



**WORLD WIDE WEB**  
FOUNDATION

# PERSONAL DATA PROTECTION IN NIGERIA

March 2018

[www.webfoundation.org](http://www.webfoundation.org)

# CONTENTS

<b>Glossary</b>	<b>3</b>
<b>Executive Summary</b>	<b>4</b>
<b>01 A Primer on Data Protection</b>	<b>6</b>
<b>02 The State of Data Protection in Nigeria</b>	<b>10</b>
<b>03 The Adequacy of Data Protections</b>	<b>18</b>
<b>04 Key Findings</b>	<b>22</b>
<b>05 Recommendations</b>	<b>25</b>



This report was written by Chukwuyere Ebere Izuogu, LL.B (UNIBEN), BL, LL.M (Hannover), ACI Arb, AMBCS, Senior Associate, Streamsowers & Köhn for the Web Foundation.

It was produced by the [Web Foundation](#) and [Paradigm Initiative](#), in collaboration with Google and with support from [Omidyar Network](#).

The Web Foundation was established in 2009 by Sir Tim Berners-Lee, inventor of the World Wide Web. Our mission is to establish the open web as a public good and a basic right.

Paradigm Initiative is a social enterprise that builds an ICT-enabled support system and advocates digital rights in order to improve livelihoods for under-served youth across Africa.

## **Acknowledgements**

With thanks to the Web Foundation's Craig Fagan; Nnenna Nwakanma; Ana Brandusescu and Paradigm Initiative's Babatunde Okunoye, for their support and guidance during this study.

Copyright 2018, World Wide Web Foundation, [CC BY 4.0](#)



# GLOSSARY

ACRONYMS	MEANING
API	Application Programming Interface
AU	African Union
CPC	Consumer Protection Council
DPA	Data Protection Act (Ghana)
ECOWAS	Economic Community of West African States
EU	European Union
FGN	Federal Government of Nigeria
FIPs	Fair Information Practices
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
HTML	Hypertext Markup Language
ICT	Information Communications Technology
ISP	Internet Service Provider
IT	Information Technology
LEAs	Law Enforcement Agencies
MDAs	Ministries, Departments or Agencies
MNO	Mobile Network Operator
NCA	Nigerian Commissions Act
NCC	Nigerian Communications Commission
NHA	National Health Act
NHRC	National Human Rights Commission
NIMC	National Identity Management Commission
NITDA	National Information Technology Development Agency
NIS	Nigerian Immigration Service
OECD	Organization for Economic Cooperation and Development
OBA	Online Behavioural Advertising
OS	Operating System
PETs	Privacy Enhancing Technologies
POPI	Protection of Personal Information Act (South Africa)
SSS	State Security Services
UN UDHR	United Nations Universal Declaration of Human Rights
URL	Uniform Resource Locator
US	United States of America
WTA	Wireless Telegraphy Act

*Methodological elements and definitions of terms used in this study are contained in Annex 1.*

# EXECUTIVE SUMMARY

*The collection and processing of personal data<sup>1</sup> raises significant privacy and data protection concerns for every citizen. The legal remedy to this problem is data protection to ensure privacy.*

At the international level, the right to the protection of one's privacy, especially from intrusions by the state, is enshrined in Article 12 of the United Nations (UN) Universal Declaration of Human Rights (UDHR) of 1948.

Still, this does not resolve the issue of how to address the privacy of one's personal data. Some legal frameworks have attempted to set out under what conditions personal data may be collected and/or processed. In the European Union (EU), the data protection landscape is presently undergoing a comprehensive reform with the introduction of the General Data Protection Regulation (GDPR), which is expected to come into force on 25 May 2018 across member states of the EU<sup>2</sup>.

At the African regional level, the African Union Convention on Cybersecurity and Data Protection (2014) and the Economic Community of West African States (ECOWAS) Data Protection Act (2010) both seek to, inter alia, provide a common framework for data protection among member states, including Nigeria.

In Nigeria, while privacy is a fundamental human right guaranteed by the Constitution of the Federal Republic of Nigeria (the Constitution), comprehensive data protection legislation has yet to be enacted — even as several government and private organisations routinely collect and process personal data. Instead, the existing regulatory frameworks that apply to personal data protection are from the broadly phrased Section 37 of the Constitution, which provides that: “The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected”, as well as a hodgepodge of other industry (or situation-specific) frameworks<sup>3</sup>.

- 1 In this study, “personal data”, “personal information” and “personally identifiable information” are used interchangeably.
- 2 The GDPR plans to replace the extant Data Protection Directive of the European Commission, which has been in force since 1995.
- 3 These include the National Health Act applicable to health records, the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations applicable to the communications sector and the Bank Verification Number (BVN) policy applicable within the financial services sector.

These regulatory frameworks are consistent with the data protection principle of lawful processing of personal data and, in at least one case, expressly set limits on how personal data is collected and may be used. However, most of these frameworks do not clearly define the level of protection afforded to the personal data collected, state the data controller's accountability obligation(s), or contain any other data protection principle, as is the norm in the data protection legislation of other countries. As a result, there is currently no overarching legislation on data protection in Nigeria.

To better understand the current context, the Web Foundation and Paradigm Initiative commissioned a review of the data collection practices in the country, as well as the policies and regulations in place to govern the collection, protection, and use of this data.

## Findings

**The review shows** that there are five primary concerns around the collection and use of personal data — both online and offline — in Nigeria:

- Q The use of personal data may be incompatible with the purpose for which it was collected;**
- Q Individuals have no rights in relation to the collection, use, and storage of their personal information;**
- Q Nigerians are not offered adequate opportunities to consent to or opt out of data collection;**
- Q There is limited to no transparency around the processing of personal data, and there is limited information available around how this personal data is used and stored, leading to greater risk of a personal data breach;**
- Q Children are exposed to privacy risks online and often lack the legal capacity to give valid consent, and may unknowingly disclose personal information to online platforms due to the appealing nature of their visual content.**

## Policy recommendations

Given these findings, we recommend that Nigeria's National Assembly draft and approve a data protection framework or bill that ensures:

- **The use of personal data is in accordance with the purpose for which it was collected (purpose specification);**
- **The consent of the individual is obtained prior to collecting his/her personal data;**
- **The rights of the individual to seek legal remedies for misuse and/or unauthorised access to his/her personal data is guaranteed.**

