REQUEST FOR COMMENTS AND OBSERVATIONS ON DRAFT DATA PROTECTION AND PRIVACY BILL, 2018 AND INVITATION TO 1-DAY VALIDATION WORKSHOP

Earlier this year, the Senate Committee on Judiciary, Human Rights and Legal Matters held a one-day public hearing for the purpose of considering the provisions of the draft Data Protection and Privacy Bill and eliciting comments from stakeholders on the merits of the proposed legislation.

Previously, a Personal Information and Data Protection Bill, 2016 covering various aspects of personal data protection, was prepared by the National Identity Management Commission (NIMC) and sent to the House of Representatives. This Bill was not passed into law. In 2017, the House of Representatives passed another data protection Bill sponsored by the Speaker of the House, sent to the Senate, but it has also not been passed into law.

At the public hearing, the NIMC and other stakeholders made representations and submitted comments on the draft Bill. The Senate Committee came to the conclusion that, there was need for further work to be done on the provisions of the draft Bill before consideration for passage into law. The Committee mandated the stakeholders to conduct a review of both draft legislations and to propose a harmonized updated Data Protection and Privacy Bill which will address all the salient and pertinent issues bothering on personal information, data protection and privacy in Nigeria, for approval by the Senate, and subsequent concordance in Joint Committee with the House of Representatives and final enactment for Presidential assent.

Further to this recommendation, the Federal Ministry of Justice, with the support of the GLACY+ Project of the Council of Europe and European Union, in collaboration with the Cybercrime Advisory Council and the Experts Group of the Senate Committee on ICT and Cybersecurity held a Data Protection Legislative drafting workshop in September 2018, with most public and private sector stakeholder organizations in attendance.

At the workshop, participants reviewed the draft Data Protection and Privacy legislations along international standards and best practices, and carried out a harmonization and drafting exercise leading to a sound data protection legislation for the country.

The Federal Ministry of Justice has concluded drafting work on the harmonized updated Data Protection and Privacy Bill. As part of the process leading up to enactment of the legislation, I, on behalf of the collaborating stakeholders,

invite members of the general public and interested stakeholders to review the draft Bill below. A copy of the draft Bill is also available and can be accessed via www.justice.gov.ng and www.cybersecurity.gov.ng

We request that you forward comments, observations, suggestions/corrections and feedback on the draft Bill to terlumun.tyendezwa@justice.gov.ng and hadiza.dagabana@nimc.gov.ng on or before **Tuesday 13th November 2018.** Thank you very much.

Engr. Aliyu A. Aziz
Director General/CEO
National Identity Management Commission, Abuja

DATA PROTECTION AND PRIVACY BILL, 2018

ARRANGEMENT OF SECTIONS:

DATA PROTECTION AND PRIVACY BILL, 2018

A BILL

FOR

AN ACT TOREGULATE THE PROCESSING OF PERSONAL DATA AND DISCLOSURE OF INFORMATION,AND TO ESTABLISH THE DATA PROTECTION COMMISSION FOR THE PROTECTION OF PERSONAL DATA AND PRIVACY, AND FOR RELATED MATTERS

[ ] Commencement

ENACTED by the National Assembly of the Federal Republic of Nigeria –

PART I - OBJECTIVE, SCOPE AND DEFINITIONS

1. Objectives

The objective of this Act is to provide the framework for the protection of personal data and to regulate the processing of information relating to individuals, to safeguard fundamental rights and freedoms, in particular the right to privacy.

2. Scope - Protection of Personal Data

(1) This Act protects individuals with regard to the processing of personal data by automated and non-automated means, whatever his or her nationality or residence, and in particular by -

(a) requiring that personal data is processed in a transparent, fair and lawful manner, on the basis of an individual's consent or another specified lawful basis;

(b) conferring on individuals a number of rights as set in Part VI, including the right to be informed about the processing of their personal data, to obtain a copy of such data, the right to the rectification of inaccurate data and the right to remedy.

(2) This Act applies to processing of personal data carried out by entities in the private and public sectors.

(3) This act does not apply to personal data processed by an individual in the course of purely personal or household data.

PART II - BASIC PRINCIPLES AND LEGAL BASIS

3. Basic principles relating to processing of personal data

(1) Personal data shall be -

(a) processed lawfully, fairly and in a transparent and proportionate manner;

(b) collected for specified, explicit and legitimate purposes. Personal data should not be further processed for a purpose that is incompatible with those purposes for which the data were initially collected. Further processing for archiving purposes in the public interest, for scientific purposes or historical research purposes and statistical purposes would not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) Furthermore, personal data should be accurate and regularly kept up to date;

(e) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Data should be deleted once the purpose for which they were processed has been achieved or should be kept in a form that prevents any direct or indirect identification of the data subject;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and access, against accidental loss, destruction or damage. The controller and processor shall use appropriate technical or organizational measures to ensure the integrity and the confidentiality of the personal data;

(2) The controller shall be responsible for and be able to demonstrate compliance with all the basic principles.

4. Lawfulness of processing

(1) The processing of personal data shall be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or on some other legitimate basis laid down by law.

(2) Such legitimate basis shall be at least one of the following -

(a) 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;

(b) processing is necessary for compliance with a legal obligation as provided by law and to which the controller is subject;

(c) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(d) 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 controller;

(g) processing is necessary for the purposes of the prevailing legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Validity of consent

(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.

(2) The consent of the data subject shall represent the free expression of an intentional choice given by a statement (either in written or orally) or by a clear affirmative action.

(3) Mere silence, inactivity or pre-validated forms or boxes shall not constitute consent by the data subject.

(4) Where the data subject has no genuine choice or is unable to refuse consent, consent is given under such circumstances shall not be regarded as given freely.

(5) Where the processing of personal data is based on the consent of the data subject, he or she shall have the right to withdraw his or her consent at any time.

(6) The withdrawal under subsection (5) of this section shall not affect the lawfulness of the data processing that occurred before the data controller has received the notification for withdrawal of consent.

6. Transparency of processing

(1) Every data subject has the right to be informed ('to know') about the processing of their personal data and their rights.

(2) A controller shall act transparently when processing personal data in order to ensure fair processing and to enable data subjects to understand and exercise their rights with regards to the processing of their personal.

(3) A Controller shall inform the data subject of -

(a) the controller's official identity and habitual residence or place of establishment;

(b) the contact details of the controller, and, where applicable, the controller's representative;

(c) the legal basis and the purposes of the intended processing;

(d) the categories of personal data processed;

(e) the recipients or categories of recipients of the personal data,

(f) any intended transfer of personal data to a third country or international organisation and a description of the safeguards provided to ensure the adequate protection of personal data;

(g) the period for which personal data will be retained or if that is not possible, the general criteria used to determine that period;

(h) the existence of automated decision-making, together with the significance and envisaged consequence of such processing for the data subject, including the right to challenge such processing;

(i) the existence of profiling and the consequences of such profiling and the right to object;

(j) the existence of rights set out in Part VI of this Act including the right to lodge a complaint with the national supervisory authority and the means for exercising those rights.

(4) The information referred to in subsection (3) of this section shall be provided in an appropriate format adapted to the relevant data subjects and shall be presented in a concise, transparent, intelligible and easily accessible form, using clear plain language.

(5) The provision of subsection (3) of this section shall not apply where the data subject already received the information.

(6) Where the personal data are not collected directly from the data subject, the controller shall provide the information in (3) of this section within a reasonable period but at the latest within one month or on first

communication with the data subject, except where the processing is expressly prescribed by law or it proves to be impossible or involves disproportionate efforts.

PART III - RIGHTS OF THE DATA SUBJECTS

7. Rights of the Data Subject

(1) A data subject shall have the rights set out in this Part.

(2) A data subject's rights may only be limited –

(a) in accordance with the provisions of section 40 of this Act;

(b) as may be provided for by law; or

(c) where it constitutes a necessary and proportionate measure in a democratic society.

