

NIGERIA DATA PROTECTION ACT, 2023

EXPLANATORY MEMORANDUM

This Act provides a legal framework for the protection of personal information and establishes the Nigeria Data Protection Commission for the regulation of the processing of personal information.

NIGERIA DATA PROTECTION ACT, 2023

Arrangement of Sections

Section:

PART I — OBJECTIVES AND APPLICATION

1. Objectives
2. Application
3. Exemption of application

PART II — ESTABLISHMENT OF THE NIGERIA DATA PROTECTION COMMISSION, AND ITS GOVERNING COUNCIL

4. Establishment of the Nigeria Data Protection Commission
5. Functions of the Commission
6. Powers of the Commission
7. Independence of the Commission
8. Establishment of the Governing Council of the Commission
9. Appointment of members of the Council
10. Tenure of members of the Council
11. Cessation of membership
12. Functions and powers of the Council
13. Conflict of interest

PART III — APPOINTMENT OF THE NATIONAL COMMISSIONER, AND OTHER STAFF OF THE COMMISSION

14. Appointment of the National Commissioner for the Commission
15. Secretary to the Council
16. Staff of the Commission
17. Staff regulations and discipline
18. Pension

PART IV — FINANCIAL PROVISIONS

19. Funds of the Commission
20. Expenditure of the Fund
21. Power to borrow and accept gifts
22. Account and audit
23. Annual reports and estimates

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

24. Principles of personal data processing
25. Lawful basis of personal data processing
26. Consent
27. Provision of information to the data subject

- 28. Data privacy impact assessment
- 29. Obligations of the data controller and data processor
- 30. Sensitive personal data
- 31. Children or persons lacking the legal capacity to consent
- 32. Data Protection Officers
- 33. Data protection compliance services

PART VI — RIGHTS OF A DATA SUBJECT

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

PART VII — DATA SECURITY

- 39. Security, integrity, and confidentiality
- 40. Personal data breaches

PART VIII — CROSS-BORDER TRANSFERS OF PERSONAL DATA

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

PART IX — REGISTRATION AND FEES

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

PART X — ENFORCEMENT

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

PART XI — LEGAL PROCEEDINGS

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

PART XII — MISCELLANEOUS PROVISIONS

- 60. Directives by the Minister

- 61. Regulations
 - 62. Directives, codes, and guidelines
 - 63. Priority of the Act
 - 64. Transitional provisions
 - 65. Interpretation
 - 66. Citation
- Schedule

NIGERIA DATA PROTECTION ACT, 2023

A Bill

For

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

[] Commencement

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

PART I — OBJECTIVES AND APPLICATION

1. The objectives of this Act are to —

Objectives

- (a) safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999;
- (b) provide for the regulation of processing of personal data;
- (c) promote data processing practices that safeguard the security of personal data and privacy of data subjects;
- (d) ensure that personal data is processed in a fair, lawful and accountable manner;
- (e) protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights;
- (f) ensure that data controllers and data processors fulfil their obligations to data subjects;
- (g) establish an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues, and supervise data controllers and data processors; and
- (h) strengthen the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data.

2. (1) This Act shall apply to the processing of personal data, whether by automated means or not. Application

(2) This Act shall apply, where the —

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

3. (1) This Act shall not apply to the processing of personal data carried out by one or more persons solely for personal or household purposes: Exemption of application

Provided that such processing for personal or household purposes does not constitute a violation of fundamental right to privacy of a data subject.

(2) Subject to the rights and freedoms under the Constitution and the limitations, the obligations under Part V, other than sections 24, 25, 32, and 40 of this Act, shall not apply to a data controller or data processor if the processing of personal data is —

- (a) carried out by a competent authority for the purposes of the prevention, investigation, detection, prosecution, or adjudication of a criminal offence or the execution of a criminal penalty, in accordance with any applicable law;
- (b) carried out by a competent authority for the purposes of prevention or control of a national public health emergency;
- (c) carried out by a competent authority, as is necessary for national security;
- (d) in respect of publication in the public interest, for journalism, educational, artistic and literary purposes to the extent that such obligations and rights are incompatible with such purposes; or
- (e) necessary for the establishment, exercise, or defense 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 may be exempted from application of this Act.

(4) Notwithstanding the provisions of this Act, the Commission may issue a guidance notice containing legal safeguards and best practices to a data controller or processor, in respect of any aspect of data processing exempted under this section where in the opinion of the Commission, such processing violates or is likely to violate sections 24

and 25 of this Act.

PART II — ESTABLISHMENT OF THE NIGERIA DATA PROTECTION COMMISSION, AND ITS GOVERNING COUNCIL

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

Establishment of
Nigeria Data
Protection
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 acquire, hold and dispose of its property.

- (3) The Commission —

- (a) shall have its head office in the Federal Capital Territory; and
- (b) may maintain other offices, in any part of Nigeria, for the purposes of achieving the objects of the Commission.

- (4) Subject to the approval of the Council, the National Commissioner may acquire other offices and premises for the use of the Commission.