These three areas can be addressed through six particular measures and channels:

- 1. Legislative measures by the National Assembly**
  - Enact a Data Protection Act
  - Amend the National Identity Management Commission (NIMC) Act
  - Enact a Child Online Privacy Protection Act
- 2. Non-legislative (soft law) measures**
  - Undertake administrative rulemaking by the NIMC
- 3. Judicial measures**
  - Encourage superior courts of records in Nigeria to engage in judicial activism
- 4. Enforcement measures**
  - Engage the National Human Rights Commission (NHRC) to enforce data protection cases
  - Engage the Consumer Protection Council (CPC) to provide redress
  - Ensure that the NIMC and sector-specific regulators (including the CPC and NCC) with consumer protection authority take action
- 5. Executive measures**
  - Call on the Federal Government of Nigeria (FGN) to harmonise institutional efforts and remits
- 6. Social measures**
  - Encourage civil society organisations (CSOs) to advocate for change

# 01

## A PRIMER ON DATA PROTECTION

*Data protection is the legal mechanism that ensures privacy.<sup>4</sup> While conceptually distinct from the 'right to privacy', most good data protection regulatory frameworks are similar in the sense that they contain similar principles for collecting, processing, and transferring personal data.*

**I**n Nigeria, there is currently no legislation on data protection. The National Assembly is reviewing the Data Protection Bill 2017, which seeks to make provisions for the regulation of information relating to individuals. Under the Bill, personal data is defined to mean "data which relates to a living individual who can be identified either from those data or from those and other information which is in the possession of or is likely to come into the possession of the data controller, and includes any expression or any expression of opinion about the individual and indication of the intentions of the data controller or any other person in respect of the individual".<sup>5</sup>

<sup>4</sup> Jovan Kurbalija. (2017). 'An Introduction to Internet Governance' <https://www.diplomacy.edu/resources/books/introduction-internet-governance>, p. 211.

<sup>5</sup> Clause 10.

## 1.1 Relevant Regional Legal Instruments

### AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION 2014

The African Union Convention on Cyber Security and Personal Data Protection (the Convention) is an international legal instrument entered into by the members of the African Union (AU), including Nigeria<sup>6</sup>. Respecting data protection, the Convention has the goal to address the need for a harmonised legislation in the area of cyber security in member states of the African Union, and to establish in each state party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use.

However, the Convention — like any international treaty entered into by the government of Nigeria — does not acquire the force of law in Nigeria, until enacted into law by the National Assembly, pursuant to Section 12 of the Constitution. As of the time of this study, the Convention is yet to come into force in Nigeria.

### SUPPLEMENTARY ACT ON PERSONAL DATA PROTECTION WITHIN ECOWAS (THE ECOWAS DATA PROTECTION ACT)

On 16 February 2010, the signatories of the ECOWAS<sup>7</sup> Treaty, including Nigeria, adopted the ECOWAS Data Protection Act on the protection of personal data within ECOWAS member states. The ECOWAS Data Protection Act obligates member states to establish a legal framework of protection of data privacy relating to the collection, processing, transmission, storage, and use of personal data, subject to the general interest of the state<sup>8</sup>. However, the ECOWAS Data Protection Act is yet to acquire the force of law, pursuant to Section 12 of the Constitution.

## 1.2 Good legislative model

There are various examples from across the regions of good models for personal data protection.

In the EU, personal data is defined as information relating to an identified or identifiable person<sup>9</sup>. An ‘identifiable’ person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location information, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person<sup>10</sup>. As a general rule, a person is ‘identified’ when they can be ‘distinguished’ from all other persons within a group of persons. In contrast, ‘anonymous’ information is information which does not relate to an identified or identifiable person or to personal data rendered anonymous, the data subject is not identifiable and information about them does not constitute personal information<sup>11</sup> for the purpose of data protection<sup>12</sup>.

In the US, there is no singular definition of what constitutes personal (identifiable) information; instead, the definition of personal information is derived from the particular law applied and the circumstance of its application. For example, in the US, certain laws define personal information to include social security numbers and other government-issued identification numbers, financial account information, medical information, health insurance information, and identifiable information collected from children

In South Africa, personal information is statutorily defined under the Protection of Personal Information Act 2013 (POPI) to mean “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to” information such as one’s race, gender, sex, ethnicity, colour, sexual orientation or age.

6 The AU comprises of the following member states; Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central Africa Republic, Chad, Comoros, Congo, Cote d'Ivoire, Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sahrawi Arab Democratic Republic, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somali, South Africa, South Sudan, Sudan, Swaziland, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe.

7 ECOWAS is a regional group of 15 Member States comprised of Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

8 Article 2.

9 Article 4 (1), GDPR.

10 Ibid.

11 However, according to the Information Commissioner's Office (ICO) in the UK, “If the risk of identifying anonymous data] is reasonably likely the information should be regarded as personal data”, See Information Commissioner's Office. (2014). ‘Anonymisation: managing data protection risk code of practice’ <https://ico.org.uk/media/1061/anonymisation-code.pdf>, p. 6.

12 Recital 26, GDPR.

In Ghana, personal data under the Data Protection Act 2012 (DPA) is statutorily defined to mean “data about an individual who can be identified from the data; or from the data or other information in the possession of, or likely to come into the possession of the data controller”.

A good data protection framework such as the GDPR, POPI, DPA and/or the Fair Information Practices (FIPs) will contain all or most of the following data protection principles as illustrated in the table on the following page.



