

DATA PROTECTION Bill, 2020

A Bill

For

An Act to establish the Data Protection Commission charged with the responsibility for the protection of personal data, rights of data subjects, regulation of the processing of personal data and for related matters.

[]

Commencement

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

PART I — OBJECTIVES, APPLICATION AND SCOPE

1. The primary objective of this Act is to establish and provide an efficient regulatory framework for the protection of personal data, regulate the processing of information relating to data subjects, and to safeguard their fundamental rights and freedoms as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999 ('the Constitution') and particularly to — Objectives of the Act.
- (a) promote a code of practice that ensures the privacy and protection of data subject's data without unduly undermining the legitimate interests of commercial organisations and government security agencies for such personal data;
 - (b) minimise the harmful effect of personal data misuse or abuse on data subjects and other victims;
 - (c) establish an impartial, independent and effective regulatory authority that will coordinate data protection and privacy issues and superintend over data controllers and data processors within the private and public sectors;
 - (d) ensure that personal data is processed in a transparent, fair, and lawful manner, in accordance with the data protection principles stipulated in this Act or any other extant legislation.
2. (1) This Act applies to — Application and scope.
- (a) the collection, storage, processing and use of personal data relating to persons residing in Nigeria and persons of Nigerian nationality, by automated and non-automated means, irrespective residence and in particular by —
 - (i) 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, and

(ii) conferring on individuals a number of rights as set in Part V of this Act.

(b) personal data processed by entities in the private and public sectors in Nigeria; and

(c) a data controller and data processor in respect of personal data where —

(i) the data controller and data processor are both established in Nigeria, and the personal data of data subjects in Nigeria are processed within Nigeria,

(ii) the data subject resides within or outside Nigeria,

(iii) the data controller is not established in Nigeria but uses equipment or a data processor in Nigeria to process personal data of data subjects who reside within or outside Nigeria, or

(iv) processing is carried out in respect of information relating to data subjects who reside within or outside Nigeria and personal data which originates partly or wholly from Nigeria.

(2) This Act does not apply to processing of personal data carried out by a data subject in the course of a purely personal or household activity.

(3) For the purposes of this Act, the following shall be required to comply with the provisions of this Act:

(a) a data subject who is a citizen of Nigeria;

(b) a data subject who is ordinarily resident in Nigeria;

(c) a body incorporated under the laws of Nigeria;

(d) an unincorporated joint venture or association operating in part or in whole in Nigeria; 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 Nigeria.

(f) Foreign entities targeting persons resident in Nigeria

(4) The categories of data to which this Act applies include —

(a) personal and biometric data revealing a data subject's identity, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership;

(b) personal banking and accounting records;

- (c) personal data revealing a data subject's flight reservation or itinerary;
- (d) student's academic transcripts records;
- (e) personal medical and health records;
- (f) telephone calls, call data records, messages, websites, and other information stored on any electronic device
- (g) personal subscription data which reveals data subject behavior; and
- (l) such other categories of data usually processed by service providers and commercial entities as may be determined by the guidelines of the Commission to be protected under this Act.

(5) On an annual basis, every Data Controller or processor shall, not later than the 30th of March of the following year, submit a report of its data protection audit to the Commission. The Commission shall compile and publish an annual report containing the list of organisations who have submitted the audit report.

PART II — BASIC PRINCIPLES AND LEGAL BASIS FOR PROCESSING OF PERSONAL DATA

3. (1) Personal data shall be —

- (a) processed for specific, explicit and legitimate purposes;
- (b) processed in a lawful, fair and transparent manner.
- (c) further processed for purposes compatible with those for which the data was initially collected.
- (d) processed for archiving,, scientific, historical research and statistical purposes in accordance with any relevant law in Nigeria
- (e) adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed;
- (f) accurate and regularly kept up to date;
- (g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and access against loss, destruction or damage and the data controller and data processor shall use appropriate technical and organisational measures to ensure the integrity, confidentiality and availability of the personal data; and
- (h) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, and data shall be deleted once the purpose for which it was processed has been achieved or kept in a form that prevents any direct or indirect identification of the data subject.

Basic principles relating to processing of personal data.

4. (1) The processing of personal data shall be carried out on the principles and legal basis stipulated in this Act. Lawfulness of personal data processing.
- (2) From the commencement of this Act, legal basis for processing of personal data includes —
- (a) the performance of a contract to which the data subject is party to, or in order to take steps at the request of the data subject, prior to entering into a contract;
 - (b) compliance with a legal obligation as provided by law and to which the data controller is subject;
 - (c) the protection of the vital interests of the data subject or of another natural person;
 - (d) the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
 - (e) the purposes of prevailing legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedom.
5. (1) Where processing of personal data is based on consent, the data controller shall show that the data subject has consented to the processing of his personal data. Consent of data subjects.
- (2) The consent of the data subject shall represent the free expression of an intentional choice given by a statement (either in writing or orally) or by a clear affirmative action.
- (3) Silence or inactivity does not constitute consent by the data subject.
- (4) Where the processing of personal data is based on the consent of the data subject, the data subject shall have the right to withdraw his consent at any time.
- (5) The withdrawal of consent under subsection (4) does not affect the lawfulness of the data processing that occurred before the withdrawal of the consent —by the data subject.
6. (1) Every data subject has the right to be informed about the processing of his personal data Transparency of personal data processing.
- (2) A data controller shall act with fairness and transparency when processing the personal data of data subjects.
- (3) A data controller shall inform the data subject of —
- (a) the data controller's official identity, residence or place of establishment;
 - (b) the contact details of the data controller, data protection officer and, where applicable, the data 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 party or foreign nation 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, including profiling, significance and envisaged consequence of such processing for the data subject, including the right to object and 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 V of this Act;
- (k) where processing is based on consent, the data subject shall be informed of the rights to withdraw his consent at any time.

