states were at different stages of developing their national ICT related legal frameworks. At the time, 3 out of the 5 EAC member states had drafted Bills including Kenya, Uganda and Rwanda. Burundi and Tanzania did not have any drafts.

The Taskforce held 3 meetings in 2008 that saw discussions on developing a framework for harmonization take center stage. In the first meeting held in January 2008, the Taskforce recommended that member states conduct a comparative review of existing laws and Bills to ensure harmonization and that any reform processes be coordinated among members. This would have identified areas of divergence in the laws and Bills of member states. The efforts culminated in the adoption of Phase 1 of

[16] These include Kenya, Uganda, South Sudan, Tanzania, Rwanda, Burundi, Democratic Republic of Congo (not pictured) and Somalia (not pictured).

the Cyber Law Framework[17] in May 2010, which included provisions for data protection and privacy (Part 5 of the Framework). However, the framework explicitly acknowledged it is not a model law and did not include detailed provisions in recognition of the existing national legislative efforts at the time.

Further, in 2012, the East African Legislative Assembly (EALA), EAC's main legislative body, adopted a Bill of Rights: the chapter on privacy outlines the right of individuals to not have their person, home, or communications unlawfully searched (Article 7). Measuring the impact of the Bill on the national situations in each member state remains challenging because constitutional debates in each country have proceeded on their own terms and in their own contexts.

The EAC **Legal Framework for Cyber Laws** contains provisions on a range of matters outside of traditional data protection law, including electronic transactions, authentication, consumer protection, computer crime, intellectual property, and taxation. As a voluntary framework, it proposes recommendations for member states to create a consistent legal framework for cyber-related fields. The Legal Framework contains some notable provisions on data protection.

- **Objectives** - The Framework seeks to harmonize ICT and Internet policies and regulations in the EAC. It recognizes the importance of data protection, the need to ensure privacy on the Internet, and the need for member states to align their laws with international best practices. However, it does not specify such best practices.
- **Scope** - The Framework proposes that data protection legislation focuses on individuals as data subjects. Implementation of the data protection obligations rests on both the private and public sectors.
- **Data Protection Principles** - The Framework recommends that member states require controllers to comply with principles of good practice, including accountability, transparency, fair and lawful processing, purpose limitation, data accuracy, and data security.
- **Data Subject Rights (Notification and Correction)** - The Framework also recommends that controllers supply data subjects with a copy of any processed personal data and provide them with a chance to correct inaccurate data.

However, the Framework suffers from some notable limitations. First, it recognizes that member states **should take into account the costs** of implementing data protection laws before instituting broad obligations on processing, acknowledging the limitations of establishing a data protection authority to enforce the law without adequate resources. Second, while it advocates for member states to align their

17 http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq

laws with international best practices, the Framework **does not identify such practices**, leaving member states to select best practices themselves and **undermining regulatory harmonization and unity**. Thirdly, it is a voluntary framework, making it clear that the framework acts as a set of "recommendations" to member states. As a voluntary framework, it is difficult to determine the scope of its influence on the development of data protection law in the East African region. Some countries such as Kenya and Uganda had initiated data protection and privacy reforms before the adoption of the Framework. Even for EAC member states which are in the process of enacting legal frameworks with data protection provisions, the influence of the Framework is unclear.

The Economic Community of Central African States (ECCAS)

