

A BILL ENTITLED

THE DATA PROTECTION AND RIGHT TO ACCESS INFORMATION REGULATORY COMMISSION ACT, 2025

PART I- PRELIMINARY

1. Interpretation.
2. Application.
3. General exemption from application of Act.
4. Exemption for research, etc.
5. Power to make further exemptions.

PART II - THE DATA PROTECTION AND RIGHT TO ACCESS INFORMATION REGULATORY COMMISSION.

6. The Data Protection and Right to Access Information Regulatory Commission.
7. Composition of Board.
8. Meetings of Board.
9. Disclosure of interest.
10. Immunity of members.
11. Committees of Board.
12. Remuneration of members.
13. Filling of vacancies.
14. Powers and functions of Board.

PART III – THE FUNCTIONS AND POWERS OF THE COMMISSION

15. Functions of Commission.
16. Powers of Commission.

PART IV - ADMINISTRATIVE PROVISIONS

17. Executive-Chairman.
18. Functions of Executive-Chairman.
19. Data Protection Commissioner and Access to Information Commissioner
20. Other staff.
21. Directorates.

PART V – FINANCIAL PROVISIONS

22. Funds of Commission.
23. Accounts and audit.
24. Financial year.
25. Annual report.

PART VI–PRINCIPLES OF DATA PROTECTION.

26. Principles of data protection.
27. Collecting, processing, holding or use of personal data.
28. Restriction on processing.
29. Prohibition of collecting and processing of sensitive personal data.
30. Protection of privacy.

31. Collection of data from data subject.
32. Collection of personal data for specific purpose.
33. Data protection impact assessment.
34. Personal data relating to a child.
35. Processing of sensitive personal data.
36. Commercial use of personal data.
37. Consent necessary for processing personal data.
38. Processing personal data without consent.
39. Use of data collected for specific purpose.
40. Retention of records of personal data.
41. Processing personal data outside Sierra Leone.

PART VII -RIGHTS OF DATA SUBJECT

42. Correction of personal data.
43. Right to access personal information.
44. Right to prevent processing of personal data.
45. Right to prevent processing of personal data for direct marketing.
46. Rights in relation to automated decision-taking.
47. Right to confirmation and access.
48. Right to data portability.

PART VIII - DATA CONTROLLER OR DATA PROCESSOR

49. Certificate of Registration.
50. Duration of Certificate of Registration.
51. Cancellation or variation of Certificate of Registration.
52. Compliance and audit.
53. Register of Data Controllers and Data Processors.

PART IX - TRANSPARENCY, ACCOUNTABILITY MEASURES AND SECURITY OF DATA

54. Privacy design policy.
55. Technical and organisational measures.
56. Determining organisational measures
57. Transparency in personal data processing.
58. Security measures relating to data processed by data processor.
59. Data processed by entity or authorised person.
60. Notification of breach.

PART X – THE RIGHT TO ACCESS INFORMATION

61. Access to information.
62. Submission and form of application.
63. Time limit for compliance.
64. Transfer of application.
65. Fee notice.
66. Application expressing preference.
67. Proactive publication.

- 68. Approval of publication scheme.
- 69. Model publication scheme
- 70. Other proactive schemes.

PART XI–EXEMPT INFORMATION

- 71. Exempt information.
- 72. Notice of exempt information.
- 73. Information accessible by other means.
- 74. Non-application of duty to disclose information.
- 75. Historical records.
- 76. Severability.

PART XII–MEASURES TO PROMOTE OPENNESS

- 77. Development of information communication facilities.
- 78. Maintenance of records
- 79. Code of Practice.

PART XIII – OFFENCES AND PENALTIES

- 80. Denying or obstructing access to record or information.
- 81. Failure to supply information requested.
- 82. Unauthorised disclosure of storage of personal data.
- 83. Offence by corporation.
- 84. General penalty.