**Table 1** — Data Protection Principles of the GDPR, POPI, DPA and/or the FIPs.

DATA PROTECTION PRINCIPLE	DESCRIPTION	GDPR	FIPS	POPI	DPA
<b>Fair and lawful processing</b>	Data controllers must have a lawful basis for processing personal data and sensitive personal data.	Article 5 (1) (a)	Article 12	Sections 9 & 11	Sections 18 & 20
<b>Purpose specification</b>	The purpose for which personal data is processed must be clearly stated by the data controller, at a time no later than when the information is collected. Where information is processed for an alternative purpose, there must be a corresponding legal basis since the data controller cannot rely on the initial legal basis.	Article 5 (1) (b)	Article 10	Sections 9 & 11	Section 22
<b>Relevant (or data minimisation)</b>	The data controller should limit the processing and/or collection of personal information to directly achieving the specific purpose for which the information is collected or processed.	Article 5 (1) (c)	Article 8	Sections 9 & 11	No equivalent provision
<b>Accurate</b>	The data controller holding personal information shall not use that information without taking steps to ensure with reasonable certainty that the data is accurate and up-to-date.	Article 5 (1) (d)	Article 8	Sections 9 & 11	Section 26
<b>Retention</b>	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article 5 (1) (e) GDPR). <sup>13</sup>	Article 5 (1) (e)	No equivalent provision	Section 15	Section 24
<b>Data subject's rights</b>	Data controllers have in place an administrative mechanism to protect certain rights granted to the data subject. These include the right to: <ul style="list-style-type: none"> <li>– request from any controller information as to whether the controller is processing his/her data;</li> <li>– access his/her own data from any controller who processes such data;</li> <li>– have his/her data rectified (or blocked, as appropriate) by the controller processing his/her data, if the data is inaccurate; and</li> <li>– have his/her data deleted or blocked, as appropriate, by the controller if the controller is processing his data illegally.</li> </ul>	Articles 5 (1) (d), 12, 15, 16, 17, 18, 19, 20 & 21	Article 13	Sections 23, 24 & 25	Sections 32 & 33
<b>Data security</b>	Data processing operations adopt security measures that safeguard the confidentiality, integrity and availability of the personal data processed, and the systems used for processing them.	Articles 5(1) (f), 24 (1), 25 (1) (2), 28, 32, 33 & 34, and Recital 39	Article 11	Sections 19, 20, 21 & 22	Sections 28 & 30
<b>Accountability</b>	Data controller shall be accountable for implementing and/or complying with measures which give effect to the other data protection principles.	Article 5 (2)	Article 14	Section 8	No equivalent provision

<sup>13</sup> Article 5 (1) (e) GDPR.

# 02

## THE STATE OF DATA PROTECTION IN NIGERIA

*The Nigerian National Policy for Information Technology 2000 (IT Policy) is arguably the first attempt by the Federal Government of Nigeria (FGN) to articulate a policy direction concerning its intention to protect personal data.*

**T**he IT Policy has as one of its general objectives the promotion of legislation (Bills & Acts) for the protection of online, business transactions, privacy and security<sup>14</sup>. Unfortunately, at the time of this study, no legislation has been enacted in Nigeria to protect privacy or personal data.

### 2.1 Existing and Proposed Legislation

In Nigeria, the right to privacy is a fundamental human right guaranteed in Section 37 of the Constitution. In particular, Section 37 provides that: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected". Although phrased in a broad manner, it is pertinent to state that Section 37 is only available to 'citizens' of Nigeria.<sup>15</sup>

<sup>14</sup> Paragraph 4 xxiii.

<sup>15</sup> In the context of communications services, this constitutional provision was asserted in *Barr. MTN v. Barr. Godfrey Nya Eneye*, where the Plaintiff claimed that MTN's unauthorised disclosure of his mobile number to third parties, who subsequently sent a flood of unsolicited SMS to his phone violated his right to privacy. In giving judgment against MTN, the court stated, "the innumerable text messages without [Plaintiff's] consent ... is a violation of his fundamental right to privacy".

A series of other acts provide different elements of protections:

- **Credit Reporting Act 2017:** Provides a legal framework for credit reporting, licensing and regulation of credit bureaux in Nigeria.
- **The Cybercrime Act 2015:** Provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.
- **The National Health Act (NHA) 2014:** Provides a framework for the regulation, development and management of a health system and sets standards for rendering health services in Nigeria.
- **The Freedom of Information Act (FOIA) 2011:** Grants an individual the statutory right to request access to information in the custody or possession of a public official, agency or institution.
- **The National Identity Management Commission Act (NIMC Act) 2007:** Establishes the national identity database and the National Identity Management Commission (NIMC) charged with maintaining the national database, the registration of individuals and issuance of general multipurpose identity cards
- **The Nigerian Commissions Act (NCA) 2003:** Provides, amongst other things, for: the reform of the Nigerian Communications Commission (NCC) as an independent regulatory body for the communications sub-sector; the establishment of the National Frequency Management Council; and the establishment of the Universal Service Fund.
- **The Child's Rights Act 2003:** Makes provisions to provide and protect the rights of a Nigerian child and for other related matters.
- **The Wireless Telegraphy Act 1998 (WTA):** Regulates wireless telegraphy in Nigeria.

There also are currently two proposed draft laws that would address data protections:

- **The Data Protection Bill 2017 (HB. 02):** Seeks to make provisions for the regulation of information relating to individuals.
- **The National Information Technology Development Agency (NITDA) Draft National Guidelines on Data Protection 2013:** Covers the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. At the time of this study, the Guidelines are still in draft, and yet to come into force.



















































## 2.2 Types of Personal Data Collected

### OFFLINE COLLECTION

Table 2 on the following page gives a representation of individual instances of the offline collection of personal data in Nigeria, which is done by both public and private institutions (as noted)<sup>16</sup>. As seen, it is impossible not to leave a personal data footprint as part of one's daily interactions. This not only includes one's name and address, but often even fingerprints and a facial photo.

<sup>16</sup> The assumption is that the data subject provided accurate information in all these instances.