8. Right of Access

(1) A data subject shall have the right to obtain, on request and at reasonable intervals, confirmation as to whether personal data relating to him are being processed and if so, the communication in an intelligible form of the data, together with all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with section 7of this Act.

(2) The controller shall provide a copy of the personal data processed free of charge, provided that, in exceptional circumstances, the controller may charge a reasonable fee based on administrative costs where a request is excessive or manifestly unfounded, in particular because of their repetitive character, or as may be provided in a law.

(3) The controller shall provide a copy of the personal data requested together with the information under subsection (1) of this section within a period one month from the date of receipt of the request.

(4) The period stated in subsection (3) of this section, may be extended by a period not exceeding an additional two months where necessary, taking into account the complexity of the request.

(5) A data subject shall also have the right, on request, to obtain knowledge of the reasoning underlying data processing where the result of such processing is applied to him, including the consequence of such reasoning.

9. Right in respect of Automated decision making

(1) A data subject shall have the right not to be subject to a decision significantly affecting him based solely on an automated processing of data without having his view taken into consideration.

(2) Subsection (1) of this section shall not apply where a decision is authorised by law to which the Controller is subject and that provides appropriate measures to safeguard the legitimate interests, rights and freedoms of a data subject.

(3) The Controller shall implement suitable measures to safeguard the data subject's rights and legitimate interests, at least the right to obtain human intervention on the part of the Controller.

10. Right to rectification and erasure

(1) The data subject shall have the right to obtain from the Controller, without excessive delay, free of charge, (if justified) the rectification or erasure of inaccurate, false or unlawfully processed personal data.

(2) Where the data subject has submitted a valid request for the rectification or erasure of his or her data, the controller shall communicate such request to all controllers, processors or other recipients in order to ensure complete rectification or erasure.

(3) Where accuracy of the data is contested by the data subject, the data subject opposes the erasure of his or her data, or the data subject has objected the processing of his or her personal data and the legal basis must be verified, the controller shall temporarily block processing until the grounds for restriction have been resolved. Where the temporary blocking of data is lifted, the data subject shall be informed by the controller.

11. Right to Remedy

Where a right of a data subject under this Act is violated, the data subject shall have the right to a remedy under this Act.

12. Right to assistance of a supervisory authority

A data subject has the right to benefit, whatever his nationality or residence, from the assistance of the Commission within the meaning of section 55, in exercising his or her rights under this Act.

13. Right to object,including to profiling and direct marketing

(1) Data subjects shall have the right to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her, including profiling. A controller shall no longer process the personal data unless the controller demonstrates legitimate grounds for the processing which override the interests or rights and fundamental freedoms of the data subject.

(2) Data subjects shall have the right to object to the processing of their personal data for the purposes of direct marketing at any time and free of charge.

(3) Where personal data is processed to provide direct marketing via electronic means, this shall require the consent of the data subject.

(4) Where a data subject makes an objection under subsection (3) of this section, he shall be entitled to have the unconditional erasure, removal or suppression of the personal data covered by the objection.

(5) The data subject's consent pursuant to section 5 is required where personal data is processed to provide direct marketing through electronic means.

PART IV – PROCESSING OF SENSITIVE DATA

14. Processing of Sensitive data prohibited

(1) Unless otherwise provided by this Act or other legislation, a person shall not process personal data which relates to
(a) a child who is under parental control in accordance with the law, or
(b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or behavior of an individual.

(2) A data controller may process sensitive personal data in accordance with this Act where

(a) processing is necessary, or
(b) the data subject consents to the processing.

(3) The processing of sensitive data is necessary where it is for the exercise or performance of a right or an obligation conferred or imposed by law on an employer.

(4) c data shall not be processed unless the processing is necessary for the protection of the vital interests of the data subject where
(a) it is impossible for consent to be given by or on behalf of the data subject,
(b) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
(c) consent by or on behalf of the data subject has been unreasonably withheld.

(5) Sensitive data shall not be processed unless the processing is carried out for the protection of the legitimate activities of a body or association which
(a) is established for non-profit purposes,
(b) exists for political, philosophical, religious or trade union purposes;
(c) relates to individuals who are members of the body or association or have regular contact with the body or association in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

(6) The processing of sensitive shall be presumed to be necessary where it is required
(a) for the purpose of or in connection with a legal proceeding,
(b) to obtain legal advice,
(c) for the establishment, exercise or defence of legal rights,
(d) in the course of the administration of justice, or.
(e) for medical purposes and the processing is
    (i) undertaken by a health professional, and
    (ii) pursuant to a duty of confidentiality between patient and health professional.

(7) In this section, "medical purposes" includes the purposes of preventive medicine, medical diagnosis, medical research, provision of care and treatment and the management of healthcare services by a medical or dental practitioner or a legally recognised traditional healer.

(8) A person shall not process sensitive data in respect of race or ethnic origin unless the processing of the sensitive data is

(a) necessary for the identification and elimination of discriminatory practices, and

(b) carried out with appropriate safeguards for the rights and freedoms of the data subject.

(9) The Minister may in consultation with the Commission by legislative instrument prescribe further conditions which may be taken by a data controller for the maintenance of appropriate safeguards for the rights and freedoms of a data subject related to processing of sensitive personal data.

35. Exemption related to religious or philosophical beliefs of data subject.

(1) The prohibition on processing of personal data which relates to the religious or philosophical beliefs of a data subject does not apply if the processing is carried out by

(a) a spiritual or religious organisation or a branch of the organisation

and the processing is in respect of persons who are members of the organisation,

(b) an institution founded on religious or philosophical principles and the

processing is

(i) with respect to the members, employees or other persons

belonging to the institution,

(ii) consistent with the objects of the institution, and

(iii) necessary to achieve the aims and principles of the institution. (2) An individual who believes that data is being processed under subsection (1) may at any time by notice in writing to a data controller require a data controller to provide particulars of data processed under this exemption.

16. Right to prevent processing of personal data

(1) An individual shall at any time by notice in writing to a data controller require the data controller to cease or not begin processing for a specified purpose or in a specified manner, personal data which causes or is likely to cause unwarranted damage or distress to the individual.

(2) A data controller shall within twenty-one days after receipt of a notice inform the individual in writing

(a) that the data controller has complied or intends to comply with the notice of the data subject, or

(b) of the reasons for non-compliance.

(3) Where the Commission is satisfied that the complainant is justified, the Commission may order the data controller to comply.

17. Right to prevent processing of personal data for direct marketing.

(1) A data controller shall not provide, use, obtain, procure or provide information related to a data subject for the purposes of direct marketing without the prior written consent of the data subject.

(2) A data subject is entitled at any time by notice in writing to a data controller to require the data controller not to process personal data of that data subject for the purposes of direct marketing.

(3) Where the Commission is satisfied on a complaint by a person who has given notice in subsection (1), that the data controller has failed to comply with the notice, the Commission may order that data controller to comply with the notice.

(4) In this section "direct marketing" includes the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

18. Rights in relation to automated decision-taking.

(1) An individual is entitled at any time by notice in writing to a data controller

to require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects that individual is

not based solely on the processing by automatic means of personal data in respect of which that individual is the data subject.

(2) Despite the absence of a notice, where a decision which significantly affects an individual is based solely on that processing

(a) the data controller shall as soon as reasonably practicable notify the individual that the decision was taken on that basis, and

(b) the individual is entitled, by notice in writing to require the data controller to reconsider the decision within twenty-one days after receipt of the notification from the data controller.

(3) The data controller shall within twenty-one days after receipt of the notice, inform the individual in writing of the steps that the data controller intends to take to comply with the notice.

(4) This section does not apply to a decision made

(a) in the course of considering whether to enter into a contract with the data subject,

(b) with a view to entering into the contract,

(c) in the course of the performance of the contract,

(d) for a purpose authorized or required by or under an enactment, or

(e) in other circumstances prescribed by the Commissioner.