5. The Commission shall —

Functions of the
Commission

- (a) regulate the deployment of technological and organisational measures to enhance personal data protection;
- (b) foster the development of personal data protection technologies, in accordance with recognised international best practices and applicable international law;
- (c) where necessary, accredit, license, and register suitable persons to provide data protection compliance services;
- (d) register data controllers and data processors of major importance;
- (e) promote awareness on the obligation of data controllers and data processors under this Act;
- (f) promote public awareness and understanding of personal data protection, rights and obligations imposed under this Act, and the risks to personal data;
- (g) receive complaints relating to violations of this Act or subsidiary legislation made under this Act;

- (h) collaborate with any relevant ministry, department, agency, body, company, firm, or person for the attainment of the objectives of this Act;
- (i) ensure compliance with national and international personal data protection obligations and best practice;
- (j) participate in international fora and engage with national and regional authorities responsible for data protection with a view to developing efficient strategies for the regulation of cross-border transfers of personal data;
- (k) determine whether countries, regions, business sectors, binding corporate rules, contractual clauses, codes of conduct, or certification mechanisms, afford adequate personal data protection standards for cross-border transfers;
- (l) collect and publish information with respect to personal data protection, including personal data breaches;
- (m) advise government on policy issues relating to data protection and privacy;
- (n) submit legislative proposals to the Minister necessary for strengthening personal data protection in Nigeria; and
- (o) carry out other legal actions as are necessary for the performance of the functions of the Commission.

6. The Commission shall have powers to —

Powers of the
Commission

- (a) oversee the implementation of the provisions of this Act;
- (b) prescribe fees payable by data controllers and data processors in accordance with data processing activities;
- (c) issue regulations, rules, directives and guidance under this Act;
- (d) prescribe the manner and frequency of filing, and content of compliance returns by data controllers and data processors of major importance to the Commission;
- (e) call for information from a person, or inspect any documents with respect to any thing done under this Act;
- (f) conduct investigations into any violation of a requirement under this Act or subsidiary legislation made under this Act by a data controller or a data processor;
- (g) impose penalties in respect of any violation of the provisions of this Act or subsidiary legislation made under this Act;

- (h) acquire assets, and sell, let, lease, or dispose of any of its property; and
- (i) perform such other acts as are necessary to give effect to the functions of the Commission.

7. The Commission shall be independent in the performance of its functions under this Act. Independence of Commission

8. (1) There shall be for the Commission, a Governing Council (in this Act referred to as "the Council"), which shall consist of — Establishment of Governing Council of the Commission
 - (a) a part-time Chairman, who shall be a retired judge of Nigeria;
 - (b) the National Commissioner;
 - (c) a representative, not below the rank of a Director or its equivalent, from —
 - (i) the Federal Ministry responsible for Justice,
 - (ii) the Federal Ministry responsible for communications and digital economy,
 - (iii) the Central Bank of Nigeria, and
 - (iv) a law enforcement agency; and
 - (d) one representative from the private sector.
- (2) Members of the Council other than the National Commissioner shall be paid such allowances as may be determined, in collaboration with the Revenue Mobilisation Allocation and Fiscal Commission.
- (3) The supplementary provisions set out in the Schedule to this Act shall apply with respect to the proceedings of the Council, and other matters contained in it. Schedule

9. (1) The Chairman and non-*ex-officio* members of the Council shall be appointed by the President, on the recommendation of the Minister. Appointment of members of the Council
- (2) A member appointed to the Council under section 8 of this Act from —
 - (a) the private sector shall be a Nigerian and possess not less than five years cognate experience and proficiency in data protection and privacy; and
 - (b) government, under section 8(1)(c) of this Act, may have proficiency in data protection and privacy.

10. (1) Members of the Council other than the National Commissioner shall be part-time members.

Tenure of meml
of the Council

(2) The Chairman and non-*ex-officio* members of the Council shall hold office —

- (a) for a term of four years, and may be eligible for re-appointment for another term of four years, and no more; and
- (b) on such terms and conditions, as may be specified in their letters of appointment.

11. (1) A person shall cease to be a member of the Council, where the person —

Cessation of
membership

- (a) dies;
- (b) becomes bankrupt or compounds with his creditors;
- (c) is convicted of a felony or any offence involving dishonesty or fraud;
- (d) is disqualified from professional qualification;
- (e) is guilty of a serious misconduct with regard to the discharge of the person's duties;
- (f) under section 8(1)(c) of this Act, ceases to occupy the office by virtue of which he became a member of the Council; or
- (g) resigns from appointment by giving at least two months' notice, in writing, addressed to the President.

(2) The President, on the recommendation of the Minister, may remove a member of the Council, where satisfied that it is not in the interest of the Commission or the public that the member continues in that office.

(3) Where a member of the Council ceases to hold office before the expiration of the term, the President shall appoint a person to fill the vacancy, and the person so appointed shall hold office for the remainder of the term of office of that member.

12. (1) The functions of the Council are to —

Functions and
powers of the
Council

- (a) formulate and provide overall policy direction of the affairs of the Commission;
- (b) approve strategic plans, action plans and budget support programmes submitted by the National Commissioner;
- (c) approve annual reports and financial reports submitted by the National

Commissioner;

- (d) approve 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) approve staff regulations for the appointment, promotion and discipline of staff of the Commission;
- (f) provide advice and counsel to the National Commissioner;
- (g) assist the National Commissioner in matters relating to compliance by ministries, departments and agencies of government with this Act; and
- (h) handle such other matters, as may be prescribed by any other provision of this Act.

Act No. 4, 2014

- (2) The Council shall have the power to delegate any of its functions under this Act to a committee set up by it, in accordance with the provisions of this Act.

