ECONOMIC COMMISSION FOR AFRICA

AFRICAN UNION COMMISSION

DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBER SECURITY IN AFRICA

Version 01/01.2011

Summary

The Draft Convention gives effect to a Resolution of the last session of the Assembly of Heads of State and Government of the African Union, and seeks to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control.

In pursuance of the principles of the African Information Society Initiative (AISI) and the African Regional Action Plan for the Knowledge Economy (ARAPKE), the Draft Convention is intended not only to define the objectives and broad orientations for the Information Society in Africa, but also to strengthen existing legislations in Member States and the Regional Economic Communities (RECs) on the Information and Communication Technologies.

It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa.

It lays the foundation for an African Union-wide cyber ethics and enunciates fundamental principles in the key areas of cyber security. It also defines the basis for electronic commerce, puts in place a mechanism for combating intrusions into private life likely to be generated by the gathering, processing, transmission, storage and use of personal data and sets broad guidelines for incrimination and repression of cyber crime. Its adoption would capitalize African and international experiences in cyber legislations and speed up relevant reforms in African States and the RECs.

Conceptual Framework

Based on a reappraisal of the legal and institutional climate in African Union regions as a starting point, the report proposes the adoption at the level of the African Union, of a Convention establishing a credible framework for cyber security in Africa through organization of electronic commerce, protection of personal data and combating cyber crime.

1) Context

In a world characterized by the globalization of risks, crimes and threats to cyber security, Africa is faced with security gap which, as a result of poor mastery of security risks, increases the technological dependence of individuals, organizations and States

on information systems and networks that tend to control their information technologies needs and security facilities.

African States are in dire need of innovative criminal policy strategies that embody State, societal and technical responses to create a credible legal climate for cyber security.
It should however be observed that most States do not have communication tools that integrate adequate means as required to achieve or guarantee a minimum level of security, nor the human resources capable of conceiving and creating a credible legal framework.

The computer systems that have been networked are accessible only remotely and have become potential targets of cyber attacks which compromise the capacity to process, safeguard, communicate informational capital, intangible values and symbols, and the process of production or decision of those possessing such symbols, with implications for the security and survival of States and organizations.

Today, Africa more than elsewhere in the world, should as a matter of urgency offer individuals, organizations and States measures, procedures and tools for more effective management of technological, informational and legal risks. The stakes inherent in the effective control of technological risks are extremely high, and have to be addressed globally at the international level, by taking all Member States of the Union on board the security initiative, while respecting the fundamental rights of persons and of the States.
Noteworthy efforts (national, community and international level) have been deployed in the realm of legal protection. In this regard, the ECA has initiated a comprehensive harmonization project in cooperation with the authorities of UEMOA and ECOWAS. Other Regional Economic Communities have followed in the same path at a time when the States are increasingly enacting legislations on cyber security and ICTs in general. The ITU has similarly produced a guide on cyber security for use by developing countries.

This Convention pursues and deepens this momentum. It paves the way for a huge qualitative leap while giving content to political will.

2) Stakes and challenges

Cyber security raises stakes that are both multiple and complex, against which the magnitude of the challenges are to be measured.

The plurality of the stakes is such that calls for a focused attention on its multiple dimensions – scientific, technological, economic and financial, political and socio-cultural.

The interaction of these dimensions reinforces the complexity of cyber security which manifests at several levels:

- Informational security impacts on the security of the **digital and cultural heritage** of individuals, organizations and nations;

- The vulnerability in the normal functioning of institutions can compromise the **survival and sovereignty of States;**

- Addressing cyber security calls for clear-sighted **political will** to define and implement a strategy for development of digital infrastructure and services (e-services) and articulate a coherent, effective and controllable multi-disciplinary cyber security strategy.

The major challenges faced by Member States of the African Union are the need to:

- Achieve a level of **technological security** adequate enough to prevent and effectively control technological and informational risks;

- Build an information society that respects **values,** protects **rights and freedoms,** and guarantees the security of the property of persons, organizations and nations;

- Contribute to the knowledge economy, guarantee equal access to information while stimulating the creation of **authentic knowledge**;

- Create a climate of confidence and trust, that is a climate:

    - **Predictable** in terms of prevention and resolution of disputes; and evolving because it takes into account the continued technological evolution;

    - **Organized:** covering the relevant sectors;

    - **Protective:** of consumers and intellectual property (civil and penal) of citizens, organizations and nations;

- **Secured:** striking proper balance between legal and technological security;

- **Integrated** into the international order: providing meaningful articulation between the national, regional and global levels.

3) Objective and goal

The objective of the Convention on Cyber Security is to contribute to the preservation of the institutional, human, financial, technological and informational assets and resources put in place by institutions to achieve their objectives. The Convention embodies the treatment of cyber crime and cyber security in its strict sense, but is not confined solely to these elements. It also embraces important elements of electronic commerce and the protection of personal data.

Its ultimate goal is eminently protective given that it is geared to protecting:

- Institutions against **the threats and attacks** capable of endangering their survival and efficacy;

- The rights of **persons** during data gathering and processing against the threats and attacks capable of compromising such rights.

Similarly, the Convention seeks to:

- Reduce related institutional **intrusions or gaps** in the event of disaster;

- Facilitate the return to normal functioning at reasonable cost and within a reasonable timeframe;

- Establish the legal and institutional mechanisms likely to guarantee **normal exercise of human rights** in cyber space.

4) Strategic Orientations

The Convention defines a legal mechanism based on the following five strategic orientations:

- It spells out the options for an African Union wide cyber security policy;

- It lays the foundations for an African Union wide cyber ethics and enunciates fundamental principles in the key areas of cyber security;

- It organizes electronic commerce, electronic signature and electronic publicity;

- It organizes the legal and institutional framework for protection of personal data;

- It lays the foundation for a penal cyber law and a penal procedure for the treatment of cyber crime.

DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBER SECURITY IN AFRICA

PREAMBLE

The Member States of the African Union:

Considering that this Draft Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society, seeks to define the objectives and broad orientations of the Information Society in Africa and to strengthen existing Information and Communications legislations of Member States and the Regional Economic Communities (RECs);

Mindful of the need to mobilize all public and private players (State, local communities, private sector enterprises, civil society organizations, the media, training and research institutions, etc) towards achieving cyber security;

Guided by the principles of the African Information Society Initiative (AISI) and the Regional Action Plan for the Knowledge Economy (RAPKE);

Aware that it seeks to regulate a particularly evolving technological domain, is a response to the high expectations of several players often with divergent interests and sets forth the security rules essential for establishing a credible digital space through electronic commerce organization, personal data protection and the combating of cyber crime;

Considering that the major obstacles to electronic commerce development in Africa are linked to problems of security, particularly:

- The gaps affecting the regulation of legal recognition of data messages, as well as recognition of electronic signature;
- The absence of specific legal rules that protect consumers, intellectual property, personal data and information systems;
- The absence of appropriate teleservices and teleabour legislation;
- The application of electronic techniques to commercial and administrative acts;

- The probative elements introduced by digital techniques (time-date stamping, certification, etc);

- The rules applicable to cryptology devices and services;
-
- The oversight of on-line publicity

- The absence of appropriate fiscal and customs legislations for electronic commerce;

Considering that the afore-listed observations justify the need to establish an appropriate normative framework consistent with the African legal, cultural, economic and social climate; and that the objective of this Convention is therefore to offer the security and legal framework necessary for the emergence of a reliable electronic commerce in Africa;

Considering that protection of personal data and private life constitutes a major challenge of the Information Society for both public authorities and other players; and that the sustainability of this new technology naturally depends on the said protection which needs to combine the protection of the privacy of citizens in their daily and professional activities and guarantee the free circulation of information;

Considering the urgent need to establish a mechanism to address the dangers and risks deriving from the use of electronic data and individual records, with a view to respecting private lives and freedoms while enhancing the promotion and development of ICTs in Member States of the African Union;

Considering that the ambition of this Convention is to bridge this “legal gap”; that it seeks to establish in each Member State of the Africa Union a mechanism capable of combating intrusions into private life likely to be generated by personal data gathering, processing, transmission, storage and use; that, by offering a standard institutional basis, it ensures that any personal data treatment, regardless of its form, respects the basic freedoms and rights of individuals while also taking into account the prerogatives of the States, the rights of local communities and the interests of businesses; that by taking on board internationally recognized best practices in matters of personal data protection it offers several regulatory platforms and modalities facilitating such protection;

Aware of the need, given the pervasive existence of cyber crime which constitutes a real threat to the security of computer networks and the development of the Information

