NIGERIA DATA PROTECTION REGULATION 2019

TABLE OF CONTENTS

PREAMBLE:

WHEREAS, The National Information Technology Development Agency (NITDA, hereinafter referred to as The Agency) is statutorily mandated by the NITDA Act of 2007 to, inter alia; develop regulations 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;

RECOGNIZING that many public and private bodies have migrated their respective businesses and other information systems online, information solutions in both the private and public sectors now drive service delivery in the country through digital systems. These information systems have thus become critical information infrastructure which must be safeguarded, regulated and protected against atrocious breaches;

COGNIZANT of emerging data protection regulations within the international community geared towards security of lives and property and fostering the integrity of commerce and industry in the volatile data economy;

CONSCIOUS of the concerns and contributions of stakeholders on the issue of privacy and protection of Personal Data and the grave consequences of leaving Personal Data processing unregulated;

THE AGENCY hereby issues the Nigeria Data Protection Regulation and shall come into effect on the date issued by NITDA.

PART ONE

1.1 OBJECTIVES OF THE REGULATION

The objectives of this Regulation are as follows:

a) to safeguard the rights of natural persons to data privacy;

b) to foster safe conduct for transactions involving the exchange of Personal Data;

c) to prevent manipulation of Personal Data; and

d) to ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

1.2 SCOPE OF THE REGULATION

a) this Regulation applies to all transactions intended for the processing of Personal Data, to the processing of Personal Data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria;

b) this Regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria;

c) this Regulation shall not operate to deny any Nigerian or any natural person the privacy rights he is entitled to under any law, regulation, policy, contract for the time being in force in Nigeria or in any foreign jurisdiction.

1.3 DEFINITIONS

In this Regulation, unless the context otherwise requires:

i. “Act” means the National Information Technology Development Agency Act of 2007;

ii. “Computer” means Information Technology systems and devices, networked or not;

iii. ‘Consent’ of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

iv. “Data” means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device;

viii. “Database” means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases;

ix. “Data Administrator “means a person or an organization that processes data

x. “Data Controller” means a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed;

xi. “Database Management System” means a software that allows a computer to create a database; add, change or delete data in the database; allows data in the database to be processed, sorted or retrieved;

xii. “Data Portability” means the ability for data to be transferred easily from one IT system or computer to another through a safe and secured means in a standard format;

xiii. “Data Protection Compliance Organization (DPCO)” means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this Regulation or any foreign Data Protection Law or Regulation having effect in Nigeria;

xiv. “Data Subject” means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

xv. “Data Subject Access Request” means the mechanism for an individual to request a copy of their data under a formal process which may include payment of a fee;

xvi. “Filing system” means any structured set of Personal Data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

xvii. “Foreign Country” means other sovereign states, autonomous or semi-autonomous territories within the international community;

xviii. “Regulation” means this Regulation and its subsequent amendments, and where circumstance requires it shall also mean any other Regulations on the processing of information relating to identifiable individual’s, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, or disclosure;

xix. “Personal Data” means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural 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 data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; 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, Personal Identifiable Information (PII) and others;

xx. “Personal Identifiable Information (PII)” means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context

xxi. “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

xxii. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

xxiii. “Recipient” means a natural or legal person, public authority who accepts data;

xxiv. “Relevant Authorities” means The National Information Technology Development Agency (NITDA) or any other statutory body or establishment having government’s mandate to deal solely or partly with matters relating to Personal Data;

xxv. “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;

xxvi. “The Agency” means the National Information Technology Development Agency;

xxvii. “Third Party” means any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process Personal Data.

PART TWO

2.1 GOVERNING PRINCIPLES OF DATA PROCESSING

(1) In addition to the procedures laid down in this Regulation or any other instrument for the time being in force, Personal Data shall be:

a) collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject; provided that:

i. a further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest;

ii. any person or entity carrying out or purporting to carry out data processing under the provision of this paragraph shall not transfer any Personal Data to any person;

b) adequate, accurate and without prejudice to the dignity of human person;

c) stored only for the period within which it is reasonably needed, and

d) secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.