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

(5) Where the personal data is not collected directly from the data subject, the data controller shall provide the information in subsection (3) within a reasonable period but not later than one month or on first communication with the data subject, except where the processing is expressly prescribed by the provisions of this Act or any other legislation.

PART III — ESTABLISHMENT, COMPOSITION, POWERS AND FUNCTIONS OF THE DATA PROTECTION COMMISSION

7. (1) There is established the Data Protection Commission (in this Act referred to as “the Commission”).

Establishment of the Data Protection Commission.

(2) The Commission –

- (a) is a body corporate with perpetual succession and a common seal; and
- (b) may sue and be sued in its corporate name; and
- (c) may hold, acquire and dispose of any property, movable or immovable.

(3) The Commission may be structured into departments as it may deem appropriate for the effective performance of its functions under this Act.

8. (1) There is established for the Commission a Governing Board (“The Board”) which shall consist of — Composition of the Governing Board

- (a) a full-time Data Protection Commissioner;
- (b) one representative who shall be a Director or its equivalent from:
 - (i) Federal Ministry of Justice,
 - (ii) Office of the National Security Adviser
 - (iii) Independent National Electoral Commission
 - (iv) National Population Commission
 - (v) Nigeria Police Force
 - (vi) Central Bank of Nigeria
 - (vii) Nigeria Immigration Service
 - (viii) Federal Road Safety Commission
 - (ix) National Identity Management Commission,
 - (x) Nigerian Communications Commission,
 - (xi) National Information Technology Development Agency,
- (c) one representative nominated by private sector data controllers;
- (d) one representative nominated by independent data protection professional service providers
- (e) one representative nominated by civil society organizations involved in data and privacy protection matters; and
- (f) the Secretary to the Commission.

(2) Members of the Board appointed under this section shall be paid such remunerations and allowances as the President may, from time to time direct. Remuneration and allowances

(3) The tenure of the members of the Board shall be for an initial period of 5 years and may be renewed for an additional period of 5 years, upon the approval of the President. Tenure Of Board Members

(4) The supplementary provisions contained in the Schedule to this Act shall have effect with respect to the tenure of members of the Board and the proceedings of the Board and other matters mentioned therein. Schedule.

9. The Commission shall — Functions of the Commission.

- (a) protect the personal data and privacy of data subjects by regulating the processing of personal information;
- (b) provide the process to obtain, store, process, use or disclose personal information;
- (c) ensure that data controllers and data processors adhere to the data protection principles as provided for by this Act 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) act as the supervisory authority, and exercise regulatory, powers to —
 - (i) advise and approve risk management processes and systems for data controllers and data processors in order to ensure compliance with the provisions of this Act,
 - (ii) issue directives in the event that their operations are likely to infringe the provisions of this Act,
 - (iii) receive and process complaints 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) impose administrative fines or sanctions where data controllers and data processors infringe any provision of this Act.
- (f) act with complete independence and impartiality in performing its functions and exercising its powers
- (g) promote public awareness of the rights of data subjects and the exercise of their rights and shall inform data controllers and data processors of their duties and responsibilities and shall share best practices in order to ensure the free flow of personal data;
- (h) be consulted on proposals for any legislative or administrative measures which relate to the processing of personal data;
- (i) provide relevant regulations, guidelines, and policies relating to transfers of personal data provided for under this Act, or any other legislation.
- (j) make regulations for the licensing and certification of data protection compliance officers and organizations.
- (k) muster the resources necessary for the effective performance of its functions and the exercise of its powers;
- (l) prepare and publish its reports annually, outlining its activities which shall be submitted to the President.

10. The Commission shall have powers to —

Powers of the Commission.

- (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) impose fines and penalties to enforce compliance and

seek redress.

- (e) make such regulations as may be necessary for carrying out its functions and enforcing the provisions of this Act and such other things that are incidental thereto under this Act;
- (f) apply to the appropriate court as an option for the issuance of such warrant relevant for the performance of its functions under this Act.
- (g) perform its functions with the aid of law enforcement agencies.

PART IV — THE DATA PROTECTION COMMISSIONER AND OTHER STAFF OF THE COMMISSION

11. There shall be for the Commission, a Data Protection Commissioner, who shall be — Appointment of Data Protection Commissioner.

- (a) appointed by the President subject to the confirmation of the Senate
- (b) the Chief Executive and Accounting Officer of the Commission and be responsible for —
 - (i) the administration of the Commission,
 - (ii) the execution of policies and decisions of the Commission, and
 - (iii) performance of such other functions as may be necessary or incidental for executing the mandate of the Commission;
- (c) hold office in the first instance for 5 (five) years and may be reappointed for another term of 5 (five) years and no more;
- (d) be non-partisan and a person of unquestionable integrity; and
- (e) not be qualified for appointment as a Data Protection Commissioner unless he has sound knowledge of and possesses professional skills and at least 15 (fifteen) years cognate experience in the fields of -
 - (i) law,
 - (ii) data protection policy,
 - (iii) cybersecurity management,
 - (iv) information communication technology, or
 - (v) management science.

12. Notwithstanding the provisions of section 11 of this Act the Data Protection Commissioner may cease to hold office in the following circumstances — Cessation or removal from office.

- (a) he resigns his appointment by a notice in writing to the President
- (b) He is removed from office by the President for-

- (i) inability to discharge the functions of the office whether arising from infirmity of mind or body,
- (ii) any act of gross misconduct; and
- (iii) where it is established that it is not in the interest of the Commission or the public for the Data Commissioner to continue in the office.