Society in Africa, to define broad orientations for cyber crime repression strategy in Member States of the African Union, taking into account their existing commitments at sub-regional, regional and international levels;

Considering that this Convention seeks, in terms material penal law, to modernize cyber crime repression instruments by formulating a policy for adoption of new incriminations specific to ICTs, and aligning certain incriminations, sanctions and extant penal liability regime in Member States with the technological climate;

Considering further that, in terms of procedural penal law, the Convention defines the framework for management of the classical procedures regarding ICTs and outlines the conditions for introduction of procedures specific to cyber crimes;

Recalling Decision Assembly/AU/11(XIV) of the 14th Ordinary Session of the Assembly of Heads of State and Government of the African Union on Information and Communication Technologies in Africa: Challenges and Prospects for Development, held in Addis Ababa, Ethiopia, from 1 to 2 February 2010;

Considering Oliver Tambo Declaration adopted by the Conference of African Ministers in charge of Information and Communication Technologies held in Johannesburg in November 2009;

HAVE AGREES AS FOLLOWS:

PART 1: ORGANIZATION OF ELECTRONIC COMMERCE

Section 1: Definitions

Article I – 1:

For the purpose of this Convention,

1) **Cryptology activity** means all such activity as seeks to produce, use, import, export or market cryptology tools;

2) **Accreditation** means formal recognition that the product or evaluated system can offer protection up to a level specified by an accredited body;

3) **Enciphering** means all techniques consisting in the processing of digital data in an unintelligible format using cryptology tools;

4) **Electronic commerce** means all economic activity by which a person offers or provides goods and services remotely or by electronic means;

5) **Communication with the public by electronic means** refers to all circulation to the public or segments of the public, signs, signals, written matter, pictures, sounds or messages of any type without the features of a private correspondence, through an electronic communication procedure;

6) **Secret conventions** refers to unpublished codes required to implement a cryptology facility or service for the purpose of enciphering or deciphering operations;

7) **Electronic mail** means any message in the form of text, voice, sound or picture sent by a public communication network, and stored in a server of the network or in a terminal facility belonging to the addressee until it is retrieved;

8) **Cryptology** means the science of protecting and securing information particularly for the purpose of ensuring confidentiality, authentication, integrity and non-repudiation;

9) **Information** refers to any element of knowledge likely to be represented with the aid of devices and to be used, conserved, processed or

communicated. Information may be expressed in written, visual, audio, digital and other forms;

10) **Cryptology tools** means the range of scientific and technical tools (equipment or software) which allows for enciphering and/or deciphering;

11) **Cryptology service** refers to any operation that seeks to implement cryptology facilities on behalf of oneself or of another;

12) **Cryptology services provider** means any person, be it a physical person or corporate body who provides cryptology services;

13) **Direct prospection** refers to the dispatch of any message that seeks to directly or indirectly promote the goods and services or the image of a person selling such goods or providing such services.

Section II: Electronic Commerce

Chapter 1: Field of application of electronic commerce

Article I – 2:

Electronic commerce is an economic activity by which a person offers or provides goods and services by electronic means.

The field of electronic commerce also comprises services such as those providing information on-line, commercial communications, research tools, access, data retrieval and access to communication or information hosting network, even where such services are not remunerated by the recipients.

Article I – 3:

The activities defined in Article 1 – 2 of this Convention shall be exercised freely in the African Union space except:

1) Gambling, even in the form of legally authorized betting and lotteries;

2) Legal representation and assistance activities; and

3) Activities exercised by notaries in application of extant texts.

Article I – 4:

Without prejudice to other information obligations defined by extant legislative and regulatory texts in African Union Member States, any person exercising the activities set forth in Article I – 2 of this Convention shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access using an open standard in regard to the following information:

1) Where a physical person is involved, his/her name and surname; and where it is a corporate body, its corporate name;

2) Full address of the place of establishment, electronic mail address and telephone number;

3) Where the person is subject to business registration formalities or registration in the national directory of businesses and associations, the registration number, the share capital and corporate headquarters;

4) Whether the person is subject to value added tax;

5) Where his/her activity is subject to a licensing regime, the name and address of the issuing authority;

6) Where the person is member of a regulated profession, the applicable professional rules, his/her professional title, the African Union member country in which he/she was granted such authorization, as well as the name of the order or professional body with which he/she is registered.

Article I – 5:

Any person exercising the activities defined in Article I – 2 of this Convention, even in the absence of offer of contract and provided he/she has posted a price for the said activities, shall clearly and unambiguously indicate such a price, especially where it is inclusive of taxes and delivery charges.

Chapter II: Contractual responsibility of the electronic provider of goods and services

Article I – 6:

Any physical individual or corporate body exercising the activity defined in the first paragraph of Article I – 2 of this Convention shall, *ipso facto*, be accountable to his/her contracting partner for the proper execution of the obligations resulting from the contract, regardless of whether or not such obligations are to be executed by him/herself or by other service provider, without prejudice to his/her right of recourse against the latter.

However, he/she may discharge him/herself from the whole or part of his/her responsibility by providing proof that the non-execution or poor execution of the contract is attributable either to the contracting partner or to *force majeure*.

Article I – 7:

The activity defined in Article I – 2 of this Convention shall be subject to the laws of the African Union Member State on the territory of which the person exercising such activity

is established, subject to the intention expressed in common by the said person and the recipient of the goods or services.

Section III: Publicity by electronic means

Article I – 8:

Any publicity action, irrespective of its form, accessible through on-line communication service, shall be clearly identified as such. It shall clearly identify the individual or corporate body on behalf of whom it is undertaken.

Article I – 9:

Publicity actions, especially promotional offers such as price discounts, bonuses or free gift, as well as promotional competitions or games disseminated by electronic mail, shall upon receipt be clearly and unequivocally identified in the title of the message by their addressees or, where this is technically impossible, on the body of the message.

Article I – 10:

The conditions governing the possibility of promotional offers as well as the conditions for participating in promotional competitions or games where such offers, competitions or games are electronically disseminated, shall be clearly spelt out and easily accessible.

Article I – 11:

Direct prospection through messages forwarded with automatic message sender, facsimile or electronic mail in whatsoever form, using the particulars of an individual who has not given prior consent to receiving the said direct prospection through the means indicated, shall be prohibited in the African Union.

Article I – 12:

The provisions of Article I – above notwithstanding, direct prospection by electronic mail shall be permissible where:

1) Where the particulars of the addressee have been obtained directly from him/her; and

2) The direct prospection concerns similar products or services provided by the same individual or corporate body.

Article I – 13:

The transmission, for the purposes of direct prospection, of messages using automatic message sender, facsimile and electronic mails without indicating valid particulars to which the addressee may usefully transmit a request for a stop to such communications without incurring charges other than those arising from the transmission of such request, shall be prohibited in the African Union.

Article I – 14:

Concealing the identity of the person on behalf of whom the communication is issued or mentioning a subject unrelated to the transaction or service offered, shall equally be prohibited in the African Union.

Article I – 15:
The consent of the persons whose particulars were obtained prior to the publication of this Convention may be solicited by electronic mail.

Section IV: Treaty obligations in electronic form

Chapter 1: Contracts in electronic form

Article I – 16:

Electronic means may be used to disseminate contractual conditions or information on goods or services.

Article I – 17:

The information requested for the purpose of concluding a contract or information available during contract execution may be transmitted by electronic means where the addressee of such information has agreed to the use of the said means.

Article 1 – 18:

Information meant for a professional may be addressed to him/her by electronic mail provided he/she has communicated his/her electronic professional address.

Article I – 19:

A service provider or supplier, who offers goods and services in professional capacity by electronic means, shall make available the applicable contractual conditions in a way that facilitates the conservation and reproduction of such conditions. The offer shall comprise:

1) The various stages to be followed to conclude the contract by electronic means;

2) Such technical facilities as would enable the user to identify the errors committed in data input and to correct such errors prior to conclusion of the contract;

3) The languages to be used for concluding the contract;

4) Where the contract is to be lodged, the modalities for this action by the author of offer and the conditions for accessing the contract so lodged;

5) The means of electronic consultation of the professional and commercial rules by which the author of the offer intends to be guided, if need be.

Article 1 – 20:

For the contract to be validly concluded, the recipient of the offer shall have had the opportunity to verify details of his/her order, especially the price thereof, prior to confirming the said order and signifying his/her acceptance.

Article I – 21:

The author of the offer shall acknowledge receipt of the order so addressed to him/her without unjustified delay and by electronic means.