(5) Where the Commission is satisfied on a complaint by a data subject that a person taking a decision has failed to comply, the Commission may order the data controller to comply.

(6) An order for compliance under subsection (5) shall not affect the rights of a person other than the data subject or the data controller.

19. Rights in relation to exempt manual data

(1) A data subject is entitled at any time by notice in writing to require a data controller

(a) to rectify, block, erase or destroy exempt manual data which is inaccurate or incomplete, or

(b) to cease to hold exempt manual data in a manner which is incompatible with the legitimate purposes pursued by the data controller.

(2) A notice under subsection (1) shall state the reasons for believing that the data

(a) is inaccurate or incomplete, or

(b) is held in a manner which is incompatible with the legitimate purposes pursued by that data controller.

(3) Where the Commission is satisfied on a complaint by a person who has given notice that the data controller has failed to comply with the notice, the Commission shall give appropriate direction to the data controller to comply with the notice.

(4) For the purposes of thissection, personal data isincomplete if the data is of the kind that its incompleteness would constitute a contravention of data protection principles provided in this Act.

20. Compensation for failure to comply

(1) Where an individual suffers damage or distress through the contravention by a data controller of the requirements of this Act, that individual is entitled to compensation from the data controller for the damage or distress.

(2) In proceedings against a person under this section, it is a defence to prove that the person took reasonable care in allthe circumstances to comply with the requirements of this Act.

21. Rectification, blocking, erasure and destruction of personal data.

(1) Where the Commission is satisfied on a complaint of a data subject that personal data on that data subject is inaccurate, the Commission may order the data controller to

(a) rectify,
(b) block,
(c) erase, or
(d) destroy the data.

(2) Subsection (1) applies whether or not the data is an accurate record of information received or obtained by the data controller from the data subject or a third party.

(3) Where the data is an accurate record of the information, the Commission may make an order requiring the data controller to supplement the statement of the true facts which the Commission considers appropriate.

(4) Where the data complained of has been rectified, blocked supplemented, erased or destroyed, the data controller is required to notify third parties to whom the data has been previously disclosed of the rectification, blocking, supplementation, erasure or destruction.

(5) To determine whether it is reasonably practicable to require the notification, the Commission shall have regard, in particular, to the number of persons to be notified.

22. Application of the Act

(1) Except as otherwise provided, this Act applies to a data controller in respect of data where

(a) the data controller is established in this country and the data is processed in this country,

(b) the data controller is not established in this country but uses equipment or a data processor carrying on business in this country to

process the data, or

(c) processing is in respect of information which originates partly or wholly from this country.

(2) A data controller who is not incorporated in this country shall register as an external company.

(3) For the purposes of this Act the following are to be treated as established in this country:

(a) an individual who is ordinarily resident in this country;

(b) a body incorporated under the laws of this country;

(c) a partnership, persons registered under the relevant laws of the country.

(d) an unincorporated joint venture or association operating in part or in whole in this country; and

(e) any person who does not fall within paragraphs (a),(b), (c) or (d) but maintains an office, branch or agency through which business activities are carried out in this country.

(4) This Act does not apply to data which originates externally and merely transits through this country.

PART V - Data Protection Register

23. Establishment of Data Protection Register

(1) There is established by this Act a register of data controllers to be known as the Data Protection Register.

(2) The Commission shall keep and maintain the Register and make regulations for its proper maintenance.

(3) A data controller shall register with the Commission.

24. Application for registration

(1) An application for registration as a data controller shall be made in writing to the Commission and the applicant shall furnish the following particulars:

(a) the business name and address of the applicant;

(b) the name and address of the company's representative where the company is an external company;

(c) a description of the personal data to be processed and the category of persons whose personal data are to be collected;

(d) an indication as to whether the applicant holds or is likely to hold sensitive data;

(e) a description of the purpose for which the personal data is being or is to be processed;

(f) a description of a recipient to whom the applicant intends to disclose the personal data;

(g) the name or description of the country to which the applicant may transfer the data;

(h) the class of persons or where practicable the names of persons whose.

personal data is held by the applicant;

(i) a general description of measures to be taken to secure the data; and

(j) any other information that the Commission may require.

(2) An applicant who knowingly supplies false information in support of an application for registration as a data controller commits an offence and is liable on summary conviction to aterm of imprisonment of not less than one year or a fine of not less than N5,000,000.00 or to both.

(3) Where a data controller intends to keep personal data for two or more purposes the Commission shall make separate entries for each purpose in the Register.

25. Right to refuse registration.

(1) The Commission shall not grant an application for registration under this Act where

(a) the particulars provided for inclusion in an entry in the Register are insufficient;

(b) the appropriate safeguards for the protection of the privacy of the data subject have not been provided by the data controller; and

(c) in the opinion of the Commission, the person making the application for registration does not merit the grant of the registration.

(2) Where the Commission refuses an application for registration as a data controller, the Commission shall inform the applicant in writing within fourteen days

(a) of its decision and the reasons for the refusal, and

(b) the applicant may apply for judicial review to the Federal High Court againstthe refusal.

(3) A refusal of an application for registration is not a bar to re-application.

26. Grant of registration

(1) The Commission shall

(a) register an applicant if it is satisfied that the applicant has satisfied the conditions required for registration, and

(b) provide the applicant with a certification of registration upon approval of the application.

(2) The applicant shall pay the prescribed fee upon registration.

27. Removal from Register.

The Commission may at the request of the person to whom an entry in the Register relates, remove that person's name from the Register at any time.

28. Cancellation of registration

The Commission has the power to cancel a registration for good cause.

29. Processing of personal data without registration prohibited

A data controller who has not been registered under this Act shall not process personal data.

30. Access by the public

(1) The Commission shall provide facilitiesto make the information contained in the Register available for inspection by members of the public.

(2) The Commission shall supply a member of the public with a duly certified manual or electronic copy of the particulars contained in an entry made in the Register on payment of the prescribed fee.

31. Duty to notify changes

A person in respect of whom an entry as a data controller is included in the Register shall notify the Commission of changes in the registered particulars within fourteen days.

32.Failure to register

A person who fails to register as a data controller but processes personal data commits an offence and is liable on summary conviction to a term of imprisonment of not less than 2 years or a fine of not less than N10,000,000.00 or to both.

33. Assessable processing

(1) The Commisoner may by Regulations/Guidelines specify actions which constitute assessable processing if the Minister considers the assessable processing likely to

(a) cause substantial damage or substantial distress to a data subject, or

(b) otherwise significantly prejudice the privacy rights of a data subject;

(2) On receipt of an application for registration, the Commission shall consider

(a) whether the processing to which the notification relates is assessable,

or

(b) if the assessable processing complies with the provisions of this Act.

(3) The Commission shall within twenty-eight days from the day of receipt of the application, inform the data controller whether the processing is likely to comply with the provisions of this Act.

(4) The Commission may extend the initial period by a further period which does not exceed fourteen days or other period that the Commission may specify.

(5) The assessable processing in respect of which a notification has been given to the Commission shall not be carried on unless

(a) the period of twenty-eight days has elapsed, or

(b) before the end of that period, the data controller receives a notice from the Commission under subsection (3).

(6) A data controller who contravenes this section commits an offence and is liable on summary conviction to a term of imprisonment of not less than 2 years or a fine of not less than N10,000,000.00 or to both.

34. Appointment of data protection supervisors

(1) A data controller may appoint a certified and qualified data supervisor to act as a data protection supervisor.

(2) The data protection supervisor is responsible for the monitoring of the data controller's compliance with the provisions of this Act.

(3) This section is subject to the exemptions or modifications specified in the authorisation.

(4) An authorisation under this section may

(a) impose a duty on a data protection supervisor in relation to the Commission, and

(b) confer a function on the Commission in relation to a data protection supervisor.

(5) A data protection supervisor may be an employee of the data controller.

(6) The Commission shall provide the criteria for qualification to be appointed as a data protection supervisor.

