Data Protection Report Nigeria

AUGUST 6

American Business Council

AMERICAN BUSINESS COUNCIL
Promoting Nigeria America Economic Partnership

Contents

Introduction **3**

General Legal Framework for Data Protection in Nigeria **4**

Data Protection Act 2019 ..... **5**

Insights from Data Protection Experts **6**

Scope of Application **8**

Cross Border Transfer of Data **10**

Enforcement **11**

Conclusion and Recommendations **12**

Photos from the workshop 2020 ..... **14**

Appendix **15**

Introduction

The OECD defines data as the physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means [OBJ].
That definition helps us understand that data can cover a lot, ranging from employment records, criminal records, personal emails, bank records, health records, trade secrets and other vital information concerning individuals and corporations. The world contains an unimaginably vast amount of digital information which is getting even vaster more rapidly.

According to Domo, a fully mobile, cloud-based operating system, there are 2.5 quintillion bytes of data created each day at our current pace, but that pace is only accelerating with the growth of the Internet of Things (IoT). By 2025, it's estimated that 463 exabytes of data will be created each day globally – that's the equivalent of 212,765,957 DVDs per day according to the World Economic Forum. This huge availability of data is what the term 'Big Data' refers to. For a working definition, big data is a term that describes "a large volume of structured, semi-structured and unstructured data that has the potential to be mined for information[1].

Online media spend in the US totaled $145.3 billion in 2019, up 19.1% over 2018. The global ad spends for 2020 is projected to grow to $656 billion, driven in part by the U.S. Presidential Election and the Olympic Games, which will be held in Tokyo. So, it is clear that these data handlers may be dealing with the new oil or the new gold as the case may be. The huge value of data has made it attractive to governments, companies, and even hackers[2]. Data is now subject to cyber threats for example, millions of workers are using personal laptops–on unsecured home internet connections–to access work files. Many of which likely contain confidential information and personal data. During the Corona Virus pandemic, hackers broke into the networks of America's largest defense contractor, Lockheed Martin, by targeting remote workers.

"Data protection issues are a human rights issue" -
Teki Akuetteh, Former Executive Director of Data Protection Commission of Ghana & Founder and Executive Director, Africa Digital Rights' Hub

[1] https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#13588ffc60ba
[2] https://www.marketingcharts.com/advertising-trends/spending-and-spenders-111801

General Legal Framework for Data Protection in Nigeria

Most of the data that the world has produced are either personal data (or data that can be traced back to specific individuals). Traditionally, organisations used various methods of de-identification (anonymisation, pseudonymisation, encryption, key-coding, data sharing) to distance data from real identities and allow analysis to proceed while at the same time containing privacy concerns.

Over the past few years, however, computer scientists have repeatedly shown that even anonymized data can often be re-identified and attributed to specific individuals[3]. With the importance ascribed to data, it is pertinent that laws be established to protect the data so the persons who own the data, as well as the recipient of the data, are not put at risk. Data protection and privacy is an extension of the fundamental right of citizens to privacy. Section 37 of the 1999 Constitution (as Amended) protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication.

Aside from the Constitution, there are several other legislations that contains provisions that touch on the protection of data and privacy. Some of them include the Freedom of Information Act No. 4 of 2011 which enables public access to public records and information, and prevents a public institution from disclosing personal information to the public unless the individual involved consents to the disclosure.

The Cybercrimes Act 2011 prevents the interception of electronic communications and imposes data retention requirements on financial institutions.

The Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission requires telecommunication operators to take reasonable steps to protect against "improper or accidental disclosure" and must ensure that such information is securely stored. It also provides that customer information must "not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations".

The Consumer Protection Framework issued by the Central Bank of Nigeria in 2016 contains provisions that restrain financial institutions from disclosing the personal information of their customers. It has however been evident that though these preceding pieces of legislation exist, there has been no comprehensive data protection and data privacy legislation in Nigeria.

The Data Protection Regulation 2019: The National Information Technology Development Agency ("NITDA/the Agency") was set up by the National Information Technology Development Agency Act 2007 (NITDA Act) as the statutory agency with the responsibility for planning, developing and promoting the use of information technology in Nigeria.

The NITDA Act also empowers the Agency to do the following:

"Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information".

It was further to the foregoing powers that on 28th January 2019, NITDA published its Data Protection Regulation which aims at protecting personal data of all Nigerians and non-Nigerian residents in Nigeria[4].

Data Protection Act 2019

This is an Act to establish the Data Protection Commission charged with the responsibility for the protection of personal data and data subject rights and regulation of the processing of personal information and for related matters.