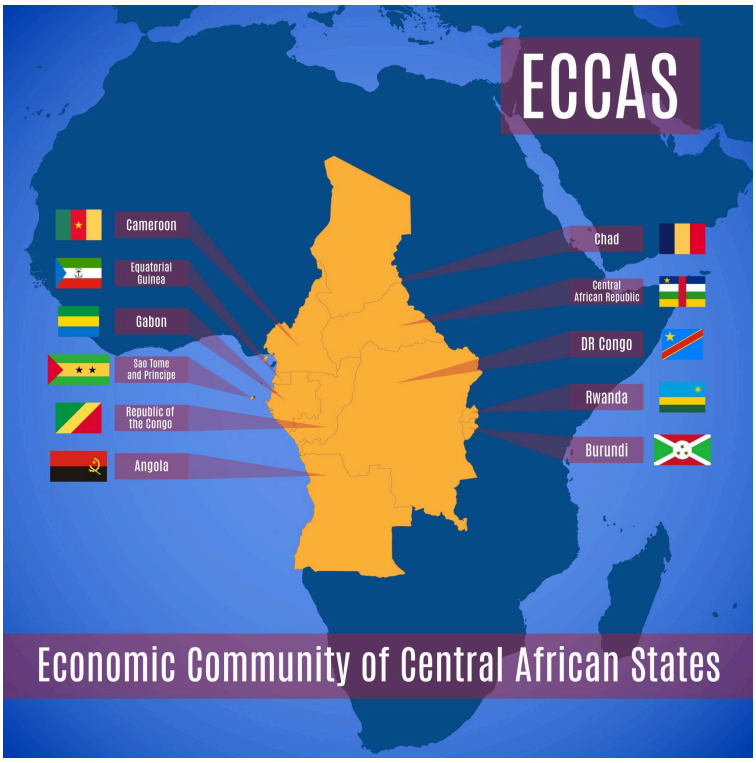


Image Source:

The Economic Community of Central African States (ECCAS) has also undertaken various data protection initiatives. The regional community introduced a model personal information protection law in

2013 as part of a three-part package covering data protection, e-commerce, and cybercrime.[18] The data protection model law contains similar wording as its SADC counterpart and adopts similar provisions (see above). For this reason, this report will not provide an extensive overview as it did for the SADC model law. Instead, it will highlight some key differences, which include:

- **Processing of Sensitive Personal Data** - Unlike the SADC Model Law that requires a national supervisory authority to specify situations when limitations to such processing cannot be lifted, even with a data subject's consent, the ECCAS model law does not make this specification.
- **Cross-Border Transfers** - The model law contains three articles on cross-border data transfers and restricts the transfer of personal data to non-ECCAS members unless the recipient jurisdiction can ensure an adequate level of protection compared to the ECCAS model law, or when the data controller offers sufficient guarantees for protection. This is different from the SADC, which imposes a similar requirement on transfers *within* SADC member states.

3. The Relationship of the RECs to Other Harmonization Efforts - The Malabo Convention

While each REC has attempted to harmonize data protection law across applicable member states, other initiatives at the continental level also contribute to the harmonization efforts. A notable example is the African Union Convention on Cybersecurity and Personal Data Protection ("Malabo Convention"), adopted in 2014. The Malabo Convention came into effect in June 2023 and represents the culmination of a multi-year legislative process initiated in 2009 to establish a harmonized framework for data protection, electronic transactions, and cybercrime. Nineteen countries have signed the Convention.[19]

Notably, the RECs played an instrumental role in drafting the Convention. Efforts at the AU level to promote harmonization directly influenced the creation of the regional frameworks in ECOWAS, the ECCAS, and the SADC.[20] All three of these bodies actively participated in regional expert groups leading up to the adoption of the Convention, which seems to be directly inspired by the HIPSSA project. The EAC was targeted in this process, but the role it played in the drafting of the Malabo convention is unclear.

---

18 https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/REGIONAL%20documents/projets_des_lois_types-directives_cybersecurite_CEEAC_CEMAC.pdf

19 Benin, Cameroon, Chad, Comoros, Congo, Djibouti, Gambia, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, South Africa, Sierra Leone, Sao Tome & Principe, Sudan, Togo and Tunisia

20 https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/itu-j-f_le_bihan-presentation_general_du_projet-en.pdf

Data protection harmonization through the RECs thus must be contextualized against this larger continental trend. On the one hand, the RECs played an important role in the development of the Convention, engaging in regional workshops as institutional participants. Such participation created space for harmonization of data protection policies, while also generating fragmentation as the RECs have adopted their own frameworks with small but significant differences. On the other hand, the RECs will likely operate as a central fulcrum through which additional larger continental policies will be implemented and enforced. This is visible in the 2020 Southern African Development Community Parliamentary Forum's efforts to create a regional model law that responds to the concerns of the 21st century.[21] In the absence of a centralized enforcement mechanism, RECs may continue to monitor and coordinate the implementation of data protection laws among member states, a role stressed in the 2022 AU Data Policy Framework.

This section provides an analysis of the relationship between the RECs and the Malabo Convention. Efforts to formulate regional data protection frameworks occurred simultaneously with those at the continental level. As a result, there is significant overlap between the Malabo Convention and the various RECs instruments. However, there are also notable shortcomings of the Convention that have hindered harmonization. As a result, the RECs will likely continue to mediate between national authorities and inter-governmental bodies like the AU on data protection matters (acknowledging that the Malabo Convention is currently under review[22]).