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

Conflict of interest

- (a) ensure that personal interest shall not conflict with the member's duties under this Act;
 - (b) not make secret profit in the course of discharging official duties;
 - (c) fully disclose to the Council any personal, commercial, financial, or other interest, which may directly or indirectly hold or be connected with the business of the Commission or becomes the subject of consideration by the Council;
 - (d) subject to subsection (3), be ineligible to participate in any Council deliberation and voting-related matter; and
 - (e) not accept any gift or advantage in whatever form or manner, for anything done or likely to be done with respect to the responsibilities of the Council.
- (2) A member of the Council, who contravenes the provisions of paragraphs (b) and (e), commits an offence and is liable on conviction to —
- (a) in the case of a contravention of paragraph (b), a fine of at least N10,000,000 or imprisonment for a term not more than three years, or both; or

- (b) in the case of a contravention of paragraph (d), a fine of at least N 5,000,000, or imprisonment for a term not more than two years, or both.

PART III — APPOINTMENT OF THE NATIONAL COMMISSIONER, AND OTHER STAFF OF THE COMMISSION

14. (1) There shall be for the Commission, a National Commissioner, who shall be —

Appointment of
National
Commissioner
the Commission

- (a) appointed by the President, on the recommendation of the Minister;
- (b) the chief executive and accounting officer of the Commission; and
- (c) responsible for the execution of the policies and administration of the affairs of the Commission.

(2) The National Commissioner shall —

- (a) hold a certification in data protection from a training body which is duly accredited in line with international best practices; and
 - (b) possess at least 10 years cognate experience, at a senior management level, in data protection, cybersecurity management, information and communication technology, law, consumer protection, management science, or other relevant disciplines.
- (3) A person appointed as the National Commissioner shall not hold any other management position in a Ministry, Department, or Agency of Government, corporation, company, or any other business establishment.
- (4) The National Commissioner shall hold office —
- (a) for a term of five years, and may be re-appointed for another term of five years, and no more; and
 - (b) on such other terms and conditions as may be specified in the letter of appointment.

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

Secretary to the
Council

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

16. The Commission shall, subject to the approval of the Council, recruit directly or by secondment from the Public Service of the Federation, such number of staff, as it deems necessary and expedient — Staff of the Commission
- (a) for the proper and efficient performance of its functions; and
 - (b) on such terms and conditions, with remunerations, allowances, and benefits.
17. (1) The Commission may make staff regulations relating generally to the conditions of service of the staff, and such regulations may provide for — Staff regulation discipline
- (a) the appointment, promotion, and disciplinary control of staff of the Commission; and
 - (b) appeals by staff against dismissal or other disciplinary measures:
- Provided that pending the making of such staff regulations, any instrument relating to conditions of service in the Public Service of the Federation shall be applicable, with such modifications, as may be necessary to the staff of the Commission.
- (2) The staff regulations made under subsection (1) shall not have effect until approved by the Council.
18. (1) Staff of the Commission shall be entitled to pension and other retirement benefits, as prescribed under the Pension Reform Act. Pension
- (2) Without prejudice to the provisions of subsection (1), nothing in this Act shall prevent the appointment of a person to any office on conditions, which preclude the grant of pension and other retirement benefits in respect of that office. Act No. 4, 201
- (3) For the application of the provisions of the Pension Reform Act, any power exercisable by a Minister or other authority of the Federal Government, other than the power to make regulations under the Pension Reform Act, shall be vested in, and exercisable by the Council.

PART IV — FINANCIAL PROVISIONS

19. (1) The Commission shall establish a Fund (in this Act referred to as "the Fund") for the performance of its functions under this Act. Fund of the Commission
- (2) There shall be paid into the Fund established under subsection (1) —
- (a) a take-off grant as may be appropriated by the National Assembly which shall be drawn in the following manner —

- (i) 20% of the take-off grant shall be from the Consolidated Revenue Fund of the Federation,
 - (ii) 40% of the take-off grant shall be from the Nigerian Communications Commission, and
 - (iii) 40% of the take-off grant shall be from the National Information Technology Development Agency;
 - (b) donations, gifts, loans, grants, aids, endowments, and voluntary contributions;
 - (c) returns on investments of the Commission;
 - (d) levies, fees, penalties, and fines collected by the Commission; and
 - (e) such other money or assets that may accrue to the Commission.
- (3) 50% of the total amount of the take-off grant shall be provided to the Commission on the commencement of this Act, and the remaining 50% of the take-off grant shall be provided on the anniversary of the date on which this Act commences.
- (4) Subject to any applicable law, the Commission may borrow such sums of money, as may be required in the performance of its functions under to this Act.

20. (1) There shall be chargeable to the Fund —

Expenditure of
Fund

- (a) the cost of administration of the Commission;
 - (b) allowances and remuneration payable to members of the Council;
 - (c) remunerations, allowances, retiring benefits, such as pensions and gratuities, and such other money payable to the staff of the Commission;
 - (d) the payment for consultancies and contracts, including mobilisation, fluctuations, variations, and legal fees;
 - (e) expenses necessary to meet capital expenditure, such as, for the purchase, acquisition, or maintenance of property or other equipment of the Commission;
 - (f) repayment of funds borrowed by the Commission, including interest on such borrowed funds; and
 - (g) any other expenditure, approved by the Council, for the purposes of performing the functions of the Commission under this Act.
- (2) The Fund of the Commission shall be managed in accordance with the rules made by

the Council.