PART XIV - MISCELLANEOUS

- 85. Appeal mechanism
- 86. Complaints against breach or non-compliance.
- 87. Code of practice.
- 88. Compensation for failure to comply with Act.
- 89. Regulation.
- 90. Transitional provisions.
- 91. Repeal and savings.

BILL ENTITLED

Short title.

THE DATA PROTECTION AND RIGHT TO ACCESS INFORMATION REGULATORY COMMISSION ACT, 2025

Being an Act to provide for the establishment, functions and powers of the Data Protection and the Right to Access Information Regulatory Commission and to provide for other related matters.

Date of commencement.

1

ENACTED by the President and Members of Parliament in this present Parliament assembled.

PART I- PRELIMINARY

Interpretation.

1. In this Act unless the context otherwise requires –

“anonymisation” means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

“Board” means the Data Protection Right to Access Information Regulatory Commission Board established under section 7;

“child” shall be given the meaning contained in the Child Rights Act 2009;

“Commission” means the Data Protection Right to Access Information Regulatory Commission established under section 6;

“consent” means a manifestation of express unequivocal, free, specific and informed indication of the data subject’s wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject;

“data” means information which is –

- (a) processed by means of equipment operating automatically in response to instructions given for that purpose;
- (b) recorded with intention that it should be processed by means of such equipment;
- (c) recorded as part of a relevant filing system; or

- (d) recorded information which is held by a public entity and does not fall within paragraphs (a) to (c);

“data controller” means a natural or legal person, agency or other body which alone or jointly with others, determines the purpose and means of processing of personal data;

“data processor” in relation to personal data means a person other than an employee of the data user, who processes the personal data solely on behalf of the data user and does not process the personal data for any of their own purposes;

“data processing” means an operation or set of operations performed on personal data such as collection, recording, organisation, structuring, storage or preservation, adaptation or alteration, access, retrieval or consultation, transmission, disclosure, sharing or making available, restriction, erasure, or destruction of, or the carrying out of logical or arithmetical operations within a structured set of such data which are accessible or retrievable according to specific criteria;

“data subject” means an individual who is the subject of the personal data;

“data user” include a data controller or data processor or a person who either alone or jointly or in common with other persons processes personal data or has control over or authorises the processing of personal data”

“data portability” means the capability to receive or transmit data from one platform or service to another in a structured, commonly used and machine-readable format with a degree of accessibility;

“data protection impact assessment” means an assessment of the impact of a processing operation on personal data under [section 33](#);

“encryption” means the process of converting the content of any readable data using technical means into coded form;

“entity “means an entity including a public agency or statutory body engaged in or responsible for a component of data processing;

“filing system” means a structured set of personal data which is readily 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 of Information and Communications;

“notice in writing” means a written communication, whether physical or electronic, which effectively conveys an intended information or message in a legally recognised and readily accessible format;

“personal data” means information relating to an identified or identifiable natural person;

“processing” in relation to personal data means collecting recording holding or storing the personal data or carrying out an operation or set of operations on personal data including, –

- (a) the organisation, adaptation or alteration of personal data;
- (b) the retrieval consultation nor use of personal data;
- (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available;
- (d) the alignment, combination, correction, erasure or destruction of personal data;
- (e) the alignment, combination, correction, erasure or destruction of personal data;

“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 and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable person;

“Register of Data Controllers and Data Processors” means the list or entry of data controllers or data processors maintained by the Commission whether in digital or other format under section 53;

“sensitive personal data” means personal data consisting of information as to the race, physical or health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex, political opinions, religious beliefs or other beliefs of similar nature of a data subject.”

“third party” means, in relation to personal data, a person or entity other than a data subject, data controller, or data processor or other person authorised to process data for a data controller or processor.

Application.

2. This Act shall apply, in the case of –

- (a) the right to access information, to –
 - (i) a public authority;
 - (ii) a private body,
that is holding or is in control of information necessary for the enforcement or protection of a right;
- (b) the protection of personal data, to a person, institution or public body that collects, processes, holds or uses personal data relating to a Sierra Leonean citizen or non-citizen residing, -
 - (i) within Sierra Leone; or
 - (ii) outside Sierra Leone but with some commercial, legal or taxable presence in Sierra Leone.