Areas of convergence

There is broad overlap between the Malabo Convention and some of the regional frameworks on data protection, both in terms of the objectives of the framework and the underlying provisions and structure of the instruments. These areas notably include:

- **Objectives** - The Malabo Convention grounds its data protection chapter on upholding and respecting **fundamental rights** and freedoms, including the **protection of physical data and privacy**. This resonates with ECOWAS' Supplementary Act which explicitly recognizes upholding fundamental rights as a key objective of the framework. Protection of fundamental rights is also specified under the SADC and ECCAS Model Laws.

[21] https://researchictafrica.net/wp/wp-content/uploads/2020/11/digital-economy-report_04.pdf

[22] https://au.int/en/bids/20220617/consultancy-services-review-malabo-convention-cyber-security-and-personal-data

- **Definitions** - With the exception of the EAC, which does not provide definitions, there is broad overlap between many key concepts of the Convention and the RECs frameworks, such as **personal data, data processing, controllers and processors, and sensitive data**. While there are notable differences between some of the definitions when compared with each regional framework, each definition of the Malabo Convention is similar to at least one of those contained in a RECs instrument.

- **Data Protection Principles -** The Malabo Convention provides for seven data protection principles that converge with those found in the RECs. These include: consent and legitimacy; lawfulness and fairness; purpose, relevance, and preservation; accuracy; transparency; and confidentiality and security. The actual wording of the principles resembles the model law in ECOWAS most closely.

- **Processing Obligations** - The Convention sets forth processing obligations that mirror those found in other RECs instruments. Different lawful grounds for processing of personal data may be found throughout the frameworks, including consent, compliance with legal obligations, and protection of vital interests of data subjects among others. Controllers must also not violate any of the core principles when processing data. The Convention also imposes similar **security and accountability obligations**, as well as requirements and exceptions when processing **sensitive data**. Notably, the Malabo Convention **prohibits direct marketing** without prior consent, much like the ECOWAS model law, but it contains this provision in the chapter governing electronic transactions, rather than data protection law.

- **Data Subject Rights** - There is broad overlap in the data subject rights under the Malabo Convention and the RECs instruments. These include (i) information, (ii) access, (iii) objection, and (iv) rectification and erasure.

Shortcomings and Limitations

Despite areas of broad overlap, there are key limitations and shortcomings of the Convention that have hindered harmonization and prevented effective personal data protection throughout the continent. Some of these limitations have resulted from differences between the Convention and regional instruments. For instance, some regional frameworks like the SADC and ECCAS model laws have set forth definitions and processing obligations around biometric data that are not mirrored in the Convention. This has left national policymakers who must implement their own laws with decisions about which aspects to include, creating uncertain and confusing variation between national legislation, regional frameworks, and the continental Convention. For example, Zambia's Data Protection Act, 2021

includes a definition of biometric data, while Ghana's Data Protection Act, 2018 does not include the definition.

Other limitations arise from shortcomings in the Convention itself, as well as the institutional structure through which it operates. These include:

- **Absence of crucial definitions such as biometric data and profiling** - Despite the growing number of digital identity (ID) systems in the continent that rely on biometric data, the Malabo Convention does not define the term. Consequently, countries must look to other existing data protection regimes for an interoperable definition. For instance, Mauritius and Zambia have adopted the definition of biometric data from the GDPR. Additionally, the Convention does not define profiling, which creates space for fragmentation of national and regional frameworks, especially as more sophisticated financial services technologies come into play.

- **No harmonized mechanism for data transfers between member states** - While the Convention prohibits the flow of data outside AU territories without adequate protection, it has no similar requirement for protection between member states, though not all countries have adopted national data protection laws. To be sure, this approach could be justified on the grounds that at the time of adoption, restrictions of data flows could hamper attempts to create common data transfer practices among countries.

- **Lack of a continental enforcement mechanism -** The Malabo Convention leaves individual member states to develop their own data protection authorities (DPAs). This may hinder harmonization because some AU countries have yet to create DPAs, while others have yet to become operational. However, collaboration between national DPAs has increased in recent years, most notably through the Network of African Data Protection Authorities (NADPA), which is a forum for African DPAs to coordinate enforcement and support the adoption and implementation of data protection laws. Despite the possibility of collaboration among countries as proposed in national laws, the lack of a continental enforcement mechanism has hampered harmonization.