21. (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 under this Act. Power to borrow
accept gifts
- (2) The Commission may accept gifts, grants of money, aids, or other assets, provided that the terms and conditions of the acceptance are consistent with the objectives and functions of the Commission under this Act.
22. (1) The Commission shall keep and maintain proper accounts and records, including records of — Account and au
- (a) receipts, payments, assets, and liabilities; and
- (b) income and expenditure, in a form which conforms with existing laws on accounts and audit.
- (2) The Commission shall cause the accounts to be audited, not later than six months after the end of each year, by auditors appointed from the list maintained by the Auditor-General for the Federation, and in accordance with the guidelines provided by the Auditor-General for the Federation.
- (3) An auditor appointed under subsection (2) shall have full and free access to all account records, documents, and papers of the Commission.
- (4) For the purpose of this section, the financial year of the Commission shall be from 1 January to 31 December of every year, or such other period, as may be determined by the Council.
23. (1) The Commission shall, not later than six months after the end of each financial year, submit to the National Assembly through the Minister — Annual report
estimates
- (a) a report of its activities during the preceding year, including the audited accounts of the Commission; and
- (b) an estimate of the expenditure and income for the next succeeding year.
- (2) Notwithstanding the provisions of subsection (1), the Commission may, in any financial year, submit supplementary or adjusted statements of estimated income and expenditure to the National Assembly.

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

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

- (a) processed in a fair, lawful and transparent manner;
 - (b) collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these 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 not 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 is collected or is further processed; and
 - (f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.
- (2) A data controller and data processor shall use appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data.
- (3) 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.
- (4) For the purposes of subsection (1) (b) —
- (a) compatibility of further processing shall be assessed considering —
 - (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 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, historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes.

25. (1) Without prejudice to the principles set out in this Act, data processing shall be lawful, where —

Lawful basis of
personal data
processing

(a) the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed; or

(b) the processing is necessary —

(i) for the performance of a contract to which the data subject is a party or 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) to protect the vital interest of the data subject or another person,

(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 in personal data processing shall not be legitimate for the purposes of subsection (1) (b)(v), where—

(a) they override the fundamental rights, freedoms and the interests of the data subject;

(b) they are incompatible with other lawful basis of processing under subsection (1)(b) (i)-(iv); or

(c) the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

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

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

(3) Silence or inactivity of 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 be informed of the right to withdraw consent, prior to the granting of consent.

(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) A request for consent shall be in clear and simple language and accessible format.

(7) Consent —

(a) shall be in the affirmative, and not based on a pre-selected confirmation;
and

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

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

Provision of
information to
data subject

(a) identity, residence or place of business of, and means of communication with the data controller and its representatives, where necessary;

(b) specific lawful basis of processing under section 25(1) or 30(1) of this Act, and the purposes of the processing for which the personal data are intended;

(c) recipients or categories of recipients of the personal data, if any;

(d) existence of the rights of the data subject under Part VI;

(e) retention period for the personal data;

(f) right to lodge a complaint with the Commission in accordance with section 46 (1) of this Act; and

(g) existence of automated decision-making, including profiling, the significance and envisaged consequences 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, the data controller shall inform the data subject of the matters set out in subsection (1), except where the —

(a) data subject already has been provided with such information; or

(b) provision of such information is impossible or would involve a disproportionate effort or expense.

(3) The information referred to in subsection (1) shall be contained in a privacy policy and expressed in clear, concise, transparent, intelligible, and easily accessible format,

taking into consideration the class of data subjects targeted by the data processing.

28. (1) Where the processing of personal data may likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes, a data controller shall, prior to the processing, carry out a data privacy impact assessment. Data privacy impact assessment
- (2) The data controller shall consult the Commission prior to the processing if, notwithstanding the measures envisaged under this section, the data protection impact assessment indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.
- (3) The Commission may make regulations or issue directives with regards to this section, including the categories of processing and persons subject to the requirement for the conduct of a data privacy impact assessment.
- (4) For purposes of this section, a “data privacy impact assessment” is a process designed to identify the risks and impact of the envisaged processing of personal data, and it comprises —
- (a) a systematic description of the envisaged processing and its purpose, including 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 a data subject; and
 - (d) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data, taking into account the rights and legitimate interests of a data subject and other persons concerned.
29. (1) Where a data controller engages the services of a data processor, or a data processor engages the services of another data processor, the data controller or data processor engaging another shall ensure that the engaged data processor — Obligations of data controller and data processor
- (a) complies with the principles and obligations set out in this Act as applicable to the data controller;
 - (b) assists the data controller or data processor, as the case may be, by the use of appropriate technical and organisational measures, in the fulfilment of the data controller’s obligations to honour the rights of a data subject under Part VI;
 - (c) implements appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data as required in Part VII;

(d) provides the data controller or engaging data processor, where applicable, with information reasonably required to comply and demonstrate compliance with this Act; and

(e) notifies the data controller or engaging data processor, where applicable, when a new data processor is engaged.

(2) The 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.

30. (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 the —

Sensitive personal data

(a) data subject has given and not withdrawn consent to the processing for the specific purpose or purposes for which it will be processed;

(b) processing is necessary for the purposes of performing the obligations of the data controller or exercising rights of the data subject under employment or social security laws or any other similar laws;

(c) processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities, with appropriate safeguards, by a foundation, association, or such other non-profit organisation with charitable, educational, literary, artistic, philosophical, religious, or trade union purposes, and the —

(i) processing relates solely to the members or former members of the entity, or to persons, who have regular contact with it in connection with its purposes, and

(ii) sensitive personal data is not disclosed outside of the entity without the explicit consent of the data subject;

(e) processing is necessary for the establishment, exercise, or defense of a legal claim, obtaining legal advice, or conduct of a legal proceeding;

(f) 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, freedoms and interests of the data subject;

(g) processing is carried out for purposes of medical care or community welfare,

and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality;

- (h) processing is necessary for reasons of public health and provides for suitable and specific measures to safeguard the fundamental rights, freedoms and interests of the data subject; or
- (i) 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 make regulations or issue directives prescribing —

- (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) The Commission shall, in making regulations or issuing directives under subsection (2), have regard to the —

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

31. (1) Where a data subject is a child or a person lacking the legal capacity to consent, a data controller shall obtain the consent of the parent or legal guardian, as applicable, to rely on consent under this Act.