General exemption from application of Act.

3. The processing of personal data shall be exempt from the application of this Act if the personal data processed is to be used –

- (a) by an individual in the course of a purely personal or household activity;
- (b) for national security or public interest;
- (c) for the prevention or detection of a crime;
- (d) for the purpose of an investigation;

- (e) for the assessment or collection of a tax or duty or any other imposition of a similar nature;
- (f) for the purpose of or in connection with an order or judgment of a court;
- (g) for the purpose of discharging a statutory function.

Exemption for research, etc.

4. The Commission may, where the processing of personal data is necessary for research, archiving or statistical purpose and the Commission is satisfied that -

- (a) compliance with the Act shall not disproportionately divert resources from such purpose;
- (b) the purpose of processing cannot be achieved if the personal data is anonymised;
- (c) the data controller or data processor has carried out the de-identification in accordance with any law and the purpose of processing cannot be achieved if the personal data is in de-identified form;
- (e) personal data shall not be used to take a decision specific to or action directed to a data subject;
- (f) the personal data shall not be processed in the manner that gives rise to a risk of significant harm to a data subject,

by notice published in the Gazette, exempt such class of research, archiving or statistical purposes from the application of the Act.

Power to make further exemptions.

5. The Minister may, upon the recommendation of the Commission, by statutory instrument, exempt the application of this Act to a data controller or data processor or class of data controllers or data processors.

PART II - THE DATA PROTECTION AND THE RIGHT TO ACCESS INFORMATION REGULATORY COMMISSION.

The Data Protection and the Right to Access to Information Regulatory Commission.

6. (1) There is hereby established a body to be known as the Data Protection and Right to Access Information Regulatory Commission which shall be responsible for data protection and the protection of the right to access information.

(2) The Commission shall be a body corporate having perpetual succession and capable of acquiring, holding and disposing of any property, whether movable or immovable, and of suing and being sued in its corporate

name and, subject to this Act, of performing all such acts as bodies corporate may by law perform.

(3) The Commission shall have a common seal, the use of which shall be authenticated by the signatures of the Executive-Chairman and other officer of the Commission authorised by the Board for that purpose.

(4) A document purporting to be an instrument executed or issued by or on behalf of the Commission and to be sealed with the common seal authenticated in the manner stated in subsection (3) shall be deemed to be so executed or issued without further proof unless the contrary is proved.

(5) In appropriate cases the common seal of the Commission may be affixed to documents outside Sierra Leone.

Board of Commission.

7. (1) The governing body of the Commission shall be a Board in which shall be vested, subject to this Act, the supervision of the Commission.

(2) The Board shall consist of an Executive Chairman and the following other members -

- (a) the Data Protection Commissioner; and
- (a) the Access to Information Commissioner; and
- (c) other Commissioners, each representing an administrative region of Sierra Leone.

(3) Members of the Board shall be appointed by the President on the recommendation of the Minister, subject to the approval of Parliament.

(4) A person shall not be appointed as a member of the Board if he –

- (a) is an employee of a political party or holds an elected or appointed position in the central or a local government; or
- (b) has been convicted of an offence involving fraud or dishonesty.

(5) The Executive-Chairman and the other members of the Board shall hold office for a term of 5 years and shall be eligible for re-appointment to a further term of 5 years only.

Meetings of Board.

8. (1) The Board shall meet for the dispatch of its business at least once every 3 months.

(2) The Executive-Chairman shall preside at every meeting of the Board, and in his absence, the members present shall appoint a member from among their number to preside.

(3) A minimum of 4 members of the Board may, by notice in writing signed by them, request the Executive-Chairman to summon a special meeting of the Board for such purposes as may be stated in the notice.

(4) The Executive-Chairman or, in his absence, the member appointed to act on his behalf shall summon a special meeting within 5 days of his receipt of the notice referred to in subsection (3).