Table 2 — Offline collection of personal data<sup>17</sup>
















































DATA CONTROLLER/PROCESSOR	PURPOSE(S) OF COLLECTION	TYPE OF PERSONAL INFORMATION COLLECTED
<b>Legend:</b> <ul style="list-style-type: none"> <li style="width: 25%;"><span style="color: green;">●</span> Public organisation</li> <li style="width: 25%;"><span style="color: blue;">●</span> Private organisation</li> <li style="width: 25%;"><span style="color: red;">●</span> Public and private organisation(s)</li> <li style="width: 25%;"> Name</li> <li style="width: 25%;"> Fingerprints</li> <li style="width: 25%;"> Facial Photograph</li> <li style="width: 25%;"> Residential address</li> <li style="width: 25%;"> Utility bill</li> <li style="width: 25%;"> Telephone number</li> <li style="width: 25%;"> Financial/credit information</li> <li style="width: 25%;"> Health information</li> <li style="width: 25%;"> Email address</li> <li style="width: 25%;"> Passenger name record (PNR)</li> </ul>		
<span style="color: green;">●</span> <b>The National Identity Management Commission (NIMC)</b>	<ul style="list-style-type: none"> <li>- Creation of national identification number (NIN)</li> <li>- Issuance of the national electronic identity card</li> <li>- Issuance of multipurpose identity card (e-ID card)</li> <li>- Issuance of multipurpose identity card</li> </ul>	  
<span style="color: blue;">●</span> <b>Providers of mobile telecommunications services</b>	<ul style="list-style-type: none"> <li>- Activation of mobile telecommunications services</li> </ul>	  
<span style="color: blue;">●</span> <b>Independent Registration Agents<sup>18</sup></b>	<ul style="list-style-type: none"> <li>- To verify the identity of owner of a SIM card used in connection with the commission of a crime</li> </ul>	  
<span style="color: blue;">●</span> <b>Subscriber Registration Solution Providers<sup>19</sup></b>		
<span style="color: green;">●</span> <b>Independent National Electoral Commission (INEC)</b>	<ul style="list-style-type: none"> <li>- Issuance of voter card</li> <li>- To authenticate the identity of registered voters</li> </ul>	  
<span style="color: green;">●</span> <b>Nigerian Immigration Service (NIS)</b>	<ul style="list-style-type: none"> <li>- Issuance of ePassport</li> </ul>	   
<span style="color: green;">●</span> <b>Directorate of Road Traffic Services, Abuja</b>	<ul style="list-style-type: none"> <li>- Issuance of driver's license</li> <li>- Issuance of vehicle license</li> </ul>	   
<span style="color: blue;">●</span> <b>Deposit Money Banks (DMBs)</b>	<ul style="list-style-type: none"> <li>- Issuance of bank verification number (BVN)</li> </ul>	     
<span style="color: blue;">●</span> <b>Other Financial Institutions (OFIs)</b>	<ul style="list-style-type: none"> <li>- Bank account opening</li> </ul>	     
<span style="color: green;">●</span> <b>Federal Road Safety Corps (FRSC)</b>	<ul style="list-style-type: none"> <li>- Issuance of driver's license</li> <li>- Issuance of vehicle license</li> </ul>	   
<span style="color: green;">●</span> <b>National Population Commission (NPC)</b>	<ul style="list-style-type: none"> <li>- Census calculation</li> </ul>	  
<span style="color: green;">●</span> <b>Central Criminal Registry of the Nigerian Police Force (NPF)</b>	<ul style="list-style-type: none"> <li>- Issuance of police clearance certificate</li> </ul>	  

<sup>17</sup> All of the data controllers/processors listed in the table collect names. Over half (54%) collect residential addresses while nearly one in three collect telephone numbers. Lastly, almost one-fourth collect many key personal data points at the same time as part of one's interaction with them: names, residential addresses and telephone numbers.

<sup>18</sup> The Registration of Telephone Subscribers Regulations defines Independent Registration Agents in Regulation 1 (2) as "a company contracted by the Commission for the registration of existing subscribers on such terms as may be agreed upon between the Commission and the company".

<sup>19</sup> The Registration of Telephone Subscribers Regulations defines Subscriber Registration Solution Providers in Regulation 1 (2) as a company contracted by the Commission for the conceptualisation, design, development and delivery of Registration Solutions covering all Licensees and providing detailed Subscriber Information in a manner facilitating seamless integration into the Central Database.

Table 2 — Continued

DATA CONTROLLER/PROCESSOR	PURPOSE(S) OF COLLECTION	TYPE OF PERSONAL INFORMATION COLLECTED
<ul style="list-style-type: none"> <li>● Airline operators</li> <li>● Travel agencies</li> <li>● Hotels</li> <li>● Transportation service providers</li> </ul>	- Airline flight booking/reservation	  
● Credit bureaux	- Credit information of individual borrowers	   
<ul style="list-style-type: none"> <li>● Federal Inland Revenue Service (FIRS)</li> <li>● Joint tax board (JTB)</li> </ul>	- Issuance of tax identification number (TIN)	  
● Corporate Affairs Commission (CAC)	- Registration of a company or business name	  
<ul style="list-style-type: none"> <li>● Health Establishments</li> <li>● Health Management Organizations (HMOs)</li> <li>● National Health Insurance Scheme (NHIS)</li> </ul>	- Medical diagnosis and treatment	  
● Central Motor Registry of NPF	- Vehicle registration	  
● Educational institutions	- Registration and attendance at classes	   
● Pension Fund Administrator (PFA)	- Registration for pension	 
<ul style="list-style-type: none"> <li>● The Nigerian Social Insurance Trust Fund (NSITF)</li> <li>● Private and public sector employers</li> </ul>	- Registration under the workmen’s compensation scheme for the payment of compensation to employee or their dependants for any death, injury, disease or disability arising out of or in the course of the employee’s employment	
<ul style="list-style-type: none"> <li>● Private and public sector employers</li> <li>● Recruitment agencies</li> </ul>	- Employment	   
● Federal Civil Service Commission (FCSC)	- Employment with the Federal Civil Service	 
● Lottery/Gaming operators	- Participation in a lottery/gaming event	 
● Insurance companies	- Application for an insurance policy	 
● Marriage registries	- Issuance of a marriage certificate	  
● Registrar of births and deaths of the NPC	<ul style="list-style-type: none"> <li>- Issuance of a birth certificate</li> <li>- Issuance of a death certificate</li> </ul>	  
<ul style="list-style-type: none"> <li>● Commissioners for oath</li> <li>● Notary publics</li> </ul>	- Depositing to an affidavit	  
<ul style="list-style-type: none"> <li>● MDAs</li> <li>● Private guard companies providing security at the respective MDAs</li> </ul>	- Requirement for visitor’s tag for access into a premise occupied by Ministries, Departments or Agencies (MDAs) at the federal and state level	  

## ONLINE COLLECTION

The online collection of personal data occurs in the context of online behavioural advertising (OBA). OBA consists of tracking users' behaviour online through the collection of unique identifiers, and using the information obtained to identify patterns for building a profile of the data subject, so as to send targeted advertisements to the individual that are consistent with his interests.

For example, Facebook uses the data obtained from users of its social network to provide more targeted markets for advertisers<sup>20</sup>; Google, in analysing the search queries of users of its search engine service, is able to identify the interest of users or websites visited, as a commercial basis for targeted advertisement<sup>21</sup>.