Children or persons lacking the legal capacity to consent

(2) A data controller shall apply appropriate mechanisms 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) shall not apply, where the processing is —

- (a) necessary to protect the vital interests of the child or person lacking the legal capacity to consent;

(b) carried out for purposes of education, medical, or social care, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or

(c) necessary for proceedings before a court relating to the individual.

(5) Where the circumstance relates to the processing of personal data of a child of 13 years and above in relation to the provision of information and services by electronic means at the specific request of the child, the Commission shall make regulations in accordance with the objectives of this Act.

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

Act No. 26, 200

32. (1) A data controller 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 prescribed under this Act and subsidiary legislation made under it.

Data Protection
Officers

(2) The Data Protection Officer may be an employee of a data controller or engaged by a service contract.

(3) The Data Protection Officer shall —

(a) advise the data controller or the data processor, and their employees, who carry out processing made under this Act;

(b) monitor compliance with this Act and related policies of the data controller or data processor; and

(c) act as the contact point for the Commission on issues relating to data processing.

33. The Commission may license a person having a requisite level of expertise, in relation to data protection and this Act, to monitor, audit and report on compliance by data controllers and data processors with —

Data protection
compliance ser

(a) this Act; and

(b) regulations, guidelines, directives, and codes of conduct issued by the Commission made under the provisions of this Act.

PART VI — RIGHTS OF A DATA SUBJECT

34. (1) A data subject has the right to obtain from a data controller, without constraint or unreasonable delay—

Rights of a dat
subject

- (a) confirmation as to whether 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, particularly recipients in third countries or international organisations,
 - (iv) where possible, the 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 is not collected from the data subject, any available information as to their source, and
 - (viii) the existence of automated decision-making, including profiling, the significance and envisaged consequences for the data subject;
- (b) a copy of data subject's 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) the correction or, if correction is not feasible or suitable, deletion of the data subject's personal data that is inaccurate, out of date, incomplete, or misleading;
- (d) the erasure of personal data concerning the data subject, without undue delay; and
- (e) restriction of data processing pending —
 - (i) the resolution of a request,
 - (ii) objection by the data subject under this Act, or
 - (iii) the establishment, exercise, or defense of legal claims.

- (2) A data controller shall erase personal data without undue delay, where —
- (a) the personal data is no longer necessary, in relation to the purposes for which it was collected or processed, or
 - (b) the data controller has no other lawful basis to retain the personal data.
35. (1) A data subject shall have the right to withdraw, at any time, consent to the processing of personal data under this Act. Withdrawal of consent
- (2) The data controller shall ensure that it is as easy for the data subject to withdraw, as to give consent.
36. (1) A data subject shall have the right to object to the processing of personal data relating to the data subject. Right to object
- (2) A data controller shall discontinue the processing of personal data, unless the data controller demonstrates a public interest or other legitimate grounds, which overrides the fundamental rights and freedoms, and the interests of the data subject.
- (3) Where personal data is processed for direct marketing purposes, the data subject shall have the right to object, at any time, to the processing of personal data concerning the data subject, 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.
37. (1) A data subject shall have 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 the data subject. Automated decision making
- (2) Subsection (1) shall not apply, where the decision is—
- (a) necessary for entering into or the performance of a contract between the data subject and a data controller;
 - (b) authorised by a written law, which 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) The data controller shall implement suitable measures to safeguard the data subject's fundamental rights, freedoms and interests, including the rights to —
- (a) obtain human intervention on the part of the data controller;

- (b) express the data subject's point of view; and
- (c) contest the decision.

38. (1) The Commission may make regulations establishing a right of personal data portability. Data portability

(2) Right of data portability under this Act shall entitle the data subject to —

- (a) receive, without undue delay from a data controller, personal data concerning the data subject in a structured, commonly used, and machine-readable format;
- (b) transmit the personal 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 —

- (a) circumstances and conditions on which the data subject may exercise the right of data portability; and
- (b) 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 VII — DATA SECURITY

39. (1) A 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, 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 a data subject 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) pseudonymisation 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 of 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 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.

40. (1) Where a personal data breach has occurred with respect to personal data being stored or processed by a data processor, the data processor shall, on becoming aware of the breach —

Personal data
breaches

- (a) notify the data controller or data processor that engaged 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; and
 - (b) respond 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) A data controller shall, within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals, notify the Commission of the breach and, where feasible, describe the nature of the personal data breach including the categories and approximate numbers of data subjects and personal data records concerned.
- (3) Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject the data controller shall immediately communicate the personal data breach to the data subject 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 if a direct communication to the data subject 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 the data subject is 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 subsection —
 - (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 Commission may, at any time, make a public communication about a personal data breach notified to it under subsection (2), where it considers the steps of the data controller to inform data subjects inadequate.
- (6) 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 (3).
- (7) In evaluating whether a personal data breach is likely to result in a risk to the rights and freedoms of a data subject under subsection (3), a 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.
- (8) A 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.
- (9) Where it is not possible to provide information under this section at the same time, the information may be provided in phases without undue delay.