(5) The quorum at a meeting of the Board shall be 4.

(6) The Executive-Chairman or other person presiding shall have a casting vote where there is an equality of votes.

(7) A proposal circulated among all members and agreed to in writing by a two-thirds majority of all members shall be of the same force or effect as a decision made at a duly constituted meeting of the Board and shall be incorporated in the minutes of the next succeeding meeting of the Board:

Provided that, if a member requires that such proposal be placed before a meeting of the Board, this subsection shall not apply to such proposal.

(8) The Board may co-opt a person to attend and participate in its deliberations on any matter but such person shall not vote on any issue for the decision by the Board.

(9) The Board shall cause minutes of all its meetings to be taken and signed by the Executive-Chairman and kept in proper form.

(10) Subject to this Act, the Board shall regulate its own procedure.

**Disclosure
of interest.**

9. (1) A member of the Board who has an interest, whether direct or indirect, in a matter being considered or to be considered by the Board, shall disclose the nature of his interest to the Board and the disclosure shall be recorded in the minutes of the Board and such member shall not take part in a deliberation or decision of the Board relating to that matter.

(2) A member of the Board who contravenes subsection (1) shall be guilty of misconduct and shall be removed from the Board.

**Immunity of
members.**

10. (1) An action or other proceedings shall not lie or be instituted against a member of the Board or member of a committee of a Board for or in respect of an act or thing done or omitted to be done in good faith in the exercise of his functions under this Act.

(2) A member of the Board shall not be personally liable for any debt or obligation of the Commission.

**Committees
of Board.**

11. (1) The Board may, for the discharge of its functions, appoint one or more committees to perform such functions as the Board may determine.

(2) A committee shall consist of members of the Board or non-members or both as the Board may decide.

(3) Without prejudice to the generality of subsection (1), the Board shall appoint an audit committee consisting of such members of the Board, excluding the **Executive-Chairman** and performing such functions as the Board may determine.

(4) A committee shall submit a report of its proceedings to the Board at such time as the Board may determine.

**Remuneration
of members.**

12. The Executive-Chairman and the other members of the Board and a person co-opted by the Board shall be paid such remuneration, fees and allowances approved by the Minister and shall be reimbursed by the Commission for expenses incurred in connection with the discharge of their functions as the Board may, with the approval of the Minister, determine.

**Filling of
vacancies.**

13. (1) Where the Executive-Chairman or a member of the Board dies, resigns, is removed from office or is absent for a continuous period exceeding 3 months or is by reason of illness unable to perform the functions of his office for a continuous period of 6 months, in the case of -

- (a) the Executive-Chairman, the members of the Board shall elect one of their number to act as Executive-Chairman until such time as the Executive-Chairman resumes his office or another is appointed in his stead; and
- (b) a member, the Executive-Chairman shall, subject to this Act, have another person appointed to the Board.

(2) Where a person is appointed as Chairman or appointed as a member to fill a vacancy, he shall hold office for the remainder of the term of the previous Chairman or member, as the case may be, and shall, subject to this Act, be eligible for re-appointment.

**Powers and
functions
of Board**

14. (1) Subject to this Act, the Board shall have supervision of the Commission, including overseeing the sound and proper financial management of the Commission.

(2) It shall also be the responsibility of the Board to provide such policy guidance and advice as will secure the efficient overall performance of the functions of the Commission.

PART III – THE FUNCTIONS AND POWERS OF THE COMMISSION

Functions of Commission.

15. (1) The object for which the Commission is established is for the regulation of data protection and the protection of the right of access to information.