On the 3rd of March, 2020, the American Business Council in partnership with Microsoft Nigeria and Hewlett Packard operated by Selectium held a Data Protection workshop to set the right foundation for the Data Protection Bill by bringing all stakeholders from both the public and private sector to deliberate on the laws and guidelines on data protection that would be best fit for Nigeria.

"The Senate is ready to support data protection and enhance ease of business for investors in Nigeria" - Senator Yakubu Oseni, The Chairman, Senate Committee on ICT.

[3] Paul Ohm,Broken, Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010); Arvind Narayanan & Vitaly Shmatikov,
Robust De-anonymization of Large Sparse Datasets, 2008 Proc. of IEEE Symp. on Security & Privacy 111; Latanya Sweeney, Simple Demographics Often Identify
People Uniquely 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).
[4] NITDA Data Protection Regulation.

Insights from Data Protection Experts

A Data Protection expert from Ghana, Ms. Teki Akuetteh gave insights on how Ghana developed and implemented its Data Protection Laws whose main purpose was to create an enabling environment for the ICT sector in Ghana.

Ghana's pathway to attaining a Data Protection law is enumerated below

I. Laws that provide a framework encourage growth in the ICT sector. 419 issues had stunted the growth, Ghana was trying to tackle the bad issue because e-commerce and online trade were affected and decided to create a trust system that would enable 3rd parties to deal well with Ghana and complete online legitimate transactions

II. To build trust in the system and to build individuals trust in ICT systems, an Independent Regulator must be created, and the laws and protection must be assured.

III. To determine the MDA that will take charge of this, it was important to explore issues like who has the technical capacity and purview. It was decided there would be collaboration but with one lead ministry.

IV. Determine the key stakeholders and include them in the conversation at an early stage. Stakeholder engagements are crucial with those in the industry, civil society, consumer groups, individuals and beneficiaries. Data Protection is a highly specialized area, so it was important to keep that in mind when choosing experts, one must engage key stakeholders at every stage.

V. Comprehensive review of existing laws by identifying the gaps and what is needed to create an enabling environment. Also adopting features that enable your market to participate in the global stage by benchmarking against regional and international best practices.

VI. The Ghanaian Government used the U.K. as a model because of the legislative structure and nature of economy. The Ghanaian Government determined which resources will be available as this will determine where the law will be positioned, understand the environment and ensure the Law is streamlined for international cooperation and enforcement.

"Privacy is a fundamental right, essential to autonomy and the protection of human dignity serving as the foundation upon which many other human rights are built" - Otilia Phiri, Attorney Emerging Markets. Middle East & Africa.

VII. The enforcement of powers had to be determined if the implementing Agency would have only administrative powers and/or the right to give criminal sanctions. The powers given to the Data Protection Regulator determine the level of respect the office will hold. Administrative powers for the Agency enable them to take decisions and enforce them in the quickest possible time.

VIII. The level of compliance for SMEs and MSMEs is expectedly lower compared to multinationals and big businesses. When applying the rules, it was less stringent for smaller businesses. Free training was also provided to bring the companies up to standard.

IX. Implementation at the inter-ministerial level involved creating necessary buy-in, building their understanding of the law and the rationale behind certain decisions/inclusions

X. Setting up of the Regulator:

- An interim body was established to facilitate the set-up of the Agency while a Blueprint for setting up the agency was designed
- Appointment of the governing body comprising of people from the ministry and industry ensuring the independence of the agency and protecting it from political interference
- The appointment of the Administrative Head

- Admin and Staff training
- Implementation: the most challenging stage. Involved awareness creation using mostly online tools, short videos etc. the first year was focused on awareness creation. The next phase involved registration and compliance structures. This was followed by the development of internal policies.
- Enforcement: it was decided to use a carrot and stick approach. In instances of criminal enforcement, the Agency would work closely with other Government Agencies. Independence must be seen. The same stick that is being used on one actor must be used on another to ensure that the process is seen as serious and fair. i.e. when regulating state actors, state actors accused of the same offence must be treated the same as non –government organizations. This affects compliance rates and integrity of the Agency.

The Commercial Attorney, Emerging Markets for Microsoft Otilia Phiri gave an overview on Privacy, Models & Principles of Data Protection and focused on 3 sections: Privacy as a fundamental human right, comparative models of data protection and core principles of data protection.

