DATA PROTECTION GUIDELINES
2017

Table of Contents

1.0 PREAMBLES

The National Information Technology Development Agency (NITDA) is mandated by the NITDA Act of 2007 to develop Information Technology in Nigeria through regulatory policies, guidelines, standards, and incentives. Part of which is to ensure the safety and protection of the Nigerian Citizen's personal identifiable information otherwise known as Personal Data, Object Identifiable Information and a successful implementation of the Data Protection Guidelines;

Many establishments have migrated their businesses and other information systems online. Information solutions in both the private and public sectors now drive service delivery in the country. These information systems have thus become critical information infrastructure which must be safeguarded, regulated and protected; and

The regulator of Information Technology, NITDA, after serious consideration of the concerns and contributions of stakeholders in the sector, on the issue of privacy and protection of Personal Data; and upon evaluation of the challenges of leaving Personal Data unregulated, hereby issue this Guidelines on Data Protection in Nigeria.

2.0 SHORT TITLE AND COMMENCEMENT

This Guidelines shall be cites as 'Data Protection Guidelines' and shall come into effect on the ……

3.0 AUTHORITY

In exercise of the powers conferred on it by Section 6 of the National Information Technology Development Agency (NITDA) Act of 2007, NITDA in consultation with key stakeholders hereby issues the following Guidelines on Data Protection.

4.1 PART ONE- PRELIMINARIES

1. These Guidelines may be cited as Guidelines for Data Protection.
2. In these Guidelines unless the context otherwise permits:
    a. **Act** means the National Information Technology Development Agency Act of 2007
    b. **Computer** means Information Technology systems and devices, whether networked or not
    c. **Database** means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, non-structured, cached and file system type databases.
    d. **Data Controller** means any person, public authority, Agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by an Act of National Assembly or regulations, the controller or the specific criteria for his nomination will be as stated by the Act or regulation.
    e. **Database Management System** means software that allows a computer to create a database, add, change and delete data

in the database; allows data in the database to be processed, sorted and retrieved and reports to be generated.

f. **Data Portability** means the ability for data to be transferred easily from one IT system to another through a safe and secure means in a standard format
g. **Data Protection Guidelines** means this Guidelines and it's subsequent amendments and any other Guidelines on the processing of information relating to identifiable individual's Personal Data, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, and disclosure.
h. **Data Subject** means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
i. **Data Subject Access Request** means the mechanism for an individual to request a copy of their data under a formal process and payment of a fee.
j. **OII** means Object Identifiable Information
k. **Personal Data** means any information relating to an identified or identifiable natural person ("data subject"); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.
l. **Personal Data Filing System** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed.
m. **Processing of Personal Data** means any operation or set of operations which is performed upon personal data, whether or

not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

n. **Data Administrator** means a persons or organization that processes data
o. **Sensitive Personal Data** means Data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.
p. **The Data Subject's Consent** means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
q. **Third Party** means any natural or legal person, public authority, Agency or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who, under the direct authority of the Data Controller or the Data Administrator, are authorized to process personal data.
r. **Recipient** means a natural or legal person, public authority, Agency or any other body to whom data is disclosed, whether a Third Party or not.
s. **Relevant Authorities** means the National Information Technology Development Agency (NITDA) or any other statutory body
t. **The Agency** means the National Information Technology Development Agency (NITDA)
u. **Data** means characters, symbols and binary on which operations are performed by a computer. Which maybe stored or transmitted in the form of electronic signals is stored in any format or any device

v. **Guidelines** means provisions of this document in its entirety
w. **Data Owner** means the organization or a hired third party in possession of any data collected by from a Data Subject either directly or indirectly

3. The persons and bodies to which these Guidelines shall apply include:
   a. Public and Private Sector as defined in these Guidelines.
   b. Federal, State and Local Government Agencies and Institutions as well as other organizations which own, use or deploy information systems within Federal Republic of Nigeria.
   c. Data Collectors, Data Custodians, Data Administrator, Data Systems Auditors and Data Security Organizations, including their Staff and Agents.
4. These Guidelines shall cover:
   a. Persons based in Nigeria, including but not limited to Data Controller or Data Administrators and Data Subject ; and to persons based outside Nigeria if they process personal data of Nigerian residents and citizens
   b. The collection, accessing and processing of personal data wholly or partly by automatic and non-automatic means,.