(2) Without prejudice to the generality of subsection (1), it shall be the function of the Commission to -

- (a) to ensure compliance by public authorities or by persons providing services for them, with requests for the disclosure of information made under this Act;
- (b) investigate complaints of noncompliance of public authorities to requests for the disclosure of information or infringements of data protection rights;
- (c) monitor and report on the compliance by public authorities with their obligations under this Act;
- (d) co-operate with or undertake training activities for public authorities on the right to access information and the effective implementation of this Act;
- (e) regulate data protection in Sierra Leone;
- (f) carry out inspections of public and private entities to evaluate the processing of personal data;
- (g) establish and maintain a register of data controllers and data processors;
- (h) conduct research and studies and promote capacity building and educational activities relating to data protection, including organising and conducting seminars, workshops, and symposia and supporting other organisations conducting similar activities;
- (i) create and maintain online resources such as guides, FAQs, and best practice manuals to assist data controllers and data processors in complying with this Act;

- (j) manage technical co-operation and exchange in the area of data protection with other organisations including foreign data protection authorities and international or inter-governmental organisations, on its own behalf or on behalf of the Government;
- (k) do such things as are conducive to the attainment of the objects stated under subsection (1).

Powers of Commission.

16. (1) The Commission shall, in the performance of its functions under this Act, have the power to -

- (a) issue summons or other orders requiring the attendance of a person before the Commission to give oral or written evidence and the production of a document or record relevant to an investigation by the Commission;
- (b) examine a person in respect of a subject matter under investigation before the Commission;
- (c) require a person, by a notice in writing stating the reasons for such requisition, to disclose information within the person's knowledge relevant to an investigation by the Commission;
- (d) enter premises occupied by a data controller or data processor to carry out an investigation;
- (e) issue directions to a data controller or data processor who shall be bound to comply with such directions;
- (f) prescribe the threshold required for mandatory registration of data controllers and data processors and in making such determination, the Commission shall consider –
 - (i) the fact of existence of statutory data processing entities or judicial bodies;
 - (ii) the nature of the industry;
 - (iii) the volumes of data processed;
 - (iv) whether sensitive personal data is being processed; and

- (v) any other criteria that the Commission may specify.

(2) The Commission shall not issue directions under paragraph (e) of subsection (1) unless the data controller or data processor concerned has given a reasonable opportunity of being heard.

(3) The Commission shall by regulations specify the manner in which a data controller or data processor shall provide the information sought under subsection (1), the period within which such information is to be furnished and the form in which such information may be provided.

PART IV - ADMINISTRATIVE PROVISIONS

Executive-Chairman.

17. (1) The Executive-Chairman shall be the chief executive officer of the Commission and shall be a person who has considerable knowledge and experience in matters related to data protection and right to access information

(2) A person shall not be appointed **Executive- Chairman** unless he –

- (a) is a person of high integrity and has a Masters degree in law, data science or information technology or a related field; and
- (b) has knowledge and relevant work experience, appropriate to the functions of the Commission, of not less than 10 years.

(3) The **Executive- Chairman** shall hold office for a period of 5 years and shall be eligible for reappointment for another period of 5 years.

Functions of Executive-Chairman.

18. The **Executive- Chairman** shall be responsible for -

- (a) the day-to-day administration of the **Commission**;
- (b) the implementation of such operational policies, programmes and plans relating to the functions of the Commission as may be approved by the Commission;
- (c) the supervision and discipline of other staff of the **Commission**;
- (d) the management of the funds, property, and business of the Commission; and
- (e) performing such other duties as the Commission may determine.

**Data protection
and Access to
Information
Commissioner**

19. The Data Protection Commissioner and the Access to Information Commissioner, shall have the requisite professional and other qualifications relevant to data protection and the protection of the right to access information respectively.

Other staff.

20. (1) The Commission shall have, in addition to the Executive-Chairman, the Data Protection Commissioner and the Access to Information Commissioner, such other staff, including a Finance Officer, Internal Auditor, Administrative Officer and such other additional technical and administrative staff, as may be required for the efficient performance of the functions of the Commission.

(2) The staff other of the Secretariat shall be appointed by the Commission, subject to such terms and conditions as the Commission shall determine.

Directorates.

21. (1) The Commission may, for the purpose of carrying out its functions under this Act, have a Data Protection Directorate, an Access to Information Directorate and such other directorates as the Commission may, on the recommendation of the Executive-Chairman, approve.