13. The Commission shall have a Secretary, who shall also be the Head of Legal Services of the Commission, appointed by the Board. Secretary to the Commission.
14. (1) The Commission may employ such number of staff as it deems necessary for the proper and effective performance of its functions under this Act. Staff of the Commission.
- (2) The employment of staff of the Commission is subject to such terms and conditions as may be stipulated by the Commission and contained in staff' employment contract.
15. The conditions of service and remuneration of employees of the Commission shall be as approved by the President. Conditions of service.
16. The appointment, promotion and discipline of staff shall be in accordance with the conditions of service of the Commission. Appointment, Promotion and discipline of staff.

PART V — RIGHTS OF THE DATA SUBJECTS

17. (1) A data subject shall have the rights set out in this Part. Rights of data subjects.
- (2) A data subject's right may only be limited in accordance with the provisions of section 38.
- (3) right to be notified of the data breach affecting him or her within 48 hours after notification to the Commission
- (4) The notification referred to in subsection (3) shall —
- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

18. (1) A data subject shall have the right to -

Right of access.

- (a) obtain, on request and at reasonable intervals and without excessive delay or expense, confirmation as to whether personal data relating to the data subject has been processed and if so, the communication in an intelligible form of the data, together with all available information on the origin of the data, on the preservation period as well as any other information that the data controller is required to provide, in order to ensure the transparency of processing in accordance with section 6;
- (b) obtain, on request, the reasons for the processing of data where such processing applies to the data subject.

(2) The data controller shall, at no cost, provide a copy of the personal data processed, and in exceptional circumstances may charge a reasonable fee based on administrative costs. provided that.

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

(4) The period stated in subsection (3), may be extended by a period not exceeding an additional 2(two) months where necessary, taking into account the complexity of the request.

(5) A data subject shall have the right, on request, to obtain knowledge of the reasoning behind data processing where the result of such processing is applicable to him.

19. (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.

Right in respect of automated decision making.

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

(3) The data 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 data controller.

20. (1) The data subject shall have the right to the rectification, blockage, or erasure of inaccurate, false or unlawfully processed personal data without delay and free of charge from the data controller.

Right to rectification, erasure, and restitution of processing.

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

rectification or erasure.

- (3) The data controller shall temporarily block processing where:
- (a) the accuracy of the data is contested by the data subject;
 - (b) the data subject opposes the erasure of personal data; or
 - (c) the data subject has objected to the processing of his or her personal data,

until the grounds for restriction have been resolved

- (4) where the temporary blocking of personal data is lifted, the data subject shall be informed by the data controller.

21. Where the provisions of this Act is violated, the data subject shall have the right to a judicial remedy under this Act. Right to judicial remedy.
22. (1) A data subject shall have the right to object at any time, on grounds relating to the processing of personal data, including profiling. Right to object, including profiling and direct marketing.
- (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 at no cost.
- (3) A data controller shall not provide, use, obtain or procure information related to a data subject for the purposes of direct marketing without the prior written consent of the data subject.
- (4) Where a data subject makes a valid objection under this section, he is entitled to have the unconditional erasure, removal or suppression of the personal data covered by the objection.
- (5) Where the Commission receives a complaint by a person who has been given notice under this section that the data controller has failed to comply with such notice, the Commission may order the data controller to comply accordingly
23. (1) A data controller shall no longer process the personal data unless the data controller demonstrates legitimate grounds for the processing and a legitimate interest which overrides the interest or rights and fundamental freedoms of the data subject. Right to have data processing suspended.
24. (1) Where the processing of data is not authorized by law or other valid legal ground, the data subject shall request in writing at any time to the data controller and data processor, to cease or not begin the processing of personal data which causes or is likely to cause unwarranted damage or distress. Right to prevent processing of personal data.
- (2) A data controller and data processor shall within one month days after receipt of a notice inform the data subject in writing —
- (a) that the data controller or data processor 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 in accordance with this Act any other extant law is satisfied

that the complaint is justified, the Commission shall order the data controller or data processor to comply with the notice submitted pursuant to subsection (1) of this section.

25. (1) A data subject shall have the right to receive personal data concerning him which was provided to a data controller, in a structured, commonly used and machine readable format and have the right to transmit such data to another data controller without hindrance from the data controller from where the personal data is withdrawn provided the processing is based on consent or on a contract. Right to data portability.
- (2) In exercising his right to data portability under subsection (1) of this section, the data subject shall have the right to have his personal data transmitted directly from one data controller to another where technically feasible.
- (3) The exercise of the right referred to in subsection (1) of this section shall not apply to data processing necessary for the performance of the task carried out in the public interest or in the exercise of official authority vested in the data controller, and the right shall not adversely affect the rights and freedoms of others.

PART VI — PROCESSING OF SENSITIVE DATA

26. (1) Unless otherwise provided by this Act or any other extant legislation, a person shall not process personal data which relates to — Processing of sensitive data.
- (a) a child who is under parental or guardian control in accordance with existing law, or
 - (b) the religious or philosophical beliefs, ethnic origin, race, political opinions, health, sexual life or behavior of a data subject.
- (2) A data processor or data controller may process sensitive personal data in accordance with this Act where —
- (a) processing is necessary as provided under this Act; or
 - (b) the data subject consents or in the case of a child under parental control, the prior consent of the parent or guardian is obtained before 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) Personal data shall not be processed unless such 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 processor or data controller cannot reasonably be expected to obtain the consent of the data subject, or

(c) where it is impossible or impracticable to obtain the consent of the data subject, the data processor or data controller shall depose to an affidavit to the effect that it is impracticable to obtain the requisite consent necessary to carry out the processing of the sensitive data in accordance with the provisions of this section.

(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 data subjects 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 personal data can be performed where it is required —

- (a) for any purpose(s) 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 such processing should be —
 - (i) undertaken by a health professional, and
 - (ii) pursuant to a duty of confidentiality between the patient and health professional.

(7) 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.

