



African Forum on Cybercrime

October 16-18, 2018

African Union Commission

***African Union Convention on Cybersecurity and
Personal Data Protection***

“Malabo Convention”





Ministers in charge of communications and Information technologies adopted a declaration [EXT/CITMC/MIN/Decl. (I)] (Olivier Tambo Declaration) in 2009 in which they " requested the African Union Commission to develop jointly with the United Nations Economic Commission for Africa, a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection".

This Declaration has been endorsed by the 14th AU Summit of Head of State and government in 2010 [Assembly/AU/11(XIV)] and confirmed again by the third ordinary conference of Ministers in charge of ICT held in Abuja in August 2010 in their declaration ([AU/CITMC/MIN/Decl.(III)].





The AU convention objective is setting the essential rules for establishing a credible digital environment (cyber space) and address the gaps affecting the regulation and legal recognition of electronic communications and electronic signature; as well as the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems and privacy online.

The convention aims also to set up a minimum standards and procedures to reach a common approach on the security issues in Africa and Address the need for harmonized legislations necessary to enhance cooperation in the area of cyber security in Member States of the African Union.





- ❑ A draft Convention on Cyber Security has been developed (2010-11)
- ❑ Regional Workshops have been organized on Cyber Legislation and on the AU Draft Convention on Cyber Security:
 - **ECCAS**: Libreville, Gabon, November 2011
 - **ECOWAS**: Abidjan, Côte d'Ivoire, February 2012
 - Tripartite [**COMESA, SADC, CEAC**] + **UMA** (Northern Africa): Addis-Ababa, Ethiopia , June 2012
- ❑ Final Expert Group meeting to finalize the Draft Convention before the CITMC-4 Addis- Ababa, Ethiopia, August 2012
- ❑ Endorsement of the AU Final Draft Convention on Cyber legislation by the 4th Ministerial Conference of the African Union Ministers in charge of Communication and Information Technologies (CITMC-4).
- ❑ Adoption of the convention by the Conference of Ministers in charge Justice and Legal Affairs
- ❑ **The African Union Convention on Cyber security and personal data protection has been adopted by the 23rd Assembly of Heads of States and Governments held in Malabo , Equatorial Guinea in June 2014 .**





The AU Convention main parts

PART I: ORGANIZATION OF ELECTRONIC COMMERCE

PART II: PROTECTION OF PERSONAL DATA

PART III: PROMOTING CYBER SECURITY AND COMBATING CYBER CRIME

PART IV: COMMON AND FINAL PROVISIONS

Available on: <https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>





PART I: Electronic Transactions

Section I : Electronic Commerce

Section II: Contractual Obligation in Electronic Form

Section III : Security of Electronic Transactions



PART II: Personal Data Protection

Section I : Personal Data Protection

Section II : Institutional framework for the protection of personal data

-

Section III : Obligation relating to conditions governing personal data processing

Section IV : The Data Subject Rights

Section V : Obligation of personal data controller





PART III: PROMOTING CYBER SECURITY AND COMBATING CYBER CRIME

Section I : Cyber Security Measures to be taken at National Level.

Chapter 1: National cyber security framework

Chapter 2: Legislative measures

Chapter 3 : National cyber security system

Chapter 4 : National cyber security monitoring structures

Chapter 5 : International cooperation

- Harmonization
- Mutual assistance
- Exchange of information
- Means of cooperation





Section II: Criminal Provisions

Chapter I: Adapting certain ICTs offenses

Chapter II: Adapting certain sanctions to the ICTs

Chapter III : Offenses specific to ICTs

- Attack on computer systems
- Attack on computerized data
- Offenses relating to electronic message security measures.
- Content related offenses / definition of cyber threats against children





Signature, Ratification and Entry into Force

- ❑ This Convention is open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures.
- ❑ This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.
- ❑ Upon entry into force of this Convention, the Chairperson of the Commission shall register it with the Secretary General of the United Nations, in accordance with Article 102 of the Charter of the United Nations.
- ❑ **Senegal, Guinea , Mauritius and Ghana** have ratified the Malabo Convention and so far nine (09) Countries have already signed : **Benin, Tchad, Comoros , Congo, Guinée Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia.**





The implementation of Malabo Convention covers notably the following areas:

- Ratification of the AU Cybersecurity Convention by at least 15 countries .
- Transposition of the Convention's provision into National and Regional Cyber legislations
- Assist MS to develop National cyber-security strategies, in line with international standards and practices , and support the creation of national governance for Cyber-security;
- Support Human and Institutional Capacity Building on Cybersecurity and Cybercrime. Conduct Capacity building for policy makers/legislators, law enforcement technical and business communities;
- Development of technical capabilities to monitor and defend national networks such as setting up National and Regional Computer Emergency Readiness Team (CERTs /CIRTs)





- ❑ Considerable progress has been made in developing regional model legislation in the area of Cyber Security , notably related to data protection, e-transactions and cybercrime (**ECOWAS Cybersecurity guidelines, ECCAS Model Law/CEMAC Directives on Cybersecurity, SADC Model Law on data protection, e-transactions and cybercrime**).
- ❑ African Union Commission in collaboration with Internet Society (ISOC) developed guidelines on the Internet Infrastructure Security in Africa <https://isoc.box.com/s/f708wcbt9rm8ho6skxz1azy5wjxqp2s2>
- ❑ African Union Commission in collaboration with Internet Society (ISOC) developed Personal Data Protection Guidelines for Africa.

https://www.internetsociety.org/wp.../05/AUCPrivacyGuidelines_2018508_EN.pdf





- ❑ Given the international nature of cybercrime in general which constitutes a real threat to the development of the Information Society in Africa. There is need to implement the AU convention on cybersecurity and define the broad guidelines of an African Strategy for the security of Cyberspace and repression of cybercrime in Member States of the African Union, taking into account the existing commitments at sub-Regional, Regional and International levels and the international Best practices .
- ❑ Considering the multiple dimensions and complexity of Cyber security , The African Union believes that by creating an appropriate legal framework and harmonized legislations at Regional and Continental level we will enhance confidence and trust in the use of ICTs/ Internet enable the continent to reap the benefits of its Digital transformation.





THANK YOU FOR YOUR ATTENTION

Mrs. Souhila Amazouz
Senior ICT policy Officer , AUC
<https://www.au.int>