Another application of (personal) information collected by online platforms is in the context of predictive analysis, which enables the extraction of huge amounts of information<sup>22</sup>. For example, through the collection of personal information of consumers with the pregnancy prediction algorithm, Target (a discount store retailer) was able to accurately predict which women were likely to be in their early stages of pregnancy so that it could target advertising to them before any other company<sup>23</sup>.

## THE AVAILABLE ONLINE TRACKING TECHNOLOGIES EMPLOYED BY ONLINE PLATFORMS TO CAPTURE PERSONAL DATA ARE:

**Web-bugs:** A web-bug is an invisible HTML object inserted in a webpage designed to track a visitor's movement across the internet.

**Cookies:** Cookies allow web servers to identify repeat visitors, preferences, and usage patterns.

**JavaScript:** JavaScript programmes can access information stored in the browser, including cached objects and the history of visited websites.

**Device fingerprinting:** An individual's fingerprint is a set of information elements that identifies a device or an application. Therefore, device fingerprinting<sup>24</sup> is a technology that combines a set of information elements in order to uniquely identify particular devices or applications<sup>25</sup>.

20 Cassandra Liem, Georgios Petropoulos, (2016, January 14). 'The Economic Value of Personal Data for Online Platforms, Firms and Consumers' <http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/>

21 Ibid.

22 Paul M. Schwartz. (2010). 'Data Protection Law And the Ethical Use of Analytics' [https://iapp.org/media/pdf/knowledge\\_center/Ethical\\_Underpinnings\\_of\\_Analytics.pdf](https://iapp.org/media/pdf/knowledge_center/Ethical_Underpinnings_of_Analytics.pdf), p. 5.

23 Charles Duhigg. (2012, February 12). 'How Companies Learn Your Secrets' <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?mcubz=3>.

24 A. Cooper, B. Aboba, J. Peterson, M. Hansen, J. Morris, R. Smith (2013, July). 'Privacy Considerations for Internet Protocols' <https://tools.ietf.org/pdf/rfc6973.pdf>.

25 Article 29 Data Protection Party. (2014, November 25). 'Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting': <http://www.dataprotection.ro/servlet/ViewDocument?tid=1089>, p.4.

## TYPES OF PERSONAL INFORMATION COLLECTED BY ONLINE PLATFORMS:

**IP addresses:** An IP address is a binary number that uniquely identifies a host computer connected to the internet.

**Location information:** Online platforms with location sensitive sensors and/or geotagging functionality have the capability to process a huge amount of location data of their users. For example, location-based services (LBS) such as Foursquare, Nearby, Tinder, Loopt, and Uber enable the providers to pinpoint the geographical location of their users and objects at any point in time with near-perfect accuracy.

**Clickstream data:** Clickstream data refers to the collection of data that describes the browsing habits and actions of an individual while surfing the internet. For an ISP, the collection of clickstream data is particularly easy, since the web traffic of each of its users must go through its network.

For this study, 23 websites were identified from a list of the 50 most-visited websites in Nigeria (as ranked by Alexa<sup>26</sup>) to analyse the type of personal data collected by these online platforms in Nigeria (see full table in Annex 3). The privacy policies of the selected websites (as of 9 August 2017) were reviewed to ascertain the type of personal information that each website declares to collect and the declared purpose(s) for the collection of personal information. In addition to these 23 websites that were randomly selected as ranked by Alexa, other apps that were rated as 'popular' on the Google Play were selected, with platforms that were widely used in Nigeria (see the full list in Annex 4).

































<sup>26</sup> Alexa is a company that measures and reports web traffic: <https://www.alexa.com/topsites/countries/NG>

Table 3 — Prominent data controller / processors that operate in Nigeria and the type of personal information collected

TYPE OF PERSONAL INFORMATION COLLECTED											
	IP ADDRESS	NAME	EMAIL ADDRESS	TELEPHONE	LOCATION/ADDRESS	CREDIT/DEBIT CARD DETAILS	PICTURE	PHOTOS	CLICK STREAM DATA	SEARCH QUERIES	OTHER
www.google.com.ng											
www.youtube.com											
www.facebook.com											
www.yahoo.com											Birthdate, Social security number
www.jumia.com.ng											
www.eskimi.com											
www.wikipedia.com											
www.instagram.com											
www.twitter.com											
www.linkedin.com											
www.xvideos.com											Sexual preferences, Racial or Ethnic origin, Religious beliefs
www.whatsapp.com											Device identifiers
www.opera.com											



Table 3 — Continued

	TYPE OF PERSONAL INFORMATION COLLECTED										
	IP ADDRESS	NAME	EMAIL ADDRESS	TELEPHONE	LOCATION/ADDRESS	CREDIT/DEBIT CARD DETAILS	PICTURE	PHOTOS	CLICK STREAM DATA	SEARCH QUERIES	OTHER
www.livescore.com											
www.kiloo.com											
www.trucaller.com			@								Twitter address, Facebook page
www.outfit7.com (My Talking Tom)			@								
www.uber.com/en-NG/.com			@								
www.netflix.com			@								
www.irokovt.com			@								
www.android.com			@								
www.mtnonline.com			@								Driver's license (or international passport bio-data page), Race, Fax number
www.smile.com.ng			@								

The URLs of the online platforms listed in Table 3 indicate the operators and data controllers/processors of those websites.<sup>27</sup> Of the 23 online platforms listed, 19 collect names and 20 collect IP addresses. Over one-third collect email addresses and one-fourth collect facial photographs/pictures. Moreover, 50% collect the online user's telephone number and 40% collect credit/debit card information.

**Only one platform ([www.livescore.com](http://www.livescore.com)) declares in its privacy policy that it does not collect any personal information.**

<sup>27</sup> Apps 13 (www.opera.com) to 17 (www.smile.com.ng) were listed as only popular as at 31 August 2017 on google play without any indication of their rankings on this platform, while I randomly selected platforms 18 - 23 due to their widespread use in Nigeria.

# 03

## THE ADEQUACY OF DATA PROTECTIONS

*The question whether Nigeria offers an adequate level of protection to personal data as compared to more robust frameworks can be tested by looking at cross-border data flows.*

**F**or example, what happens when data is transferred from the EU to the country? What does the coverage of current protections look like? Are Nigeria's existing and proposed rules for data protection — and the means for ensuring the effective application of these rules — consistent with those contained in the GDPR?

