

NIGERIA DATA PROTECTION BILL, 2022

MEMORANDUM

An Act to provide the legal framework for the protection of personal data, and establish the Nigeria Data Protection Commission for the regulation of the processing of personal data, and for related matters.

THE DATA PROTECTION BILL, 2022

ARRANGEMENT OF SECTIONS

PART I—OBJECTIVES AND APPLICATION

1. Objectives
2. Application of this Act
3. Exemptions

PART II— ESTABLISHMENT OF THE NIGERIA DATA PROTECTION COMMISSION,

4. Establishment of the Nigeria Data Protection Commission
5. Offices of the Commission
6. Independence of the Commission
7. Functions of the Commission
8. Powers of the Commission

PART III — ESTABLISHMENT OF THE GOVERNING COUNCIL, AND ITS ADMINISTRATION

9. Composition of the Council
10. Tenure and remuneration of part-time members of the Council
11. Cessation
12. Resignation and removal of Council Members
13. Filling of vacancy in the Council
14. Conflict of interest
15. Responsibilities and powers of the Council
16. Responsibilities of the National Commissioner
17. Secretary to the Council

PART IV—FINANCIAL PROVISIONS

18. Funds of the Commission

19. Expenditure of the Fund
20. Power to borrow and accept gifts
21. Investments

PART V—ANNUAL ACCOUNTS

22. Financial year and audit by the Commission
23. Annual reports
24. Annual estimates of income and expenditure

PART VI— PRINCIPLES AND LAWFUL BASIS GOVERNING PROCESSING OF PERSONAL DATA

25. Principles of personal data processing
26. Lawful basis of personal data processing
27. Conditions of consent
28. Provision of information to the data subject
29. Data protection impact assessment
30. Obligations of the data controller and data processor
31. Sensitive personal data
32. Children or individuals lacking the legal capacity to consent
33. Data protection officers
34. Data protection compliance services

PART VII—RIGHTS OF A DATA SUBJECT

35. Rights of the data subject
36. Withdrawal of consent
37. Right to object
38. Automated decision-making
39. Data portability

PART VIII—DATA SECURITY

40. Security, integrity and confidentiality
41. Personal data breaches

PART IX—CROSS-BORDER TRANSFERS OF PERSONAL DATA

42. Basis for cross-border transfer of personal data
43. Adequacy of protection
44. Other bases for transfer of personal data outside Nigeria

PART X—REGISTRATION AND FEES

- 45. Registration of data controllers and data processors of major importance
- 46. Fees and levies

PART XI—ENFORCEMENT

- 47. Complaints and investigations
- 48. Compliance orders
- 49. Enforcement orders
- 50. Offence
- 51. Judicial review
- 52. Civil remedies
- 53. Forfeiture
- 54. Joint and vicarious liability

PART XII – LEGAL PROCEEDINGS

- 55. Procedure in respect of suits against the Commission
- 56. Service of documents
- 57. Restriction on execution against property of the Commission
- 58. Indemnity of staff, members, and employees of the Commission
- 59. Power of arrest, search, and seizure
- 60. Right to appear in court

PART XIII—MISCELLANEOUS

- 61. Regulations
Error! Reference source not found. Regulations, guidelines, and review thereof
- 62. Exemption from taxation
- 63. Application of other enactments
- 64. Transitional provisions
- 65. Interpretation

SCHEDULE I—SUPPLEMENTARY PROVISIONS RELATING TO PROCEEDINGS OF THE

A BILL

FOR

An Act to provide the legal framework for the protection of personal data, and establish the Nigeria Data Protection Commission for the 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 AND APPLICATION

1. The objective of this Act is to safeguard the fundamental rights and freedoms and the interests of data subjects as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999, particularly to —
 - (a) provide for the regulation of processing of personal data;
 - (b) promote data processing practices that protect security of personal data and privacy of data subjects;
 - (c) ensure that personal data is processed in a fair, lawful and accountable manner;
 - (d) protect data subjects’ rights, and provide remedies and means of recourse in case of breach of those rights;
 - (e) ensure that data controllers and data processors fulfil their obligations to data subjects;
 - (f) minimize the harmful effect of personal data misuse or abuse on data subjects and other victims;
 - (g) establish an impartial, independent and effective regulatory Commission that will superintend over data protection and privacy issues and supervise data controllers and data processors; and
 - (h) contribute to the legal foundations of the digital economy of Nigeria and its participation in the regional and global economies through the beneficial, trusted use of personal data.

Objectives

Application

2. — (1) This Act applies to the processing of personal data whether by automated means or not.

(2) This Act applies only where—

- (a) the data controller or data processor is domiciled, ordinarily resident, or ordinarily operating in Nigeria;
- (b) the processing of personal data occurs within Nigeria; or
- (c) the data controller or the data processor is not domiciled, ordinarily resident or ordinarily operating in Nigeria, but is processing personal data of a data subject in Nigeria.

Exemptions

3. — (1) This Act shall not apply to the processing of personal data to the extent it is carried out by one or more individuals solely for personal or household purposes.

(2) Without prejudice to rights under the Constitution, the obligations under Parts VI (other than section 25), VIII, IX and X do not apply to a data controller or data processor when processing of personal data is—

- (a) carried out by competent authorities for the purposes of the prevention, investigation, detection, prosecution or adjudication of criminal offences or the execution of criminal penalties in accordance with any applicable law;
- (b) carried out by competent authorities for the purposes of prevention or control of a national public health emergency;
- (c) carried out by competent authorities as necessary for national security;
- (d) in respect of publication in the public interest for journalism, educational, academic, artistic and literary purposes to the extent that such obligations and rights would be incompatible with such purposes; or
- (e) necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(3) The Commission may by regulation prescribe types of personal data and processing that shall be exempt from this Act or any provision thereof.

**PART II— ESTABLISHMENT OF THE NIGERIA DATA
PROTECTION COMMISSION, FUNCTIONS AND POWERS**

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

(2) The Commission —

- (a) shall be a body corporate with perpetual succession and a common seal;
- (b) may sue or be sued in its corporate name; and
- (c) may, for the purposes of its functions under this Act and subject to the Land Use Act, hold, acquire, and dispose of any property, movable or immovable.

5. — (1) The Commission shall have its Head Office in the Federal Capital Territory.

(2) The Commission may open other offices in any part of Nigeria in the interests of achieving the objects of the Commission.

6. — (1) The Commission shall be independent in the discharge of its functions under this Act.

(2) Further to subsection (1), the Commission may develop, adopt and, as appropriate from time to time, amend, revoke or supplement appropriate regulations, codes, guidelines, and procedures to regulate its operations in furtherance of the discharge of its functions.

(3) Regulations, codes, guidelines, and procedures referred to in subsection (2) shall, without limitation to the generality of subsection (2), govern the—

- (a) conduct of the business and operations of the Commission in a manner that –
 - (i) fosters accountability and ensures transparency and consistency with the highest ethical standards, and
 - (ii) ensures the maintenance of international best practice as it relates to the regulation of data protection and privacy;
- (b) budgeting and expenditure of the Commission in accordance with the provisions of this Act;
- (c) governance code for the Commission;
- (d) code of conduct of members of the governing body and staff of the Commission; and
- (e) any other matter relevant to the operations of the Commission as may be directed by the Commission.

