Mr Franky Lwelela
Communication & PR Officer
African Ombudsman Research Centre (Aorc)

University of KwaZulu-Natal, Durban, 4041
Campus: Howard College
Email: Lwelela@ukzn.ac.za
Website: www.ukzn.ac.za
Tel: 0312603768
Cell: 0714591306

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

INSPIRING GREATNESS

Protection and Processing of Personal Data

Endale Haile (Ph.D.)
Chief Ombudsman of Ethiopia

contents

1. Introduction of Historical background of Personal data
2. Definition of Privacy, data processing and Personal data and the Principle of data processing and personal data
3. International legal basis of protection of Personal data
4. Personal Data in Africa and in Ethiopia
5. The challenges and the way forward

Historical Perspective

- Governments and other human consortia have for years gathered important and personal information on people.
- While much of this information was recorded in relatively primitive filing systems, its mere existence made the concept of privacy virtually non-existent.
- For example, government officials of the Roman Empire maintained an extensive system of taxation records on its subjects throughout its sphere of rule.
- Taxation records, while recorded by scribes on papyrus scrolls, were surprisingly complete. Taxpayers were identified through Rome's census-taking activities.
- In Greek and Egyptian cities personal information was maintained by bibliophylakes, or record keepers, who were placed in charge of the Public Records Offices.

Contd.

- Over the past 25 years, especially those in Europe, have implemented extensive legislation to cover the uses and misuses of personal information by government, and in some cases, by the private sector.
- Europe presently leads other technologically advanced nations in the protection of information.

Contd.

- Most data protection legislation deals with the collection and use of aggregate data organized in databases, filing systems and storage media.
- The development of multimedia workstations, however, will change what is considered a traditional 'file.' system
- Therefore, the need the data protection laws to reflect technological changes will become a critical factor
- The 1990s ushered in many dramatic advances in information technology, especially in the areas of artificial intelligence, relational databases and interactive telecommunications and distributed data processing.

Privacy

- Zelman Cowan stated that, a man without privacy is a man without dignity
- Privacy has historical roots in ancient Greek philosophers discussions
- The most well-known of these was Aristotle's distinction between two spheres of life: the public sphere of the *polis* associated with political life, and the private sphere of the *oikos*, associated with domestic life.
- Corresponding to different meanings of the adjective ‘private’, from which the English noun ‘privacy’ derives.

Contd.

- Privacy has been described in three ways.
- Firstly, privacy in making certain significant self-defining choices.
- Secondly, privacy of personal information; and
- thirdly, privacy as it relates to an individual's personal space and bod
- The Universal Declaration of Human Rights (UDHR),

Article 12 that '(n)o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation'.

Contd.

- Privacy can include protecting all forms of personal communications; the personal body (biometrics and medical); personal data and personal information (name and address; personal possession such as property)
- Therefore, privacy, while considered a principle of data protection, is a fundamental right within itself, and is associated with protecting a person's identity.

Data Processing

Under the General Data Protection Regulation (GDPR)

'Processing' is defined broadly as the performance of operations on Personal Data and will include, *inter alia*, collection, storage, retrieval, usage, disclosure, transfer, structuring, alignment or combination, indexation, and erasure.

Legal Bases for Processing Personal Data

1. **Consent t**he data subject has given permission for the organization to process their personal data for one or more processing activities. Consent must be freely given, clear, and easy to withdraw, so organizations need to be careful when using consent as their legal basis..
2. **Performance of a Contract-** Self-explanatory, right? The data processing activity is necessary to enter into or perform a contract with the data subject. If the processing activity does not relate to the terms of the contract,.
3. **Legitimate Interest- t**his is a processing activity that a data subject would normally expect from an organization that it gives its personal data to do, like marketing activities and fraud prevention.
4. **Vital Interest-** A rare processing activity that could be required to save someone's life. This is most commonly seen in emergency medical care situations.
5. **Legal Requirement -t**he processing activity is necessary for a legal obligation, such as an information security, employment or consumer transaction law.
6. **Public Interest-** A processing activity that would occur by a government entity or an organization acting on behalf of a government entity.