The order, the confirmation of acceptance of offer and acknowledgement of receipt shall be deemed to have been received when the parties to whom they were addressed, can access them.

Article I – 22:

Agreements concluded between professionals may be exempted from the provisions of Articles I – 20 and 21 of this Convention.

Chapter II: Written matter in electronic form

Article I – 23:

In the absence of legal provisions to the contrary, no person shall be compelled to take a legal action by electronic means.

Article I – 24:

Where a written matter is required to validate a legal act, such act may be established and conserved in electronic form under conditions defined by the legal texts enacted for the purposes of application of the legal act.

Article I – 25:

The following acts shall be exempted from the provisions of Article I - 24 of this Convention:

1) Acts under the signature of a private individual, relating to family law and law of succession; and

2) Acts of civil or commercial nature under the signature of a private individual, relating to personal or real security, except where such acts have been established by a person for the purposes of his/her profession.

Article I – 26:

The written matter emanates from a sequence of letters, characters, figures or all other signs and symbols with intelligible meaning, regardless of their base and transmission modalities.

Article I – 27:

A registered letter may be transmitted by electronic means provided such mail is dispatched by a third party in accordance with a procedure that makes it possible to identify the third party, designate the sender, guarantee the identity of the addressee and ascertain whether or not the said letter has been delivered to the addressee.

Article I – 28:

The delivery of a written matter in electronic form shall be effective when the addressee takes due note and acknowledges receipt thereof.

Article I – 29:

Where a matter written on paper has been subject to special legibility or presentation requirements, a written matter in electronic form shall be subject to the same requirements.

Article I – 30:

The requirement to transmit several copies of a written matter shall be deemed to have been met, where the said written matter can be printed by the addressee.

Article I – 31:

A written matter in electronic form shall be admissible for the purpose of invoicing, on equal terms as paper based written matter, provided the authenticity of the origin of the data therein and the integrity of the content are guaranteed.

Section V: Ensuring the security of electronic transactions

Article I – 32:

For the purposes of this Convention,

1) "Electronic signature" means data in electronic form attached to or logically subjoined to a data message, and which can be used to identify the data message signatory and indicate consent for the information contained in the said message;

2) Written proof means such proof as has been established in accordance with the provisions of Article I – 26 of this Convention.

Article I – 33:

An electronic written matter shall be admissible as proof on equal terms as paper based written matter and shall have the same evidentiary weight as the latter, provided the person who is source thereof can be duly identified and that it is prepared and conserved in conditions that guarantee its integrity.

Article I – 34:

A supplier of goods or provider of services by electronic means demanding execution of an obligation shall prove the existence of such obligation and, where he/she demands

to be relieved of such obligation, shall prove that the obligation does not exist or has expired.

Article I – 35:

Where the legal provisions of Member States have not laid down other provisions, and where there is no valid agreement between the parties, the judge shall resolve proof related conflicts by determining by all means possible the most plausible claim regardless of the message base employed.

Article I – 36:

A copy or any other reproduction of acts undertaken by electronic means shall have the same weight as the act itself, where the said copy has been certified as a true copy of the said act by bodies duly accredited by a State authority.

The certification shall culminate in the issuance of an authenticity certificate, where necessary.

Article I – 37:

An electronic signature on an electronic written matter shall be admissible on the same terms as a signature in manuscript written on paper based matter.

The signature shall use such reliable identification procedure as guarantees its linkage with the act to which it relates.

Such procedure shall be presumed to be reliable until proved otherwise, where the electronic signature has been created by a security signature device, and where the procedure guarantees the integrity of the act and the signature thereof has been identified.

Article I – 38:

An electronic signature created by a security device which the signatory is able to keep under his/her exclusive control and is appended to a digital certificate shall be admissible as signature on the same terms as a signature in manuscript.

Article I – 39:

Subject to legal provisions to the contrary, no one shall be compelled to undertake a legal act by electronic means.

PART II: PROTECTION OF PERSONNAL DATA

Section 1: Definitions

Article II – 1:
For the purpose of this Convention:

1) **Code of conduct** means usage charters formulated by the processing official with a view to introducing the correct use of computer resources, the Internet and the electronic communication of the structure concerned, and approved by the protection authority.

2) **Consent of the person concerned** means any manifestation of express, unequivocal, free, specific and informed will by which the person concerned or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing.

3) **Recipient of processed personal data** means any person entitled to receive communication of such data other than the person concerned, the data processing official, the sub-contractor and persons who, for reasons of their functions, have the responsibility to process the data.

4) **Personal data** means any information relating to a physical person directly or indirectly identified or identifiable by reference to an identification number or to one or several elements relating to his/her physical, physiological, genetic, psychic, cultural, social or economic identity.

5) **Sensitive data** means all personal data relating to religious, philosophical, political and labor union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions.

6) **Health data** means all information relating to the physical or mental state of the person concerned, including the aforementioned genetic data.

7) **Personal data file** means all structured package of data accessible in accordance with set criteria, regardless of whether or not such data are centralized, decentralized or distributed functionally or geographically.

8) **Interconnection of personal data** means any connection mechanism that harmonizes processed data designed for a set goal with other data processed for

goals that are identical or otherwise, or interlinked by one or several processing official(s).

9) **Person concerned** means any physical person that is the subject of personal data processing.

10) **Direct prospection** means any solicitation carried out through message dispatch, regardless of the message base or nature, especially messages of commercial, political or charitable nature, designed to promote, directly or indirectly, goods and services or the image of a person selling the goods or providing the services.

11) **Data processing official** means any physical person or corporate body, be it public or private, any other body or association which, on its own or jointly with others, takes the decision to gather and process personal data and determine the objective of the said processing.

12) **Sub-contractor** means any physical person or corporate body, be it public or private, other body or association which processes data on behalf of the data processing official.

13) **Third party** means any physical person or corporate body, be it public or private, any other body or association other than the person concerned, the data processing official, the sub-contractor and persons entitled to process data under the direct authority of the data processing official or sub-contractor.

14) **Personal data processing** means any operation or set of operations conducted or with or without the aid of automated or unautomated procedures and applicable to data, such as gathering, exploitation, registration, organization, conservation, adaptation, modification, extraction, safeguarding, copying, consultation, utilization, communication through transmission, dissemination or any other form of circulation, exposure or interconnection, as well as the interlocking, ciphering, deletion or destruction of personal data.

Section II: Legal framework for personal data protection

Chapter 1: Objectives of this Convention with respect to personal data

Article II – 2:

Each Member State of the African Union shall put in place a legal framework with a view to establishing a mechanism to combat breaches of private life likely to arise from the gathering, processing, transmission, storage and use of personal data.
The mechanism so established shall ensure that any data processing, in whatsoever form, respects the freedoms and fundamental rights of physical persons while recognizing the prerogatives of the State, the rights of local communities and the interest of enterprises.

Chapter II: Scope of application of the Convention

Article II – 3:

The following actions shall be subject to this Convention:

1) Any gathering, processing, transmission, storage and use of personal data by a physical person or the State, local communities and public or private law corporate bodies;

2) Any processing, be it automated or not, of data contained or expected to feature in a file, with the exception of the processing defined in Article II – 4 of this Convention;

3) Any processing of data undertaken in the territory of a Member State of the African Union;

4) Any processing of data relating to public security, defense, research, criminal prosecution or State security, subject to the exceptions defined by specific provisions of other extant laws.

Article II – 4:

This Convention shall not be applicable to:

1) Data processing undertaken by a physical person within the exclusive context of his/her personal or domestic activities, provided however that such data are not meant for systematic communication to third parties or for dissemination;

2) Temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary lodging of data and for the sole purpose of offering

other beneficiaries of the service the best possible access to the information so transmitted.

Chapter III: Preliminary formalities for personal data processing

Article II - 5:

The following actions shall be exempted from the preliminary formalities stipulated in Article II *et sequentia:*

1) The processing mentioned in Article II – 4 of this Convention;

2) The processing undertaken with the sole objective of maintaining a register meant exclusively for private use;

3) The processing undertaken by an association or any non-profit making, religious, philosophical, political or labor union structure, provided the data so processed are consistent with the objective of the said association or structure, that they relate only to the members of the association or structure and are not meant for communication to third parties.

Article II – 6:

With the exception of the cases defined in Article II – 5 above and in Article II – 8 and 9 of this Convention, personal data processing shall be subject to a declaration before a protection authority.