Establishment
of the Nigeria
Data
Protection
Commission

Offices of the
Commission

Independence
of the
Commission

7. The Commission shall —

- (a) ensure the deployment of technological and organisational measures to enhance personal data protection;
- (b) promote awareness of data controllers and data processors of their obligations under this Act;
- (c) promote public awareness and understanding of personal data protection and the risks to personal data, including the rights granted and obligations imposed under this Act;
- (d) foster the development of personal data protection technologies in accordance with recognized international good practices and applicable international law;
- (e) participate in international fora and engage with other national and regional authorities responsible for data protection with a view to developing consistent and efficient approaches to regulation of cross-border transfers of personal data;
- (f) receive complaints relating to violations of this Act or regulations issued pursuant to this Act;
- (g) conduct investigations of potential violations by a data controller or a data processor of any requirement under this Act or other subsidiary legislation made pursuant to this Act;
- (h) determine whether or not countries, regions or sectors, or binding corporate rules, contractual clauses, codes of conduct or certification mechanisms, afford adequate personal data protection standards for cross-border transfers;
- (i) ensure compliance with national and international personal data protection good practice and obligations laid down by international agreements and treaties to which Nigeria is a party;
- (j) register data controllers and data processors of major importance;
- (k) license, accredit and register bodies to provide data protection compliance services where in the Commission's opinion it facilitates the attainment of the objective of this Act;
- (l) collaborate with any relevant ministry, department, agency, body, company, firm, or person in any activity that in the Commission's opinion facilitates the attainment of the objective of this Act;

- (m) collect and publish information with respect to personal data protection, including personal data breaches;
- (n) advise the government on policy issues relating to data protection and privacy;
- (o) submit legislative proposals to the Minister, including amending existing laws, with a view to strengthening personal data protection in Nigeria; and
- (p) generally implement the provisions of this Act and do such other things as are necessary to the carrying out of the functions of the Commission.

8. The Commission shall have powers to —

- (a) issue regulations, rules, directives and guidance under this Act;
- (b) hire consultants, and license, accredit or register consultants, to assist the Commission in the discharge of its functions, where necessary;
- (c) require any person that is subject to this Act to provide an explanation, information, documents and assistance in person and in writing;
- (d) impose penalties in case of violations of the provisions of this Act or other subsidiary legislation made pursuant to this Act;
- (e) prescribe fees payable by data controllers and data processors in accordance with data processing activities; and
- (f) prescribe the manner and frequency of filing, and content, of compliance returns by data controllers and data processors of major importance to the Commission.

Powers of the Commission

PART III — ESTABLISHMENT OF THE GOVERNING COUNCIL, AND ITS ADMINISTRATION

9. — (1) There is established for the Commission a Governing Council (in this Act referred to as “the Council”) which shall consist of the following—

- (a) the Chairman who shall be a retired judge of a superior court of record;
- (b) the National Commissioner;

Composition of the Council

- (c) one representative from the Federal Ministry of Justice not below the rank of a Director or its equivalent;
- (d) one representative from the Ministry responsible for communications and digital economy not below the rank of a Director or its equivalence;
- (e) one representative from the Central Bank of Nigeria not below the rank of a Director or its equivalent;
- (f) one representative from a law enforcement agency not below the rank of a Director or its equivalent; and
- (g) one representative from the private sector.

(2) The President shall, on the recommendation of the Minister, appoint the National Commissioner and other members of the Council.

(3) The members of the Council other than the National Commissioner shall be part-time members.

(4) The members of the Council shall be citizens of Nigeria and—

- (a) in the case of the National Commissioner, such a person shall be certified in data protection and shall possess not less than ten years cognate experience, and proficiency, in law, data protection, cybersecurity management, information and communication technology, consumer protection, management science or other relevant disciplines at a senior management level;
- (b) in the case of the representative from the private sector, such a person shall possess not less than five years cognate experience, and proficiency in data protection and privacy; and
- (c) in the case of members of the Council other than those referred to in paragraphs (a), (b) and (g) of subsection (1), such a person shall have proficiency in data protection and privacy.

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

10. — (1) The part-time members of the Council shall hold office for four years and may be reappointed for another term of four years and no more.

(2) The part-time members of the Council shall be paid such reasonable remuneration and allowances as

Tenure and remuneration of part-time members of the Council

approved by the President on the recommendation of the Council.

11. — (1) A person shall not be appointed or remain a member of the Council if –

Cessation

- (a) he is an undischarged bankrupt, having been adjudged or otherwise declared bankrupt under any law in force in any part of Nigeria, suspends payment or compounds with his creditors;
- (b) he is convicted of a felony or any offence involving dishonesty, fraud or forgery by any competent court of law in Nigeria;
- (c) he is medically certified to be of unsound mind or becomes incapable through illness or injury of performing his duties;
- (d) he is guilty of serious misconduct in relation to his duties following an investigation into any matter relating to his duties in which he was accorded fair hearing; or
- (e) in the case of a person possessing professional qualifications, he is disqualified or suspended other than at his own request from practising his profession in any part of the world by an order of a competent authority made in that respect.

12. — (1) A member of the Council may at any time resign his office by giving at least two months' notice in writing to the President through the Minister of his intention to do so.

Resignation and removal of Council Members

(2) The President, upon the recommendation of the Minister, may remove a member at any time from membership of the Council if the member is disqualified on any of the grounds specified in section 11.

13. — (1) If a member of the Council dies, resigns, is disqualified or removed, or otherwise vacates office before the expiration of his term, the President shall in accordance with section 9(4) appoint another person to fill the vacancy so occasioned, and the person so appointed shall hold office for the remainder of the term of office of that member.

Filling of vacancy in the Council

(2) A person to be appointed under subsection (1) shall, without undue delay, be appointed after the occurrence of the vacancy.

14. — (1) Each member of the Council owes fiduciary duties to the Commission and shall ensure that his personal interest does not conflict with his duties under this Act.

Conflict of interest

(2) No member of the Council shall make a secret profit in the course of discharging his duties as a member of the Council.

(3) Every member of the Council shall fully and promptly disclose to the Council any personal, commercial, financial, or other interest which he may directly or indirectly hold or be connected with, and which becomes the subject of consideration by the Council, and shall be ineligible to participate in any Council deliberations and voting-related matter thereto; Provided that such an interest, if so disclosed, shall not disqualify such member for the purpose of constituting a quorum.

(4) No member of the Council shall accept any gift or advantage for himself or on behalf of any person with whom he may have a family, business, or financial relationship if the acceptance thereof would impair, or may reasonably be viewed as likely to impair, his impartiality in the performance of his duties under this Act.

(5) Any member of the Council who contravenes the any of the provisions of subsections (2) and (4) of this section shall be guilty of an offence and shall be liable on conviction—

- (a) in the case of a contravention of subsection (2), to a fine of not less than ₦ 10,000,000 or to imprisonment for a term of up to three years, or to both fine and imprisonment; and
- (b) in the case of a contravention of subsection (4), to a fine of not less than ₦ 5,000,000 or to imprisonment for a term of up to two years, or to both fine and imprisonment.