(7) A person shall not be appointed as a data protection supervisor unless the person satisfies the criteria set by the Commission.

35. Commission Fees

The Commissioner may by Regulations prescribe fees for the purpose of sections 26, 27 and 30.

PART VI - DUTIES OF CONTROLLERS AND PROCESSORS

35. Duties of the Controller

(1) The Controller shall -

(a) take all necessary measures to comply with the obligations of this Act;

(b) ensure the processing of personal data is proportionate, that is, necessary in relation to the legitimate purpose pursued and having regard to the interests, rights and freedoms of the data subject or the public interest;

(c) take into consideration the risks arising from the interests, rights and fundamental freedoms of data subjects, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor;

(d) be able to establish, in particular, to the data protection supervisory authority, that the processing under their control is in compliance with the provisions of this Act.

36. Processors

(1) The controller shall be responsible for the processing of personal data carried out by a processor on behalf of the controller.

(2) The controller shall use only a processor who provides sufficient guarantees to implement appropriate technical and organisational measures, taking into account the controller's obligations under this Act and otherwise meet the requirements of this Act and the protection of data subject rights.

(3) The processing of personal data by the controller shall be subject to a legally binding contract that sets-out the nature of the processing agreement, including the personal data to be processed and the purpose of processing, that stipulates the obligations and restrictions to be imposed on the

processor, including sub-processing or transfers of personal data to third countries.

37.Duties of the Processor

A processor shall comply with section 38 to ensure data protection by design (and default).

PART VII - DATA PROTECTION BY DESIGN AND SECURITY OF PROCESSING

38.Data Protection by Design (and by default)

The controller and, where applicable, the processor, shall -

(a) examine the likely impact of the intended processing of personal data on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and

(b) design the data processing in such a manner, and integrate appropriate technical and organisational measures, as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

39. Security of Processing

(1) The controller, and where applicable, the processor, shall take necessary technical and organisational measures to protect personal data against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

(2) When considering necessary measures, the controller shall take into account -

(a) the current state of the art of data-security methods and techniques in the field of data processing, commensurate with the seriousness and probability of the potential risk;

(b) factors such as the –

(i) potential adverse consequences for the data subject,

(ii) nature of the personal data,

(iii) volume of personal data processed,

(iv) degree of vulnerability of the technical architecture used for the processing,

(v) need to restrict access to the data, and

(vi) requirements concerning the long-term storage of the data.

(3) Controllers and processors shall establish a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

PART VII- EXCEPTIONS ,RESTRICTIONSANDEXEMPTIONS

40. Exceptions and restrictions

(1) No exception to the provisions set out in the this Act shall be allowed except to the provisions of section 4 of this Act, when such an exception is provided for by law, respects the essence of the fundamental rights and

freedoms and constitutes a necessary and proportionate measure in a democratic society.

(2) The exception in order to be considered as necessary and proportionate in a democratic society has to be provided for by law, (to observe quality requirements of the national law: rule of law, accessible, foreseeable), needs to serve a legitimate purpose as set out in the Constitution or a national legislation and has to be proportionate to the legitimate aim pursued being suitable, necessary and proportionate.

(3) Processing activities for national security and defense purposes shall be subject to independent and effective review and supervision, by the Commissionas well as any appropriate authority empowered with these functions, provided that it is independent and carry out these functions in an effective manner.

EXEMPTIONS

(3) National security

(a) The processing of personal data is exempt from the provisions of this Act for the purposes of
(b) public order,
(c) public safety,
(d) public morality,
(e) national security, or
(f) public interest.

(4) Crime and taxation

(1) The processing of personal data is exempt from the provisions of this Act for the purposes of
  (a) the prevention or detection of crime,
  (b) the apprehension or prosecution of an offender, or

(c) the assessment or collection of a tax or duty or of an imposition of a similar nature.

(2) Personal data is exempt from the non-disclosure provisions in any case in which

(a) The disclosure is for a purpose mentioned in subsection (4,1a), and

(b) the application of those provisions in relation to the disclo- sure is likely to prejudice any of the matters mentioned in that subsection.

(5) Health, education and social work

Personal data on the following subjects shall not be disclosed except where the disclosure is required by law:

(a) Personal data which relates to the physical, mental health or mental condition of the data subject,

(b) personal data in respect of which the data controller is an educational institution and which relates to a pupil at the institution, or

(c) personal data of similar description.

(6) Regulatory activity

(1) The provisions of this Act do not apply to the processing of personal data for protection of members of the public

(a) against loss or malpractice in the provision of

(i) banking,

(ii) insurance,

(iii) investment,

(iv) other financial services, or

(v) management of a body corporate;

(b) against dishonesty or malpractice in the provision of professional services;

(c) against the misconduct or mismanagement in the administration of a non-profit making entity;

(d) to secure the health, safety and welfare of persons at work; or

(e) to protect non-working persons against the risk to health or safety arising out of or in connection with the action of persons at work.

(2) The processing of personal data is exempt from the subject information provisions of this Act if it is for the discharge of a function conferred by or under an enactment on

(a) Parliament,
(b) a local government authority,
(c) the administration of public health or public financing of health care, prevention, control of disease and the monitoring and eradication of disease .

(7) Journalism, literature and art

(1) A person shall not process personal data unless

(a) The processing is undertaken by a person for the publication of a literary or artistic material;
(b) the data controller reasonably believes that publication would be in the public interest; and
(c) the data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

(2) Subsection (1) does not exempt a data controller from compliance with the data principles related to
(a) lawful processing,
(b) minimality,
(c) further processing,
(d) information quality, and
(e) security safeguards.

(3) For the purposes of subsection (1) (b), in considering whether the data controller believes that the publication would be in the public interest or is reasonable, regard may be had to the compliance by the data controller with any code of practice which is
(a) relevant to the publication in question, and
(b) designated by the Minister for purposes of this subsection.

(8) Research, history and statistics

(1) The further processing of personal data for a research purpose in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained.

(2) Personal data which is processed for research purposes in compliance with the relevant conditions may be kept indefinitely.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if

(a) the data is processed in compliance with the relevant conditions, and

(b) the results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

(4) Personal data is not to be treated as processed otherwise than for research purposes merely because the data is disclosed

(a) to any person for research purposes only,

(b) to the data subject or a person acting on behalf of the data subject,

(c) at the request or with the consent of the data subject or a person acting on behalf of the data subject ,or

(d) in circumstances in which the person making the disclosure has reasonable grounds to believe that the disclosure falls within this section.

(9) Disclosure required by law or made in connection with a legal proceeding

(a) Personal data is exempt from the provisions on non-disclosure where the disclosure is required by or under an enactment, any rule of law or by the order of a court.

10. Domestic purposes.

(b) Personal data which is processed by an individual only for the purpose of that individual's personal, family or household affairs is exempt from the data protection principles.

11. Confidential references given by data controller

(1). Personal data is exempt from the data protection principles if it consists of a reference given in confidence by the data controller for the purposes of

(a) education, training or employment of the data subject,

(b) the appointment to an office of the data subject, or

(c) the provision of any service by the data subject.

12. Armed Forces

Personal data is exempt from the subject information provisions where the application of the provisions is likely to prejudice the combat effectiveness of the Armed Forces of the Republic.

13. Judicial appointments and honours

Personal data processed to

(a) assess a person's suitability for judicial office, or

(b) confer a national honour, is exempt from the subject information provisions of this Act.

14. Public service or ministerial appointment.

The Minister may by legislative instrument make Regulations to prescribe exemptions from the subject information provisions of personal data processed to assess a person's suitability for

(a) employment by the government, or

(b) any office to which appointments are made by the President.

15. Examination marks

Personal data is exempt from the provisions of this Act if it relates to examination marks processed by a data controller

(a) to determine the results of an academic, professional or other examination or to enable the results of the examination to be determined, or

(b) in consequence of the determination of the results.