Article II – 7:

With regard to the most common categories of personal data processing which are not likely to constitute a breach of private life or individual freedoms, the protection authority may establish and publish standards with a view to simplifying or introducing exemptions from the declaration obligation.

Article II – 8:

The following actions shall be undertaken after authorization by the protection authority:

1) Processing of personal data involving genetic information and health research;

2) Processing of personal data involving information on offenses, convictions or security measures;

3) Processing of personal data for the purpose of interconnection of files as defined in Article Ii – 42 of this Convention; data processing involving national identity number or any other identification of similar nature;

4) Processing of personal data involving physiometric information;

5) Processing of personal data of public interest, especially for historical, statistical or scientific purposes.

Article II – 9:

The processing of personal data undertaken on behalf of the State, a public institution, a local community or a private law corporate body operating a public service, shall be in accordance with a legislative or regulatory act enacted after an informed advice of the protection authority.

Such data processing shall be undertaken for the purpose of:

1) State security, defense or public security;

2) Prevention, investigation, indictment or prosecution of criminal offenses or execution of penal convictions or security measures;

3) Population census;

4) Compilation of personal data directly or indirectly portraying racial, ethnic or regional origin, parentage affiliation, political, philosophical or religious persuasions or labor union membership of persons, or data relating to health or sex life;

5) Processing salaries, pensions, taxes, levies and other payments.

Article II – 10:

Requests for opinion, declarations and applications for authorization shall indicate:

1) The identity and address of the data processing official or, where he/she is not established in the territory of a Member State of the African Union, the identity and address of his/her duly mandated representative;

2) The object of the processing and a general description of his/her functions;

3) The interconnections envisaged or all other forms of harmonization with other processing activities;

4) The personal data processed, their origin and the category of the persons concerned by the processing;

5) Duration of conservation of the processed data;

6) The service or services with responsibility to undertake the processing as well as the category of persons who, for reasons of their functions or the needs of the service, have direct access to registered data;

7) The persons entitled to receive data communication;

8) The function of the person or the service before which the right of access is to be exercised;

9) Measures taken to ensure the security of processing actions and of data;

10) Indication regarding use of a sub-contractor;

11) Envisaged transfer of personal data to a third country that is not a Member of the African Union, subject to reciprocity.

Article II – 11:

The protecting authority shall take the requisite decision within a set timeframe counting from the date of receipt of the request for opinion or authorization. Such timeframe may however be extended or not extended on the basis of an informed decision of the protection authority.

Article II – 12:

The opinion, declaration or request for authorization may be addressed to the protection authority by electronic means or by post.

A**rticle II – 13:**

The protection authority may be seized by any person acting on his/her own, or through a lawyer or any other duly mandated physical person or corporate body.

Section III: Institutional framework for protection of personal data

Chapter 1: Status, composition or organization

Article II – 14:

Each Member State of the African Union shall establish an authority with responsibility to protect personal data.

The body so established shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of this Convention.

Article II – 15:

The protection authority shall inform the concerned persons and the processing officials of their rights and responsibilities.

Article II – 16:

The protection authority shall comprise parliamentarians, deputies, senators, senior judges of the Tribunal of Accounts, Council of State, Civil and Criminal Appeal Court, personalities qualified as a result their knowledge of computer science, as well as professional networks or sectors.

Article II – 17:

Sworn agents may be invited to participate in audit missions in accordance with extant provisions in Member States of the African Union.

Article II – 18:

Members of the protection authority shall be subject to professional secrecy in accordance with the extant texts of each Member State.
Each protection authority shall formulate rules of procedure containing*, inter alia*, rules governing deliberations, processing and presentation of cases.

Article II – 19:

Membership of a protection authority shall be incompatible with membership of Government, the exercise of the functions of enterprise executive and shareholding in enterprises of the computer or telecommunication sector.

Article II – 20:

Members of a protection authority shall enjoy full immunity for views expressed in the exercise or on the occasion of the exercise of their functions.
Members of the protection authority shall not receive instructions from any authority in the exercise of their functions.

Article II – 21:

The protecting authority shall be afforded budgetary subvention for accomplishment of its missions.

Chapter II: Functions of the protection authority

Article II – 22:
The protection authority shall ensure that the processing of personal data is consistent with the provisions of this Convention.

Article II – 23:

The protection authority shall ensure that ICTs do not constitute a threat to public freedoms and private life. To this end, it shall:

1) Respond to every request for opinion regarding personal data processing;

2) Inform the persons concerned and the data processing official of their rights and responsibilities;

3) In several cases, authorize the processing of data files, especially sensitive files;

4) Receive the preliminary formalities for personal data processing;

5) Entertain claims, petitions and complaints regarding the processing of personal data and inform the authors about the outcomes thereof;

6) Speedily inform the judicial authority of certain types of offenses that have come to its knowledge;

7) Undertake the audit of all processed personal data, through sworn agents;

8) Impose sanctions, both administrative and pecuniary, on any defaulting data processing official ;

9) Update the processed personal data directory and circulate to the public;

10) Proffer advice to the persons and bodies engaged in personal data processing or in conducting trials or experiences likely to culminate in data processing;

11) Authorize cross-border transfer of personal data;

12) Make suggestions likely to simplify and improve legislative and regulatory framework for data processing;

13) Establish mechanisms for cooperation with the personal data protection authorities of third countries;

14) Participate in international negotiations on personal data protection;

15) Prepare an activity report in accordance with well-defined periodicity, for submission to either the President of the Republic, President of the National Assembly, Prime Minister or Minister of Justice.

Article II – 24:

The protection authority may take the following measures:

1) Issuance of warning to any data processing official that fails to comply with the responsibilities arising from this Convention;

2) A formal demand for an end to any particular breaches within a timeframe set by the authority.

Article II – 25:

Where the data processing official fails to comply with the formal demand addressed to him/her, the protection authority may impose the following sanctions after adversarial proceedings:

1) Provisional withdrawal of license;

2) Definitive withdrawal of license;

3) Pecuniary fine.

Article II – 26:

In case of emergency, where the processing or use of personal data results in violation of rights and freedoms, the protection authority may, after adversarial proceedings, decide as follows:

1) Interruption of data processing;

2) Locking up some of the personal data processed;

3) Temporary or definitive prohibition of any processing at variance with the provisions of this Convention.

Article II – 27:

The sanctions imposed and decisions taken by the protection authority are subject to appeal.

Part IV: Obligations relating to the conditions governing the processing of personal data

Chapter 1: Basic principles governing the processing of personal data

Section 1: Principle of consent and of legitimacy of personal data processing

Article II – 28:

Processing of personal data shall be deemed to be legitimate where the person concerned has given his/her consent.
This requirement may however be excepted where the processing is required to:

1) Obtain compliance with a legal obligation to which the processing official is subject;

2) Execute a mission of public interest or deriving from the exercise of public authority vested in the processing official or a third party to whom the data have been communicated;

3) Execute a contract to which the concerned person is party or pre-contractual measures undertaken at his/her request;

4) Safeguard the interest or fundamental rights and freedoms of the person concerned.

Section II: Principle of licitness and honesty of personal data processing

Article II – 29:

The gathering, registration, processing, storage and transmission of personal data shall be undertaken licitly, with honesty and non-fraudulently.

Section III: Principle of objective, relevance and conservation of processed personal data

Article II – 30:

Data gathering shall be undertaken for a set objective that is explicit and legitimate, and the data so gathered may not be processed thereafter in a manner incompatible with the said objectives.

Data gathered shall be adequate, relevant and non-excessive in relation to the ultimate objective for which they have been gathered and subsequently processed.

The data shall be conserved for a duration not exceeding the period required to achieve the ultimate objective for which the said data have been gathered or processed.

Beyond the said period, the data may be conserved only to specifically meet the needs of data processing undertaken for historical, statistical or research purposes under the law.

Section IV: Principle of accuracy of personal data

Article II – 31:

Data gathered shall be accurate and, where necessary, updated. Every reasonable measure shall be taken to ensure that data that are incorrect and incomplete in relation

to the objective for which they were gathered and subsequently processed are deleted or corrected.

Section V: Principle of transparency of personal data

Article II – 32:

The principle of transparency implies the obligation on the part of the processing official to provide information on personal data.

Section VI: Principle of confidentiality and security of personal data processing

Article II – 33:

Personal data shall be processed confidentially and protected, especially where the processing involves transmission of the data in a network.

Article II – 34:

Where processing is undertaken on behalf of a processing official, the latter shall choose a sub-contractor with adequate guarantees. It is incumbent on the processing official and the sub-contractor to ensure compliance with the security measures defined in this Convention.