15. — (1) The Council shall be responsible for –

- (a) the overall policy direction of the affairs of the Commission;
- (b) approving strategic plans, action plans and budget support programmes submitted by the National Commissioner;
- (c) approving annual reports and financial reports submitted by the National Commissioner;
- (d) fixing the terms and conditions of service of the employees of the Commission, including remuneration, allowances and pension benefits in accordance with the Pension Reform Act;
- (e) making, altering, or revoking disciplinary rules and procedures and measures for the staff, officers and other employees of the Commission;

Responsibilities and powers of the Council

- (f) providing advice and counsel to the National Commissioner;
- (g) assisting the National Commissioner in matters relating to compliance by ministries, departments and agencies of government with this Act; and
- (h) such other matters as may be prescribed by any other provision of this Act.

(2) The Council may delegate any part of its responsibilities under any provision of this Act to a Committee set up by the Council as it may deem fit, in accordance with the provisions of this Act.

16. (1) The National Commissioner shall be responsible for—

- (a) exercising the powers and performing the duties of the Commission under this Act;
- (b) implementing the policies and decisions of the Council;
- (c) representing the Commission before third parties;
- (d) day-to-day management of the Commission;
- (e) acquiring and approving the acquisition of offices and other premises for the use of the Commission;
- (f) appointing such number of officers and staff as may appear expedient and necessary for the proper and efficient conduct of the business and functions of the Commission;
- (g) making, altering and revoking rules, guidelines, circulars, and regulations for attaining the objectives and discharging the functions, carrying on the operations, activities, and business of the Commission under this Act; and
- (h) performance of such other functions as may be necessary or incidental for executing the mandate of the Commission.

(2) A person appointed as the National Commissioner shall not, while holding that office, hold any management position in any other commission, corporation, company, or any other business establishment.

(3) The National Commissioner shall hold office for a period of five years and may be eligible for reappointment for a further period of five years only.

(4) The National Commissioner may delegate any part of his responsibilities under any provision of this Act as he may deem fit.

Responsibilities of
the National
Commissioner

(5) Subject to subsection (3), the terms and conditions of service, including remuneration and allowances, of the National Commissioner shall be as approved by the President on the recommendation of the Minister.

17. The National Commissioner shall be the Secretary to the Council and shall—

- (a) be responsible to the Council;
- (b) keep the Council's records;
- (c) conduct its correspondence; and
- (d) perform such other duties as the Council may from time to time determine.

Secretary to the Council

PART IV—FINANCIAL PROVISIONS

18. — (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) There shall be paid into the Fund established in pursuance to sub-section (1) of this Section —

- (a) a take-off grant of ₦5,000,000,000 of which:
 - (i) 20% shall be from the Consolidated Revenue Fund of the Federation;
 - (ii) 20% shall be from the Central Bank of Nigeria;
 - (iii) 35% shall be from the Nigerian Communications Commission;
 - (iv) 20% shall be from the National Information Technology Development Agency;
 - (v) 5% shall be from the National Identity Management Commission; and
 - (vi) 50% of the total amount is to be provided upon the coming into force of this Act and the remaining 50% of the total amount is to be provided upon the anniversary of the date on which this Act comes into force;
- (b) donations, gifts, loans, grants, aids, and endowments, voluntary contributions or otherwise to the Commission for its activities under this Act;
- (c) levies, fees, penalties and fines collected by the Commission; and
- (d) all other monies or assets that may, from time to time, accrue to the Commission.

19. — (1) There shall be chargeable to the Fund established under section 18—

Expenditure of the Fund

- (a) all expenses incurred by the Commission as approved by the Council or in pursuance of any expenditure policy approved by the Council;
- (b) the repayment of funds borrowed by the Commission, including interest on such borrowed funds;
- (c) allowances and remuneration payable to members of the Council;
- (d) remunerations and other allowances, retiring benefits such as pensions and gratuities and, any other remunerations payable to the staff of the Commission;
- (e) the cost of administration of the Commission; Commission;
- (f) the payment for consultancies, contracts, including mobilization, fluctuations, variations, legal fees and cost on contract administration as approved by the Council or in pursuance of the expenditure or procurement plan approved by the Council;
- (g) expenses necessary to meet capital expenditure, for the purchase, acquisition, or maintenance of property or other equipment of the Commission;
- (h) for purposes of investment; and
- (i) the payment of any such other expenditure necessary for the discharge of the functions of the Commission.

(3) The Fund of the Commission shall be managed in accordance with the rules made by the Council.

20. — (1) Subject to any applicable law, the Commission may borrow such sums of money as may be required in the performance of the functions of the Commission pursuant to this Act.

Power to borrow and accept gifts

(2) The Commission may accept gifts, grants of money, aids or other property upon such terms and conditions, that are not inconsistent with the objectives and functions of the Commission under this Act.

21. The Commission may, subject to the provisions of this Act, invest any surplus funds as may be approved by the Council and the net incomes so generated shall be paid into the Fund.

Investments

PART V—ANNUAL ACCOUNTS

22. — (1) The Commission shall –

- (a) keep proper accounts in respect of each financial year;
- (b) keep proper records in relation to those accounts; and
- (c) cause the accounts to be audited within six months after the end of the financial year.

Financial year and
audit by the
Commission

(2) For the purpose of subsection (1) of this section the financial year of the Commission shall be from 1st January to 31st December of every year, or such other period as may be determined by the Council.

(3) The accounts of the Commission shall be audited by an independent firm of auditors appointed from time to time on such terms as may be determined by the Council and shall be subject to reappointment on an annual basis provided that such independent firm of auditors is on the list of auditors approved by the Auditor-General for the Federation.

23. The Commission shall prepare and submit to the National Assembly, not later than six months after the end of each financial year, a report which shall be in such form as the Council may direct and shall relate to the activities of the Commission during the immediately preceding financial year and the Commission's audited accounts for the year under review.

Annual reports

24. — (1) The Commission shall, in each financial year, prepare and present to the National Assembly, a statement of estimated income and expenditure for the next financial year.

Annual estimates of
income and
expenditure

(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.

PART VI— PRINCIPLES AND LAWFUL BASIS GOVERNING PROCESSING OF PERSONAL DATA

25. — (1) A data controller or data processor shall ensure that personal data is—

- (a) processed, by such data controller or any data processor processing personal data on its behalf, fairly, lawfully and in a transparent manner;

Principles of
personal data
processing

- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- (c) adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;
- (d) retained for no longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed;
- (e) accurate, complete, not misleading and, where necessary, kept up to date having regard to the purposes for which the personal data was collected or is further processed; and
- (f) 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 confidentiality, integrity and availability of the personal data.

(2) Notwithstanding anything to the contrary in this Act or any other law, a data controller or data processor owes a duty of care in respect of data processing and shall demonstrate accountability in respect of the principles contained in this Act.

(3) For the purposes of subsection (1)(b)—

- (a) compatibility of further processing shall be assessed in light of:
 - (i) the relationship between the original purpose and the purpose of the intended further processing,
 - (ii) the nature of the personal data concerned,
 - (iii) the consequences of the further processing,
 - (iv) how the personal data has been collected, and
 - (v) the existence of appropriate safeguards; and
- (b) further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Lawful basis of
personal data
processing

26. — (1) Without prejudice to the principles set out in this Act, data processing shall be lawful if one of the following applies—

- (a) the data subject has given and not withdrawn his consent for the specific purpose or purposes for which it will be processed;
- (b) the processing is necessary:
 - (i) 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,
 - (ii) for compliance with a legal obligation to which the data controller or data processor is subject,
 - (iii) in order to protect the vital interest of the data subject or another individual,
 - (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or
 - (v) for the purposes of the legitimate interests pursued by the data controller or data processor or by a third party to whom the data is disclosed.