For the purpose of this study, the methodology adopted for assessing the adequacy of protection of existing and proposed data protection frameworks in Nigeria is a modified version of the methodology adopted for assessing the adequacy in the context of cross-border transfer of personal data under the GDPR<sup>28</sup>. While the GDPR has its own weaknesses, it remains one of the best set of protections in policy currently on the books.

<sup>28</sup> See generally, European Commission. (1998, July 24). 'Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf) on how adequacy is assessed in the context of cross-border transfer of personal data under the EU Data Protection Directive.

## The core criteria used for this assessment are:

- 1. Purpose limitation:** Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of collection (Article 5 (1) (b) of the GDPR).
- 2. Data quality and proportionality:** Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed (Article 5 (1) (c) and Article 5 (1) (d) of the GDPR).
- 3. Transparency:** Individuals should be provided with information as to the purpose of the processing and the identity of the data controller, and other information insofar as this is necessary to ensure fairness (Article 12 of the GDPR).
- 4. Security:** Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing (Article 5 (1) (c) of the GDPR).
- 5. Rights of access, rectification and opposition:** Individuals should have a right to obtain a copy of all data relating to him or her that are processed, and a right to rectification of those data where they are shown to be inaccurate (Articles 5 (1) (d), 12, 16, 17, 18, 19, 20 and 21 of the GDPR).
- 6. Restrictions on onward transfers:** Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection (Article 45 of the GDPR).
- 7. Additional principles in appropriate types of processing, such as those concerning (i) sensitive data, (ii) direct marketing and (iii) automated decisions:**
  - i. Sensitive data:** Where 'sensitive' categories of data are involved — such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life — additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing (Article 9 (2) (a) of the GDPR).

- ii. Direct marketing:** Where data is transferred for the purposes of direct marketing, the individual should be able to 'opt-out' from having his/her data used for such purposes at any stage (Article 21 (2) – (3) of the GDPR).
- iii. Automated individual decision:** Where the purpose of the collection is the taking of an automated decision which entails the automated processing of data intended to evaluate certain personal aspects relating to the data subject, such as his/her performance at work, creditworthiness, reliability, conduct, etc., the data subject should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest (Article 22 (4) of the GDPR).

### 3.1 Enforcement Mechanisms

The objectives of a good data protection framework or a well-developed privacy policy are essentially threefold:

- 1.** To deliver a good level of compliance with the rules (Articles 82 – 84 of the GDPR)
- 2.** To provide support and help to individuals in the exercise of their rights (Articles 77 – 79 of the GDPR)
- 3.** To provide appropriate redress to the injured party where rules are not complied with (Article 77 of the GDPR).

These principles are important to any data protection framework that seeks to regulate the collection and processing of information in the context of cross-border data flows.

Table 4 below gives a representation of whether the core principles and procedural/enforcement mechanisms contained in the GDPR are also contained in any other data protection frameworks.

**Table 4** — Analysis of GDPR core principles and procedural/enforcement mechanisms.

	<b>PURPOSE LIMITATION</b>	<b>DATA QUALITY AND PROPORTIONALITY</b>	<b>TRANSPARENCY</b>	<b>SECURITY</b>	<b>RIGHTS OF ACCESS, RECTIFICATION AND OPPOSITION</b>	<b>RESTRICTIONS ON ONWARD TRANSFERS</b>	<b>CORE CRITERIA FOR DATA PROTECTION</b>	<b>APPROPRIATE REDRESS</b>
<b>The Constitution</b>	-	-	-	-	-	-	-	-
<b>Credit Reporting Act</b>	Sections 6(b), & 7	Section 6(a)	-	Section 6(c)	Sections 6(d),(f), & 13	Section 7	Section 3(3)(d)	Section 13
<b>Cybercrime Act</b>	Section 38(4)	Section 39	-	Section 38(5)	-	-	-	-
<b>NHA</b>	Section 27	-	-	-	Section 29	-	-	-
<b>FoIA</b>	-	-	-	-	-	-	-	-
<b>NIMC Act</b>	Section 15	-	-	-	-	-	-	-
<b>NCA</b>	-	-	-	-	-	-	-	-
<b>CRA</b>	-	-	-	-	-	-	-	-
<b>WTA</b>	-	-	-	-	-	-	-	-
<b>Registration Regulations</b>	Regulation 8	Regulation 9(5)	-	Regulation 9(4)	Regulation 9(1)	Regulation 10 (4)	-	-
<b>Consumer Regulations</b>	Paragraph 35(1) (b) of Schedule 1	Paragraphs 35(1) (c), (d) & (e); 38 (1) of Schedule 1	Paragraph 35(2) (a) of Schedule 1	Paragraph 35(2) (d) of Schedule 1	Paragraph 38(2) of Schedule 1	Paragraph 35(1) (h) of Schedule 1	-	Paragraph 35(2) (d) of Schedule 1
<b>Guidelines for ISPs</b>	-	-	-	-	-	-	-	-
<b>Data Protection Bill 2017</b>	Yes. Clause 1(b)	Clause 1(2)	Clause 2(1)	Clause 1(3)	Clauses 3(1) & 7(1)	Clause 1(4)	-	-
<b>NITDA Guidelines</b>	Paragraphs 2.1(3); 2.2(1)(a); 3.1.1	Paragraphs 2.2(1) (b); 2.2(1)(d); 3.1.3; 3.1.4; 3.1.5	Paragraphs 2.2(1)(a); 2.2(2) (a); 3.1.1	Paragraphs 2.4; 3.1.7	Paragraphs 2.2 (3); 3.1.6	Paragraphs 2.3(4) – (5); 3.1.8	Paragraph 2.2(7)	Paragraph 2.3(6)
<b>ECOWAS Data Protection Act</b>	Article 25 (1)	Article 26	Articles 27; & 38	Article 28	Articles 39 – 41	Article 36	Article 30	-
<b>The Convention</b>	Article 13, Principle 3(a)	Article 13, Principle 3(b) & 4	Article 16	Article 13, Principle 6	Articles 17 - 19	Article 14(6)	Article 14(1)	Articles 11 - 12
<b>BNV Policy</b>	Yes	-	CBN Circular 16/003 and CBN Circular 01/015	Yes	CBN Circular 16/003 and CBN Circular 01/015	-	-	-

As shown in Table 4, existing gaps represent either a lack of one or more content principles of data protection and/or a total lack of an enforcement mechanism to enforce data protection breaches or to provide redress to the data subject.