Chapter II: Specific principles governing the processing of certain categories of personal data

Article II – 35:

Data gathering and processing based on racial, ethnic and regional considerations, parentage relationship, political views, religious or philosophical persuasion, trade union membership, sex life and genetic information or, more generally, data on the state health of the person concerned, is prohibited in the African Union.

Article II – 36:

The prohibitions set forth in Article II - shall not apply to the following types of data processing, where:

1) The personal data processing involves data manifestly published by the person concerned;

2) The person concerned has given his/her written consent, by whatsoever means, to the processing and in conformity with extant texts;

3) The personal data processing is required to safeguard the vital interest of the person concerned or of another person in the event that the person concerned finds him/herself in a situation whereby he/she is physically or legally unable to give such consent;

4) The processing of genetic data in particular is required for investigation purposes, and the exercise or defense of the right to justice;

5) A judicial procedure or criminal investigation has been opened;

6) The personal data processing is necessary in the public interest, especially for historical, statistical or scientific purposes;

7) The processing is required to execute a contract to which the person concerned is party or pre-contractual measures undertaken at the request of the person concerned during the pre-contractual period;

8) The processing is necessary to obtain compliance with a legal or regulatory obligation to which the processing official is subject;

9) The processing is required to execute a mission of public interest or a mission undertaken by a public authority or assigned by a public authority to the processing official or to a third party, to whom the data have been communicated;

10) The processing is undertaken within the framework of the legitimate activities of a foundation, association or any other non-profit making body or for political, philosophical, religious, self-help or trade union related purposes. The processing shall however concern only members of the said body or persons in regular contact with the latter in pursuance of its objective, provided the data are not transmitted to third parties without the consent of the person concerned.

Article II – 37:

Personal data processing for journalistic purposes or for the purpose of research or artistic or literary expression shall be admissible where the processing is meant exclusively for literary and artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions.

Article II - 38:

The provisions of this Convention shall not impede the application of laws relating to the print media or the audio-visual sector and the provisions of the penal code which prescribe the conditions for the exercise of the right of response, and prevent, restrict, compensate for and, where necessary, repress breaches of private life and the reputation of physical persons.

Article II – 39:

Direct prospection with the aid of any means of communication in whatsoever form, using the personal data of a physical person who has not given prior consent to receiving such prospection, is prohibited in the African Union.

Article II – 40:

No legal ruling involving an appraisal of the comportment of a person shall serve as grounds for the automated processing of personal data for the purpose of evaluating certain aspects of his/her personality.

No decision producing legal effects on a person shall be taken, on the exclusive grounds of automated processing of personal data for the purpose of defining the profile of the person concerned or evaluating certain aspects of his/her personality.

Article II – 41:

The data processing official shall not transfer personal data to a non-Member State of the African Union unless such a State offers sufficient level of protection of the private life, freedoms and fundamental rights of persons whose data are being or are likely to be processed.

Before any personal data is transferred to the said third country, the data processing official shall give prior notice of such transfer to the protection authority.

Chapter III: Interconnection of personal data files

Article II – 42:

The interconnection of files prescribed in Article II – 8 of this Convention should help attain the legal or statutory objectives that present legitimate interest for data treatment officials. It shall not result in discrimination or in erosion of the rights, freedoms and guarantees in respect of the persons concerned and nor loaded with security measures. The interconnection shall take into account the principle of relevance of the data that are to be interconnected.

Section V: The rights of the person whose personal data are to be processed

Chapter 1: Right to information

Article II – 43:

The data processing official shall furnish the person whose data are to be processed with the following information, not later than the time of gathering the said data regardless of the means and facilities utilized:

1) His/her identity and, where necessary, that of his/her representative;

2) Ultimate purpose for which the data processed will be used;

3) Categories of data involved;

4) Recipient(s) to which the data are likely to be transmitted;

5) The capacity to request to feature no longer in the file;

6) Existence of the right of access to the data concerning the person and the right to correct such data;

7) Duration of conservation of the data;

8) Possibility of transfer of the data to third countries.

Chapter II: Right of access

Any physical person whose personal data are to be processed may request the official conducting such processing to provide:

1) Such information as would enable him/her to evaluate and contest the processing;

2) Confirmation as to whether the personal data concerning the person are to be processed or not;

3) Communication of the personal data concerning the person as well as other available information on the origin of such data;

4) Information regarding the purpose of the processing, the categories of the personal data processed, the recipients of the processed data or the categories of the destinations to which the data are to be transmitted.

Chapter III: Right of opposition

Article II – 45:

Any physical person shall have the right to object, on legitimate grounds, to the processing of the personal data concerning him/her.
He/she shall have the right to be informed before the data concerning him/her are transmitted, in the first instance, to a third party or used on behalf of the third party for the purpose of prospection; and to be expressly offered the right to object to such communication or use, free of any cost.

Chapter IV: Right of correction or suppression

Article II – 46:

Any physical person may require the data processing official to rectify, complete, update, interlock or suppress, as the case may be, the personal data concerning him/her where such data are incorrect, incomplete, equivocal or outdated, or the gathering, use, communication or conservation thereof have been prohibited.

Section VI: Obligations of the personal data processing official

Chapter 1: Confidentiality obligations

Article II – 47:

Processing of personal data shall be confidential. Such processing shall be undertaken exclusively by persons operating under the authority of a data processing official and exclusively on the latter's instruction.

Chapter 2: Security obligations

Article II – 48:

The processing official shall take all such precautions as are necessary depending on the nature of the data, and in particular, prevent such data from being distorted or damaged or from being accessed by unauthorized third parties.

Chapter 3: Conservation obligations

Article II – 49:

Personal data shall be conserved for a period set by a regulatory text and solely for the purposes for which they were obtained.

Chapter 4: Sustainability obligations

Article II – 50:

The processing official shall take all appropriate measures to ensure that processed personal data can be utilized regardless of the technical device employed in the process.

The processing official shall, in particular, ensure that technological changes do not constitute an obstacle to the said utilization.

PART III – COMBATING CYBER CRIME

Section 1: Basic principles

Chapter 1: Definitions

Article III – 1:
For the purpose of this Convention:

1) **Electronic communication** means any transmission to the public or a section of the public by electronic or magnetic means of communication, signs, signals, written matter, pictures, sounds or messages of whatsoever nature;

2) **Computerized data** means any representation of facts, information or concepts in any form that lends itself to computer processing;

3) **Racism and xenophobia in ICTs** means any written matter, picture or any other representation of ideas or theories which advocates or encourages hatred, discrimination or violence against a person or group of persons for reasons of race, color, ancestry or national or ethnic origin or religion, where these serve as pretext for either racism and xenophobia or as motivation thereof;

4) **Minor** means any person aged less than eighteen (18) years in terms of the United Nations Convention on the Rights of the Child;

5) **Child pornography** means any data, regardless of the nature or form, which visually represents a minor lending him/herself to explicit sexual act, or realistic images representing a minor lending himself/herself to explicit sexual behavior;

6) **Computer system** means any device, be it isolated or otherwise, and a range of interconnected devices used in part or in whole for automated processing of data for the purpose of executing a programme.

Chapter 1: National cyber security framework

Article 1: National policy

Each Member State, in collaboration with key stakeholders comprising all levels of Government, industry and professional organizations, the civil society and citizens in general, shall put in place a national cyber security policy which recognizes the importance of essential information infrastructure for the nation, identifies the risks

facing the nation in using the all-risk approach and broadly outlines the way by which the objectives are to be implemented.

Article 2: National strategy

Member States shall adopt such strategies as they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legal reform and development, awareness-raising and capacity-building, public-private partnership, international cooperation, etc. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and of international cooperation.

Chapter 2: Legal measures

Article III – 1 – 1: Laws against cyber crime

Each Member State shall adopt such legislative measures as it deems effective to set up material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as effective procedural measures for the arrest and prosecution of offenders. Member States shall take into account the approved language choice in international cyber crime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary.

Article III – 1 – 2: Statutory authorities

Each Member State shall adopt such legislative measures as it deems necessary to confer specific responsibility on institutions, be they newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory authority and legal capacity to act in all aspects of cyber security application, including but not limited to response to cyber security incidence and coordination in the field of restorative justice, forensic investigations, prosecution, etc.