(2) Interests shall not be legitimate for the purposes of paragraph (1)(b)(v) of section 26 where—

- (a) they are overridden by the fundamental rights and freedoms and the interests of the data subject;
- (b) they are incompatible with other lawful basis of processing under subsection (1)(b) of this section;
- or
- (c) the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

27. — (1) A data controller shall bear the burden of proof for establishing a data subject's consent.

Conditions of
consent

(2) In determining whether consent was freely and intentionally given, account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(3) Silence or inactivity by the data subject shall not constitute consent.

(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 consent at any time.

(5) The withdrawal of consent under subsection (4) shall not affect the lawfulness of data processing that occurred before the withdrawal of the consent.

(6) Consent may be provided in writing, orally, or through electronic means.

28. — (1) Before a data controller collects personal data directly from a data subject, the data controller shall, inform the data subject of—

- (a) the identity, residence or place of establishment of, and means of communication with, the data controller;
- (b) the specific lawful basis of processing under section 26(1) or 31(1) and the purposes of the processing for which the personal data are intended;
- (c) the recipients or categories of recipients of the personal data, if any;
- (d) the existence of the rights of the data subject under Part VII;
- (e) the right to lodge a complaint with the Commission in accordance with Section 47(1); and
- (f) the existence of automated decision-making, including profiling, significance and envisaged consequence of such processing for the data subject, and the right to object to and challenge such processing.

(2) Before a data controller collects personal data other than directly from the data subject, it must inform the data subject of the items set out in subsection (1) unless the data subject already has been provided such information or provision of such information is impossible or would involve a disproportionate effort or expense.

29. — (1) Where processing appears likely to result in high risk to the rights and freedoms of data subjects by virtue of its nature, scope, context and purposes, a data controller shall, prior to the processing, carry out a data protection impact assessment.

(2) The data controller shall consult the Commission prior to the processing if, notwithstanding the measures envisaged under subsection (4)(d), the data protection impact assessment indicates that the processing of the data would result in a high risk to the rights and freedoms of data subjects.

Provision of
information to
the data subject

Data protection
impact
assessment

(3) The Commission shall issue guidelines and directives with regards to this Section, including the categories of processing and persons subject to the requirement for a data protection impact assessment pursuant to subsection (1).

(4) For purposes of this section, a “data protection impact assessment” is an assessment of the impact of the envisaged processing on the protection of personal data comprising—

- (a) a systematic description of the envisaged processing and its purpose, including where applicable the legitimate interest pursued by the data controller, data processor or third party;
- (b) an assessment of the necessity and proportionality of the processing in relation to the purposes for which the personal data would be processed;
- (c) an assessment of the risks to the rights and freedoms of data subjects; and
- (d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

30. — (1) Where a data controller engages the services of a data processor, or any data processor engages the services of another data processor, the data controller or data processor shall take reasonable measures to ensure that the engaged data processor shall—

- (a) comply with the principles and obligations set out in section 25 applicable to the data controller;
- (b) assist the data controller or data processor, as the case may be, by appropriate technical and organisational measures, in the fulfilment of the data controller’s obligations to honour the rights of data subjects under Part VII;
- (c) implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data as required in Part VIII;
- (d) provide the data controller or data processor, as applicable, with any information it reasonably requires to comply and demonstrate compliance with this Act; and

Obligations of
the data
controller and
data processor

(e) notify the data controller or data processor, as the case may be, when any new data processors are engaged.

(2) Reasonable measures under subsection (1) include a written agreement between the data controllers and the data processor or between data processors, as the case may be.

31. — (1) Without prejudice to the principles set out in this Act, a data controller or data processor shall not process, or permit a data processor to process on its behalf, sensitive personal data unless one of the following applies—

Sensitive
personal data

- (a) the data subject has given and not withdrawn his consent to the processing for the specific purpose or purposes for which it will be processed;
- (b) the processing is necessary for the purposes of exercising or performing rights or obligations of the data controller or of the data subject under employment or social security laws or any other similar laws;
- (c) the processing is necessary to protect the vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent;
- (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a charitable, educational, literary, artistic, philosophical, religious or trade union aim and—
 - (i) the processing relates solely to the members or former members of the entity or to individuals who have regular contact with it in connection with its purposes, and
 - (ii) the sensitive personal data is not disclosed outside of the entity without the explicit consent of the data subject;
- (e) the processing relates to personal data which are manifestly made public by the data subject;
- (f) the processing is necessary for the establishment, exercise or defence of a legal claim, obtaining legal advice or conduct of a legal proceeding;
- (g) the processing is necessary for reasons of substantial public interest, on the basis of a law which shall be proportionate to the aim pursued, and provides for suitable and specific measures to

safeguard the fundamental rights and freedoms and the interests of the data subject;

- (h) the processing is carried out for purposes of medical care or community welfare and is undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality;
- (i) the processing is necessary for reasons of public health and provides for suitable and specific measures to safeguard the fundamental rights and freedoms and the interests of the data subject; or
- (j) the processing is necessary for archiving purposes in the public interest, or historical, statistical or scientific research, in each case on the basis of a law, which shall be proportionate to the aim pursued, and provides for suitable and specific measures to safeguard the fundamental rights and freedoms and the interests of the data subject.

(2) The Commission may prescribe in rules—

- (a) further categories of personal data that may be classified as sensitive personal data,
- (b) further grounds on which such personal data may be processed, and
- (c) safeguards that may apply.

(3) In prescribing rules under subsection (2), the Commission shall have regard to—

- (a) the risk of significant harm that may be caused to a data subject or class of data subjects by the processing of such category of personal data;
- (b) the reasonable expectation of confidentiality attached to such category of personal data; and
- (c) the adequacy of protection afforded to personal data generally.

32. — (1) Subject to subsection (5), when a data subject is a child or another individual lacking the legal capacity to consent, a data controller shall obtain consent of a parent or other appropriate legal guardian of the child or other individual, as applicable, to rely on consent under section 26(1)26(a)(a) or 31(1)(a).

(2) A data controller shall apply appropriate mechanisms where feasible to verify age and consent, taking into consideration available technology.

(3) For the purposes of subsection (2), presentation of any government approved identification documents shall be an appropriate mechanism.

(4) Subsection (1) does not apply when—

Children or individuals lacking the legal capacity to consent

- (a) the processing is necessary to protect the vital interests of the child or individual lacking the legal capacity to consent;
- (b) the processing is carried out for purposes of education or medical or social care and is undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or
- (c) the processing is necessary for proceedings before a court relating to the individual.

(5) A data controller may rely on consent provided by a child aged thirteen or more for the purposes of section 26(1)(a) and 31(1)(a) in relation to the provision of information and services by electronic means at the individual request of the recipient thereof.

(6) Nothing in this Act shall be construed as authorizing data processing in respect of a child in a manner that is inconsistent with the provisions of the Child's Right Act.

33. — (1) Data controllers of major importance shall designate a data protection officer with expert knowledge of data protection law and practices and the ability to carry out the tasks referred to in subsection (3).

(2) The data protection officer may be an employee or engaged by service contract.

(3) The data protection officer shall have the tasks of—

- (a) advising the data controller or the data processor and the employees who carry out processing of their obligations under this Act;
- (b) monitoring compliance with this Act and related policies of the data controller or data;
- (c) acting as the contact point for the Commission on issues relating to data processing.