16. Examination scripts.

17. Personal data which consists of information recorded by candidates during an academic, professional or other examination is exempt from the provisions of this Act.

18. Professional privilege

Personal data is exempt from the subject information provisions if it consists of information in respect of which a claim to professional

privilege or confidentiality between client and a professional adviser could be maintained in legal proceedings.

PART VII- ENFORCEMENT

41. Enforcement notice

(1) Where the Commission is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commission shall serve the data controller with an enforcement notice to require that data controller to do any of the following:

(a) to take or refrain from taking the steps specified within the time stated in the notice,

(b) to refrain from processing any personal data or personal data of a description specified in the notice; or

(c) to refrain from processing personal data or personal data of a description specified in the notice for the purposes specified or in the manner specified after the time specified.

(2) In deciding whether to serve an enforcement notice, the Commission shall consider whether the contravention has caused or is likely to cause damage or distress to any person.

(3) An enforcement notice issued in respect of a contravention of a provision of this Act may also require the data controller to rectify, block, erase or destroy other data held by the data controller and which contains an expression of opinion which appears to the Commission to be based on the inaccurate data.

(4) Where

(a) an enforcement notice requires the data controller to rectify, block, erase or destroy personal data, or

(b) the Commission is satisfied that personal data which has been rectified, blocked, erased or destroyed was processed in contravention of any of the data protection principles, the Commission may require the data controller to notify a third party to whom the data has been disclosed of the rectification, blocking, erasure or destruction.

(5) An enforcement notice shall contain a statement of the data protection principle which the Commission is satisfied has been contravened and the reasons for that conclusion.

(6) Subject to this section, an enforcement notice shall not require any of the provisions of the notice to be compiled with before the end of the period within which an appeal may be brought against the notice and, if the appeal is brought, the notice may not be complied with pending the determination or withdrawal of the appeal.

(7) Despite subsection (6), the Commission may in exceptional circumstances order that the notice apply immediately.

42. Cancellation of enforcement notice

(1). The Commission may on its own motion or on an application made by a person on whom a notice is served, cancel or vary the notice to that person.

43. Request for assessment

(1) A person who is affected by the processing of any personal data may on that person's own behalf or on behalf of another person request the Commission to make an assessment as to whether the processing is in compliance with the provisions of this Act.

(2) On receiving a request, the Commission may make an assessment in the manner that the Commission considers appropriate.

(3) The Commission may consider the following in determining whether an assessment is appropriate:

(a) the extent to which the request appears to the Commission to raise a matter of substance;

(b) any undue delay in making the request; and

(c) whether or not the person making the request is entitled to make an application in respect of the personal data in question.

(4) The Commission shall not publish the report of any finding (a) the request is accompanied with the prescribed fee, or

(b) the Commission waives payment based on proven pecuniary challenges of the applicant.

(5) Where the Commission finds that the processing by a data controller is contrary to the provisions of this Act, the Commission shall issue an information notice to the data controller specifying the contravention, and give the data controller notice to cease processing personal data.

44. Determination by the Commission

(1) Where at any time it appears to the Commission that personal data

(a) is being processed in a manner inconsistent with the provisions of this Act, or

(b) is not being processed with a view to the publication by a person of a journalistic, literary or artistic material which has not previously been published by the data controller the Commission may make a determination in writing to that effect.

(2) The Commission shall give a notice of the determination to the data controller.

45. Restriction on enforcement in case of processing for special purposes

(1) The Commission shall not serve an enforcement notice on a data controller in relation to the processing of personal data under section 44 (1) (a) unless a determination has been made by the Commission.

(2) The Commission shall not serve an information notice on a data controller in relation to the processing of personal data under section 44 (1) (b) unless a determination has been made by the Commission.

46. Failure to comply with notice

(1) A person who fails to comply with an enforcement notice or an information notice commits an offence and is liable on summary conviction to a term of imprisonment of not less than 2 years or a fine of not less than N10,000,000.00 or to both.

(2) A person who, in compliance with an information notice,

(a) makes a statement which that person knows to be false in a material respect, or

(b) recklessly makes a statement which is false in a material respect commits an offence and is liable on summary conviction to a fine of not more than one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both.

(3) It is a defence for a person charged with an offence under sub- section (1) to prove that, that person exercised due diligence to comply with the notice in question.

47. Authorized officers

(1) The Board may in writing authorize an officer to perform the functions determined by the Board for the purpose of enforcing the provisions of this Act and the Regulations.

(2) Without limiting subsection (1), an officer authorized by the Commission may at any reasonable time, enter to inspect and search any premises to ensure compliance with this Act.

PART XI - TRANSBORDER FLOW OF PERSONAL DATA

27. Transborder flow of personal data

(1) The transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Act is secured in the recipient State or international organization.

(2) An appropriate level of protection can be secured by -

(a) the law of that State or international organisation, including the applicable international treaties or agreements; or

(b) ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the controllers or processors involved in the transfer and further processing.

(3) Notwithstanding the provisions of subsection (2) of this section the transfer of personal data may take place where -

(a) the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards;

(b) the specific interests of the data subject require it in the particular case;

(c) prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or

(d) it constitutes a necessary and proportionate measure in a democratic society for the freedom of expression.

(4) The Commission shall be provided with all relevant information concerning the transfers of data referred to in subsection 2(b) and, upon request, subsection 3(b) and 3(c), respectively, of this section.

(5) The Commission is entitled to request that the person who carries out the data transfer demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests.

(6) The Commission may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

PART XII – OFFENCES AND PENALTIES

48. Unlawful obtaining of personal data

(1) A person commits an offence who knowingly or recklessly—

(a) obtains or discloses personal data without the consent of the controller;

(b) procures the disclosures of personal data to another person without the consent of the controller; or

(c) after obtaining personal data, retains it without the consent of the person who was the controller, and shall be liable on conviction to imprisonment for a term of 3 years or to a fine of not more than N5,000,000.00 or to both such imprisonment and fine.

(2) It is a defence for a person charged with an offence under subsection (1) of this section to prove that the obtaining, disclosing, procuring or retaining of data -

(a) was necessary for the purposes of preventing, detecting, prosecuting, or investigating crime;

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

(d) was necessary for the purposes of national security in accordance with extant legislation.

(3) It is also a defence for a person charged with an offence under subsection (1) of this section to prove that -

(a) the person acted in the reasonable belief that he or she had a legal right to obtain, disclose, procure or retain of the personal data;

(b) the person acted in the reasonable belief that he or she would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or

(c) the person acted—

(i) for specified purposes:

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.

(4) A person commits an offence who sells personal data, where the person obtained the data in circumstances described under subsection (1) of this section, shall be liable on conviction to imprisonment for a term of 5 years or to a fine of not more thanN15,000,000.00 or to both such fine and imprisonment.

(5) A person commits an offence who offers to sell personal data, where the person obtained the data in circumstances described under subsection (1) of this section.

(6) A person commits an offence who offers to sell, advertises or indicates that personal data is or may be for sale where it is an offence indicated under subsection (1) of this section, shall be liable on conviction to imprisonment for a term of 3 years or to a fine of not more than N10,000,000.00 or to both such fine and imprisonment.

49. Obstruction in the Execution of Warrants

A person commits an offence who -

(a) intentionally obstructs an officer in the execution of a warrant issued under this Act, or

(b) fails without reasonable excuse to give the officer executing such a warrant such assistance as the officer may reasonably require for the execution of the warrant.

and shall be liable on conviction to imprisonment for a term of 2 years or to a fine of not more thanN3,000,000.00 or to both such fine and imprisonment.

50. Attempt, Conspiracy, aiding and abetting.

(1) Any person who

(a) Attempts to commit any offence under this Act; or

(b) Aids, abets, conspires, counsel or procure another person(s) to commit any offence under this Act:

Commits an offence and shall be liable on conviction to the punishment provided for the principal offence under this Act

51. Confidentiality of Information

(1) No person who is or has been the Data Protection Commissioner or a staff of the Commission or an agent of the Commission shall disclose information which -

(a) has been obtained by, or provided to, the Commission in the course of, or for the purposes of, the discharging of the regulator's functions;

(b) relates to an identified or identifiable individual or business; and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.