5. These Guidelines are issued for the purpose of achieving the following National objectives of prescribing:
   a. Regulatory Instruments for all organizations or persons that control, collect, store and process personal data of Nigerian Residents and Citizens within and outside Nigeria for protecting of a specific category of data commonly known as Personal Data or Object Identifiable Information (OII).
   b. Minimum Data Protection requirements for the collection, storage, processing, management, operation, and technical controls for information in this category. Widening the domestic market for Nigerian Information Technology products

4.2 PART TWO – DATA PROTECTION PRINCIPLES

6.

a. Data Controllers shall inform Data Subjects about the purposes for which data is collected, and where applicable, that the data may be sent outside of Nigeria.
b. Informing Data Subjects of the purpose or which data is collected may be done by placing a clear notice on a websites, social media platforms, mobile communications or any other acceptable means.
c. A prior electronic or non-electronic based acceptance by the Data Subject shall constitute as a valid acceptance
d. Every Data Controller shall publish in a conspicuous part of the website or application a Privacy Policy which shall among others state the following- what constitutes the Data Subject's consent; description of collectable personal information; state how personal collected information is used; state technical methods used to collect and store personal information e.g. Cookies, JWT; state how personal information is shared; overview of information security architecture; state data confidentiality rights; state any other limitation of liability on links to other websites or systems or any particular limitation aside from the expressly mandated provisions

7.

a. The Data Controller shall publish a Privacy Policy stating for the purpose for which Data collected shall be used in compliance with Section 6. Changes to such Privacy Policy or statement shall be promptly communicated to the Data Subject who shall consent to the changes before the policy takes effect.
b. The purposes for collecting the data must be reasonable and lawful.

8. Data controllers shall, at all times, collect only needed data.

9. Data controllers shall provide individuals with the platform to update their Personal Data or to have it updated; which may include but not limited to marketing communications, opt-in and opt-out options.

10. Subject to the provisions of the Freedom of Information Act 2011, Data Controller shall respond to request by a person for a copy of his data within 7 days provided that the Data Controller may give conditions subject to the approval of the Data Owner, for the release of such data to the person.

11. Data Controllers shall develop cyber-security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and setting up a staff training program accordingly.

12. If there is need to send or transfer data outside Nigeria, Data Controllers shall ensure that:

a. The receiving country has Data Protection Guidelines or legislations.
b. It forms part of the fulfillment of a contract or a contract with clear terms on protection of personal data between the Data Controller and the receiving Organization.
c. The consent of the Data Subject to that effect was obtained.

4.3 PART THREE – DATA COLLECTION AND PROCESSING

13. Data Controllers shall protect the privacy of Natural Persons with respect to the collection and processing of Personal Data in accordance with the prescription of these Guidelines and the provisions of the National Information Systems and Network Security Standards and Guidelines.

14. Nobody shall undertake the collection of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life except:
    a. The Data Subject has given explicit consent to the collection and processing of those data; or
    b. Collection and processing is necessary for the purposes of carrying out the obligations and specific function of the Data Controller in the field of employment; or
    c. Collection and processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent; or
    d. Collection and processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the Data Subjects; or

e. The collection and processing relates to data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defense of legal claims.

15. Fair and lawful processing of Personal Data entails:
    a. Collection of Personal Data for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
    b. Further processing of data for historical, statistical or scientific purposes in compliance with the provisions of these Guidelines.
    c. Adequate, relevant and non-excessive use in relation to the purposes for which they are collected and further processed.
    d. Ensuring that inaccurate or incomplete data, having regard to the purposes for which they were collected or further processed, are erased or rectified;
    e. Keeping Personal Data in a form which permits identification of the Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

16. Personal Data may be processed only if one or more of these applies:
    a. The Data Subject has unambiguously given consent,
    b. Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract,
    c. Processing is necessary for compliance with a legal obligation to which the Data Controller is subject,
    d. Processing is necessary in order to protect the vital interests of the Data Subject,
    e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority

vested in the Data Controller or in a Third Party to whom the data is disclosed,

f. Processing of the data is required for the purposes of management of health-care services, and where those data are processed by a health professional subject to national laws or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy,
g. Processing of data related to offences, convictions and cases may be kept only under the control of official authority,
h. Data relating to administrative sanctions and judgments shall also be processed under the control of official authority,

17. Every Data Subject shall obtain from the Data Controller without constraint, at reasonable intervals and without excessive delay or expense:
    a. A confirmation as to whether or not data relating to Data Subject are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
    b. Communication to Data Subject in an intelligible form of the data undergoing processing and of any available information as to their source;
    c. Knowledge of the procedure involved in any automatic processing of data concerning data subject at least in the case of the automated decisions.
    d. Rectification, erasure or blocking of data which does not comply with the provisions of these Guidelines.
    e. Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with these Guidelines.

18.

a. The Data Controller shall implement technical and organizational measures to secure Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
b. Taking into cognizance the state of the art systems and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected with secure connection and encryption as minimums.