Defining Personal Data

- **Personal data**, also known as personal information or personally identifiable information (PII), is any information related to an identifiable person.
- For legal purposes the effective definitions vary depending on the jurisdiction and the purposes for which the term is being used.
- The term "personal data" is significantly broader, and determines the scope of the regulatory regime.

Contd.

- The National Institute of Standards and Technology defines personally identifiable information as "any information about an individual maintained by an agency, including

1. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." So, for example, a user's IP address is not classed as PII on its own, but is classified as a linked PII.
3. However, in the European Union the IP address of an Internet subscriber may be classed as personal data.

Contd.

- Personal data is defined under the GDPR as "any information which [is] related to an identified or identifiable **natural person**"
- EU directive 95/46/EC, for the purposes of the directive

Article 2a: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (not included the legal person)

In Ethiopia (590/2000)

"Personal Information" means information about an identifiable individual, including, but not limited to

A. Information relating to the medical, educational or the academic, employment , professional or criminal history, of the individual or information relating to financial transactions in which the individual has been involved;
B. Information relating to the ethnic, national or social origin, age, pregnancy, marital status color, sexual orientation, physical or mental health, well-being, disability, religion, belief, conscience, culture, language or birth of the individual;

Contd.

C. Information relating to any identifying number, symbol or other particular assigned to the individual, the address, fingerprints or blood type of the individual;

D. the personal opinions. views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

The Importance of Protection of personal data

- To protect individuals' fundamental rights and freedoms (in particular, the right to privacy) with regard to data processing and to administer all rules and procedures to be implemented during processing activities.
- The advancement of IT and databases, computer networks and mass storage techniques have exposed individuals around the world to threats of both passive and active surveillance and control.
- Data protection has also been characterized as a tool of 'privacy'.
- Data protection as a tool of privacy also helps to facilitate the economic growth in the trade of personal data

The principles of Personal data protection

1. **Preventing Harm**- to prevent the misuse of information;
2. **Notice**- ensuring that individuals are able to know what information is collected about them and for what purpose;
3. **Collection limitations**, of personal information that is relevant to the purposes;
4. **Uses**- should be used only to fulfill the purposes of collection;
5. Choice- ensure that individuals are provided with choice in relation to the collection, use, transfer, and disclosure of their personal information;
6. **Integrity**- to ensure personal information is accurate, complete, and kept up to date;
7. **Security**- so as personal information is not used in a way to compromise the individual to who the data applies;

Contd.

8. **Access and Correction-** so as individuals have the ability to access and correct their personal information; and

9. **Accountability-** to ensure organizations and individuals handling personal data are accountable.

Principles

To summarize

- Data Quality;
- Purpose Specification;
- Use Limitation;
- Security Safeguards;
- Openness;
- Individual Participation and Accountability.

International Law and legal Basis

- The international community understands the **extent of the issues that have currently surfaced and will continue** to pose challenges across the world in regards to data protection.
- However, to date **there is no single Treaty or Convention** that deals with personal data, in the same way as many other international issues.
- Moreover, there **is no clear Model** Law that has been prepared that can guide not only nation states but also the private sector in the management and use of personal data

Contd.

- This is because of the **varied nature in** which data is collected, collated, used, stored and transacted across the public and private sectors.
- Rather, the **international organizations** that have been involved in data protection have focused their efforts on developing, concepts, principles and guidance for countries to consider whether to include them into their national laws

Contd.

- The protection of privacy under the international legal framework dates back to just after world war two (WWII).
- Article 12 of the Universal Declaration of Human Rights 1948 states that
- '**no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation**.
- Everyone has the right to the protection of the law against such interference or attacks'.

Contd.

- The United Nations or the United Nations Conference on Trade and Development (UNICAD), is
- responsible for policy-oriented analytical work on the development implications of information and communication technologies (ICTs).
- it is responsible for the preparation of thematic reports on ICT for development and promotes international dialogue on issues related to ICTs for development, to measure the information economy and to design and implement relevant policies and legal frameworks.

Contd.