(2) The Data Protection Directorate shall be headed by Data Protection Commissioner, the Access to Information Directorate shall be headed by the Access to Information Commissioner and other directorates shall be headed by a Director appointed by the Board on advice of the Executive-Chairman.

PART V – FINANCIAL PROVISIONS

**Funds of
Commission.**

22. (1) The activities of the Commission shall be financed by funds consisting of –

- (a) monies appropriated from time to time by Parliament for the purposes of the Commission;
- (b) monies given to the Commission by way of gifts, endowments, bequest, grant or other contributions by persons and organisations for the purposes of the Commission; or
- (c) other moneys which may, from time to time, accrue to the Commission.

(2) The funds of the Commission shall be applied only for the purposes of the approved budget of the Commission.

**Accounts
and audit.**

23. (1) The Commission shall keep proper books of account and records in relation to the activities, property and finances of the Commission in a form approved by the Auditor-General, and shall prepare in respect of each financial year, a financial statement which shall include -

- (a) balance sheet accounts;
- (b) income and expenditure accounts; and
- (c) source and application of funds.

(2) The accounts of the Commission kept under subsection (1) shall, not later than 3 months after the end of each financial year, be audited by the Auditor-General or an auditor appointed by him.

(3) For the purposes of subsection (2), the Auditor-General or an auditor appointed by him shall be entitled to have access to all books of account, vouchers and other financial records of the Commission and to require such information and explanation thereon as he may think fit.

(4) The Auditor-General or the auditor appointed by him shall submit to the Commission, a report on the audited accounts and the financial statements referred to in subsection (1) and shall, in his report draw attention to -

- (a) irregularities in the accounts;
- (b) matters that are likely to adversely affect the operations of the Commission; and
- (c) any other matter which, in his opinion, ought to be brought to the notice of the Commission.

**Financial
year.**

24. The financial year of the Commission shall be the same as the financial year of the Government.

**Annual
report.**

25. (1) The Commission shall, within 3 months after the end of the Financial year, submit to the Minister an annual report on the performance of its functions during that year and on its policy and programmes.

(2) An annual report submitted under subsection (1), shall include the accounts and annual financial statement prepared under section 23 and the report of the audit thereon.

(3) The Minister shall lay copies of the annual report before Parliament within 2 months after he has received the report.

(4) The Commission shall make copies of the report available to all stakeholders within 30 days once it has been laid before Parliament.

(5) There shall be attached to the report referred to in subsection (2) -

- (a) an audited statement of the Commission's financial position;

- (b) an audited statement of income and expenditure; and
- (c) such other information as the Commission may consider appropriate.

PART VI – PRINCIPLES OF DATA PROTECTION.

Principles of data protection.

26. (1) A data controller or data processor shall collect, process, hold or use personal data based on the following principles –

- (a) accountability to the data subject for data collected and processed held or used;
- (b) data shall be collected and processed fairly and lawfully;
- (c) collection and processing of personal data shall be adequate, relevant and not excessive or unnecessary;
- (d) personal data shall be retained for the period authorised by law or necessary for the intended purpose, ensuring that it is kept in a form that identifies the data subject for no longer than is essential;
- (e) accuracy of information collected, processed, used or held;
- (f) confidentiality and integrity of the data collected, processed, used or held;
- (g) transparency and participation of the data subject in the collection and processing of personal data; and
- (h) observation of data safeguards.

(2) A data collector or data processor shall comply with the principles under subsection (1).

Collecting, processing, holding or use of personal data.

27. (1) A data controller or data processor shall not collect or process personal data except for a specific, clear and lawful purpose.

(2) Personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.

(3) A data controller or data processor collecting personal data shall notify the data subject at the time of the collection of the data, of the following information -

- (a) the nature and category of data being collected;

- (b) the name and address of the person responsible for the collection of data;
- (c) the purpose for which the data is required;
- (d) whether or not the supply of the data by the data subject is discretionary or mandatory;
- (e) the consequences of failure to provide the data;
- (f) the authorised requirement for the collection of the information or the requirement by law for its collection;
- (g) the recipients of the data;
- (h) the existence of the right of access to and the right to request rectification of the data collected before the collection;
- (i) the period for which the data will be retained to achieve the purpose for which it is collected; and
- (j) the existence of a right to file a complaint to the Commission.