The Convention and the NITDA Guidelines both, from the adequacy assessment conducted, appear to contain all the content principles and enforcement mechanisms of the GDPR. However, the major flaw with the Convention, as explained in Section 2 of this study, is that it is yet to acquire the force of law in accordance with Section 12 of the Constitution. A concern surrounding the NITDA Guidelines, as explained in Section 2 of this study, is that NITDA does not appear to be authorised by the NITDA Act to issue guidelines on matters of 'data protection', 'data security' or 'data privacy'; it is unlikely that NITDA can successfully rely on Section 6 of the NITDA Act as a legal basis for issuing the NITDA Guidelines if its legality were eventually challenged in court.

Except for the Convention and the NITDA Guidelines, none of the existing frameworks is of general application. Therefore, their effectiveness is limited to certain circumstances. For example, the Constitution applies to only Nigerian citizens, the consumer regulations apply to the communications sector, the Credit Reporting Act applies to credit bureaux in Nigeria, the NHA applies only to health information, and the Child Rights Act applies to only Nigerian children; meanwhile, other frameworks are yet to acquire the force of law (e.g. Data Protection Bill 2017 and the ECOWAS Data Protection Act).

In the final analysis, the adequacy assessment conducted has shown that — save for the Convention and the NITDA Guidelines — none of these regulatory frameworks contain the full complement of the core data protection principles as contained in the GDPR and thus, cannot guarantee an adequate level of protection to the data subject in Nigeria. The legal basis of the NITDA Guidelines appears to be questionable and is unlikely to be sustained in court. In addition, both the Convention and NITDA Guidelines are yet to acquire the force of law.

# 04

## KEY FINDINGS

*Based on the legal assessment of this study, the main data protection risks currently experienced in Nigeria are best categorised as affecting individuals both offline and online.*

### Risk 1:

**Use of personal data may be incompatible with the purpose for which it was collected.**

One of the data protection risks faced by Nigerians is the use of their personal information for a purpose different from the purpose specified at collection.

For instance, both the State Security Services (SSS) and Nigerian Immigration Service (NIS) jointly maintain a watchlist of individuals of interest through the collection of passenger name records from airline operators<sup>29</sup>. As seen in this example, although the passenger name record was originally collected for the purpose of flight reservation/booking, it was additionally processed for another purpose by Law Enforcement Agencies (LEAs).

<sup>29</sup> U.S. Department of State. (n.d). 'Chapter 2. Country Reports: Africa Overview' <https://www.state.gov/j/ct/rls/crt/2015/257514.htm>; WikiLeaks. (n.d). Nigeria: Govt. Practices - Info Collection, Screening & Sharing' [https://wikileaks.org/plusd/cables/07ABUJA2320\\_a.html](https://wikileaks.org/plusd/cables/07ABUJA2320_a.html)

## Risk 2:

### Nigerians have no rights in relation to their personal information

Nigerians rarely have access to their own personal information collected offline. In the cases of Google, Facebook and Twitter, the companies have a provision in their privacy policy that allows users to access their personal information obtained from these services. In addition, it is not uncommon for health establishments to refuse patients access to the case folder containing their health record. In such situations, the patient can take no step to rectify their personal information or object to it being processed<sup>30</sup>.

## Risk 3:

### Lack of adequate consent

Consent is a legal basis required for the legitimate processing of personal data<sup>31</sup>. For consent to be adequate it must be informed, freely given and specific. However, in Nigeria and many other countries, individuals are not be adequately informed in order for them to provide consent.

<sup>30</sup> Author's personal experience.

<sup>31</sup> European Union Agency for Fundamental Rights, Council of Europe (2014, April), supra, p. 55.

<sup>32</sup> Appeal No: CA/A/689/2013 (unreported).

## Risk 4:

### Lack of transparency in the processing of personal data

Transparency in the context of data protection means that the individual should be informed about how their personal data is being used. In terms of what the law provides, an individual also has the right to be told by a controller, on request, if their data is being processed, and, if so, which data. The processing operations must not be performed in secret and should not have unforeseeable negative effects. For example, OS providers, through their APIs, give app providers substantial amounts of user data without explaining to the user the type of data which the app will access. Similarly, many MNOs share the telephone numbers of their subscribers, as illustrated in the recent case of MTN v. Barr. Godfery Nya Eneye<sup>32</sup>.

## IS CONSENT JUST CHECKING A BOX?

For example, when cookies are placed by a website in the device of the individual, the operator of the website hardly ever gives a detailed explanation of the purpose of the cookies. In addition, the information contained in the privacy policy is hardly ever clear and comprehensive enough for the individual to provide adequate consent, and thus a legitimate basis for processing personal information<sup>33</sup>. This is also the case when downloading an app, **and consent is reduced to a tick box**. Consent in cases

where an app is downloaded should be granular, where consent must be asked for every type of information the app will access.

Another concern around the inadequacy of consent is where access to a particular online platform or content on websites and apps is denied unless the individual consents to be tracked by technologies like cookies, device fingerprinting, unique identifier injection, or other monitoring techniques.

<sup>33</sup> Asunción Esteve, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA', *International Data Privacy Law*, No. 1, Vol. 7 (2017), pp. 36 – 47, p. 41.

**Risk 5:****Lack of security and the risk of a personal data breach**

Security is a key requirement in data protection<sup>34</sup>. Except in very few instances<sup>35</sup>, there is no positive obligation imposed on online platforms in Nigeria to take appropriate security measures to protect the personal information of their users and the systems used for processing the personal information. As a result, individuals are exposed to the risk of a personal data breach. This risk may result in physical, material or non-material damage, such as loss of control of personal data or a restriction in using personal data.

**Risk 6:****Incompatibility between the collection and use of personal data**

Personal information collected online, such as internet search and browsing history, IP addresses, and social media network information, may give rise to incompatibility of purpose, especially in the context of big data analytics or data mining. Big data — which refers to “gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed”<sup>36</sup> — has been argued to seriously undermine the principle of purpose specification<sup>37</sup>. Due to the absence of a data protection framework, a recurring theme in this argument is that in the context of big data (analytics), there appears to be a blur in ascertaining where the compatible use of personal information ends, and an incompatible use commences. Due to the large-scale collection of personal information and use of several analytic algorithms by big data analytics, personal information initially collected for a specified purpose could be repurposed or used for a new purpose<sup>38</sup>.