34. The Commission may license a body or a person having an appropriate level of expertise in relation to data protection and this Act and any code of conduct for data controllers and data processors made hereunder to monitor, audit and report on compliance by data controllers and data processors with—

- (a) this Act, or
- (b) a code of conduct for data controllers and data processors made under this Act.

Data protection officers

Data protection compliance services

PART VII—RIGHTS OF A DATA SUBJECT

Rights of the
data subject

35. A data subject has the right to obtain from a data controller, without constraint or unreasonable delay—

- (a) confirmation as to whether or not the data controller, or a data processor operating on its behalf, is storing or otherwise processing personal data relating to the data subject and where that is the case:
 - (i) the purposes of the processing;
 - (ii) the categories of personal data concerned;
 - (iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - (iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (v) the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (vi) the right to lodge a complaint with the Commission;
 - (vii) where the personal data are not collected from the data subject, any available information as to their source; and
 - (viii) the existence of automated decision-making, including profiling, and significance and consequences for the data subject;
- (b) a copy of such personal data in a commonly used electronic format except to the extent that providing such data would impose unreasonable costs on the data controller, in which case the data subject may be required by the data controller to bear some or all of such costs;
- (c) correction, or if correction is not feasible or suitable, deletion of any such personal data that is inaccurate, out of date, incomplete or misleading;
- (d) the erasure of personal data concerning him without undue delay and the data controller shall have the obligation to erase personal data without undue delay where:

(i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or

(ii) the data controller has no other lawful basis to retain the personal data; and

(e) restriction of data processing pending resolution of a request or objection by the data subject under this Act or for the establishment, exercise or defence of legal claims.

Withdrawal of consent

36. — (1) A data subject has the right to withdraw his consent to processing of personal data under section 26(1)(a) or section 31(1)(a) at any time.

(2) The data controller shall ensure that it is as easy for the data subject to withdraw as to give consent.

Right to object

37. — (1) A data subject has the right to object on grounds relating to his particular situation to the processing of personal data relating to himself based on section 26(1)(b)(iv) or (v), including profiling.

(2) The data controller may no longer process such data unless it demonstrates a public interest or other legitimate grounds which override the fundamental rights and freedoms and the interests of the data subject.

(3) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

(4) Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Automated decision-making

38. — (1) A data subject has the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning him.

(2) Subsection (1) shall not apply where the decision is—

(a) necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) authorised by a written law which also establishes suitable measures to safeguard the fundamental rights and freedoms and the interests of the data subject; or

(c) authorised by the consent of the data subject.

(3) In the cases of paragraphs (a) and (c) of subsection (2), the data controller shall implement suitable measures to safeguard the data subject's fundamental rights and freedoms and interests, including at least the right—

- (a) to obtain human intervention on the part of the data controller;
- (b) to express his point of view; and
- (c) to contest the decision.

39. — (1) The Commission may make rules establishing a right of personal data portability.

Data portability

(2) Any such right of data portability established by the Commission shall entitle the data subject to:

- (a) receive without undue delay from a data controller personal data concerning him in a structured, commonly used and machine-readable format;
- (b) transmit the data obtained under paragraph (a) to another data controller without any hindrance; and
- (c) where technically possible, have the personal data transmitted directly from one data controller to another.

(3) The Commission may prescribe the circumstances in, and conditions on, which such a right would apply to a data subject and the obligations it would impose on a data controller or data processor, or categories of data controllers or data processors, including in relation to costs and timing.

PART VIII—DATA SECURITY

40. — (1) Each data controller and data processor shall implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorised disclosure or access, taking into account:

Security,
integrity and
confidentiality

- (a) the amount and sensitivity of the personal data;
- (b) the nature, degree and likelihood of harm to data subjects that could result from the loss, disclosure or other misuse of the personal data;
- (c) the extent of the processing;
- (d) the period of data retention; and

(e) the availability and cost of any technologies, tools or other measures to be implemented relative to the size of the data controller or data processor.

(2) Measures implemented under subsection (1) may include:

- (a) pseudonymization or other methods of de-identification of personal data;
- (b) encryption of personal data;
- (c) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services;
- (d) processes to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (e) periodic assessments of risks to processing systems and services, including without limitation where the processing involves the transmission of data over an electronic communications network;
- (f) regular testing, assessing and evaluation of the effectiveness of the measures implemented against current and evolving risks identified; and
- (g) regular updating of the measures and introduction of new measures to address shortcomings in effectiveness and accommodate evolving risks.

41. — (1) When a personal data breach has occurred with respect to personal data being stored or otherwise processed by a data processor, the data processor shall—

- (a) notify the data controller or data processor that engaged it without undue delay after becoming aware thereof, describing the nature of the personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned; and
- (b) respond without undue delay to all information requests from the data controller or data processor that engaged it as they may require to comply with their obligations under this section.

(2) When a personal data breach has occurred with respect to personal data being stored or otherwise processed by a data controller or a data processor acting on its behalf and is likely to result in a risk to the rights and freedoms of individuals, the data controller shall notify the Commission of the breach without undue delay and, where feasible, within seventy-two hours after having become aware of it, describing the nature of the

personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned.

(3) When such a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject—

- (a) the data controller shall communicate the personal data breach to the data subject without undue delay in plain and clear language, including advice about measures the data subject could take to mitigate effectively the possible adverse effects of the data breach; and
- (b) if a direct communication to the data subject under paragraph (a) would involve disproportionate effort or expense or is otherwise not feasible, the data controller may instead make a public communication in one or more widely-used media sources such that data subjects are likely to be informed.

(4) The notifications and communications referred to in subsections (1), (2) and (3) shall, in addition to the requirements of those subsections, at least:

- (a) communicate the name and contact details of a point of contact of the data controller where more information can be obtained;
- (b) describe the likely consequences of the personal data breach; and
- (c) describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) The data controller may extend the seventy-two-hour period set out in subsection (2) to accommodate the legitimate needs of law enforcement or as reasonably necessary to implement measures required to determine the scope of the breach, provided that the data controller provides to the Commission the grounds for such extension, including supporting evidence.

(6) The Commission may at any time make a public communication about a personal data breach notified to it under subsection (2) if it considers the steps of the data controller to inform data subjects inadequate.

(7) The Commission shall issue and publish Regulations on the steps to be taken by a data controller to adequately inform data subjects of a personal data breach for purposes of subsection (6).

(8) In evaluating whether a personal data breach is likely to result in a high risk to the rights and freedoms of

a data subject under subsection (3), the data controller and the Commission may take into account—

- (a) the likely effectiveness of any technical and administrative measures implemented to mitigate the likely harm resulting from the personal data breach, including any encryption or de-identification of the data;
- (b) any subsequent measures taken by the data controller to mitigate such risk; and
- (c) the nature, scope and sensitivity of the personal data involved.

(9) The data controller and data processor shall keep a record of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a manner that enables the Commission to verify compliance with this section.

(10) Where, and in so far as, it is not possible to provide information under this section at the same time, the information may be provided in phases without undue further delay.

PART IX—CROSS-BORDER TRANSFERS OF PERSONAL DATA

Basis for cross-border transfer of personal data

42. — (1) A data controller or data processor shall not transfer or permit to be transferred personal data from Nigeria to another country unless—

- (a) the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data in accordance with section 43; or
- (b) one of the conditions set forth in section 44 applies.