I. Privacy as a fundamental human right

Privacy is a fundamental right which enables individuals to exercise other rights. Privacy and Power are interlinked and play a huge part in the ethics of modern life – we are more reliant on technology and data than ever before and with that comes more considerations and implications for personal data.

Data is increasingly being used for scenarios such as:

- Decision making use of personal data to make decisions that impact the individual such as allocation of resources e.g.: creditworthiness
- Monetization – commercialization of personal data by companies or individuals
- Surveillance – use of personal data to track or monitor data subjects

It has been said that data is the new oil and while the commercialization of personal data is a powerful conduit for commerce and has the ability to empower lives, it is important for this opportunity to be balanced in light of rising cybersecurity concerns. Data is also central to many states' e-government or digital government strategies and essential to enable states to scale access to government services and enhance citizen engagement but the dark side of that is potential for abuse via pervasive surveillance.

These growing concerns on privacy are fueling the emergence of data protection regulation aimed at balancing the opportunity presented by the digital economy with the best interests of citizens.

II. Comparative Models of Data Protection

Data Protection Regulation must consider:

- The best of technology
- Trade and economic development
- Protecting individual citizens
- Public safety and security

International Initiatives	Regional Initiatives	Examples with focus on the African region	Challenges with existing Models:
UN General Assembly Statement of Right to Privacy in the Digital Age	EU General Data Protection Regulation	**Mauritius**	Addressing gaps in coverage
Organization for Economic Cooperation and Development Guidelines on Protection of Privacy and Trans border Flows of Personal Data	Asia Pacific Economic Cooperation Privacy Framework	**South Africa**	Addressing new technologies
	African Union Convention on Cybersecurity & Personal Data (Malabo Convention)	**Kenya**	Managing cross-border data transfers
			Balancing surveillance and data protection
			Strengthening enforcement
			Determining jurisdiction
			Managing the compliance burden

III. **Data Protection Core Principles include the following:**

- Openness/transparency
- Collection limitation
- Purpose specification
- Use limitation
- Security
- Access
- Correction
- Accountability

The workshop looked at three areas of the Data Protection Act - Scope of Application, Cross Border Transfer of Data and Enforcement.

Scope of Application

Participants in the session include Paradigm Initiative, World Bank, Facebook, Microsoft, Punuka Attorneys, NCC, NITDA and the vice-chairman, House Committee on Telecommunication at the 8th National Assembly.

The Session highlighted several key issues along the line of scope of Application by the bill and developed a common consensus. Various sections of the bill were drilled into for further understanding and recommendations.

I. **Enforcement:**

Conscious of the concerns around privacy and protection of Personal Data and the grave consequences of leaving personal data processing unregulated, data gathered by various parties such as NGOs/NFP, Multilateral agencies, private sector and the public institutions needs to be checked as this will minimize the risk of data mismanagement as most institutions run an analogue system.

For third party apps that run on social media platforms and access the data of Nigerians and its residents, the NCC stated that a committee has been set up to look at Digital Service Providers formerly known as OTT because it is assumed it has gone beyond an app thereby having access to personal data. Currently, these platforms such as the social media platforms lay out the data protection laws of the countries to the third-party applications to abide to. It is also been noted that the scope of the bill will look at transactional data and not the static data i.e. the data an individual generates while using the internet, as people actively leave digital footprints on the internet or use unsecure internets which is as a result of low awareness of the dangers to data abuse.

Whilst making the application of the law broad there is a need to apply various sector use cases on how they interact with data instead of limiting it to NCCs definition of Digital Service Providers as Over the top (OTT). For instance, there are direct carrier billers who connect with mobile network operators and digital service providers (for instance apps on google play store) to ensure that customers pay for subscription through their airtime billings. Other platforms use social media to disseminate information. The aim is for the bill to be technologically neutral and as much as possible be broad enough to cover and apply to any new use cases.

Identification of the core Ministries, Departments and Agencies that regulate industries interfacing with individual's data either in their own processes (surveillance) or those that they regulate (usage - data monitoring or monetization) such as, the credit bureau, the NFIU (surveillance) EFCC, CBN, NCC, NITDA is pertinent. This will ensure the necessary buy-in from the relevant stakeholders. In this way compliance and enforcement are easily adopted.

From an enforcement perspective, Agencies that their operators (controller or processor) interact with non-resident data should ensure that they have a form of existence in Nigeria either by creating a designated officer or power of attorney to existing local entities for enforcement purposes.