(2) For the purposes of subsection (1) of this section, a disclosure is made with lawful authority only if and to the extent that -

(a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business;

(b) the information was obtained or provided as described in subsection (1)(a) for the purpose of its being made available to the public (in whatever manner);

(c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner's functions;

(d) the disclosure was made for the purposes of criminal or civil proceedings, or for the purposes of national security.

(3) A person commits an offence who knowingly or recklessly to disclose information in contravention of subsection (1) of this section.

52.Order for payment of compensation or restitution.

In addition to any other penalty prescribed under this Act, the Commission may order a person in breach under this Act to make restitution or pay compensation to the victim and the order of restitution/compensation may be enforced by the Commission on behalf of the victim in the same manner as a judgment in a civil action

PART XIII- RECORDS OBTAINED UNDER DATA SUBJECT'S RIGHTS OF ACCESS.

53. Conditional request for personal data prohibited

(1) A person who provides goods, facilities or services to the public shall not require a person to supply or produce a particular record as a condition for the provision of the goods, facilities orservices to that person.

(2) Subsection (1) does not apply where the imposition of the requirement is required or authorised under an enactment, rule of law or in the public interest.

(3) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not more than two hundred and fifty penalty units orto a term of imprisonment of not more than two years or to both.

54. Demand for health records

(1). A person shall not be required to provide records which

(a) consist of information related to the physical, mental health or mental condition of an individual, or

(b) has been made by or on behalf of a health professional in connection with the care of that individual.

PART XIV - PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION

STORED IN THEIR TERMINAL EQUIPMENT (E-PRIVACY)

55.Confidentiality of electronic communications data (e-Privacy)

(1) Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Act or any other law.

Permitted processing of electronic communications data

(2) Providers of electronic communications networks and services may process electronic communications data only if:

(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

(3) Providers of electronic communications services may process electronic communications metadata only if:

(a) it is necessary to meet mandatory quality of service requirements pursuant to any Directive of the DPC for the duration necessary for that purpose; or

(a) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(b) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

(4) Providers of the electronic communications services may process electronic communications content only:

(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or

(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority.

Storage and erasure of electronic communications data

(5) (a) Without prejudice to any other provisions, the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with this Act.

(b) Without prejudice to any other provisions, the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a

communication.

(c) Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with this Part, the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued.

Protection of information stored in and related to end-users' terminal equipment

(6) The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the end-user has given his or her consent; or

(c) it is necessary for providing an information society service requested by the end-user; or

(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.

(7) The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required where personal data are collected,

as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, have been applied.

(8) The information to be provided pursuant to sub-section (7) above may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

(9) The Commission shall be empowered to adopt delegated acts in determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

Consent

(10) The definition of and conditions for consent provided for under this Act shall apply.

(11) Without prejudice to Sub-section10, where technically possible and feasible, consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.

(12) End-users who have consented to the processing of electronic communications data as set out in this Part, shall be given the possibility to withdraw their consent at any time and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

Information and options for privacy settings to be provided

(13) Software placed on the market permitting electronic

communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

(14) Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting. In the case of software which has already been installed, the requirements shall be complied with at the time of the first update of the software.

Restrictions

(15) An Act of the National Assembly may restrict the scope of the obligations and rights provided for in this Part, where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in this Act or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.

(16) Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on this Part. They shall provide the Commiission or other competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

56. NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS

Presentation and restriction of calling and connected line identification

(1) Where presentation of the calling and connected line identification is offered in accordance with any Communication Code, the providers of publicly available number-based interpersonal communications services shall provide the following:

(a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;

(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;

(c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user;

(d) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user.

(2) The possibilities referred to in points (a), (b), (c) and (d) of sub-section (1) shall be provided to end-users by simple means and free of charge.

(3) Point (a) of sub-section (1) shall also apply with regard to calls to third countries originating in Nigeria. Points (b), (c) and (d) of sub-section (1) shall also apply to incoming calls originating in third countries.

(4) Where presentation of calling or connected line identification is offered, providers of publicly available number-based interpersonal communications services shall provide information to the public regarding the options set out in points (a), (b), (c) and (d) of sub-section (1).

Exceptions to presentation and restriction of calling and connected line identification

(5) Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

(6) The Commission shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls.

Incoming call blocking

(7) Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge:

(a) to block incoming calls from specific numbers or from anonymous sources;

(b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.

Publicly available directories

(8) The providers of publicly available directories shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, consequently, shall obtain consent from

these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.

(9) The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.

(10) The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.

(11) The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

Unsolicited communications

(12) Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent.

(13) Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.

(14) Without prejudice to sub-sections 12 and 13, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

(a) present the identity of a line on which they can be contacted; or

(b) present a specific code/or prefix identifying the fact that the call is a marketing call.

(15) Notwithstanding sub-section 12, the Commission may provide by Regulation that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.

(16) The Commission shall ensure, in the framework of this Act and other applicable laws, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under sub-section 12are sufficiently protected.

(17) Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.

(18) The Commission is empowered to adopt implementing measures in specifying the code/or prefix to identify marketing calls.

Information about detected security risks

(19) In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of

an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.

PART XV - ESTABLISHMENT, OBJECTIVES, POWERS AND FUNCTIONS OF THE DATA PROTECTION COMMISSION

57. Establishment of the Data Protection Commission

(1) There is established a commission to be known as the Data Protection Commission (in this Act referred to as the Commission) which -

(a) shall be a body corporate with perpetual succession and a common seal; and
(b) may sue and be sued in its corporate name.

(2) The Commission shall be structured into departments as the Board may from time to time deem appropriate for the effective discharge of its functions.

(3) The Commission shall have its head office in a location which is by law designated as the Capital of the Federal Republic of Nigeria and may establish zonal offices in any part of Nigeria in accordance with the decision of the Board of the Commission.

58. Functions of the Commission

1. The Commission shall

(a) Protect the privacy of the individual and personal data by regulating the processing of personal information, and

(b) provide the process to obtain, hold, use or disclose personal information.

(c) ensure that controllers and processors adhere to the data protection principles in order to protect the fundamental rights and freedoms, particularly privacy of natural persons in relation to the processing of their personal data.

(d) assist the facilitation of the free flow of personal data through consultation and cooperation with other relevant agencies in compliance with established data security best practices.

(e) as supervisory authority, exercise investigative, corrective, regulatory, authorization and advisory powers. To this end, the Commission shall -

(i) Give advice and approve high risk processing operations and systems of controllers and processors in order to ensure compliance of their processing operations with the provisions of this Act;

(ii) issue warnings to a controller or processor in the event that intended processing operations are likely to infringe the provisions of this Act;

(iii) receive and process claims from data subjects whose rights have been infringed;

(iv) order the rectification, completion or deletion of personal data and impose a temporary or definitive limitation, including a ban, on processing operations;

(v) receive information concerning data breaches from controllers and processors, investigate such breaches and communicate those breaches to the data subjects and the public, where necessary;

(vi) impose administrative fines or sanctions where controllers infringed any provision of this Act and where the infringement is of an intentional or negligent character; and

(vii) have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Act.

(f) The Commission shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions.

(g) The Commission shall promote public awareness of the rights of data subjects and the exercise of their rights. It shall inform controllers and processors of their duties and responsibilities and shall share best practices in order to ensure the free flow of personal data.

(h) The Commission shall be consulted on proposals for any legislative or administrative measures which relate to the processing of personal data.

(i) The Commission shall perform the functions relating to transfers of personal data provided for under this Act, or any other legislation, notably the approval of standardised safeguards.

(j) The Commission shall muster the resources necessary for the effective performance of its functions and the exercise of its powers.