(2) A data controller or data processor shall record the basis for transfer of personal data to another country under subsection (1) and the adequacy of protection under section 43, if applicable.

(3) The Commission may make rules requiring data controllers and data processors to notify it of the measures in place under subsection (1) and to explain their adequacy in terms of section 43, if applicable.

(4) The Commission may designate categories of personal data that are subject to additional specified restrictions on transfer to another country based on the nature of such personal data and risks to data subjects.

43. — (1) A level of protection is adequate for the purposes of section 42(1)(a) if it upholds principles that are substantially similar to the conditions for processing of the personal data provided for in this Act, including in relation to the onward transfer of personal data to other countries.

(2) The adequacy of protection referred to in subsection (1) shall be assessed taking into account:

- (a) the availability of enforceable data subject rights, the ability of data subjects to enforce their rights through administrative or judicial redress, and the rule of law generally;
- (b) the existence of any legally binding instrument between the Commission and a relevant public Commission in the recipient country addressing elements of adequate protection referred to in subsection (1);
- (c) the access of a public authority to personal data;
- (d) the existence of an effective data protection law;
- (e) the existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement powers; and
- (f) international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.

(3) The Commission shall issue a guideline as to the assessment of adequacy and the factors set forth under subsection (2).

(4) The Commission may from time to time determine whether any country, region or specified sector within a country, or standard contractual clauses, afford an adequate level of protection under subsection (1).

(5) The Commission may approve binding corporate rules, codes of conduct or certification mechanisms proposed to it by a data controller, where the Commission determines that the aforesaid meets the adequacy requirements of subsection (1).

(6) The absence of a determination by the Commission under subsection (4) or (5) with respect to a country, territory, sector, binding corporate rule, contractual clause, code of conduct or certification mechanism shall not imply the adequacy of the protections afforded by it.

(7) The Commission may make a determination under subsection (4) based on adequacy decisions made by competent data protection authorities of other

jurisdictions where such decisions have taken into account factors similar to those listed in subsection (2).

Other bases for transfer of personal data outside Nigeria

44. In the absence of adequacy of protection under section 43, a data controller or data processor shall only transfer personal data from Nigeria to another country if—

- (a) the data subject has provided and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections;
- (b) the transfer is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
- (d) the transfer is for the sole benefit of the data subject and—
 - (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer, and
 - (ii) if it were reasonably practicable to obtain such consent, the data subject would likely give it;
- (e) the transfer is necessary for important reasons of public interest;
- (f) the transfer is necessary for the establishment, exercise or defence of legal claims; or
- (g) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

PART X—REGISTRATION AND FEES

45.— (1) Data controllers and data processors of major importance shall register with the Commission within six months after the commencement of the Act or becoming a data controller or data processor of major importance.

Registration of data controllers and data processors of major importance

(2) Registration under subsection (1) shall be made by notifying the Commission of—

- (a) name and address, or name and address of the data protection officer;

- (b) a description of the personal data and the categories and number of data subjects to which the personal data relate;
- (c) the purposes for which the personal data is processed;
- (d) the categories of recipients to whom the data controller or data processor intends or is likely to disclose the personal data;
- (e) the name and address, or name and address of any representative of any data processor operating directly or indirectly on its behalf;
- (f) any country to which the data controller or data processor intends, directly or indirectly, to transfer the personal data;
- (g) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data; and
- (h) any other information required by the Commission.

(3) The data controller or data processor of major importance shall notify the Commission of any significant change to the information submitted under subsection (2) within sixty days after such change.

(4) The Commission shall maintain and publish on its website a register of data controllers and data processors of major importance that have duly registered with it under this section.

(5) The Commission shall remove a data controller or data processor from the register if it notifies the Commission that it is no longer a data controller or data processor of major importance.

(6) The Commission may exempt a class of data controller or data processor of major importance from the registration requirements of this section where it considers such requirement to be unnecessary or disproportionate.

46. — (1) The Commission may prescribe fees or levies which shall be paid by data controllers and data processors of major importance.

(2) The Commission may prescribe fees or levies under subsection (1) applicable to different classes of data controllers or data processors of major importance.

PART XI—ENFORCEMENT

47. — (1) A data subject who is aggrieved by the decision, action or inaction of a data controller or data processor in violation of this Act, subsidiary legislation or orders may lodge a complaint with the Commission.

(2) The Commission shall investigate any complaint referred to it where it appears to the Commission that—

(a) the complainant has an interest in the matter to which the complaint relates; and

(b) the complaint is not frivolous or vexatious.

(3) The Commission may initiate an investigation of its own accord where it has reason to believe a data controller or data processor has violated or is likely to violate this Act or any regulations, rules or other subsidiary legislation or orders.

(4) The Commission may, for the purpose of an investigation, order any person to—

(a) attend at a specific time and place for the purpose of being examined orally in relation to a complaint;

(b) produce such document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other written law from disclosing; or

(c) furnish a statement in writing made under oath or an affirmation setting out all information which may be required under the order.

(5) Where material to which an investigation relates consists of information stored in any document, record, minute, mechanical or electronic device, the Commission may require the person named to produce or give access to and inspect it in a form in which it is visible and legible in a structured, commonly used and machine-readable format.

(6) The Commission may, where necessary, make representations to the data controller or data processor on behalf of a complainant or to a complainant on behalf of relevant the data controller or data processor, as the Commission may deem appropriate.

(7) The Commission shall establish a section that shall receive and follow up on complaints from data subjects and conduct investigations.

(8) The Commission shall adopt rules and procedures on handling complaints and conducting investigations referred to it under this Act.

48. — (1) Where the Commission is satisfied that a data controller or data processor has violated or is likely to violate any requirement under this Act or any regulations, rules or other subsidiary legislation or orders issued thereunder, the Commission may make an appropriate compliance order against that data controller or data processor.

(2) The order made by the Commission under subsection (1) may include any of the following—

- (a) a warning that certain acts or omissions are likely to be a violation of one or more provisions under this Act or any subsidiary legislation or orders issued thereunder;
- (b) a requirement that the data controller or data processor complies with such provisions, including complying with the requests of a data subject to exercise one or more rights under this Act; or
- (c) a cease and desist order requiring the data controller or data processor to stop or refrain from doing an act which is in violation of this Act, including stopping or refraining from processing personal data that is the subject of the order.

(3) An order made under this section shall be in writing and shall specify—

- (a) the provisions of this Act that the Commission is satisfied the data controller or data processor has violated or is likely to violate;
- (b) in the case of an actual violation, specific measures to be taken by the data controller or data processor to avoid, remedy or eliminate the situation which has resulted in the violation;
- (c) in the case of an actual violation, a period within which to implement such measures; and
- (d) in the case of an actual violation, a right to judicial review under section 51.

49. — (1) Notwithstanding any criminal sanctions under this Act, if the Commission, after completing an investigation under Section 47, is satisfied that a data controller or data processor has violated any provision of this Act, or any regulation, rule or other subsidiary legislation made thereunder, it—

- (a) may make any appropriate enforcement order or impose a sanction on the data controller or data processor; and
- (b) shall inform the data controller or data processor, and if applicable, any data subject who lodged a

complaint leading to the investigation, in writing of its decision.