II. Data Controller/processor:

Section 2
(c) a data controller and data processor in respect of personal data where----

This section makes mention of a data controller and a data processor but has no clarity of who is a data controller and processor. If an agency is regarded as a data controller the scope of work by the Agency needs to be clarified. Agencies such as NITDA or NIMC are not data controllers. NIMC can collect it and decide what to do with it.

III. Localization:

Section 2 (c) a data controller and data processor in respect of personal data where----

ii. The data controller is not established in Nigeria but uses equipment or a data processor in Nigeria to process personal data of data subjects who are within the territory of Nigeria, or

iii. Processing is carried out in respect to data subjects who are within the territory of Nigeria and personal data which originates partly or wholly from Nigeria.

This section looks at foreign companies that have little or no presence in Nigeria but also sounds restrictive. The GDPR covers data processors or controllers who interact or process data of EU members irrespective of whether it emanates from the EU. The scope must be widened considering the virtual nature of certain platforms. As they may not use data equipment or data processors in Nigeria, they may not process data of data subjects who are domesticated or residing in Nigeria and personal data may not originate partly or wholly from Nigeria. It may also be from data subjects who are

Nigerians but are not based in Nigeria and this does not cover that. It is important to note the NDPR which is a secondary policy initiative will throw more light on the composite sections of the primary legislation.

IV. Data Categories and Principles:

The stakeholders looked at the categories of data and the basic principles on Section 3 (1) B &C of the Act and suggested that there is a need to have guidelines for institutions as some data are being processed for a purpose that is incompatible with those purposes for which the data were initially collected.
In some cases, agencies request for data from the private sector which should be curtailed to prevent abuse of private information.

Cross Border Transfer of Data

Participants include representatives from IBM, Citibank, NIPC, Advocat Law, Jumia, NITDA and Lagos Business School.

I. Benefits and risks with Localization of Data

With the inclusion of localization requirements in Data Protection Agreements, there is the perception that this provides increased security of the data; and increases the ability for the Regulator/State to protect the privacy of their citizens. In addition, there is perhaps the belief that localization would encourage the growth of Nigerian based data center infrastructure and encourage growth of local content driven digital economy. The implications for both rationales should be examined carefully, as localization of data does not necessarily make for the most secure option nor does local data center infrastructure mean an increase in jobs nor directly result in increased growth for the digital economy. By insisting on the physical location of data within Nigeria we may be limiting ourselves to less viable options.

While in the Nigerian context, provisions are made for the transfer of data, i.e. localization is primarily a requirement for Government data and Customer data, the conditions and timeframes associated with permission can be lengthy. For example, Under the Bill, Nigerian organizations are permitted to share data across borders as long as the recipient host country is on a 'White List' - countries deemed to meet the minimum requirements of data protection principles by NITDA. If the countries they wish to send data to, are not on the White List, then they must either apply for permission from NITDA who approve/reject the proposal together with the Office of the Attorney General. Additionally, when businesses send data across borders, they are required to duplicate the data for physical storage in the country.

This in effect is an added bureaucratic and economic burden to business operations and could reduce the attractiveness of foreign direct investment in Nigeria, most especially for businesses where the cross-border flow of data is key, and impediments to this movement have business implications for example, financial services and e-commerce.

II. Impact of restriction on Data flows for Trade and Development

Cross border data flows are key to enabling participation in the global economy, especially as it becomes increasingly digital. A number of businesses (banking, mobile money, e-commerce, miscellaneous SMEs/MSMEs) in Nigeria have access to a world market through the digital economy, and or have businesses that are heavily reliant on the unencumbered flow of data across borders. Restrictions on cross-border data flows, especially if they do not serve the purpose of security and safety of data and privacy may lead to the stagnation of these businesses and leave them unable to take full advantage of opportunities the digital economy provides.

Stakeholders can take a cue from the standard driven framework by APEC, or the standard contractual clauses as leveraged by US and Europe and free flow of data within EU as something plausible under the Africa Continental Free Trade Area (AfCFTA) for easy flow of data.

In learning for Nigeria's case, any data that is requested by firms or State should be justifiable and it should be made clear in the Bill what 'justifiable' means i.e. data requested should be fit for stated aim, rather than collecting unnecessary data to stated aim.

III. Opportunities presented by the Digital Economy

In order to take full advantage of the digital economy while also remaining well regulated, it is necessary to do economic projections of the impact these restrictions have on all sectors of the economy that utilize the digital economy.

Conditions such as prior consent before transfers – it is arguable if they really protect the consumer, as most people agree to Terms and Conditions without a comprehensive/full understanding of the implications. However, when companies must comply with presenting these additional permissions, it can be quite a large added time cost and at times has financial implications for companies to comply with. Additionally, storage of certain information to comply with requests of information, also adds to added technical processes and costs.