(8) The Commission may, by notice, guidelines or regulations, prescribe further conditions to be taken into consideration by the data processor and data controller for the maintenance of appropriate safeguards for the rights and freedoms of a data subject related to processing of sensitive personal data.

27. (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 —

Prohibition on processing of sensitive data which relates to religious beliefs.

- (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) A data subject who believes that their personal data is being processed under subsection (1) of this section may at any time by notice in writing to a data controller require a data processor or data controller to provide particulars of data processed under this exemption.

28. (1) A data subject shall not be subjected to a decision significantly affecting him based solely on an automated processing of data, in violation of his rights under this Act.

Rights in relation to automated decision making.

(2) Where a decision which significantly affects a data subject is based solely on automated processing —

- (a) the data controller shall, as soon as reasonably practicable notify the data subject that the decision was taken on that basis, and
- (b) the data subject is entitled, by notice in writing to require the data controller to reconsider the decision within 21 days after receipt of the notification from the data controller.

(3) The data controller shall within 30 days after receipt of the notice, inform the data subject 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 authorised or required by or under an enactment; or
- (e) in other circumstances prescribed by the Commission.

(5) Where a data subject under this section is not satisfied with the response of the data controller, the data subject may file a complaint against the data controller to the Commission.

(6) Where the Commission is satisfied on a complaint by a data subject that a data

controller taking a decision has failed to comply, the Commission shall order the data controller to comply.

(7) An order for compliance under subsection (6) of this section does not affect the rights of a person other than the data subject or the data controller.

29. (1) Where a data subject suffers damage through the contravention by a data controller or data processor of the requirements of this Act, he is entitled to compensation from the data controller or data processor for the damages as may be determined by the Court. Compensation for failure to comply.

(2) In proceedings against a data controller or data processor under this section, it is a defense to prove that the data controller or data processor took reasonable care in all the circumstances to comply with the requirements of this Act.

PART VII —DUTIES OF DATA CONTROLLERS AND DATA PROCESSORS

30. (1) The data controller in the discharge of his duties shall —

Duties of data controllers.

- (a) take all necessary measures, including technical and managerial measures to comply with, and be able to demonstrate, in particular to the Commission, that the processing of personal data is performed in accordance with this Act;
- (b) ensure the processing of personal data is proportionate, 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, volume, scope and purpose of processing the data;
- (d) subject to Regulations made by the Commission, appoint a data protection officer responsible for compliance with the obligations under this Act,
- (e) 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
- (f) design the data processing in such a manner, and integrate appropriate technical and organisational measures, as to prevent or minimize the risk of interference with those rights and fundamental freedoms.
- (g) perform such other duties as may be required by this Act.

(2) For the purpose of this Act, a data controller shall include a Ministry, Department and Agency and other public institutions of government.

(3) 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 in relation to —

- (a) Executive, the relevant Permanent Secretary or Chief Executive Officer;
- (b) Legislature, the Clerk to the National Assembly, Clerk to the State House of Assembly and Local Government Legislative Councils; and
- (c) Judiciary, the Secretary, National Judicial Council or relevant Chief Registrar. and
- (d) other Public institutions, the Chief Executive Officer

31. (1) The data controller shall be liable for the processing of personal data carried out on its behalf by the data processor. Vicarious liability

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

(3) The processing of personal data by the data processor on behalf of the data controller is subject to a legally binding contract between the data controller and the data processor that sets-out –

- (a) the nature of the processing agreement,
- (b) the personal data to be processed
- (c) the purpose of processing
- (d) the obligations and restrictions to be imposed on the data processor, including sub-processing or transfers of personal data to other countries. and
- (e) penalties for breach (s)

32. (1) A data processor shall -

Duties of data processors.

- (a) process personal data on behalf of a data controller only on the written instructions of the data controller;
- (b) not engage another data processor without the prior written authorisation of the data controller;
- (c) inform the data controller of changes concerning the addition or replacement of data processors;
- (d) inform the data controller of any legal requirement that may create risks to the rights and fundamental freedoms of data subjects, unless the law prohibits such notice;
- (e) take appropriate technical and managerial security measures pursuant to section 34 of this Act
- (f) assist the data controller by putting in place the appropriate technical and managerial measures for the

fulfillment of the data controller's obligations to respond to the rights under this Act;

- (g) assist the data controller in ensuring compliance with its security obligations under section 34, including security breach notification;
- (h) at the request of the data controller, delete or return all personal data to the data controller at the end of the provision of services, and delete any copies of personal data unless prohibited by law; and
- (i) make available to the data controller all information necessary to assist the data controller demonstrate compliance with its obligations under this Act and facilitate audits conducted by the data controller or a third-party auditor determined by the data controller;

- (2) Where a data processor engages a third party to meet its obligations to the data controller, the data processor shall impose the same data protection obligations set in its contract with the data controller and the data processor is liable to the data controller for ensuring the performance of the third party's obligations.
- (3) The data processor and any other party acting under the authority of the data processor or data controller, who has access to the personal data shall not process such data except on instructions from the data controller, unless otherwise required by law.
- (4) The data processor, and where applicable a third party engaged by the data processor shall maintain a record of processing activities pursuant to this Act.

PART VIII: DATA LOCATION AND SECURITY

- 33. Every data controller and data processor under this Act, shall process personal data on devices under its control whether physically located within Nigeria or not. Data location
- 34. (1) The data controller, and where applicable, the data processor, shall take optimal technical and managerial measures to protect personal data against risks such as but not limited to accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. Security of processing.
 - (2) When considering optimal measures, the data controller shall take into account —
 - (a) state-of-the-art data-security techniques and technology in the field of data processing, commensurate with the seriousness and probability of the potential risk; and
 - (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.
 - (3) Data controllers and data processors shall establish a process to regularly test, assess and evaluate the effectiveness of technical and organisational measures for

ensuring the security of the processing.