(k) The Commission shall prepare and publish its reports, biannually, outlining its activities.

59. Powers of the Commission

(1). To carry out its functions, the Commission shall have power to -

(a) Implement and monitor compliance with the provisions of this Act;

(b) make the administrative arrangements it considers appropriate for the discharge of its duties;

(c) investigate any complaint under this Act and determine it in the manner the Commission considers fair.

(d) powers to impose fines and penalties to enforce compliance and redress.

(e) make such regulations as may be necessary or expedient for carrying out its functions and enforcing the provisions of this Act and do all such things as are necessary for or incidental to the carrying out of its functions and duties under this Act.

PART XVI - MANAGEMENT AND STAFF OF THE COMMISSION

60. Appointment of Data Protection Commissioner of the Commission

(1) There shall be for the Commission, a Data Protection Commissioner , who shall-

(a) be appointed by the President on the recommendation of the Honorable Attorney general of the Federation;

(b) not be qualified for appointment as a Data Protection Commissioner unless theypossessesprofessional skills and 15 years cognate experience in any of the following fields: law, Data Protection Policy, Cybersecurity Management, information communication technology, management science, or related fields.

(c) be the Chief Executive and accounting officer of the Commission and be responsible for:

i. The day to day administration of the Commission;
ii. the execution of the policies and decisions of the Commission and the Board ; and

iii. performing other functions as the Board may from time to time assign to him.

(d) hold office in the first instance for a term of 4 years and may be reappointed for another term of 4 years and no more.

61. Cessation or removal from office

(1) Notwithstanding the provisions of section 1 of this Act, the Data Protection Commissioner may be removed from office by a two third majority resolution of the Senate.

(a) for inability to discharge the functions of his office (whether arising from infirmity of mind or body or any other cause) or for misconduct;

(b) where it is established that it is not in the interest of the Commission or the public for him to continue in the office;

(c) where the Data Protection Commissioner resigns his appointment by a notice in writing under his hand addressed to the President.

62. Appointment of Secretary to the Board of the Commission.

(1) The Commission shall have a Secretary to the board, who shall also be the Director Legal Services, to be appointed by the Honourable Attorney General of the Federation from the Federal Ministry of Justice.

63. Staff of the Commission

(1) The Commission shall have powers to appoint such number of other staff as it deems necessary for the proper and effective performance of its functions as staff of the Commission.

(2) The employment of the Commission's staff, shall be subject to such terms and conditions as may from time to time be stipulated by the Board and contained in the respective staff's employment contracts

64. Terms and condition of service

(1) The terms and conditions of service and remuneration of employees of the Commissions hall be determined in line with the appropriate authorities.

65. Removal and discipline of staff.

(1) The removal and discipline of staff shall be in accordance with existing Public Service Rules and Regulations.

PART XVI - GOVERNING BOARD AND THE MEMBERSHIP OF THE COMMSSION

66. Establishment of the Governing Board

(1) There is established for the Commission, a governing board (in this Act referred to as the Board).

(2) The Board shall consist of the following members –

(a) A Chairperson
(b) one representative not below the Directorate cadre from the following:
  (i) Federal Ministry of Justice.
  (ii) Office of the National Security Adviser.
  (iii) National Identity Management Commission
  (iv) Nigerian Communication Commission
  (v) National Information Technology Development Agency.
  (vi) Central Bank of Nigeria
  (vii) Federal Inland Revenue Service.
  (viii) Nigerian Immigration Service
  (ix) Independent National Electoral Commission;
  (x) National Health Insurance Scheme;

(xi) National Population Commission;

(c) One representative elected by the Industry Forum

(d) One representative elected by the Nigerian Bar Association

(e) The Secretary to the Board of the Commission, and

(f) The Data Protection Commissioner and Chief Executive Officer of the Commission

3. The members of the Board shall be appointed by the President, upon the recommendation of the Attorney General of the Federation.

4. The member of the Board, other than the Data Protection Commissioner and the Secretary to the Board, shall be on part-time basis.

5. Notwithstanding any other provision of this Act, the Attorney General of the Federation shall ensure at all times that there is a duly constituted Board.

67. Tenure of Office

(1). The Chairman and other members of the Board, other than *ex officio* members, shall each hold Office-

(a) for a term of four years renewable once only;

(b) on such terms and conditions as may be specified in the letter of appointment.

68. Cessation of membership

(1) Notwithstanding the provisions of section of 64 this Act, a member of the Board shall cease to hold office as a member of the Board where -

(a) he resigns his appointment as a member of the Board by notice, under his hand;

(b) he becomes of unsound mind;

(c) he becomes bankrupt or makes a compromise with his creditors;

(d) he is convicted of a felony or of any offence involving dishonesty or corruption;

(e) he becomes incapable of carrying on the functions of his Office either arising from an infirmity of mind or body;

(f) in the case of a person possessing a professional qualification, he is disqualified by a competent authority; or

(g) in the case of a person who becomes a member by virtue of the Office he occupies, he ceases to hold such Office.

69. Meetings of the Board

(1) The Board shall meet at least once every three months for the dispatch of business at the times and in the places determined by the chairperson.

(2) The Chairperson shall at the request in writing of not less than one-third of the membership of the Board convene an extra-ordinary meeting of the Board at the place and time determined by the chairperson.

(3) The quorum at a meeting of the Board is seven members of the Board or a greater number determined by the Board in respect of an important matter.

(4) The Chairperson shall preside at meetings of the Board and in the absence of the Chairperson, a member of the Board elected by the members present from among their number shall preside.

(5) Matters before the Board shall be decided by a majority of the members present and voting and in the event of an equality of votes, the person presiding shall have a casting vote.

(6) The Board may co-opt a person to attend a Board meeting but that person shall not vote on a matter for decision at the meeting.

70. Disclosure of interest

(1) A member of the Board who has an interest in a matter for consideration -

(a) shall disclose the nature of the interest and the disclosure shall form part of the record of the consideration of the matter; and

(b) shall not participate in the deliberations of the Board in respect of that matter.

(2) A member ceases to be a member of the Board if that member has an interest on a matter before the Board and he -

(a) fails to disclose that interest; or

(b) participates in the deliberations of the Board in respect of the matter.

71. Emoluments of members of the Board.

1. The Chairman and members of the Board shall be paid such emoluments, allowances and incidental expenses as the National Salaries, Incomes and Wages Commission may, from time to time, approve.

72. Powers of the Board

The Board shall -

(a) ensure the proper and effective performance of the functions of the Commission.

(b)provide the general policy guidelines relating to the functions of the Commission;

(c) manage and superintend the policies of the Commission on matters relating to the protection of data under this Act or any enactment or law;

(d) review and approve the strategic plans of the Commission;

(e) employ and determine the terms and conditions of service including disciplinary measures of the employees of the Commission;

(f) stipulate remuneration, allowances, benefits and pensions of staff and employees in consultation with the National Salaries, Income and Wages Commission; and

(g) The Board may establish committees consisting of members of the Board or non-members or both to perform a function. A committee of the Board may be chaired by a member of the Board.

(h) do such other things which in its opinion are necessary to ensure the efficient performance of the functions of the Commission under this Act.

73. Ministerial directives

The Minister may give general directives to the Board on matters of policy.

PART XVII- FINANCIAL PROVISIONS

74. Funds of the Commission

1. The Commission shall establish and maintain a fund from which all expenditures incurred by the Commission shall be defrayed.
2. The Fund shall comprise funds derived from but not limited to the following sources -
    a. such monies as may be appropriated to the Commission from time to time by the National Assembly ;
    b. gifts, loans, grants, aids, etc. ; and

c. all other assets that may from time to time accrue to the Commission.

d. The provisions of any enactment relating to the taxation of companies or trust funds shall not apply to the Commission.