(2) An enforcement order made or sanction imposed under subsection (1) include the following—

- (a) requiring the data controller or data processor to remedy the violation;
- (b) ordering the data controller or data processor to pay compensation to a data subject who suffers injury, loss or harm as a result of a violation;
- (c) ordering the data controller or data processor to account for the profits made out of the violation; or
- (d) ordering the data controller or data processor to pay a penalty.

(3) A penalty under subsection (2)(d) may be an amount up to—

- (a) in the case of a data controller or data processor of major importance, the higher maximum amount; and
- (b) in the case of a data controller or data processor other than a data controller or data processor of major importance, the standard maximum amount.

(4) The “higher maximum amount” shall be the greater of:

- (a) ₦10,000,000, and
- (b) two percent of its annual gross revenue derived from Nigeria in the preceding financial year.

(5) The “standard maximum amount” shall be the greater of:

- (a) ₦2,000,000, and
- (b) two percent of its annual gross revenue derived from Nigeria in the preceding financial year.

(6) In determining the sanctions, the Commission shall take into consideration the following factors:

- (a) the nature, gravity, and duration of the infringement;
- (b) the purpose of the processing;
- (c) the number of data subjects involved;
- (d) the level of damage and damage mitigation measures implemented;
- (e) intent or negligence;
- (f) degree of cooperation with the Commission; and
- (g) types of personal data involved.

Offence

50. A data controller or data processor who fails to comply with orders made under section 49 commits an offence for which such data controller or data processor is liable on conviction to:

(a) a fine of up to—

(i) in the case of a data controller or data processor of major importance, the higher maximum amount, and

(ii) in the case of a data controller or data processor other than a data controller or data processor of major importance, the standard maximum amount,

in each case as provided in section 49; or

(b) imprisonment for up to one year; or

(c) both fine and imprisonment.

Judicial review

51. A person who is not satisfied with an order of the Commission may apply to the appropriate court within thirty days after the date the order was made for judicial review thereof.

Civil remedies

52. A data subject who suffers injury, loss or harm as a result of a violation of this Act by a data controller or data processor, or a recognized consumer organization acting on behalf of such a data subject, may recover damages by way of civil proceedings in the appropriate court from such data controller or data processor.

Forfeiture

53. — (1) The Court may order that a convicted data controller or individual forfeit to the Government of the Federal Republic of Nigeria in accordance with the Proceeds of Crime (Recovery and Management) Act or any other similar law.

(2) For the purpose of subsection (1) the Commission shall be a “Relevant Organisation” under the Proceeds of Crime (Recovery and Management) Act.

Joint and vicarious liability

54. — (1) Where any offence against any provision of this Act has been committed by a body corporate or firm, a person who was a director, manager, partner, secretary or other similar officer of the body corporate or firm purporting to and in such capacity is, in addition to the body corporate or firm, deemed to have committed that offence unless he proves that—

(a) the offence was committed without his consent or connivance; and

(b) that he exercised all such diligence to prevent the commission of the offence as he ought to have exercised having regard to the nature of his functions in that capacity and to all the circumstances.

(2) Each data controller and data processor shall be vicariously liable for the acts or omissions of its agent, clerk, servant or other person, in so far as the acts or omissions relates to its business.

PART XII – LEGAL PROCEEDINGS

55. — (1) No suit shall be instituted against the Commission, or any officer or employee of the Commission, for any act done in pursuance or execution of this Act, any law, or any public duty of the Commission, unless—

Procedure in respect
of suits against the
Commission

- (a) it is commenced within three months after the act, neglect or default complained of; or
- (b) in the case of continued damage or injury, within three months after the ceasing of such act, neglect or default complained of.

(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 Cap P41, LFN, 2004 shall apply in relation to any suit instituted against an official or employee of the Commission.

56. 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 National Commissioner at the Head Office of the Commission.

Service of documents

57. — (1) 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.

Restriction on
execution against
property of the
Commission

(2) Any sum of money which may be the judgement of any court awarded against the Commission shall be paid from the Fund of the Commission.

Indemnity of staff,
members, and
employees of the
Commission

58. The Commission shall indemnify the National Commissioner, or other officers of the Commission or employees out of the assets of the Commission against losses, charges, claims, expenses and liabilities incurred by such person in the execution or discharge of his duties or in relation to him defending any criminal or civil proceedings in which judgement is given in his favour or in which he is otherwise acquitted or the proceedings are otherwise disposed of without any finding or admission of any material breach of duty on his part or in which the court grants him relief from liability for negligence, default, breach of duty or breach of trust in relation to the Commission.

Power of arrest,
search, and seizure

59. — (1) The Commission may apply *ex-parte* to a Judge in Chambers for the issuance of a warrant for the purpose of obtaining evidence in relation to an investigation.

(2) A Judge may issue a warrant under subsection (1) upon the satisfaction that —

- (a) a person has engaged or is engaging or likely to engage in conduct which contravenes the provisions of this Act;
- (b) the warrant is sought to prevent the commission of an offence under this Act or
- (c) the warrant is sought to prevent the interference with investigative process under this Act;
- (d) the warrant is for the purpose of investigating, data security breaches and data privacy breaches, or obtaining electronic evidence; or
- (e) the object or subject named in the warrant is preparing to commit an offence under this Act.

(3) A warrant issued under subsection (2) shall authorise the Commission to—

- (a) in the company of a law enforcement officer, enter and search any premises, where—
 - (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 the Commission is

authorised to enter and search under paragraph (a) of this subsection;

- (c) stop, enter, and search any conveyance;
- (d) seize, seal, remove or detain anything which is, or contains evidence of the commission of an offence under this Act;
- (e) use or cause to be use a computer or 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.

60. A legal officer of the commission or a private legal practitioner engaged by the Commission may represent the commission in civil proceedings in the name of and on behalf of the Commission in respect of matters relating to the business or operations of the Commission.

Right to appear in court

PART XIII—MISCELLANEOUS

61. — (1) The Commission may make regulations for carrying out its objectives under this Act.

Regulations

(2) Without prejudice to the generality of subsection (1), the regulations may provide for—

- (a) the financial management of the affairs of the Commission;
- (b) the protection of personal data and data subjects;
- (c) the manner in which the Commission may exercise any power or perform any duty or function under this Act;
- (d) any matter that under this Act is required or permitted to be prescribed;
- (e) the forms of applications and related documents required for the purposes of this Act;
- (f) the procedures to be followed under this Act in the submission of complaints to the Commission;
- (g) fees, fines and charges prescribed under this Act, and such related matters; and

(h) any matter that the Commission considers necessary or expedient to give effect to the objectives of this Act.

(3) The regulations made under this Act may create offences in respect of any contravention to the regulations and may for any such contravention impose a fine not exceeding ₦50,000,000 and to imprisonment for up to five years.

(4) The Commission may, prior to making any regulation under this Act, publish on its website, the draft regulation and a notice inviting comments to be submitted on the proposed regulation within a stipulated time.

Exemption from
taxation

62. — The Commission shall be exempted from all taxes, fees, penalties, charges, duties, levies, or other like imposts payable to any institution, agency, department or authority of the Federal Government, State Government, Federal Capital Territory, Local Government or Area Councils of the Federal Capital Territory, save income tax payable by staff of the Commission, value added tax and withholding tax which are payable by any third parties under any contract entered into by such third parties with the Commission.