35. (1) The privacy of personal data is exempt from the provisions of this Act for the purposes of —
- Exceptions on the grounds of public interest.
- (a) public order;
 - (b) public safety;
 - (c) public morality;
 - (d) national security;
 - (e) public interest;
 - (f) the prevention or detection of crime;
 - (g) the apprehension or prosecution of an offender; or
 - (d) the assessment or collection of a tax or duty or of an imposition of a similar nature.
 - (e) publication of a literary or artistic material
- (2) Personal data on health, education and social work shall not be disclosed except as provided by this Act.
- (3) The provisions of this Act do not apply to the processing of personal data for the protection of members of the public —
- (a) against loss or malpractice as it relates to —
 - (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.
- (4) For the purposes of subsection (1), 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 Commission for purposes of this subsection.
- (5) Further processing of personal data for research purposes shall be compatible with the purposes for which the data was obtained and for this reason —

- (a) personal data which is processed for research purposes in compliance with the relevant conditions shall be used for such research purposes only, and may be kept indefinitely;
 - (b) personal data which is processed only for research purposes is exempt from the provisions of this Act if —
 - (i) the data is processed in compliance with the relevant provisions, and
 - (ii) the results of the research or statistics are not made available in a form which identifies the data subject or any of them.
 - (c) personal data is not to be treated as processed otherwise than for research purposes merely because the data is disclosed;
 - (d) to the data subject or a person acting on behalf of the data subject;
 - (e) personal data shall only be processed with the consent of the data subject or a person acting on behalf of the data subject; or
 - (f) in circumstances in which the person making the disclosure has reasonable grounds to believe that the disclosure falls within this section.
- (6) The processing of Personal data shall be exempt from the provisions on non-disclosure where the disclosure is required by law or by the order of a court.
- (7) The Processing of Personal data by a data subject of his personal, family or household members for household purposes is exempted from the provision of this Act. data protection principles.
- (8) 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 for the data subject.
- (9) 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 Federal Republic of Nigeria.
- (10) The Commission may make regulations and guidelines to prescribe exemptions for the processing of personal data to assess a person's suitability for employment by government or appointment to a public office

PART IX — ADMINISTRATION AND ENFORCEMENT

36. (1) Where the Commission is satisfied that a data controller and data processor have contravened or is in contravention of any of the data protection principles stipulated under this Act, the Commission shall serve the data controller with an enforcement notice to request that data controller to —
- (a) take or refrain from taking the steps specified in the notice; and
 - (b) refrain from processing any personal data of a description specified in the notice.
- (2) an enforcement notice shall be served by the Commission where a contravention exists or its reasonably believes that there is likelihood of a contravention.
- (3) In deciding whether to serve an enforcement notice, the Commission shall consider whether the contravention has caused or is likely to cause injury or damage to any person.
- (4) 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 delete) or destroy other data held by the data controller which contains an expression of opinion which appears to the Commission to be based on inaccurate data.
- (5) 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 under this Act,
- 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.
- (6) 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.
- (7) The Commission may make regulations and guidelines for the issuance and compliance of notices
37. 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. Cancellation of enforcement notice.
38. (1) A person who is affected by the processing of any personal data may on its 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. Request for assessment.

- (2) On receiving a request, the Commission may make an assessment in the manner that the Commission considers appropriate.
- (3) In determining whether an assessment is appropriate the Commission may consider:
 - (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 unless the request is accompanied with the prescribed fee.
- (5) Where the Commission finds that the processing by a data controller is contrary to the provisions of this Act, the Commission shall issue a notice to the data controller specifying the contravention and give the data controller notice to cease processing personal data.

39. (1) Where, at any time, it appears to the Commission that personal data —

Decision by the Commission.

- (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 shall communicate its decision in writing to that effect.

(2) The Commission shall issue a notice of the decision to the data controller.

40. The Commission shall not serve an enforcement notice on a data controller in relation to the processing of personal data under section 40(1) unless a decision has been made by the Commission.

Restriction on enforcement in case of processing for special purposes.

41. (1) A data controller or data processor who fails to comply with a notice commits an offence and is liable on conviction to a fine as may be determined and imposed by the Commission.

Failure to comply with notice.

(2) The data controller or data processor shall respond in accordance with subsection (1) to prove that, he to show compliance with the notice in question.

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

Officer authorized by the Commission.

(2) Without limiting subsection (1) of this Section, an officer authorised by the

Commission may by a warrant issued by a Court of competent jurisdiction, at any reasonable time, enter to inspect and search any premises, systems and equipment to ensure compliance with this Act.

PART X — TRANS-BORDER FLOW OF PERSONAL DATA

43. (1) The trans-border transfer of personal data may only take place where an adequate level of protection based on the provisions of this Act is secured in the recipient State or international organisation. Trans- border flow of personal data.
- (2) An appropriate level of protection may be secured by —
- (a) adequacy, accountability, authorization and reciprocity in the recipient State or international organization
 - (b) the data protection laws of that State or international organisation, including the applicable international treaties or agreements;
 - (c) ad-hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the data controllers or data processors involved in the transfer and processing.
- (3) Notwithstanding the provisions of subsection (2) 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.
- (4) The Commission shall be provided with all relevant information concerning the transfer of data referred to in subsection (1) and, upon request under subsection (2) and (3) of this section respectively.
- (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 or subject them to certain conditions.
- (7) The Commission shall ensure that where there is an onward transmission of personal data under this section, to any third party, other than the first recipient, such other party shall meet the minimum requirement for transfer of personal data.

PART XI — OFFENCES AND PENALTIES

44. (1) A person who knowingly or recklessly —

Unlawful obtaining etc.
of personal data.

- (a) obtains, or discloses personal data to a third party, without the consent of the data controller,
- (b) after obtaining personal data, retains it without the consent of the data controller

commits an offence and is liable on conviction to a fine of not less than ₦5,000,000.00 (Five Million Naira) or imprisonment for a term not less than 1 (one) year or both.