19.

a. Contract or legal agreement between the Data Processor and Data Controller shall govern data processing carried out by the Third Party stipulating, among other terms, that:
    i. The Third Party should act only on instructions from the Data Controller;
    ii. The obligation in Section 14 of these Guidelines above shall also be incumbent on the Data Processor.
b. All contracts shall be in writing

20.

a. The Data Subject shall have the option to:
    i. Object to and request free of charge, the processing of Personal Data relating to him which the Data Controller intend to process for the purposes of direct marketing, or
    ii. Be informed before Personal Data are disclosed to third parties or used on their behalf for the purposes of direct

marketing, and to be expressly offered the mechanism for objection free of charge to such disclosures or uses.

b. Data Controllers shall provide information clearly to ensure Data Subjects are aware of the options in 21(1) above.

21. Any person acting under the authority of the Data Controller including the Third Party who has access to Personal Data must not process the data except on instructions from the Data Controller, unless required by law.

22. The Data Controller shall, where processing is carried out on his behalf, choose a Data Processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and ensure compliance with those measures.

23. Where the data has not been obtained from the Data Subject, Data Controller or Third Party shall, at the time of undertaking the recording of Personal Data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the Data Subject with at least the following information, except where he already has it:

a. The identity of the new Data Controller and of the representative, if any,
b. The purposes of the processing,
c. any further information such as:
    i. the categories of data concerned
    ii. the recipients or categories of recipients;
    iii. The existence of the mechanism for access to and the mechanism to rectify the data concerning the data subject

24. Subject to the provisions of this Guidelines and the National Information Systems and Network Security Standards and

Guidelines, in cases of Personal Data which are undergoing processing for transfer to another country or are intended for processing after transfer to another country, that country shall ensure an adequate level of protection of such data.

25. Data Controllers shall issue Directives and Administrative Instruments necessary for the implementation of these Guidelines within twelve months from the date of its adoption.

4.4 PART FOUR – DATA ACCESS

26. Data Controllers shall neither restrict nor hinder the free flow of Personal Data between authorized Third Parties as defined in this Guideline.

27. A Data Subject may request a copy of Personal Data being processed in a format usable by the person and transmit it manually or electronically to another processing system.

28. The adequacy of the level of protection afforded by another country shall:

a. Be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations.
b. Consider the nature of the data, the purpose and duration of the proposed processing operation or operations, the rules of law, both general and sectorial, in force in the receiving country and the professional rules and security measures which are complied within that country which should not be lower than the content of the Guidelines herein.

29. Any Third Party level of protection shall not be lower than the specifications of these Guidelines.

30.

a. Where the Data Controller finds that any country does not ensure an adequate level of protection within the contents of these Guidelines, Data Controller shall prevent any transfer of data to the country in question.
b. Where the data is already hosted in a country and the protection policy changes below the minimum of the Guideline, the Data Controller shall transfer the data in accordance to Section 30(a)

4.5 PART FIVE- IMPLEMENTATION OF GUIDELINES

31. Organizations shall designate an employee of that organization as the organization's Data Security Officer whose duty shall include:
    a. Ensuring that organization adheres to this Guidelines.
    b. Ensuring continued adherence to data protection and privacy policies and procedures.
    c. Ensuring that Personal Data is protected; and provide for effective oversight of the collection and use of personal information.
    d. Be responsible for effective data protection and management within that organization; and ensure compliance with the privacy and data security policies.
    e. Training and education for employees to promote awareness of and compliance with the privacy and data security policies
    f. Developing recommended practices and procedures to ensure compliance with the privacy and data security policies.

32. Within 12 months after the date of issuance of this Guidelines, each organization shall conduct a detailed benchmark assessment of its privacy and data protection policies and practices with at least each benchmark assessment stating:

a. The personally identifiable information the organization collects on employees of the organization; and members of the public;
b. Any purpose for which the personally identifiable information is collected;
c. Any notice given to individuals regarding the collection and use of personal information, relating to that individual;
d. Any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
e. Whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
f. The policies and practices of the organization for the security of personally identifiable information;
g. The policies and practices of the organization for the proper use of personally identifiable information;
h. Organization policies and procedures for privacy and data protection;
i. The policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies; and
j. The policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

32. Any breach of these Guidelines shall be construed as a breach of the provisions of the National Information Technology Development Agency Act of 2007 and the Guidelines issued under that Act

33. The enforcement of these Regulations shall be by Relevant Authorities

34. NITDA shall amend or review these Guidelines periodically or as the need arises in consultation with stakeholders. In reviewing the Guidelines, the Agency shall be guided, among other considerations, by global trends and practices in Information Technology and the developmental aspirations of Nigeria.