(2) Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject owes a duty of care to the said Data Subject;

(3) Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject shall be accountable for his acts and omissions in respect of data processing, and in accordance with the principles contained in this Regulation.

2.2 LAWFUL PROCESSING

Without prejudice to the principles set out in this Regulation, processing shall be lawful if at least one of the following applies:

a) the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes;

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 Controller is subject;

d) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, and

e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller;

2.3 PROCURING CONSENT

(1) No data shall be obtained except the specific purpose of collection is made known to the Data Subject;

(2) Data Controller is under obligation to ensure that consent of a Data Subject has been obtained without fraud, coercion or undue influence; accordingly:

a) where processing is based on consent, the Controller shall be able to demonstrate that the Data Subject has consented to processing of his or her Personal Data and the legal capacity to give consent;

b) if the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding on the Data Subject;

c) prior to giving consent, the Data Subject shall be informed of his right and method to withdraw his consent at any given time. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;

d) when assessing whether consent is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of Personal Data that is not necessary (or excessive) for the performance of that contract; and

e) where data may be transferred to a third party for any reason whatsoever

2.4 DUE DILIGENCE AND PROHIBITION OF IMPROPER MOTIVES

(a) No consent shall be sought, given or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts;

(b) A party to any data processing contract, other than an individual Data Subject, shall take reasonable measures to ensure the other party does not have a record of violating the principles set out in Part 3 and he is accountable to NITDA or a regulatory authority for data protection within or outside Nigeria; accordingly, every Data Processor or Controller shall be liable for the actions or inactions of third parties who handle the Personal Data of Data Subjects under this Regulation;

(c) In this Part, “a party” shall include directors, shareholders, servants and privies of the contracting party; and record shall include report of public

records and reports in credible news media. Accordingly, the distinction between legal and natural persons for the purpose of limiting due diligence is irrelevant.

2.5 PUBLICITY AND CLARITY OF PRIVACY POLICY

Notwithstanding anything contrary in this Regulation or any instrument for the time being in force**,** any medium through which Personal Data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subject being targeted can understand. The privacy policy shall in addition to any other relevant information contain the following:

a) what constitutes the Data Subject's consent;
b) description of collectable personal information;
c) purpose of collection of Personal Data;
d) technical methods used to collect and store personal information, cookies, JWT, web tokens etc.;
e) access (if any) of third parties to Personal Data and purpose of access;
f) a highlight of the principles stated in Part 2;
g) available remedies in the event of violation of the privacy policy;
h) the time frame for remedy; and
i) provided that no limitation clause shall avail any Data Controller who acts in breach of the principles set out in this Regulation.

2.6 DATA SECURITY

Anyone involved in data processing or the control of data shall develop 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 continuous capacity building for staff.

2.7 THIRD PARTY DATA PROCESSING CONTRACT

Data processing by a third party shall be governed by a written contract between the third party and the Data Controller. Accordingly, any person engaging a third

party to process the data obtained from Data Subjects shall ensure adherence to this Regulation.

2.8 OBJECTIONS BY THE DATA SUBJECT

The right of a Data Subject to object to the processing of his data shall always be safeguarded. Accordingly, a Data Subject shall have the option to:

a) object to the processing of Personal Data relating to him which the Data Controller intend to process for the purpose of marketing;
b) be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge.

2.9 ADVANCEMENT OF RIGHT TO PRIVACY

Notwithstanding anything to the contrary in this Regulation, the privacy right of a Data Subject shall be interpreted for the purpose of advancing and never for the purpose of restricting the safeguards Data Subject is entitled to under any data protection instrument made in furtherance of fundamental rights and the Nigerian laws.

2.10 PENALTY FOR DEFAULT

Any person subject to this Regulation who is found to be in breach of the data privacy rights of any Data Subject shall be liable, in addition to any other criminal liability, to the following:

a) in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater;
b) in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater.