(2) It is a defense for a person charged with an offence under subsection (1) of this Section to prove that the act —

- (a) was carried out for a legitimate purpose and for the purpose of this section
- (b) was required or authorised by an enactment, law or by an order of a Court or Tribunal; or
- (c) was justified as being in the public interest or national security.

(3) A person who sells personal data, obtained under circumstances described under subsection (1) of this Section, commits an offence and is liable on conviction to a fine of not less than ₦1,000,000.00 (One Million Naira) per record or to imprisonment for a term not less than 5 (five) years concurrently or both.

(4) A person who advertises personal data in a manner that indicates that it was obtained in circumstances described under subsection (1) of this section, commits an offence and is liable on conviction to a fine of not less than ₦500,000.00 (Five Hundred Thousand Naira) per record or to imprisonment for a term of not less than 5 (five) years concurrently or both.

45. (1) A data controller or data processor who fails to put in place appropriate data protection technical and managerial safeguards, policies, standards, and procedures described under this Act commits an offence and is liable on conviction to a fine of not less than ₦10,000,000.00 (Ten Million Naira) for every year in default or to imprisonment for a term of not less than 1 (one) year or both.

Failure to observe
security.

(2) Notwithstanding the provisions of subsection (1) of this section, the Commission shall by Regulations make provisions for the administrative procedures to ensure compliance.

46. (1) A person who —

Obstruction in the
execution of warrant.

- (a) intentionally obstructs an officer in the execution of a warrant issued under this Act; or
- (b) fails, without reasonable cause to give the officer executing a warrant such assistance as the officer may

reasonably require for the execution of the warrant

commits an offence and is liable on conviction to a fine of not less than ₦5,000,000.00 (Five Million Naira) or to imprisonment for a term of not less than six (6) months or both.

(2) A person who, in compliance with a 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 conviction to a fine of not less than ₦5,000,000.00 (Five Million Naira) or a term of imprisonment of at least one (1) year or both.

47. Any person who —

Attempt, conspiracy, aiding and abetting.

- (a) attempts to commit any offence under this Act; or
- (b) aids, abets, conspires, counsels or procures another person to commit any of the offences under this Act:

commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

48. (1) Any person who is or has been the Data Protection Commissioner or a staff of the Commission or an agent of the Commission shall not disclose information which —

Offence relating to breach of confidentiality.

- (a) has been obtained by, or provided to, the Commission in the course of, or for the purposes of, performing the regulators functions;
- (b) relates to an identified or identifiable data subject; 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) A person who knowingly or recklessly discloses information in contravention of subsection (1) of this section commits an offence and is liable on conviction to a term of not less than 2 years imprisonment or a fine of not less than ₦10,000,000.00 (Ten Million Naira) or both.

49. (1) The Court may in addition to imposing a sentence on any person convicted of an offence under this Act, order that the convicted person forfeit to the Government of the Federal Republic of Nigeria —

Order of forfeiture of assets.

- (a) any asset, money or property, whether tangible or intangible, traceable to proceeds of such offence; and

(b) any computer, equipment, software, electronic device or any other device used or intended to be used to commit or to facilitate the commission of such offence.

- (2) Where it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities for which he is convicted under this Act, such assets or properties, shall subject to any treaty or arrangement with such foreign country, be forfeited to the Federal Government of Nigeria.
- (3) The Attorney-General of the Federation and Minister of Justice shall ensure that the forfeited assets or property are effectively transferred and vested in the Federal Government of Nigeria.

50. (1) In addition to any other penalty prescribed under this Act, the Court may order a data controller, data processor or person convicted of an offence under this Act to compensate or make restitution to the victim of the offence. Order of payment of compensation or restitution.
- (2) An order of payment of compensation or restitution may be enforced by the victim or by the Commission on behalf of the victim in the same manner as a judgment in a civil action.

PART XII — RECORDS OBTAINED FROM DATA SUBJECT'S RIGHTS OF ACCESS

51. (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 or services to that person. Conditional request for personal data prohibited.
- (2) Subsection (1) does not apply where the imposition of the requirement is required for the identification of persons or authorised under an enactment, law, valid commercial transaction or in the public interest.

PART XIII — FINANCIAL PROVISIONS

52. (1) The Commission shall establish and maintain a Fund (in this Act referred to as “the Fund”) from which all expenditure incurred by the Commission shall be defrayed. Funds of the Commission.
- (2) The Fund shall consist of —
- (a) Five percent (5%) deductions from:
- (i) revenue generated from National Identification Number (NIN) and person identity verification services hosted by the National Identity Management Commission (NIMC),
 - (ii) revenue generated from issuance of Drivers’ License services hosted by the Federal Road Safety Commission (FRSC),
 - (iii) revenue generated from issuance of International Passport services hosted by the Nigeria Immigration Service (NIS),
 - (iv) revenue generated from the levy of one percent (1%) of the profit before tax of companies and enterprises covered by the National Information Technology Development Agency (NITDA) Act

accruable to the National Information Technology Development Fund,

(v) Universal Service Provision Fund of the Nigeria Communications Commission (NCC), and

(vi) Service Wide Vote.

(b) gifts, loans, grants, aids, etc.;

(c) all other assets that may accrue to the Commission; and

(d) licensing fees, penalties and fines.

53. (1) The Commission may, in accordance with the general authority given by the Minister of Finance, borrow such sums of money as the Commission may require in the performance of its functions under this Act or its subsidiary legislation. Power to borrow and accept gifts.

(2) The Commission may accept gifts, grants of money, 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.

54. (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 next financial year. Annual estimates.

(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), 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 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.

55. (1) The financial year of the Commission starts on 1st January of each year and ends on 31st December of the same year. Financial year and audit by the Commission.