The digital economy provides the opportunity to take advantage of the scaling of digital platforms – thus leading to more competitive costs with a wider choice of services e.g. cloud infrastructure.

Enforcement

Participants in the session include representatives from Facebook, American Business Council, NITDA, Paradigm Initiative, NIPC, NOTAP, Selectium, and Open Society Foundation.
This breakout session focused on five key issues.

I. Establishing a new institution for data protection/building one into an existing institution

To set up an independent institution that ensures transparency from a public perspective would require a foundation based on human rights. And for this institution to thrive, the law must empower it to sanction non-compliance with its provisions on data protection. It is also ideal that the same institution should oversee access to information (Freedom of Information) and the enforcement of Data Protection as practiced i.e. South Africa, which has a single authority that oversees data protection and access to information. This will help create synergy and ensure both rights are respected. To avoid confusion, there also needs to be legislation expressly giving this new institution oversight over FOI, which currently resides with the Attorney General.

II. Composition of the Institution

This institution overseeing data protection should be made up of the private institutions and key stakeholders such as Private sector data controllers, CSOs and Academics. A huge majority of this composition should be a diverse team including the CSOS with expertise in human rights, especially the right to privacy and data protection in Nigeria, while the minority should be public institutions.

III. Requirements of establishing DPOs (Data protection officers)

Each public and private institution should have a data protection officer to ensure that the laws on data protection are strictly adhered. However, the law should clearly state the requirements or criteria for being designated or appointed as a data protection officer.

IV. Registration of "data processors" and/or "data controllers

Various stakeholders acknowledge the DPCO (Data Protection Compliance Organisation) model introduced by NITDA which is an intermediary that interfaces between the Data Controller or Processor and the Supervising Authority but no recommendation was made on this specific feature being incorporated into the new data protection law.

V. Audit & Compliance

Stakeholders are yet to conclude on the possibility for this new institution to take on auditing and compliance to the NDPR or whether the management of data should reside within NITDA and not the new institution.

Conclusion and Recommendations

I. Awareness on data protection to the Nigerian citizens needs to be carried out effectively, especially with the youths. Citizens ought to be adequately educated about their data rights and red flags to consider before disclosing their personal data. For example, most Nigerians participate in all kinds of surveys, healthcare projects, and community projects. There has not been any kind of guidance to what kinds of information should be collected. Lean data (collating data that will be relevant by the data processor) should be encouraged and enforced by the Data Commission as unwanted information is being requested by both private and public institutions. The Regulation should cater for a data whistle blowing policy provision and mandate the data controller to have this mechanism in place.

II. A Sectoral approach at looking at the kinds of protections each sector has in place before we conclude on the Bill. For example, a look at the financial space, Immigration, Real estate, Insurance, Healthcare and others. On the other hand, while it may be difficult to properly identify how all the sectors would be protected as it relates to the disclosure or reporting requirement of their data subject, it may help to find a basic acceptable standardized approach. The best scenario is to create a standardized process before such information on their data subject can be released to a relevant agency or body i.e. through a warrant, court order, or criteria that looks at public safety that outweighs the personal protection of the data subject.

III. It is advisable that regulators and policy makers look at emerging technologies to determine the regulations around the technologies with intent of not hampering its growth. Regulation in the global stage means creating standards and not a clamp down.

IV. Engagement with critical stakeholders is crucial for the policy and this report. The rapid pace of technological advancement and innovation, stunting development at this stage with poorly articulated policy could leave us farther in the race to catch up to the global economy players. It is therefore key that the ABC and partners find quick means of engaging government stakeholders with a view to ensuring that these recommendations are considered in the Bill before it is passed into law.

V. The agencies that interface with ICT should be collaborative and not divisive in order to improve investor confidence in the market. Also, upon reasonable suspicion there should be an allowance for the Data commission to conduct unannounced vulnerability testing or data usage audit. The procedures for identifying the veracity of filings made by a DPCO to the Data Commission needs to be considered.

VI. The Bill should have a line enforcing third party applications that requires data of users on platforms such as social media. This will ensure the protection of Nigerians and its residents on such platforms.

VII. A principle-based approach should be incorporated with an agreement on common privacy outcomes. Such as the Principle of adequacy as referenced in other Data Protection Regulations e.g. EU GDPR. A delicate balance needs to be achieved giving enough flexibility to allow stakeholders to achieve operational efficiency, while allowing enough strength for the Data Protection Commission to enforce discipline.