Article III – 1 – 3: Democratic principles

In adopting legal measures in the realm of cyber security and establishing the framework for implementation thereof, each Member State shall ensure that the measures so adopted will not compromise the rights of citizens guaranteed by their national constitution and protected by international conventions, especially the African

Charter on Human and Peoples' Rights, and other rights such as freedom of expression, respect for private life, the right to equitable education, etc.

Article III – 1 – 4: Protection of essential information infrastructure

Each Member State shall adopt such legal measures as they deem necessary to identify the sectors regarded as sensitive for national security and the health of the economy, as well as the ICT systems designed to ensure the functioning of these structures as constituting essential information infrastructure; and, in this regard, introduce more severe sanctions for criminal activities against ICT systems in the sectors concerned and measures to improve vigilance, security and management.

Article III – 1 – 5: Harmonization

Each Member State shall ensure that the legislative measures adopted in respect of substantive and procedural provisions on cyber crime reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

Article III – 1 – 6: Double criminality

The cardinal principle of cooperation in the application of the law against cross-border crime reposes on the fact that the laws under which such cooperation is sought by each Member State should be uniform in terms of prohibited conduct and application procedure. Each Member State shall adopt such legal measures as respect the principle of double criminality.

Article III – 1 – 7: International cooperation

Each Member State shall adopt such measures as it deems necessary to foster exchange of information and the sharing of quick, expeditious and reciprocal data by Member States' organizations and similar organizations of other Member States with responsibility to cause the law to be applied in the territory on bilateral or multilateral basis.

Chapter III: National cyber security system

Article III – 1 – 8: Culture of security

1) Each Member State shall make it a point to inculcate a culture of security in all stakeholders, namely: Governments, enterprises and the civil society, which develop, possess, manage, operationalize and use information systems and networks. The culture of security shall place premium on security in information systems and networks development and on the adoption of new ways of thinking and behaving during the use of information systems as well as during communication or transaction across networks.

2) As part of the promotion of a culture of security, Member States may adopt the following measures: devise a cyber security plan for the systems run by Government; conduct research and devise security awareness-building programmes and initiatives for the systems and networks users; encourage the development of a culture of security in enterprises; foster the engagement of the civil society; launch a comprehensive and detailed national awareness-raising programme; strengthen scientific and technological as well as research and development activities, and raise awareness on cyber threats and available solutions.

Article III – 1 – 9: Role of Government

Each Member State shall take the lead in the development of a culture of security within its borders. Member States shall to this end enhance awareness-building, provide education and training and disseminate information to the public.

Article III – 1 – 10: Public-private partnership

Each Member State shall adopt public-private partnership as a model to engage industry, civil society and the academia in the promotion and enhancement of a culture of cyber security.

Article III – 1 – 11: Education and training

Each Member State shall develop capacity building measures with a view to offering training that covers all areas of cyber security in appropriate government institutions, and set standards for the private sector. Such training should help to promote information exchange among experts and security vendors, ICT owners, managers and users. Member States shall promote technical education for ICT professionals in and outside government structures through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational materials.

Article III – 1 – 12: Public awareness-raising

1) Each Member State shall adopt an effective national cyber security awareness-building programme with a view to promoting cyber security awareness in the public and key stakeholders; establish relation with cyber security professionals for the purpose of sharing information on cyber security initiatives and developing collaboration on cyber security issues.

2) During development of awareness-raising programme, Member States shall take into account:

   i) Stakeholders' support and commitment to develop and establish relations of confidence between industry, Government and the academia for the purpose of scaling up the level of cyber security awareness;

   ii) Coordination and collaboration on cyber security activities in the entire government outfit; and

   iii) Communication with bodies both internal and external: other governmental agencies, industry, educational institutions, domestic computer users and the wider public.

3) To raise the level of awareness on cyber security issues, political leaders and other cyber security stakeholders shall:

   i) Establish public-private partnerships when necessary;

   ii) Launch large-scale publicity campaign to reach out to the greatest possible number of persons;

   iii) Use NGOs, institutions, banks, *FAI*, bookshops, local commercial organizations, community centers, computer shops, community colleges and adult education programmes, school as well as parents' associations to inculcate the message of appropriate cyber comportment.

Chapter IV: National cyber security monitoring structures

Article III – 1 – 13: Cyber security governance

1) Pursuant to Articles 1 and 2 of these Directives, each Member State shall adopt such measures as they deem necessary to establish an appropriate cyber security institutional and governance structure;

2) The measures adopted as per paragraph 1 of this Article shall seek to establish strong leadership and commitment in all aspects of the cyber security of institutions and relevant professional bodies in a Member State. To this end, Member States shall take appropriate measures to:

   i. Establish unambiguous responsibility in matters of cyber security at all levels of Government and clearly define roles and responsibilities;

   ii. Make an unambiguous, public and transparent commitment to cyber security;

   iii. Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.

3) Cyber security governance shall be established on the basis of a national framework capable of responding to perceived challenges and to all issues relating to information security at national level in the greatest possible number of cyber security domains.

Article III – 1- 14: Institutional framework

1) Each Member State shall adopt such measures as its deems necessary to establish appropriate institutions to combat cyber crime, conduct surveillance in response to cyber crime incidents and early warning, for coordination of national and cross-border cyber security problems and for global cooperation.

2) Organizational structures may assume any of the following forms: National Cyber Security Council (NCC), National Cyber Security Authority (NCA) and a National CERT and/or CSIRT. Each Member State may adapt its structures for the purpose of introducing “a specific adjustment” depending on their level of ICT development, availability of resources and of public-private partnerships. These structures may exist under other or different nomenclatures.

3) It is recommended that Member States establish a national liaison centre or a special organizational entity for the purpose of backstopping a national cyber security policy and facilitating regional and international cooperation.

Article III – 1 -15: National Cyber Security Council (NCC)

Each Member State shall establish a National Cyber Security Council or its equivalent as a special (separate) entity or component of the National Security Council. The NCC shall serve as a high-level liaison center for cyber security in the Member State and adopt or approve the policies put forward for implementation of the said policy by the National Cyber Security Authority or its equivalent in the Member State, namely:

I. National cyber security policy and strategy;

II. National cyber security priorities and initiatives;

III. Coordination of cyber security measures at national level;

IV. Identification of the protagonists responsible for cyber security in the economy and establishment of the public-private relations required to address cyber security issues;

V. Collaboration with several government services or agencies such as intelligence services, security services, the general directorate for security, the police force, technological crime unit, etc, for the purpose of establishing standards and uniform investigation procedures and developing an institutional consensus;

VI. Collaboration with the structures responsible for application of the law at regional or international level;

VII. Surveillance of government information systems and essential infrastructure;

VIII. Coordination of measures and development of digital identity systems as well as management and best practices in digital identity, among other things; and

IX. Development of standard training and capacity-building programmes for the agencies and the creation of a national platform for the purpose of coordinating technical assistance and training initiatives at international level.

Article III – 1 – 16: National Cyber Security Authority (NCA)

1) It is highly recommended that each Member State adopt measures with a view to establishing a National Cyber Security Authority with responsibility to devise a national cyber security policy and strategy in the Member State and also to coordinate all national initiatives in matters of cyber security pursuant to Article 19 of the Directives.

2) The NCA distinct from the NCC and vested with some degree of independence, shall execute functions to facilitate establishment of the measures identified in the national policy approved by the NCC as well as verification of compliance, risk auditing and security appraisal; assist the NCC in all its functional activities and help industry to test its emergency plan; work with industry to set objectives, define directives for the security of ICT infrastructure and services and contribute to the application of international standards on cyber security as well as on accreditation and certification of ICT infrastructure, services and suppliers.

Article III – 1 – 17: Computer emergency response team (CERT)

1) Each Member State shall establish a national CERT to take charge of its information infrastructure protection actions and serve as a base for national coordination to respond to ICT security threats at regional and global levels.

2) Members States shall ensure that their national CERTs are capable of providing reactive and proactive services, communicating timely information on recent relevant threats and, whenever necessary, bringing their assistance to bear for response to incidents.

3) Member States shall ensure that the CERT so established by virtue of this Article executes the following minimum services:

i) Reactive services: early warning and precaution notice, incidents processing, incidents analysis, incident response facility, incidents response coordination, incident response on the web, vulnerability treatment, vulnerability analysis, vulnerability response and vulnerability response coordination;

ii) Proactive services: public notice, technological surveillance, security audit and assessment, security installations and maintenance, security tools development, intrusion detection services and security information dissemination, etc; and

iii) Artifacts treatment: artifacts analysis, response to artifacts, coordination of response to artifacts, risk analysis, continuation and resumption of activities after disaster, security consultation and sensitization campaign, education/training and product appraisal or certification.