(2) The Commission shall keep proper records of its accounts in respect of each year and shall cause its accounts to be audited within six 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 by the Auditor-General for the Federation.

56. The Commission shall prepare and submit to the President, not later than six 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. Annual reports.

PART XIV — MISCELLANEOUS

57. (1) Notwithstanding anything contained in any other enactment or law, no suit against the Commission, 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 after the ceasing of such act. Procedure in respect of suits against the Commission.
- (2) No suit shall be commenced against the Commission before the expiration of one month after written notice of intention to commence the suit is served upon the Commission by the intending plaintiff or his agent, and the notice shall clearly state the —
- (a) cause of action;
 - (b) particulars of the claim;
 - (c) name and place of abode of the intending plaintiff; and
 - (d) relief being sought
- (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.
58. The notice under the provision of this Act or any other notice, summons, process, or other document required or authorised 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 at the Head Office of the Commission. Cap. P41, LFN, 2004 Service of documents.
59. No execution or attachment process in the nature thereof shall be issued against the property of 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. Restriction on execution against property of the Commission.
60. The Data Protection Commissioner, member, agent, or employee for the time being of the Commission is indemnified out of the assets of the Commission against any liability incurred in defending any proceeding whether civil or criminal, where any such proceeding is brought against him in his capacity as such staff, member, agent, or employee. Indemnity of staff, members, and employees of the Commission.

61. 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. International cooperation
62. The Commission may when it deems necessary, review the 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 — Regulations, guidelines and review thereof.
- (a) which may no longer be relevant in the existing context of the Nigerian or globally accepted standards;
 - (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.
63. The Federal High Court shall have exclusive jurisdiction over all matters, suits and cases arising out of or pursuant to or consequent upon this Act or its subsidiary legislation. Jurisdiction.
64. (1) An officer of the Commission may apply ex-parte to a Judge in Chambers for the issuance of a warrant for the purpose of obtaining evidence in related investigation. Power of arrest, search and seizure
- (2) Where a Judge is satisfied on the information on oath that there is reasonable grounds for believing that any undertaking has engaged or is engaging or likely to engage in conduct constituting or likely to constitute the contravention of the provisions of this Act, the Judge may issue a warrant permitting an authorized officer to—
- (a) enter and search any premises or place if, within such premises,
 - (i) an offence under this Act is being committed;
 - (ii) there is evidence of the commission of an offence under this Act or other relevant law;
 - (iii) there is an urgent need to prevent the commission of an offence under this Act or other relevant law; or
 - (iv) where there is reasonable suspicion that a crime under this Act is or about to be committed.
 - (b) search any person or conveyance found on any premises or place which such authorized officers are empowered to enter and search under paragraph (a) of this subsection;
 - (c) stop, board and search any conveyance;
 - (d) seize, seal or remove and detain anything which is, or contains evidence of the commission of an offence

under this Act;

- (e) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network;
- (f) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format; or
- (g) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.

(3) The Judge shall issue a warrant under subsection (2) where it is satisfied that —

- (a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act; or
- (b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence; or
- (c) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; or
- (d) the object or subject named in the warrant is preparing to commit an offence under this Act.

65. Notwithstanding anything contained in any other law in force in Nigeria, a legal practitioner employed in or by the Commission in any capacity, may represent the Commission, as counsel, who appears, draws papers, pleadings or documents, or perform any act in connection with proceedings pending or prospective before a court, or a quasi-judicial body, or any other body, board, committee, commission or officer constituted or appointed by law or having authority to take evidence in or settle or determine controversies in the exercise of the judicial power of the Federation or any subdivision thereof.

Powers of Staff as
Counsel

66. In this Act —

Interpretation.

"automated data subject, decision making and profiling" means a decision based solely on automated processing, including profiling and shall only be processed under this Act;

"Commission" means the Data Protection Commission which is established under the provision of 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, and where a data controller also serves as a data processor, the provisions regarding the activities of a data controller under this Act shall apply;

"household activity" means activities which are closely and objectively linked to the private life of an individual or person, which do not impinge upon the personal sphere of others. Household activities have no professional, commercial or publicity intent.

"vital interest" refers to those relating to life and death issues.

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

- (a) collection, recording, organisation, structuring, storage or preservation;
- (b) adaptation or alteration;
- (c) access, retrieval or consultation;
- (d) transmission, disclosure, sharing or making available; or
- (e) restriction, erasure, or destruction of, or the carrying out of logical or arithmetical operations.

"data processing" where automated processing is not used, 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 processor" means the natural or legal person, public authority, service, commission or any other body which, alone or jointly with others processes personal data on behalf of the data controller;

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

"identifiable data subject or identifiable natural person" 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;

"Legitimate purpose" shall be interest in furtherance of prevention of fraud; information security; prevention of criminal acts or threats to public security.

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

"recipient" means a natural or legal person 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;

- (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;
- (f) personal data concerning the data of a child who is under the age of 16 years; or
- (g) such other personal data that may be designated as sensitive data by guidelines made by the Commission;

“third party” means a natural or legal person, public authority, agency or body other than

"direct marketing" includes the communication by whatever means of any advertising or marketing material which is directed to particular data subjects.the data subject, data controller, data processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"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 traditional healer recognised by legislation regulating traditional medicine practice.

“public institutions “Institutions funded by state or government bodies and controlled by public officials or their appointees.

67. Nothing in this Act shall nullify or invalidate any provision of an Act of the National Assembly regarding safeguarding privacy of personal data.

Transitional provisions
Savings provision.

68. This Act may be cited as the Data Protection Act, 2020.

Citation.