63. Where any of the provisions of any other law or enactment, in so far as they provide or relate directly or indirectly to the processing of personal data, is inconsistent with any of the provisions of this Act, the provisions of this Act shall prevail.

64. (1) As it relates to the provisions of this Act, the Commission is the successor-in-title in every way to the power, duties and functions of the existing Nigeria Data Protection Bureau.

Transitional
provisions

(2) For the purpose of subsection (1)–

(a) all staff of the Nigeria Data Protection Bureau prior to the commencement of this Act shall be deemed to be staff of the Commission on terms and conditions not less favourable than that enjoyed prior to the transfer of service and shall be deemed to be service for employment related entitlements as specified under any applicable law.

(b) all existing agreements and compacts currently in effect by the Nigeria Data Protection Bureau as it relates to the provisions of this Act shall continue;

(c) all records and equipment previously belonging to or allocated for use to the Nigeria Data Protection Bureau shall become, on the effective date of this

Act, part of the records and equipment of the Commission; and

- (d) all orders, rules, regulations, decisions, directions, licenses, authorizations, certificates, consents, approvals, declarations, permits, registrations, rates or other documents that are in force before the coming into force of this Act and that are made or issued by National Information Technology Development Agency or Nigeria Data Protection Bureau shall continue in force as if they were made or issued by the Commission until they expire or are repealed, replaced, reassembled or altered.

65. In this Act, unless the context otherwise requires—

Interpretation

“automated decision-making” means a decision based solely by automated processing by automated means, without any human involvement;

“applicable law” means any law enacted by the National Assembly or House of Assembly of any State in Nigeria;

“binding corporate rules” means personal data protection policies and procedures adhered to by the members of a group of firms under common control with respect to the transfer of personal data among such members and containing provisions for the protection of such personal data;

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis;

“certification mechanism” means certification by an official or professional third-party entity that evaluates the personal data protection policies and procedures of data controllers and data processors according to recognised standards;

“child” has the meaning ascribed in the Child’s Right Act;

“Commission” means the Nigeria Data Protection Commission established under this Act;

“consent” means any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual’s agreement to the processing of personal data relating to him or to another individual on whose behalf he has the Commission to provide such consent;

“Council” means the Governing Council of the Commission established under this Act;

“competent authority” means the Government of Federal Republic of Nigeria or any state government or any statutory authority, government authority, institution, agency, department, board, commission, exercising executive, legislative, judicial, investigative, regulatory or administrative functions, pursuant to any applicable law.

“court” means a High Court or Federal High Court;

“data controller” means an individual, private entity, public Commission or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal data;

“data controller or data processor of major importance” means a data controller or data processor that is domiciled, ordinarily resident, or ordinarily operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate;

“data processor” means an individual, private entity, public authority or agency or any other body who or which processes personal data on behalf of or at the direction of a data controller or another data processor;

“data subject” means an individual to whom personal data relates;

“filing system” means any structured set of personal data which is accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

“Minister” means the Minister charged with the responsibility of matters relating to communications and digital economy;

“National Commissioner” means the National Commissioner for Data Protection;

“ordinarily resident” means with respect to an individual whose physical presence in Nigeria is for a period not less than 183 days in one calendar year;

“ordinarily operating in Nigeria” means to conduct, operate, prosecute or continue a particular vocation or business as a continuous operation or permanent occupation whether operated for profit or not;

“personal data” means any information relating to an individual who can be identified or is identifiable, directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to

the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual;

“personal data breach” means a breach of security of a data controller or data processor leading to or reasonably likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

“President” means the President and Commander-in-Chief of the Armed Forces of the Federal Republic of Nigeria;

“processing” means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and does not include the mere transit of data originating outside Nigeria through the country;

“pseudonymization” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

“sensitive personal data” means personal data relating to an individual’s—

- (a) genetic and biometric data, for the purpose of uniquely identifying a natural person;
- (b) race or ethnic origin;
- (c) religious or similar beliefs, such as those reflecting conscience or philosophy;
- (d) health status;
- (e) sex life;
- (f) political opinions or affiliations;
- (g) trade union memberships; or
- (h) any other personal data prescribed by the Commission as sensitive personal data pursuant to section 31(2).

“social security laws” means “the Employee Compensation Act, Pension Reform Act, National Health Insurance Authority Act, National Housing Fund Act, Nigeria Social Insurance Trust Fund Act, Industrial Trust Fund Act or any other similar law.

SCHEDULE I

SUPPLEMENTARY PROVISIONS RELATING TO PROCEEDINGS OF THE COUNCIL

Council to Regulate Proceedings

1. Subject to the provisions of this Act, the Council may make standing orders regulating the proceedings of the Council and set up any Committee. The Council shall meet once per quarter.

Presiding Officer

2. Every meeting of the Council shall be presided over by 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.

Quorum

3. The quorum at a meeting of the Council shall be the Chairman or in an appropriate case, the person presiding at the meeting under paragraph 2 of this Schedule and four other members, and the quorum of any committee of Council shall be determined by the Council.

Voting

4. At a meeting of the Council, each member present shall be entitled to one vote and any question on which a vote is required shall be determined by a majority of votes of members present and voting but, in the case of an equal division of votes, the Chairman or the member presiding over the meeting shall have a casting vote.

5. Where the Council seeks the advice of any person on a particular nature, the Council may invite that person to attend for such period as it deems fit, but a person who is invited by virtue of this paragraph shall not be entitled to vote at any meeting of the Council and shall not count towards the quorum.

Teleconference Meeting

6. (1) In addition to meeting with all participants physically present, the Council may hold or continue a meeting by the use of any means of communication by which all the participants can hear and be heard at the same time and such a meeting is referred to in this paragraph as a "tele-conference meeting".

(2) A member of the Council who participates in a teleconference meeting shall be taken for all purposes to have been present at the meeting.

(3) The Council may establish procedure for tele-conference meetings (including recording the minutes of such meetings) in its minute's book.

Committees of the Council

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

(2) Every Committee appointed under the provisions of subparagraph (1) of this paragraph shall be presided over by a member of the Council and shall be made up of such number of persons, as the Council may determine in each case.

8. The decision of a Committee is of no effect until it is approved or ratified by the Council.

Seal of the Commission

9. The fixing of the seal of the Commission shall be done by the Secretary of the Commission and authenticated by the signature of the National Commissioner or such other member authorised generally or specifically by the Commission to act for that purpose.

10. 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 by the National Commissioner or by any other officer or staff generally or specifically authorised by the National Commissioner to act for that purpose.

11. Any document purporting to be a contract, an instrument or other document signed or sealed on behalf of the Commission shall be received in evidence and shall, unless the contrary is proved, be presumed, without further proof, to have been so signed and sealed.

Miscellaneous

12. The validity of a proceeding of the Council or its Committee is not adversely affected —

(a) by any vacancy in the membership of the Council;

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

13. (1) A member of the Council 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 shall:

- (a) disclose to the members of the Council the nature of his interest in advance of any consideration of the matter;
 - (b) not influence nor seek to influence a decision to be made in relation to the matter;
 - (c) take no part in any consideration of the matter; and
 - (d) absent himself from the meeting or that part of the meeting during which the matter is discussed.
- (2) If a member of the Council discloses an interest pursuant to paragraph 12(1), the disclosure shall be recorded in the minutes of the meeting of the Council.

OBJECTS AND REASONS

[to be added]

Attorney General