**Risk 7:****Children are exposed to privacy risks online**

According to 2014 research by the Nigerian Communications Commission, children are more vulnerable than adults when accessing the internet due to the information collection practices of online platforms trigger several privacy concerns for a child in more ways than one<sup>39</sup>. First, children are not capable of protecting themselves<sup>40</sup>; second, children “lack the cognitive ability to recognise and appreciate privacy concerns<sup>41</sup>”; third, children “may not understand the nature of the information being sought, nor its intended uses<sup>42</sup>”; fourth, even if the information provided is sufficient to form the basis of an informed consent, children often lack the legal capacity to give valid consent<sup>43</sup>; and lastly, children may unknowingly disclose personal information to these platforms due to the appealing nature of their visual content<sup>44</sup>.

34 Rosemary Jay, (2017), supra, p. 131.

35 For instance, the Credit Reporting Act 2017, Cybercrime Act 2015 and the National Health Act 2014 respectively require credit bureaux, financial institutions and health establishments to take “measures” to safeguard information in their possession.

36 Article 29 Data Protection Party. (2013, April 2), supra, p. 35.

37 World Economic Forum. (2013, February). ‘Unlocking the Value of Personal Data: From Collection to Usage’ [http://www3.weforum.org/docs/WEF\\_IT\\_UnlockingValuePersonalData\\_CollectionUsage\\_Report\\_2013.pdf](http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf), p. 4.

38 Information Commissioner’s Office. (2017). ‘Big Data, Artificial Intelligence, Machine Learning and Data Protection’ <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>, p. 38.

39 Nigerian Communications Commission. (2014, November 10). ‘Parental Control Measures for Telecommunications Networks’ <https://www.ncc.gov.ng/docman-main/industry-statistics/research-reports/578-parental-control-mesures-for-moblie-telecommunications-networks/file>, p. 6.

40 Dorothy A. Hertzler, ‘Don’t Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child’s Privacy Online’, Federal Communications Law Journal, Vol. 52, (2000), pp. 429 – 451, p. 434.

41 Kathryn C. Montgomery, Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet (MIT Press, 2009), p. 89.

42 Jerry S. Birenz, ‘Caching World Wide Web Sites’, Practicing Law Institute (1998), p. 475.

43 Article 29 Data Protection Party. (2011, July 13), supra, p. 27; Rosemary Jay, (2017), supra, p. 91.

44 Angela J. Campbell, ‘Ads2kids.Com: Should Government Regulate Advertising to Children on the World Wide Web?’, Gonzaga Law Review, Vol. 33, No. 331 (1998), pp. 320.



# 05

## RECOMMENDATIONS

*To address the gaps in the existing/ proposed data protection frameworks in Nigeria, policy options are categorised into six broad categories:*

### Legislative measures

- **Enact a Data Protection Act:** Enact into law a Data Protection Act that contains data protection principles consistent with those contained in the African Union Convention on Cyber Security and Personal Data Protection and/or the EU's General Data Protection Regulation (GDPR).
- **Amend the NIMC Act:** Amend the NIMC Act to incorporate robust data protection principles and expand the powers of NIMC to function as a data protection authority to ensure that public and private institutions in Nigeria comply with the data protection principles when processing personal data.
- **Enact a Child Online Privacy Protection Act:** Enact an Act that includes basic standards of practice by online platforms in the online collection and use of information from children.

## Non-legislative (soft law) measures

- **Undertake administrative rulemaking by the NIMC:** NIMC would exercise its Section 31 (b) power under the NIMC Act, which authorises it to make regulations for the collection and processing of personal data.

## Judicial measures

- **Encourage superior courts of records in Nigeria to engage in judicial activism:** Nigerian courts would engage in judicial activism by interpreting Section 37 of the Constitution, which guarantees a Nigerian citizen's right to privacy to include the protection of his personal information.

## Enforcement measures

- **Engage the National Human Rights Commission (NHRC) to enforce data protection cases:** The NHRC should enforce cases of personal data protection breaches by exercising its Section 5 (a) and (b) functions, which respectively authorise it to deal with human rights matters and their breaches, under the NHRC Act. The basis for this recommendation is that data protection is a substantive legal issue grounded in the right to privacy, as guaranteed by the Constitution.
- **Engage the Consumer Protection Council (CPC) to provide redress:** Exercise its Section 2 (i) function under the CPC Act to provide redress to obnoxious practices or the unscrupulous exploitation of consumers. This study argues that the “obnoxious practices” or “unscrupulous exploitation” of consumers contemplated by Section 2 (i) also includes matters of data protection.
- **Ensure that the NIMC and sector-specific regulators with consumer protection authority (including the CPC and NCC) take action:** Mandate data protection by design and transparency obligations by specifying that Ministries, Departments or Agencies, and regulated organisations (including online platforms) acting

as data controllers implement data protection by design in systems, processes and technologies that process personal information.

## Executive Measures

- **Call on the Federal Government of Nigeria (FGN) to harmonise institutional efforts and remits:** The FGN should issue a policy instrument directing that all identity databases in the custody of government authorities be harmonised and managed by the NIMC. This should allow Nigerians to register once, in a single database which can be accessed by any relevant government authority.

## Social Measures

- **Encourage civil society organisations (CSOs) to advocate for change:** CSOs should lobby for a data protection framework, condemn a breach of privacy, engage in public interest litigation to protect privacy, raise consumer awareness about protecting their personal information and advocate for the use of Privacy Enhancing Technologies (e.g. parental control programmes).

## ANNEX

An annex with the study's methodology and other supplementary information can be found online at <http://bit.ly/nigeriareportannex>.



**WORLD WIDE WEB  
FOUNDATION**

World Wide Web Foundation  
1110 Vermont Ave NW, Suite 500  
Washington, DC 20005, USA

[www.webfoundation.org](http://www.webfoundation.org)

Twitter: [@webfoundation](https://twitter.com/webfoundation)



**PARADIGM  
INITIATIVE**

Paradigm Initiative Nigeria  
2nd Floor, 385 Herbert, Macaulay Way,  
Yaba, Lagos, Nigeria

[www.paradigmhq.org](http://www.paradigmhq.org)

Twitter: [@ParadigmHQ](https://twitter.com/ParadigmHQ)