2.11 TRANSFER TO A FOREIGN COUNTRY

Any transfer of Personal Data which is undergoing processing or is intended for processing after transfer to a foreign country or to an international organisation shall take place subject to the other provisions of this Regulation and the

supervision of the Honourable Attorney General of the Federation (HAGF). Accordingly:

a) a transfer of Personal Data to a foreign country or an international organization may take place where the Agency has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organization in question ensures an adequate level of protection;
b) the HAGF shall take into consideration the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedom, relevant legislation, both general and sectoral, including public security, defence, national security and criminal law and the access of public authorities to Personal Data;
c) implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of Personal Data to another foreign country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable Data Subject rights and effective administrative and judicial redress for the Data Subjects whose Personal Data are being transferred;
d) the existence and effective functioning of one or more independent supervisory authorities in the foreign country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the Data Subjects in exercising their rights and for cooperation with the relevant authorities in Nigeria; and
e) the international commitments of the foreign country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, particularly in relation to the protection of Personal Data.

2.12 EXCEPTIONS IN RESPECT OF TRANSFER TO A FOREIGN COUNTRY

In the absence of any decision by The Agency or HAGF as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of Personal Data to a foreign country or an international organisation shall take place only on one of the following conditions:

a) that the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers;
b) the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;
d) the transfer is necessary for important reasons of public interest;
e) the transfer is necessary for the establishment, exercise or defence of legal claims; and
f) the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; Provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

PART THREE:

3.1 RIGHTS OF DATA SUBJECT

(1) The Controller shall take appropriate measures to provide any information relating to processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and for any information relating to a child. The information shall be provided in writing, or by

other means, including, where appropriate, by electronic means. When requested by the Data Subject, the information may be provided orally, provided that the identity of the Data Subject is proven by other means.

(2) If the Controller does not act on the request of the Data Subject, the Controller shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority.

(3) Except as otherwise provided by any public policy or Regulation, information provided to the Data Subject and any communication and any actions taken shall be provided free of charge. Where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

a) Charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or,

b) Write a letter to the Data Subject stating refusal act on the request and copy The Agency on every such occasion through a dedicated channel which shall be provided for such purpose.

(4) The Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(5) Where the Controller has reasonable doubts concerning the identity of the natural person making the request for information, the Controller may request the provision of additional information necessary to confirm the identity of the Data Subject.

(6) The information to be provided to Data Subject may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable.

(7) Prior to collecting Personal Data from a Data Subject, the Controller shall provide the Data Subject with all the following information:

a) the identity and the contact details of the Controller;

b) the contact details of the Data Protection Officer;

c) the purpose(s) of the processing for which the Personal Data are intended as well as the legal basis for the processing;

d) the legitimate interests pursued by the Controller or by a third party;

e) the recipients or categories of recipients of the Personal Data, if any;

f) where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by The Agency;

g) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

h) the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to Data Portability;

i) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

j) the right to lodge a complaint with a relevant authority;

k) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;

l) the existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;

m) Where the Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data were collected, the controller shall provide the Data Subject prior to that further processing with information on that other purpose, and with any relevant further information; and

n) Where applicable, that the Controller intends to transfer Personal Data to a recipient in a foreign country or international organization and the existence or absence of an adequacy decision by The Agency.

(8) Where Personal Data are transferred to a foreign country or to an international organization, the Data Subject shall have the right to be informed of the

appropriate safeguards for data protection in the foreign country. The Data Subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate Personal Data concerning him or her. Considering the purposes of the processing, the Data Subject shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

(9) The Data Subject shall have the right to request the Controller to delete Personal Data without delay, and the Controller shall delete Personal Data where one of the following grounds applies:

a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or processed;
b) the Data Subject withdraws consent on which the processing is based;
c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) the Personal Data have been unlawfully processed; and
e) the Personal Data must be erased for compliance with a legal obligation in Nigeria.

(10) The Controller who has made the Personal Data public and is obliged to delete the Personal Data shall, take all reasonable steps, to inform Controllers processing the Personal Data of the Data Subject's request.