- Article 17 of the International Covenant on Civil and Political Rights 1966, and to date, is ratified by 167 States, provides that

'no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation.'

- It further states that everyone has the right to the protection of the law against such interference or attacks

Contd.

- The OECD had developed the Guidelines on the Protection of Privacy and Trans border Flows of Personal Data ("the Personal Data Guidelines") as far back as 1980 (revised in 2013).
- In 2017, there were 192 Member States of the United Nations, while privacy and data protection authorities from approximately 79 states are accredited to the International Conference of Data Protection and Privacy Commissioners (ICDPPC) as at September 2017.

Persona data and protection in Africa

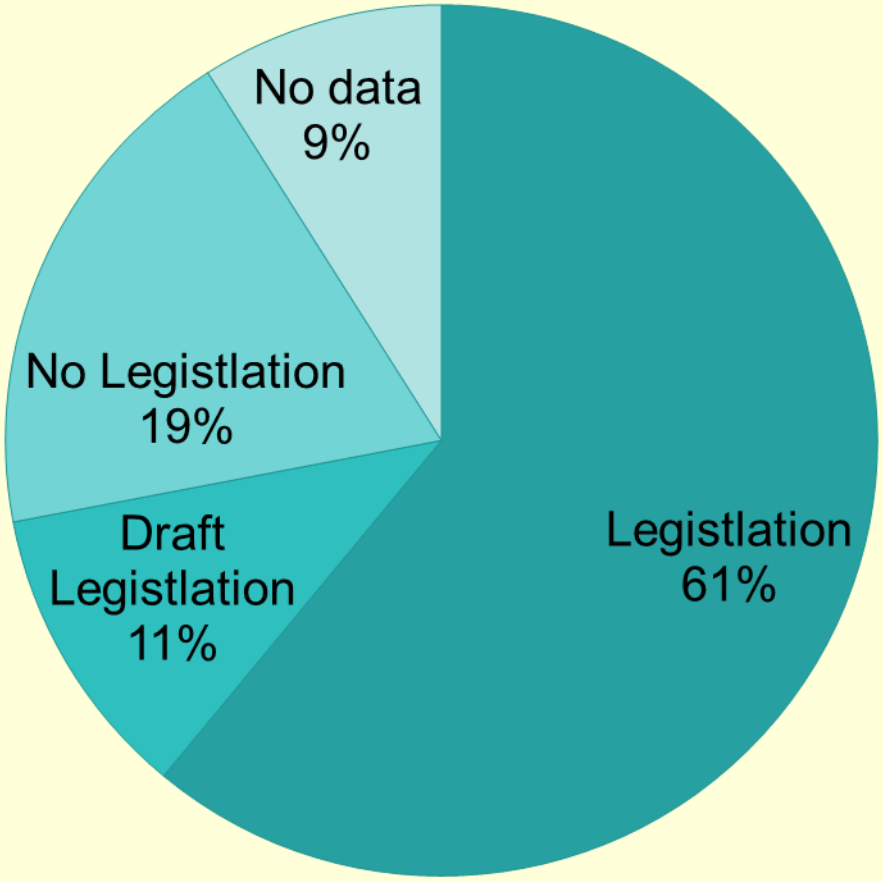
- Developing nations in Asia, Africa and Latin America have either not yet addressed the issue of personal data protection in the European sense, or they have taken a completely different approach to the subject.
- In particular, the privacy of the individual is not considered a high priority by most Asian and African governments or their respective citizenries.
- Most constitutions in Africa expressly guarantee the right to privacy.
- The formulations of these constitution provisions closely follow Articles 12 and 17 of the Universal Declaration of Human rights 1948 as well as International Covenant on Civil and Political Rights 1966.

Contd.

However,

- There are four privacy policies at the regional level and sub-regional levels in Africa. These are
- The AU Convention on Cyber security and Personal Data Protection 2014,
- The ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection,
- SADC Data Protection Model Law 2012 and
- The EAC Legal Framework for Cyber Laws 2008.
- The Francophone Binding Corporate Rules (BCR) 2013 on cross-border transfer of personal data among French speaking countries.