PART VIII — CROSS-BORDER TRANSFERS OF PERSONAL DATA

41. (1) A data controller or data processor shall not transfer or permit personal data to be transferred from Nigeria to another country, unless —
- Basis for cross-border transfer of personal data
- (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 this Act; or
 - (b) one of the conditions set out in section 43 of this Act 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 42 of this Act.
- (3) The Commission may make regulations 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 42 of this Act.
- (4) The Commission may, by regulations, 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.
42. (1) A level of protection is adequate for the purposes of this section if it upholds principles that are substantially similar to the conditions for processing of the personal data provided for in this Act.
- Adequacy of protection
- (2) The adequacy of protection referred to in subsection (1) shall be assessed taking into account the —
- (a) availability of enforceable data subject rights, the ability of a data subject to enforce such rights through administrative or judicial redress, and the rule of law;
 - (b) existence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection;
 - (c) access of a public authority to personal data;
 - (d) existence of an effective data protection law;
 - (e) 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 guidelines as to the assessment of adequacy and the factors set out under subsection (2)
- (4) The Commission may determine whether a country, region or specified sector within a country, or standard contractual clauses, affords an adequate level of protection under subsection (1).
- (5) The Commission may approve binding corporate rules, codes of conduct, certification mechanisms or similar instruments for data transfer proposed to it, where the Commission is satisfied that such instruments meet appropriate standards of data protection in accordance with the objectives of this Act.
- (6) The absence of a determination by the Commission under subsection (4) or (5) with respect to a country, territory, sector, binding corporate rules, 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 decision made by a competent authority of other jurisdictions, where such decision have taken into account factors similar to those listed in this section.

43. (1) In the absence of adequacy of protection under section 42 of this Act, a data controller or data processor shall only transfer personal data from Nigeria to another country if the—

Other bases for transfer of personal data outside N

- (a) 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) transfer is necessary for the performance of a contract to which a data subject is a party or in order to take steps at the request of a data subject, prior to entering into a contract;
- (c) transfer is for the sole benefit of a 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;
- (d) transfer is necessary for important reasons of public interest;
- (e) transfer is necessary for the establishment, exercise, or defense of legal claims; or

- (f) transfer is necessary to protect the vital interests of a data subject or of other persons, where a data subject is physically or legally incapable of giving consent.
- (2) Without prejudice to any provision of this Act, no specific international, multi-national cross border data transfer codes, rules or certification mechanisms shall be adopted as Federal Republic of Nigeria standard for the protection of data subject or data sovereignty without approval of the National Assembly.

PART IX — REGISTRATION AND FEES

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

Registration of
controllers and
processors of r
importance

- (2) Registration under subsection (1) shall be made by notifying the Commission of —
 - (a) the name and address of the data controller or data processor, and name and address of the data protection officer of the data controller or data processor;
 - (b) a description of personal data and the categories and number of data subjects to which the personal data relate;
 - (c) the purposes for which personal data is processed;
 - (d) the categories of recipients to whom the data controller or data processor intends or is likely to disclose 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) the 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) A data controller or data processor of major importance shall notify the Commission of any significant change to the information submitted under subsection (2) within 60 days after such change.
- (4) The Commission shall maintain and publish on its website a register of duly registered data controllers and data processors of major importance.
- (5) A data controller or data processor shall be removed from the register of the

Commission, where it notifies the Commission that it has ceased to operate as a data controller or data processor of major importance.

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

45. The Commission may prescribe fees or levies to be paid by data controllers and data processors of major importance. Fees and levies

PART X — ENFORCEMENT

46. (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, or subsidiary legislation made under this Act may lodge a complaint with the Commission. Complaints and investigations

- (2) The Commission may investigate any complaint referred to it, where it appears to the Commission that 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 subsidiary legislation made under this Act.

- (4) The Commission may, for the purpose of an investigation, order a 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 any material to which an investigation relates, consists of information stored in any document, record, minutes, mechanical or electronic device, the Commission may require the person named to produce such material or give access to the Commission to conduct an inspection on the material.

- (6) For the purposes of subsection (5), the person shall ensure that the information relating to the material under investigation is visible and legible, in a structured, commonly used and machine-readable format.

- (7) The Commission may, where necessary, make representations to —

- (a) the data controller or data processor on behalf of a complainant; or
- (b) a complainant on behalf of the data controller or data processor.

(8) The Commission shall —

- (a) establish a unit to receive and follow up on complaints from data subjects and conduct investigations; and
- (b) adopt rules and procedures on handling complaints and conducting investigations referred to it under this Act.

47. (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 subsidiary legislation made under this Act, the Commission may make an appropriate compliance order against that data controller or data processor. Compliance on

(2) The order made by the Commission under subsection (1) may include a —

- (a) warning that certain act or omission is likely to be a violation of one or more provisions under this Act or any subsidiary legislation or orders issued under it;
- (b) 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) 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;
- (b) 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) a period within which to implement such measures; and
- (d) a right to judicial review under section 50 of this Act.

48. (1) Notwithstanding any criminal sanctions under this Act, if the Commission, after completing an investigation under section 46 of this Act, is satisfied that a data controller or data processor has violated any provision of this Act or subsidiary legislation made under this Act, it — Enforcement

- (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) shall include —
 - (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 has suffered injury, loss, or harm as a result of a violation;
 - (c) ordering the data controller or data processor to account for the profits realised from the violation; or
 - (d) ordering the data controller or data processor to pay a penalty or remedial fee.
- (3) A penalty or remedial fee under subsection (2)(d) may be an amount up to the —
 - (a) higher maximum amount, in the case of a data controller or data processor of major importance; or
 - (b) standard maximum amount, in the case of a data controller or data processor not of major importance.
- (4) The “higher maximum amount” shall be the greater of —
 - (a) ₦10,000,000, and
 - (b) 2% of its annual gross revenue in the preceding financial year.
- (5) The “standard maximum amount” shall be the greater of —
 - (a) ₦2,000,000, and
 - (b) 2% of its annual gross revenue in the preceding financial year.
- (6) The Commission shall, in determining the sanctions, take into consideration the —
 - (a) nature, gravity, and duration of the infringement;
 - (b) purpose of the processing;
 - (c) number of data subjects involved;
 - (d) 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.