Article III – 1 – 18: Global framework for security incident surveillance, early warning and response

Each Member State shall adopt the measures required to establish and maintain cross-border collaboration with other CERT/CSIRT at regional and global levels. Member States may join existing early warning and surveillance networks (WSN) such as FIRST (Forum for Incident Response and Security Team), the European government CERT group (ECG), and others.

Chapter V: International Cooperation

Article III – 1 – 19: Harmonization

Each Member State shall ensure that the legislative measures adopted in respect of material and procedural provisions on cyber security reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

Article III – 1 – 20: Double criminality

The cardinal principle of cooperation in the application of the law against cross-border crime reposes on the fact that the laws under which such cooperation is sought by each Member State should be uniform in terms of prohibited conduct and application procedure. Each Member State shall adopt legal measures that respect the principle of double criminality.

Article III – 1 – 21: International cooperation

Each Member State shall adopt such measures as it deems necessary to foster exchange of information and the sharing of quick, expeditious and reciprocal data by Member States' organizations and similar organizations of other Member States with responsibility to cause the law to be applied in the territory on bilateral or multilateral basis.

Article III – 1 – 22: Information sharing and cooperation

Member States shall create institutions that exchange threat information and on vulnerability assessment such as CERT (Computer Emergency Response Teams) or CSIRTS (Computer Security Incident Response Team). The said teams shall be tasked

to establish relations of trust and confidence with the key stakeholders, work with the vendors to disseminate cybernetic security threat warning, develop and establish computer incident response capacities in collaboration with similar organizations and other Member States' organizations.

Article III – 1 – 23: International cooperation

In addition to the legal measures to be adopted by Member States under Article 9 to establish the legal basis required for cooperation, each Member State shall devise such mechanisms or procedures as it deems effective to establish and maintain regular contacts with the greatest possible number of national, regional and world institutions, and to enable Member States' institutions to provide, on request, or receive as required all information or assistance relating to cyber security, timely and on the basis of reciprocity.

Article III – 1 – 24: International cooperation facility

Each Member State shall take advantage of existing international cooperation facility to respond to cyber threats, improve cyber security and stimulate dialogue between the stakeholders. The said facilities could be international intergovernmental, regional intergovernmental or based on private-public partnerships, be it at regional or international level.

Article III – 1 – 25: Model of international cooperation

Each Member State shall adopt such measures and strategies as it deems necessary to participate in regional and international cooperation in cyber security. The Resolutions geared to promoting Member States' participation within this framework of relations have been adopted by a large number of international governmental bodies including the United Nations, the African Union, the European Union, the G8, etc. Organizations like the International Telecommunication Union, the Council of Europe, the Commonwealth of Nations and others, have established model frameworks for international cooperation which Member States may adopt as a guide.

Section II: Material penal law

Chapter 1: Offenses specific to Information and Communication Technologies

Section 1: Attack on computer systems

Article III – 1 – 26:

Member States of the African Union shall ensure that the measures adopted to protect *IC* and *IIC* offer a minimum of the following: resilience infrastructure, integrated network/applications, transport/transmission security, data enciphering, digital identity management, data availability in real time, and data retention and audit.

Article III – 2:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system.

Article III – 3:

Each Member State of the African Unions shall take the legislative measures required to set up as a penal offense the fact of retaining oneself or attempting to retain oneself fraudulently in a part or the whole of a computer system.

Article III – 4:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of hampering, distorting or attempting to hamper or distort the functioning of a computer system.

Article III – 5:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of introducing or attempting to introduce data fraudulently in a computer system.

Article III – 6:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of intercepting or attempting to intercept fraudulently

computerized data by technical means, during non-public transmission of the said data to, from or within a computer system.

Article III – 7:

1) Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of damaging or attempting to damage, delete or attempting to delete, spoil or attempting to spoil, alter or attempting to alter, modify or attempting to modify fraudulently computer data.

2) The Member States shall adopt rules to compel ICT product vendors to submit their products for vulnerability and guarantee tests to be conducted by independent experts and to divulge to the public any form of vulnerability found in the said products and the measures recommended for a solution thereto.

Section II: Attack on computerized data

Article III – 8:

Each Member State of the African Union shall take the legislative measures to set up as a penal offense the fact of producing or manufacturing a range of digital data by fraudulently introducing, deleting or suppressing computerized data held, processed or transmitted by a computer system, resulting in fake data, with the intention that the said data would be taken into account or used for illegal purposes as if they were the original data.

Article III – 9:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of using the data obtained with a full knowledge of a case.

Article III – 10:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of obtaining fraudulently, for oneself or for another person any advantage whatsoever by introducing, altering, deleting or suppressing computerized data or any other form of attack on the functioning of a computer system.

Article III – 11:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact, even out of negligence, of processing or causing the processing of personal data without having undertaken the preliminary formalities for the processing as prescribed by the law on personal data enacted to that effect in each Member State.

Article III – 12:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of producing, selling, importing, possessing, disseminating, offering, ceding or circulating a computer equipment, programme, any device or data designed or specially adapted to commit an offense, or a password, access code or similar computerized data allowing access to the whole or part of a computer system.

Article III – 13:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of participating in an association formed or in an understanding established with a view to preparing or committing one or several of the offense (s) defined in this Convention.

Section III: Content related offenses

Article III – 14:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of producing, registering, offering, circulating, disseminating and transmitting a picture or a representation of infant pornography by means of a computer system.

Article III – 15:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of procuring for oneself or for another person, importing or causing to be imported and exporting or causing to be exported a picture or representation of infant pornography by means of a computer system.

Article III – 16:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of possessing a picture or a representation of infant pornography in a computer system or in whatsoever means for holding computerized data.

Article III – 17:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of facilitating access to pictures, documents, sounds or representation of pornography of a minor.

Article III – 18:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the offenses defined in this Convention where they have been committed in an organized group, and liable to the maximum punishment prescribed for such offense.

Article III – 19:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of creating, downloading, disseminating or circulating in whatsoever form, written matters, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature using an a computer system.

Article III – 20:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense an attack perpetrated through a computer system, with the intention of committing a criminal offense against any person for reasons of his/her membership of a group characterized by race, color, ancestry, national or ethnic origin or religion where such membership serves as a pretext for any of these offenses, or a against a group of persons distinguishable by any of these characteristics.

Article III – 21:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense an abuse committed by means of a computer system against any person for reasons of his/her membership of a group characterized by race, color, ancestry, national or ethnic origin or religion where such membership serves as a

pretext for any of these offenses, or against a group of persons distinguishable by any of these characteristics.

Article III – 22:

Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the deliberate fact of denying, approving or justifying acts of genocide or crimes against humanity by means of a computer system.

Article III – 23:

Each Member State of African Union shall take the legislative measures required to ensure that, in case conviction, the tribunal gives a ruling for confiscation of the materials, equipment, tools, computer programmes and all devices or data belonging to the convicted person and used to commit the offenses.

Section III: Offenses relating to electronic message security measures

Article III – 23 – 1: Laws against cyber crime

Each Member State shall adopt such legislative measures as it deems effective, to define material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as procedural measures deemed effective for the arrest and prosecution of offenders. Member States shall be called upon to take on board, where necessary, the approved language choice in international cyber crime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations.

Article III – 23 – 2:

Each Member State of the African Union shall take the legislative measures required to ensure that written electronic matter in respect of criminal matters are admissible to establish offenses under criminal law, provided such written matter has been presented during debate and discussed before the judge, that the person from which the written material emanates can be duly identified and the said material has been prepared and conserved under conditions likely to guarantee their integrity.

Chapter II: Adapting certain information and communication technologies offenses

Section 1: Violation of property

Article III - 24:

Each Member State of the African Union shall take the legislative measures required to set up as an aggravating circumstance the use of ICT to commit common law offenses such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money, terrorism, money laundering, etc.

Article III – 25:

Each Member State of the African Union shall take the legislative measures required to set up as a legal offense the violations of property such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money and blackmail involving computer data.

Article III – 26:

Each Member State of the African Union shall take the legislative measures required to expressly include “means of digital electronic communication” such as the internet in the enumeration of the public dissemination facilities defined in the penal texts of Member States.

Article III – 27:

Each Member State of the African Union shall take the legislative measures required to expressly integrate the new intangible facilities such as “digitalized data” or “computerized files” which have to be kept secret in the interest of national defense.