According to UN conference on trade and development in Africa—data protection and privacy law



Data Protection and privacy in Ethiopia

- The Constitution of the Federal Democratic Republic of Ethiopia has recognized the right to privacy as a fundamental human right. For instance,
- **Article 26** 'everyone has the right to privacy [including] the right not to be subjected to search of his [or her] home, person or property, or the seizure of any property under his [or her] personal possession.'
- Article 26(2) stipulates that 'everyone has the right to inviolability of his [or her] notes and correspondence including postal letters, and communication made by telephone, telecommunications, and electronic devices.'

Contd.

- The Proclamation on Mass Media and Freedom of information contains some provision about the protection of personal data (590/2000)

'Any public relation officer, must reject a request for access to a record of the public body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual who has passed away before 20 years.'

The laws related Personal data in Ethiopia

- The Constitution; (More than 15 proclamations)
- Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 ('the Mass Media Proclamation');
- Civil Code of the Empire of Ethiopia Proclamation No. 165/1960 ('the Civil Code');
- Criminal Code of the Federal Democratic Republic of Ethiopia Proclamation No.414/2004 ('the Criminal Code');
- Criminal Procedure Code of the Empire of Ethiopia, 1961 ('the Criminal Procedure Code');
- The Food, Medicine, and Healthcare Administration and Control Council of Ministers Regulation ('the Regulation');
- The Communications Service Proclamation No.1148/2019 ('the Communications Service Proclamation')
- Computer Crime Proclamation No. 958/2016 ('the Computer Crime Proclamation')

Regulatory Authorities

- Data Protection law of the world requires, the establishment of the Office of the Data Protection Commission (DPC) whose mandate includes overseeing the implementation and enforcement of the provisions of the Personal data.
- However, there is no national data protection authority in Ethiopia,
- But there are some sector-specific government authorities have the power to regulate privacy and/or data protection issues within their regulatory scope

For Instance,

- **Ethiopian Institution of Ombudsman,** has a mandate to regulate the implementation of ATI laws (590/2000)
- **Ethiopian National Archives and Library**-is responsible to collect, systematically organize, preserve, and make the information resources of the country available for study and research purposes
- The Ethiopian Communication Agency, a regulator of the telecommunication sector, is empowered, among others, to 'promote information security, data privacy, and protection'

PB..contd.

- The Ethiopian Ministry of Revenue ('MoR'), which is the ministerial body responsible for the implementation and enforcement of tax laws including rules on the protection of tax information;
- MINT, a federal ministry organ, is empowered mainly to ensure and set general policy framework for the provision of quality, reliable and secure information technology service and oversee the implementation thereof
- The Information Network Security Agency ('INSA'), which is mandated to ensure that information and computer-based key infrastructure are secured;

PB..contd.

- The Ethiopian Food and Drug Administration ('FMHACA'), which has certain powers relating the protection of information of patients by health professionals.
- The Ethiopian Document Authentication and Registration Agency ('EDARA'), which is an organ responsible for coordinating and supporting the authentication and registration activities.
- The Financial Intelligence Center ('FIC'), which is an organ responsible for coordinating various institutions involved in the fight against money laundering and the financing of terrorism, to organize and analyze the information it receives and to perform other related tasks.

Challenges

- At international level, the fragmented approach to data protection and privacy law nationally, regionally and internationally poses many challenges going forward.
- Africa does not have a comprehensive data protection law that governs collection, storage, processing, and/or dissemination of personal data.
- Since privacy is an evolving concept, there is a weak privacy enforcement in Africa
- personal information could easily be shared with taxation authorities, the armed forces and other agencies. (Police may take your information from Banks easily)

The way forward

- An international harmonized data protection law in the form of a convention or treaty is currently is important.
- Attention should be given on developing a Model Law on the subject matter that govern all countries.
- Develop appropriate policies to facilitate the implementation of laws and guide the works of its organs in relation to privacy and data protection.
- Establish an independent organ mandated to oversee and enforce data protection and privacy in the country.
- Require all government agencies to appoint data protection officers or data protection compliance officers within their office.


THANK YOU