49. (1) A data controller or data processor, who fails to comply with orders made under section 47 of this Act commits an offence and is liable on conviction to — Offences and penalties

(a) a fine of up to the —

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

(ii) standard maximum amount, in the case of a data controller or data processor not of major importance; or

(b) imprisonment for a term not more than one year or both.

50. A person who is not satisfied with an order of the Commission, may apply to the court for judicial review within 30 days after the order was made. Judicial review

51. 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, may recover damages from such data controller or data processor in civil proceedings. Civil remedies

52. Notwithstanding anything to the contrary, the Court may make an order of forfeiture against a convicted data controller, data processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act. Forfeiture
Act No. 16, 20

53. (1) Where an offence has been committed by a body corporate or firm, the body corporate or firm, as well as principal officers of the body corporate or firm shall be deemed culpable, unless the principal officers prove that — Joint and vicar liability

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

(b) they exercised diligence to prevent the commission of the offence.

(2) A data controller and data processor shall be vicariously liable for the acts or omissions of its agent or employees, in so far as the acts or omissions relate to its business.

PART XI — LEGAL PROCEEDINGS

54. (1) A suit shall not be instituted against the Commission, a member of the Council, or staff of the Commission for an act done under or in execution of this Act, or any public duty of the Commission, unless — Limitation of
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) A suit shall not be commenced against the Commission, a member of the Council, or staff of the Commission before the expiration of one month after written notice of intention to commence the suit is served on the Commission, a member, or staff of the Commission by the intending plaintiff or plaintiff's agent.

(3) The notice referred to in subsection (2) 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 sought.

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

Cap. P41, LFI
2004

55. A notice, summons, process, or document, required or authorised to be served on the Commission under the provisions of this Act or any other law or enactment, may be served by delivering it to the National Commissioner at the head office of the Commission.

Service of
documents

56. (1) An execution or attachment process shall not 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) A sum of money which may be the judgment of any court awarded against the Commission shall be paid from the Fund of the Commission.

57. The National Commissioner, a member of Council, staff of the Commission, or other persons engaged by the Commission shall be indemnified out of the assets of the Commission against —

Indemnity of
members, and
employees of
Commission

(a) losses, charges, claims, expenses, and liabilities incurred in the discharge of official duties, or

(b) liability incurred in defending criminal or civil proceedings, where the —

(i) judgement is given in favour of the National Commissioner, a member of the Council, or staff of the Commission,

- (ii) National Commissioner, a member of the Council, or staff of the Commission is otherwise acquitted,
- (iii) proceedings are otherwise disposed of without any finding or admission of any material breach of duty, or
- (iv) court grants the National Commissioner, a member of the Council, or staff of the Commission relief from liability for negligence, default, breach of duty, or breach of trust in relation to the Commission.

58. (1) The Commission shall 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. Power of arrest, search, and seizure
- (2) A Judge may issue a warrant under subsection (1) on the satisfaction that —
- (a) a person has engaged, is engaging, or is likely to engage in a conduct that contravenes the provisions of this Act;
 - (b) the warrant is sought to prevent the commission of an offence under this Act;
 - (c) the warrant is sought to prevent 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 person 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) stop and search any person found on such premises;

- (c) enter and search any conveyance found on the premises;
- (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 used a computer or other devices 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 conversant with the operation of a computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.

59. A legal officer of the Commission or a private legal practitioner engaged by the Commission may represent the Commission in civil proceedings, in respect of matters relating to the business or operations of the Commission. Right to appeal court

PART XII — MISCELLANEOUS PROVISIONS

60. Subject to the provisions of this Act, the Minister may give to the Commission directives of a general nature or relating generally to matters of policy with respect to the objectives and functions of the Commission, and the Commission shall comply with the directives. Directives by Minister
61. (1) The Commission may make regulations for carrying out its objectives under this Act. Regulations
- (2) Without prejudice to 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, discharge any duty or perform any 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) frequency of filing and content of compliance returns by data controllers and data processors of major importance to the Commission;

(h) fees, fines, and charges prescribed under this Act and such related matters;
and

(i) 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 —

(a) create offences in respect of any contravention of the regulations; and

(b) impose penalty not more than that prescribed in this Act.

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

62. The Commission may, where necessary, issue directives, codes, or guidelines on the —

Directives, codes
and guidelines

(a) conduct of the business and operations of the Commission in a manner that —

(i) fosters accountability, ensures transparency and consistency with the highest ethical standards, and

(ii) ensures compliance with international best practices, 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; and

(d) any other matter relevant to the operations of the Commission.

63. Where 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, are inconsistent with any of the provisions of this Act, the provisions of this Act shall prevail.

Priority of the

64. (1) A reference to the Nigeria Data Protection Bureau (in this section referred to as “the Bureau”) existing before the commencement of this Act, or a document issued in the name of the Bureau, shall be read as a reference to the Commission established under this Act, and all persons engaged by the Commission shall have the same rights, powers and remedies as existed in the Bureau before the commencement of this Act.