Section II: Criminal liability

Article III – 28:

Each Member State of the African Union shall take the legislative measures required to ensure that corporate bodies other than the State, local communities and public institutions can be held responsible to the offenses defined in this Convention, committed on their behalf by their organs or representatives. The liability of the said

corporate bodies does not exclude that of the physical persons who are the authors or accomplices of the same offenses.

Article III – 29:

Each Member State of the African Union shall take the legislative measures required to submit media related offenses committed through the internet with the exception of the offenses committed by the media on the internet, to the common law regime of criminal liability.

Chapter III: Adapting certain sanctions to the Information and Communication Technologies

Section 1: Penal sanctions

Article III – 30:

Each Member State of the African Union shall take the measures required to ensure that the offenses defined in this Convention attract effective, proportional and deterrent penal sanctions.

Article III – 31:

Each Member State of the African Union shall take the measures required to ensure that the offenses defined in this Convention attract maximum prison sentence of one (1) to five (5) years at least.

Article III – 32:

Each Member State of the African Union shall take the measures required to ensure a corporate body declared liable in terms of this Convention is subject to effective, proportional and deterrent sanction which include penal and non-penal fines.

Section II: Other penal sanctions

Article III – 33:

Each Member State of the African Union shall take the measures required to ensure that, in the event of conviction for an offense committed by means of digital

communication facility, the investigating jurisdiction or the judge handling the case gives a ruling imposing additional punishment.

Article III – 34:

Each Member State of the African Union shall take the measures required to set up as a penal offense, the violation of the aforementioned prohibitions pronounced by the judge.

Article III – 35:

Each Member State of the African Union shall take the measures required to ensure that, in the event of conviction for an offense committed by means of digital communication facility, the judge handling the case makes a further binding ruling for the dissemination of the decision by extract and via the same facility at the expense of the convicted person, in accordance with the modalities prescribed in the legislations of Member States.

Section III: Procedural law

Article III – 36:

Each Member State of the African Union shall take the measures required to ensure that where the data held in a computer system or in a facility that allows for the conservation of computerized data in the territory of a Member State, are useful in revealing the truth, the investigating judge can conduct a search or access a computer system or part of the system or any other computer system where the said data are accessible from the original system or available to the initial system.

Article III – 37:

Each Member State of the African Union shall take the measures required to ensure that where an investigating judge discovers that the data held in a computer system are useful for revelation of the truth, but that seizure of the facility does not seem appropriate, the said data as well as all such data as are required to unravel the case, shall be copied into a computer storage facility that can be seized and sealed off, in accordance with the modalities defined in the legislations of Member States.

Article III – 38:

Each Member State of the African Union shall take the measures required to ensure that criminal intelligence officers can, for the purposes of investigation or execution of a judicial delegation, undertake the operations set forth by this Convention.

Section IV: Offenses specific to Information and Communication Technologies

Article III – 39:

Each Member State of the African Union shall take the measures required to ensure that, where the imperatives of the information so dictate, particularly where there are reasons to believe that the information stored in a computer system is particularly susceptible to loss or modification, the investing judge may issue an injunction to any person to conserve and protect the integrity of the data in his/her possession or under his/her control, for a duration of not more than two years in the interest of the proper conduct of the judicial investigation. The custodian of the said data or any other person with responsibility to conserve the data shall be expected to keep the secrets contained in the data.

Article III – 40:

Each Member State of the African Union shall take the legislative measures required to ensure that violation of the secrets attracts punishment applicable to the offense of violation of professional secrets.

Article III – 41:

Each Member State of the African Union shall take the measures required to ensure that, where the imperatives of the information so dictate, the investigating judge can use appropriate technical means to gather or register in real time the data in respect of the content of specific communications in its territory, transmitted by means of a computer system or compel a service supplier to gather and register the data within the framework of his/her technical capacities, using the existing technical facilities in its territory or that of States parties, or provide support and assistance to the competent authorities towards the gathering or registration of the said computerized data.

PART IV: COMMON AND FINAL PROVISIONS

Section 1: Monitoring mechanism

Article IV – 1

1) A Consultative Committee on Cyber Security is hereby established in the African Union

.

2) This Committee shall be composed of eleven (11) members elected by the Executive Council from a list of experts renowned for their high integrity, impartiality and competence in cyber security matters, and proposed by the States Parties. In the election of members of the Committee, the Executive Council shall ensure respect for adequate representation of women and equitable geographical distribution.

3) Members of the Committee shall hold their seats in their personal capacity.

4) The mandate of members of the Committee shall be for two (2) years, renewable once.

5) The functions of the Committee shall be to:

a) Promote and encourage in the African continent the adoption and application of cyber security building measures in electronic systems and to combat cyber crime and breaches of the rights of the person in cyber space;

b) Assemble documents and information on cyber security needs as well as on the nature and extent of cyber crime and breaches of the rights of the person in cyber space;

c) Devise methods to analyze cyber security needs as well as on the nature and extent of cyber crime and breaches of the rights of the person in cyber space; disseminate information and sensitize public opinion on the negative effects of these phenomena;

d) Advise government on how best to promote cyber security and combat the scourge of cyber crime and breaches of the rights of the person in national level cyber space;

e) Gather information and undertake analysis on the criminal conduct and behavior of information networks and systems users operating in Africa and transmit such information to competent national authorities;

f) Formulate and promote the adoption of harmonized codes of conduct for use by cyber security public agents;

g) Establish partnerships with the African Commission and the African Court on Human and Peoples' Rights, the African civil society, governmental, inter-governmental and non-government organizations with a view to facilitating dialogue on combating cyber crime and breaches of the rights of the person in cyber space;

h) Submit regular reports to the Executive Council on the progress made by each State Party in the implementation of the provisions of this Convention;

i) Discharge such other tasks relating to cyber crime and breaches of the rights of the person in cyber space as may be assigned to it by the policy organs of the African Union.

6) The Committee shall adopt its own Rules of Procedure.

7) States Parties shall transmit to the Committee, one year after the entry into force of this Convention, a status report on its implementation. Each State Party shall thereafter ensure that the national authorities or agencies responsible for combating cyber crime and breaches of the rights of the person in cyber space submit a report to the Committee at least once a year prior to the ordinary sessions of the policy organs of the African Union.

SECTION 2: FINAL PROVISIONS

Article IV – 2: Signature, ratification, accession and entry into force

1) This Convention shall be open to signature, ratification or accession by Member States of the African Union.

2) It shall enter into force thirty (30) days after the deposit of the fifteenth instrument of ratification or accession.

3) For each State Party that ratifies or accedes to this Convention after the date of the deposit of the fifteenth instrument of ratification, the Convention shall enter into force thirty (30) days after the date of the deposit of the instrument of ratification or accession by that State Party.

Article IV – 3: Reservations

1) Any State Party may, at the moment of adoption, signature, ratification or accession, file reservations in respect of this Convention, provided each reservation concerns one or several specific provisions and is not incompatible with the objectives and purposes of this Convention.

2) Any State Party that has filed a reservation may withdraw such reservation as soon as circumstance so permit. The withdrawal shall be effected by notification addressed to the Chairperson of the Commission.

Article IV – 4: Amendment

1) This Convention may be amended at the request of a State Party which shall address a written request to that effect to the Chairperson of the Commission.

2) The Chairperson of the Commission shall transmit the amendment request to all the States Parties which shall examine the said request only six months after the date of its transmission.

3) The amendment shall enter into force after its approval by two-thirds majority of Member States of the African Union.

Article IV – 5: Denunciation

Any State Party may denounce this Convention by written notification addressed to the Chairperson of the Commission. The said denunciation shall take effect six (6) months after the date of receipt of the notification by the Chairperson of the Commission.

Article IV – 6: Depository

1) The Chairperson of the Commission shall be the depository of this Convention and the amendments thereto.

2) The Chairperson of the Commission shall update all the States Parties on the status of signature, ratification and accession as well as the entry into force,

amendment requests introduced by the States, approval of amendment proposals and denunciations.

3) Upon the entry into force of this Convention, the Chairperson of the Commission shall register same with the Secretary General of the United Nations in accordance with Article 102 of the United Nations Charter.

Article IV – 7: Authentic texts

This Convention, drawn up in four (4) original texts in Arabic, English, French and Portuguese languages, all the four being equally authentic, shall be deposited with the Chairperson of the Commission.

IN WITNESS WHEREOF, WE THE HEADS OF STATE AND GOVERNMENT OF THE AFRICAN UNION OR OUR DULY MANDATED REPRESENTATIVES, HAVE ADOPTED THIS CONVENTION.

Done at …….. on……