75. Borrowing powers, gifts, etc.

1. The Commission may, with the consent of, or in accordance with the general authority given by the Minister of Finance, borrow such sums of money as the Commission may require in the exercise of its functions under this Act or its subsidiary legislation.
2. The Commission may accept gifts or grants of money or aids or other property from national, bilateral and multi-lateral organisations and upon such terms and conditions, if any, as may be agreed upon between the donor and the Commission provided that such gifts are not inconsistent with the objectives and functions of the Commission under this Act.

76. Budget and expenditure.

1. The Commission shall in each financial year prepare and present to the National Assembly through the President for approval, a statement of estimated income and expenditure for the following financial year.
2. Notwithstanding the provisions of subsection (1), the Commission may also, in any financial year, submit supplementary or adjusted statements of estimated income and expenditure to the National Assembly through the President for approval.
3. Subject to subsections (1) and (2) of this section, the Commission shall apply the proceeds of the Commission's Fund -
    a. to meet the administrative and operating costs of the Commission ;
    b. for the payment of salaries, wages, fees and other allowances, retiring benefits such as pensions and gratuities and, any other remunerations payable to the Commissioners and staff of the Commission ;
    c. for the purchase or acquisition of property or other equipment and other capital expenditure and for maintenance of any property

acquired or vested in the Commission ;

d. for purposes of investment ; and

e. for or in connection with all or any of the functions of the Commission under this Act or its subsidiary legislation.

77. Financial year and audit of Commission's accounts.

1. The financial year of the Commission shall start on 1st January of each year and end on 31st December of the same year.
2. The Commission shall keep proper records of its accounts in respect of each year and shall cause its accounts to be audited within 6 months from the end of each financial year by auditors whose appointment shall be approved by the Board and shall be subject to reappointment on annual basis provided that such auditors are on the list of auditors approved from time to time by the Auditor- General for the Federation.
3.

78. Annual reports .

1. The Commission shall prepare and submit to the President, not later than 3 months after the end of its financial year, a report on the activities of the Commission for the preceding financial year and shall include therein the Commission's audited accounts for the year under review together with the auditor's report thereon.

PART XI – MISCELLANEOUS

79. Procedure in Respect of Suits against the Commission

(1) Notwithstanding anything contained in any other enactment or law, no suit against the Commission, a member of the Board or any employee of the Commission, for any act done in pursuance or execution of this Act, any law, or any public duty of the Commission, or in respect of an alleged neglect or default in the execution of this Act, such law, duty or authority, shall lie or be instituted

in any court, unless it is commenced within three months next after the ceasing thereof.

(2) No suit shall be commenced against the Commission before the expiration of a period of one month after written notice of intention to commence the suit shall have been served upon the Commission by the intending plaintiff or his agent; and the notice shall clearly and explicitly state the -

(a) course of action,

(b) particulars of the claim;

(c) name and place of abode of the intending plaintiff; and

(d) relief he seeks.

(3) Subject to the provisions of this Act, the provisions of the Public Officers Protection Act shall apply in relation to any suit instituted against an official or employee of the Commission.

[CAP. P41, LFN]

80. Service of Documents

The notice under section 42 of this Act or any other notice, summons, process, or other document required or authorized to be served upon the Commission under the provisions of this Act or any other law or enactment, may be served by delivering same to the Data Protection Commissioner of the Commission, or by sending it by registered post addressed to the Data Protection Commissioner at the head office of the Commission.

81. Restriction on Execution against Property of the Commission

Subject to the consent of the Attorney-General of the Federation, no execution or attachment or process in the nature thereof shall be issued against the Commission in respect of an action or suit against the Commission but the sums of money which by judgment of the court is awarded against the Commission shall be paid from the funds of the Commission.

82. Indemnity of Board Members and Employees of the Commission

A board member, agent, auditor or employee for the time being of the Commission shall be indemnified out of the assets of the Commission against any liability incurred by him in defending any proceeding whether civil or criminal, where any such proceeding is brought against him in his capacity as such board member, agent, auditor or employee.

83. International co-operation

54. The Commission shall perform the data protection functions that are necessary to give effect to any international obligations of the Federal Republic of Nigeria, subject to the powers vested in the Attorney General of the Federation.

84. Application to the State

(1) This Act binds the Republic.

(2) For the purposes of this Act, each government department shall be treated as a data controller.

(3) Each department shall designate an officer to act as a data supervisor.

(4) Where the purposes and the manner in which the processing of personal data are determined by a person acting on behalf of the Executive, Legislature

and the Judiciary, the data controller in respect of that data for the purposes of this Act is

(a) in relation to the Executive, the Chief Director,

(b) in relation to Parliament, the Clerk to House of Assembly, and

(c) in relation to the Judiciary, the Judicial Secretary. (

5) A different person may be appointed under subsection (4) for a different purpose.

85. Regulatory Review

The Commission may when it deems necessary, review Guidelines or Regulations made under this Act that are in effect at the time of the review, and may in the process modify, vary or repeal any such Guidelines or Regulations -

(a) which may no longer be relevant in the existing context of the Nigerian Universal System;

(b) which may no longer be necessary in the national interest;

(c) which may no longer be necessary to ensure the objects of this Act or its subsidiary legislation; or

(d) for any other reason the Commission may consider necessary for giving full effect to the provisions of this Act and for its due administration.

86. Jurisdiction

The Federal High Court shall have exclusive jurisdiction over all matters, suits and cases howsoever arising out of or pursuant to or consequent upon this Act or its subsidiary legislation.

87. Definitions

In this Act -

"*Commission*" means the Data Protection Commission, which is established pursuant to section 5 of this Act;

"automated individual decision making and profiling" means a decision based solely on automated processing, including profiling and shall only be processed pursuant to this Act;

"*consent of the data subject*" means any freely given, specific (relating to such separate purpose) informed and unambiguous indication of the data subject's wishes by which he, by statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him;

"*Data Controller*" means the natural or legal person, public authority, service, Commission or any other body which, alone or jointly with others, has decision-making power concerning determining the purposes and means of data processing;

"*data processing*" means any operation or set of operations performed on personal data, such as –

(a) collection, recording, organisation, structuring, storage or preservation;

(b) adaption or alteration;

(c) access, retrieval or consultation;

(d) transmission, disclosure, sharing or making available;

(e) restriction, erasure, or destruction of, or the carrying out of logical or arithmetical operations.

Where automated processing is not used, "***data processing***" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

"***data subject***"means an identified or identifiable living natural person to whom personal data relates;

"***identifiable individual***" means a natural person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, online identifier, and includes 'singling-out' a natural person;

"***personal data***"means any information relating to an identified or identifiable natural person (data subject);

"***processor***" means a natural or legal person, public authority, Commission or body which processes personal data on behalf of the Controller;

"***recipient***" means a natural person or legal person or public authority, service, Commission or any other body to whom data is disclosed or made available;

"**sensitive data**" means –

(a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership;
(b) genetic data;
(c) biometric data for the purpose of uniquely identifying a natural person;
(d) data concerning health;
(e) data concerning a natural person's sex life or sexual orientation;
(f) personal data relating to criminal offences, including criminal records; or
(g) such other personal data that may from time to time be designated as sensitive data by Guidelines made by the Commission;

The processing of any sensitive data shall be prohibited or allowed subject to appropriate safeguards pursuant to this Act;

88. Transitional provisions

(1) A data controller incorporated or established after the commencement of this Act shall be required to register as a data controller within twenty days of the commencement of business.

(2) A data controller in existence at the commencement of this Act shall be required to register as a data controller within three months after the commencement of this Act.

89. Short Title

This Act may be cited as the Data Protection Act, 2018.

SCHEDULE 1

PRIVACY PRINCIPLES FOR THE PROTECTION OF PERSONAL INFORMATION

SCHEDULE 2

Registration _____

EXPLANATORY MEMORANDUM

This Bill seeks to provide for the protection of the privacy of individuals, to regulate the processing of personal data and disclosure of information,and to establish the Data Protection Commission for the protection of personal data and privacy, and for related matters