Transitional
provisions

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

(a) a person who, prior to the commencement of this Act, was an officer,

employee or member of staff of the Bureau shall continue in office, and be deemed to have been appointed under this Act on such terms and conditions not less favourable than that enjoyed prior to the transfer of service;

- (b) all existing agreements and contracts currently in effect by the 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 Bureau shall become, on the effective date of this Act, part of the records and equipment of the Commission;
- (d) properties held immediately before the commencement of this Act on behalf of the Bureau shall on the commencement of this Act, be vested in the Commission established under this Act;
- (e) any proceeding or cause of action pending or existing immediately before the commencement of this Act by or against the Bureau, in respect of any right, interest, obligation or liability may be commenced or continued, as the case may be by the Commission; and
- (f) all orders, rules, regulations, decisions, directions, licences, authorisations, certificates, consents, approvals, declarations, permits, registrations, rates or other documents that are in effect before the coming into effect of this Act and that are made or issued by the National Information Technology Development Agency or the Bureau shall continue in effect as if they were made or issued by the Commission until they expire or are repealed, replaced, reassembled or altered.

65. In this Act —

Interpretation

“automated decision-making” means a decision based solely on 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 best practices;

“child” has the meaning ascribed in the Child’s Right Act, No. 26, 2003;

“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 permission to provide such consent;

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

“competent authority” includes –

- (a) the Government of the Federal Republic of Nigeria or any foreign government; or
- (b) any state government, statutory authority, government authority, institution, agency, department, board, commission, or organisation within or outside Nigeria, exercising executive, legislative, judicial, investigative, regulatory, or administrative functions;

“court” means any court of competent jurisdiction;

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

“data controller or data processor of major importance” means a data controller or data processor that is domiciled, resident in, or 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 any other body, who 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;

"Minister" means the Minister responsible for matters relating to communications and digital economy;

"National Commissioner" means the National Commissioner of the Nigeria Data Protection Commission;

"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 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 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, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria;

"pseudonymisation" 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) other information prescribed by the Commission, as sensitive personal data under section 30 (2); and

“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.

66. This Act may be cited as the Nigeria Data Protection Act, 2023.

Citation

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 and the Council shall meet once in a quarter of a year.

Presiding Officer

2. Every meeting of the Council shall be presided over by the Chairman, and where the Chairman is absent, 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.
4. The quorum of any committee of Council shall be determined by the Council.

Voting

5. 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.
6. 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 the person, who is invited shall not be entitled to vote at any meeting of the Council and shall not count towards the quorum.

Teleconference meeting

7. 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 item as a "teleconference meeting".

8. A member of the Council, who participates in a teleconference meeting shall be taken for all purposes to have been present at the meeting.
9. The Council may establish procedure for teleconference meetings (including recording the minutes of such meetings) in its minutes book.

Committees of the Council

10. Subject to standing orders made by the Council under 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.
11. Every committee appointed under the provisions of paragraph 10 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.
12. The decision of a committee shall have no effect until it is approved or ratified by the Council.

Seal of the Commission

13. The affixing of the seal of the Commission shall be done and authenticated by the signature of the National Commissioner or such other member authorised by the Council to act for that purpose.
14. A 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 specifically authorised by the National Commissioner to act for that purpose.
15. A 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

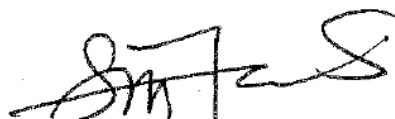
16. The validity of a proceeding of the Council or its committee is not adversely affected by
—
 - (a) any vacancy in the membership of the Council;
 - (b) any defect in the appointment of a member of the Council, staff, or committee; or
 - (c) reason that a person not entitled to do so took part in the proceeding.
17. 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 the interest, in advance of any consideration of the matter;
- (b) not influence or 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) be absent from the meeting or that part of the meeting during which the matter is discussed.

18. If a member of the Council discloses an interest under paragraph 17, the disclosure shall be recorded in the minutes of the meeting of the Council.

I, CERTIFY, IN ACCORDANCE WITH SECTION 2 (1) OF THE AUTHENTICATION ACT, CAP. A2, LAWS OF THE FEDERATION OF NIGERIA 2004, THAT THIS IS A TRUE COPY OF THE BILL PASSED BY BOTH HOUSES OF THE NATIONAL ASSEMBLY.



SANI MAGAJI TAMBAWAL, fena
CLERK TO THE NATIONAL ASSEMBLY

 DAY OF June, 2023

SCHEDULE TO THE NIGERIA DATA PROTECTION BILL, 2023

SHORT TITLE OF THE BILL	LONG TITLE OF THE BILL	SUMMARY OF THE CONTENTS OF THE BILL	DATE PASSED BY THE SENATE	DATE PASSED BY THE HOUSE OF REPRESENTATIVES
Nigeria Data Protection Bill, 2023	An Act to provide a legal framework for the protection of personal information, and establish the Nigeria Data Protection Commission for the regulation of the processing of personal information; and for related matters.	This Bill provides a legal framework for the protection of personal information, and establishes the Nigeria Data Protection Commission for the regulation of the processing of personal information.	3rd May, 2023	24th May, 2023

I certify that this Bill has been carefully compared by me with the decision reached by the National Assembly and found by me to be true and correct decision of the Houses and is in accordance with the provisions of the Acts Authentication Act Cap. A2, Laws of the Federation of Nigeria, 2004.


SANTAMAGALHES TAMBAWAL, fena

Clerk to the National Assembly


... Day of June, 2023



BOLA AHMED TINUBU, GCFR

President of the Federal Republic of Nigeria

12th Day of June, 2023

I ASSENT.