(11) The Data Subject shall have the right to obtain from the Controller restriction of processing where one of the following applies:

a) The accuracy of the Personal Data is contested by the Data Subject for a period enabling the Controller to verify the accuracy of the Personal Data;
b) The processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
c) The Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims; and

d) The Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

(12) Where processing has been restricted such Personal Data shall, except for storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest in Nigeria.

(13) The Controller shall communicate any rectification or erasure of Personal Data or restriction to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the Data Subject about those recipients if the Data Subject requests it.

(14) The Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the Personal Data have been provided, where:

(a) The processing is based on consent, or

(b) On a contract, and

(c) The processing is carried out by automated means.

(15) In exercising his right to Data Portability, the Data Subject shall have the right to have the Personal Data transmitted directly from one controller to another, where technically feasible. Provided that this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

(16) The exercise of the foregoing rights shall be in conformity with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights.

PART FOUR:

4.1 IMPLEMENTATION MECHANISMS

(1) All public and private organizations in Nigeria that control data of natural persons shall, within three (3) months after the date of the issuance of this Regulation, make available to the general public their respective data protection Policies; these Policies shall be inconformity with this Regulation.

(2) Every Data Controller shall designate a Data Protection Officer for the purpose of ensuring adherence to this Regulation, relevant data privacy instruments and data protection directives of the Data Controller; provided that a Data Controller may outsource data protection to a verifiably competent firm or person.

(3) A Data Controller or Processor shall ensure continuous capacity building for Data Protection Officers and the generality of her personnel involved in any form of data processing.

(4) The Agency shall by this Regulation register and license Data Protection Compliance Organisations (DPCOs) who shall on behalf of the Agency monitor, audit, conduct training and data protection compliance consulting to all Data Controllers under this Regulation. The DPCOs shall be subject to Regulations and Directives of NITDA issued from time to time.

(5) Within six (6) months after the date of issuance of this Regulations, each organization shall conduct a detailed audit of its privacy and data protection practices with at least each audit stating:

a. 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.

(6) Where a Data Controller processes the Personal Data of more than 1000 in a period of six months, a soft copy of the summary of the audit containing information stated in 4.1(5) shall be submitted to the Agency.

(7) On annual basis, a Data Controller who processed the Personal Data of more than 2000 Data Subjects in a period of 12 months shall, not later than the 15th of March of the following year, submit a summary of its data protection audit to the Agency. The data protection audit shall contain information as specified in 4.1(5).

(8) The mass media and the civil society shall have the right to uphold accountability and foster the objectives of this Regulation.

4.2 ADMINISTRATIVE REDRESS PANEL

(1) Without prejudice to the right of a Data Subject to seek redress in a court of competent jurisdiction, the Agency shall set up an Administrative Redress Panel under the following terms of reference**;**

(2) Investigation of allegations of any breach of the provisions of this Regulation;

(3) Invitation of any party to respond to allegations made against it within seven days;

(4) Issuance of Administrative orders to protect the subject-matter of the allegation pending the outcome of investigation;

(5) Conclusion of investigation and determination of appropriate redress within twenty-eight (28) working days; and

(6) Any breach of this Regulation shall be construed as a breach of the provisions of the National Information Technology Development Agency (NITDA) Act of 2007.

4.3 LOCAL AND INTERNATIONAL COOPERATION

In relation to foreign countries and international organizations, the Agency and relevant authorities shall take appropriate steps to:

a) Develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of Personal Data;

b) Provide international mutual assistance in the enforcement of legislation for the protection of Personal Data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of Personal Data and other fundamental rights and freedoms;

c) Engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of Personal Data; and

d) Promote the exchange and documentation of Personal Data protection legislation and practice, including on jurisdictional conflicts with third countries.

THIS INSTRUMENT WAS SIGNED THIS 25TH DAY OF JANUARY, 2019

Dr Isa Ali Ibrahim (Pantami) FNCS, FBCS, FIIM
Director General
National Information Technology Development Agency (NITDA)