- **Weak judicial authority** - While the Convention does not bind AU members under a single enforcement mechanism, the African Court on Human and Peoples' Rights, established by the Banjul Charter, may in theory enforce the human rights provisions in the Convention concerning privacy. However, this court does not have automatic jurisdiction over member states, as states must ratify the protocol establishing the court and are free to withdraw from it. Moreover, even if a member state accedes to the court's jurisdiction, there is no guarantee it will follow a decision

since there are few material consequences for ignoring a ruling. The result is a lack of uniformity in judgments related to privacy and data protection. The Convention likewise does not establish an independent African body tasked with ensuring consistent application of its data protection provisions or encouraging member states to adopt the Convention in whole. There is little legal certainty of what would happen in the event of a conflict between the Convention and a regional framework, such as ECOWAS' Supplementary Act. National states would likely prioritize their own authority.

- **Deference to member states** - The Convention explicitly recognizes the prerogative of member states in its preamble to establish and defer to their own data protection regulations. This deference is particularly acute in matters of enforcement. For instance, Article 11(3), 12(2)(h), and 12(2)(i) grant member states the ability to determine the composition of national DPAs, the scope of administrative and monetary penalties, and the parameters of a publicly available directory containing information regarding data processing in the country. Such deference may result in fragmented procedures and enforcement of data protection standards across Africa.

Harmonization is a work in progress, as there are notable discrepancies in the data protection initiatives at the continental, regional, and national levels. Since the early 2010s, numerous countries in Africa have adopted their own national laws with varying requirements, goals, and administrative contexts. These instruments have differed from the RECs frameworks and the Malabo Convention in key ways, often reflecting not only limitations in the regional model laws themselves but also the inability of the RECs to ensure implementation or persuade member states to adopt consistent approaches to data protection. The regional frameworks have not been updated since their creation. Additionally, changes in technology and the global data protection landscape in the past decade have further complicated harmonization, as some member states have turned to new tools, such as data localization, to pursue their own national interests.

4. Conclusion

Harmonization of digital policies has been a key feature and objective of African data protection for the last few decades. In coordination with the HIPSSA project in the late 2000s, the AU began prioritizing the creation of harmonized frameworks for data protection through the RECs, which also saw the release of the Malabo Convention in 2014. Four RECs – ECOWAS, the SADC, the EAC, and the ECCAS – have released their own frameworks, including one mandatory law, two voluntary model regulations, and a non-binding cyber framework. Each of these instruments was released between 2008 and 2014, signaling the interwoven process of HIPSSA, the AU, and the RECs on harmonization. The goal of each

project involved creating a standard set of laws and regulations that member states would adhere to and enforce within their own national jurisdictions.

However, harmonization of regional and continental data protection policies in Africa has faced notable barriers. Beyond one country having multiple frameworks upon which it can model its national laws, across the RECs' frameworks, there are differences in language, applicability, and enforcement structure that have hindered uniformity across regions, despite shared similarities between some of the regional instruments. On the continental level, the RECs vary in relation to the Malabo convention, which diverges in some key ways. As a result, member states, which are at varying levels of economic and regulatory development, have a panoply of frameworks and provisions to choose from, some of which may not make sense in certain national contexts. Adoption has thus far not been consistent or uniform across jurisdictions and regions.

Additionally, institutional limitations have frustrated the ability of both the continental authority (the AU) and the regional authorities (the RECs) to transpose and enforce their model frameworks among member states. The lack of a centralized judicial authority on the AU level for data protection has complicated enforcement-related provisions, as national governments have discretion in implementing and monitoring their own frameworks. While some of the RECs have enforcement powers under their own treaty systems (e.g., ECOWAS), they may lack capacity to ensure consistent implementation.

All of this has transpired while national governments have proposed and adopted their own national frameworks, which vary from country to country, and which may not always align with either the RECs frameworks or the Malabo Convention. Since the adoption of the RECs frameworks in the early 2010s, data protection laws across the continent have increased rapidly. Now that more than 35 countries have formal regulations on the books, policymakers have yet to update or modify the regional or continental instruments. This illustrates that national governments are increasingly becoming the locus where data protection developments move forward.

Despite these barriers, stakeholders should recognize the value of the RECs in promoting uniform data protection standards and their potential role for further regional and continental developments in the future. The creation of the REC model laws in many ways set the stage for and inspired national authorities to engage in their own data protection deliberations. While national data protection laws vary, many of them share core similarities in principles and structure, even if the overarching objectives and key motivation for adopting the policies vary depending on local conditions.

Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org