SUPPLEMENTARY PROVISIONS RELATING TO PROCEEDINGS OF THE
COMMISSION

1. Subject to the provisions of this Act and Section 27 of the Interpretation Act, the Commission may make standing orders regulating the proceedings of the Board and set up any Committee.
2. Every meeting of the Board shall be presided over by the Data Protection Commissioner who shall preside as the Chairman and where the Chairman is unable to attend a particular meeting, the members present at the meeting shall elect one of their members to preside at the meeting.
3. The quorum at a meeting of the Commission shall consist of the Chairman or in an appropriate case, the person presiding at the meeting under paragraph 2 of this Schedule and 7 other members.

Committees

4. (1) Subject to Standing Orders made by the Board pursuant to this Act, the Commission may appoint such number of standing and ad hoc committees as it deems fit to consider and report on any matter with which the Commission is concerned.

(2) Every Committee appointed under the provisions of subparagraph (1) of this paragraph shall be presided over by a member of the Board and shall be made up of such number of persons, as the Board may determine in each case.
5. The decision of a Committee is of no effect until it is approved or ratified by the Board.

Miscellaneous

6. The fixing of the seal of the Commission shall be done by the Secretary of the Commission and authenticated by the signature of the Data Protection Commissioner and Chief Executive Officer or such other Member or Director authorised generally or specifically by the Commission to act for that purpose.
7. Any contract or instrument which, if made by a person not being a body corporate, shall not be required to be under seal, may be made or executed on behalf of the Commission by the Data Protection Commissioner or by any other Director or staff generally or specifically authorised by the Commission to act for that purpose.
8. Any document purporting to be a contract, an instrument or other document signed or sealed on behalf of the Commission is received in evidence and, unless the contrary is proved, be presumed, without further proof, to have been so signed and sealed.
9. The validity of a proceeding of the Commission or its Committee is not adversely affected —
 - (a) by any vacancy in the membership of the Commission;

- (b) by any defect in the appointment of a member of the Commission, staff or committee; or
- (c) by reason that a person not entitled to do so took part in the proceeding.

10. A member of the Board or any of its Committees who has a personal interest in any contract or arrangement entered into or proposed to be considered by the Commission or Committee shall declare his interest and shall not vote on any question relating to the contract or arrangement.

DATA PROTECTION ACT, 2020

EXPLANATORY MEMORANDUM

This Act establishes the Data Protection Commission charged with the responsibility for the protection of personal data, data subject's rights, and regulation of the processing of personal information

DATA PROTECTION ACT, 2020

Arrangement of Sections

Section:

PART I – OBJECTIVES, APPLICATION AND SCOPE

1. Objectives of the Act.
2. Application and scope.

PART II – BASIC PRINCIPLES AND LEGAL BASIS FOR PROCESSING OF PERSONAL DATA

3. Basic principles relating to processing of personal data.
4. Lawfulness of personal data processing.
5. Consent of data subjects.
6. Transparency of personal data processing.

PART III - ESTABLISHMENT, COMPOSITION, POWERS AND FUNCTIONS OF THE DATA PROTECTION COMMISSION

7. Establishment of the Data Protection Commission.
8. Composition of the Governing Board
9. Functions of the Commission.
10. Powers of the Commission.
11. Appointment of Data Protection Commissioner.
12. Cessation or removal from office.
13. Secretary to the Commission.
14. Staff of the Commission.
15. Conditions of Service.
16. Appointment, Promotion and Discipline of Staff.

PART V – RIGHTS OF THE DATA SUBJECTS

17. Rights of data subjects.
18. Right of access.
19. Right in respect of automated decision making.
20. Right to rectification, erasure, and restitution of processing.
21. Right to judicial remedy.
22. Right to object, including profiling and direct marketing.
23. Right to have data processing suspended.
24. Right to prevent processing of personal data.
25. Right to data portability.

PART VI – PROCESSING OF SENSITIVE DATA

26. Processing of sensitive data.
27. Prohibition on processing of sensitive data which relates to religious beliefs.
28. Rights in relation to automated decision making.
29. Compensation for failure to comply.

PART VII – DUTIES OF DATA CONTROLLERS AND DATA PROCESSORS

30. Duties of data controllers.
31. Vicarious Liability.
32. Duties of data processors.

PART VIII – DATA LOCATION AND SECURITY

33. Data location.
34. Security of processing.
35. Exception on the grounds of public interest.

PART IX- ADMINISTRATION AND ENFORCEMENT

36. Enforcement notice.
37. Cancellation of enforcement notice.
38. Request for assessment.
39. Decision by the Commission.
40. Restriction on enforcement in case of processing for special purposes.
41. Failure to comply with notice.
42. Officer authorized by the Commission.

PART X – TRANS-BORDER FLOW OF PERSONAL DATA

43. Trans-border flow of personal data.

PART XI– OFFENCES AND PENALTIES

44. Unlawful obtaining of personal data.
45. Failure to localise personal data.
46. Obstruction in the execution of warrant.
47. Attempt, conspiracy, aiding and abetting.
48. Offence relating to breach of confidentiality.
49. Order of forfeiture of assets.
50. Order of payment of compensation or restitution.

PART XII – RECORDS OBTAINED UNDER DATA SUBJECTS RIGHTS OF ACCESS

51. Conditional request for personal data prohibited.

PART XIII – FINANCIAL PROVISIONS

52. Funds of the Commission.
53. Power to borrow and accept gifts.
54. Annual estimates.
55. Financial year and audit by the Commission.
56. Annual reports.

PART XIV - MISCELLANEOUS

57. Procedure in respect of suits against the Commission.
58. Service of documents.
59. Restriction on execution against property of the Commission.

60. Indemnity of staff, members, and employees of the Commission.
61. International cooperation.
62. Regulations, guidelines and review thereof.
63. Jurisdiction.
64. Power of arrest, search and seizure.
65. Powers of Staff as Counsel
66. Interpretation.
67. Transitional provisions/Savings provision.
68. Citation.

Schedule