VIII. There is a need to segment critical and non-critical data that would be subjected to stringent requirements. This would be a departure from a blanket localization measure. In addition, options for security measures provide better safeguards for the data, rather than localization, should be considered strongly.

IX. The Bill and resulting Act has to be open enough to be able to take advantage of global scaling. It should not try and maintain provision of services associated with the data pipeline especially in areas where Nigeria has not developed provision of services to a competitive level for purposes of security.

X. The resulting Act should include a Code of conduct – this is arguably more effective in ensuring higher compliance and also provides clear guidelines for stakeholders to apply to their operations.

XI. Data Localization measures should be considered within the operational environment of Nigeria and the practical availability of data centers in Nigeria i.e. are there enough data centers to meet supply and do they meet applicable service standards of economic efficiency are there measures to develop Nigeria into regional technology hub attracting foreign direct investment to enhance the digital economy. Setting up Tier 3 data centers requires huge investment in construction, energy/power supply, operations and the connectivity requirements to enable efficient operation of data centers. Others such as security implications associated with localization should be considered for the country i.e. using data storage within the country instead of using cloud services of foreign origin which could be cheaper and/or more secure.

XII. Cross border data flow is a global concern and to ensure that this is seamless, Nigeria needs to first thrive in building a good data protection regime through engagements with domestic stakeholders and then internationally by partaking in global discussions and collaborating with existing international bodies or regions. The AFTCA can also be used to facilitate data flow among participating members with an established framework. This is to get a comprehensive understanding from both sides of challenges regarding balancing data security and privacy with cross border flows of data. A more balanced treatment of challenges is needed in order to create an enabling environment for trade and development.

XIII. The Government and Civil Society Groups should undertake a comparative analysis of other data protection arrangements in different countries, together with an observation of attendant impacts and endeavor to learn from the successes and mistakes of other countries. In conjunction with stakeholders, the Government and Civil Society Groups should determine those aspects that would work in a Nigerian context and determine which parts should be amended and what form that should take.

XIV. The proposed data protection bill must empower rights-holders – the individuals or groups that have entitlements in relation to duty-bearers - to claim and exercise their rights. It must also strengthen the capacity of duty-bearers – the state or non-state actors that have the obligation to uphold the human rights of rights holders – to promote and protect those rights. The five basic principles of the human rights approach are;
Participation – everyone is entitled to active participation in decision-making processes which affect the enjoyment of their rights.
Accountability – duty-bearers are held accountable for failing to fulfil their obligations towards rights-holders. There should be effective remedies in place when human rights breaches occur.

Non-discrimination and equality – all individuals are entitled to their rights without discrimination of any kind. All types of discrimination should be prohibited, prevented and eliminated.
Empowerment – everyone is entitled to claim and exercise their rights. Individuals and communities need to understand their rights and participate in the development of policies which affect their lives.
Legality – approaches should be in line with the legal rights set out in Nigerian and international laws.

XV. This composition of the institution overseeing data protection should consist majorly of the private institutions and key stakeholders such as Private sector data controllers, Academics, CSOs with experts on human rights, while the minority should consist of the public institutions.

Photos from the workshop 2020




Appendix

Some key words identified in the Regulation and Act; they include Data Subjects, Data Controllers and Data Protection Officers. The roles of the identified persons are envisaged to be very important in driving the objectives of the Regulation.

I. **A Data Subject** is the identifiable person who is identified directly or indirectly with reference to an identification number or other factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

II. **The Data Protection Officer** is a person designated by the Data Controller to implement the Regulation. The person's responsibility is to ensure compliance of the Data Controller with the Regulation.

III. **A Data Controller** is/are the person or persons who determine how personal data is processed or will be processed.

IV. **Processing** means any action carried out on personal information. It includes collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure or dissemination.

Abbreviations

I. **NITDA:** National Information Technology Development Agency, an agency committed to implementing the National Information Technology Policy. Its mandate is to create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices in Nigeria

II. **NIMC:** National Identity Management Commission has the mandate to establish, operate, maintain and manage the National Identity Database in Nigeria, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to Nigerians as well as others legally residing within the country.

III. **AfCFTA:** The African Continental Free Trade Area is a free trade area which, as of 2018, includes 28 countries. It was created by the African Continental Free Trade Agreement among 54 of the 55 African Union nations. The free-trade area is the largest in the world in terms of the number of participating countries since the formation of the World Trade Organization.