(4) Where data is collected from a third-party data subject, he shall be given the information specified in subsection (3) before the collection of the data or as soon as practicable after the collection of the data.

(5) Subsection (4) shall not apply –

- (a) where it is necessary to avoid the compromise of the law enforcement power of a public body responsible for the prevention, detection, investigation, prosecution or punishment of an offence;
- (b) to information relating to -
 - (i) national security;
 - (ii) the enforcement of a law which imposes a pecuniary penalty;
 - (iii) the enforcement of a law on public revenue collection;
 - (iv) the preparation or conduct of proceedings before a court or tribunal.

(6) A data controller or data processor shall ensure that the personal data is complete, accurate, up-to-date and not misleading having regard to the purpose for its collection or processing.

(7) A data subject shall ensure that the personal data given to a data controller or data processor is complete, accurate up-to-date and not misleading.

(8) A data controller or data processor shall, while complying with subsection (6), have regard as to where the data is –

- (a) likely to be used to make a decision about the data subject;
- (b) likely to be disclosed to other individuals;
- (c) kept in a form that distinguishes personal data based on facts from personal data based on opinion or personal assessment.

**Restriction
on processing.**

28. (1) A data controller or data processor shall, at the request of a data subject, restrict the processing of personal data where –

- (a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller or data processor to verify the accuracy of the data;
- (b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defence of a legal claim;
- (c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
- (d) data subject has objected to the processing pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

(2) Where processing of personal data is restricted under subsection (1) –

- (a) the personal data shall, unless the data is being stored only, be processed –
 - (i) with the data subject's consent;
 - (ii) for the establishment, exercise or defence of a legal claim;
 - (iii) for the protection of the rights of another person; or
 - (iv) for reasons of public interest; and

- (b) the data controller or data processor shall inform the data subject before withdrawing the restriction on processing of the personal data.

(3) A data controller or data processor shall implement mechanisms to ensure that time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data is observed.

**Prohibition
of collecting
and processing
of sensitive
personal data.**

29. (1) A person shall not, except where information is collected in accordance with the law relating to statistics or civil registration, collect or process personal data which relates to the religious or philosophical beliefs, political opinion, financial information, health status or medical records of a data subject.

(2) Subsection (1) shall not apply to sensitive personal data collected or processed where the collection or processing of the information is –

- (a) in the exercise or performance of a right or an obligation conferred or imposed by law on an employer;
- (b) given freely and with the consent of the data subject;
- (c) for the purposes of the legitimate activities of members of a body or association which –
 - (i) is established for non-profit purposes;
 - (ii) exists for political, philosophical, religious or trade union purposes.

**Protection
of privacy.**

30. A data controller or data processor shall not collect hold or process personal data in a manner which infringes on the privacy of a data subject, except where such infringement is permitted under this Act or any other law.

**Collection
of data from
data subject.**

31. (1) Personal data may, subject to subsection (2), collected directly from a data subject.

(2) Personal data may be collected from another person, source or public body where –

- (a) the data is contained in a public record;
- (b) the data subject has made the data public;
- (c) the data subject has consented to the collection of the information from another source;
- (d) the collection of the data from another source is not likely to prejudice the privacy of the data subject.

- (e) the collection of the data from another source is necessary for the-
 - (i) prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
 - (ii) enforcement of a law which imposes a pecuniary penalty;
 - (iii) enforcement of a law which concerns public revenue collection;
 - (iv) conduct of proceeding before any court or tribunal that have commenced or are reasonably contemplated; or protection of national security
 - (v) compliance would prejudice a lawful purpose for the collection; or
 - (vi) it is not reasonably practicable to obtain the consent of the data subject.

Collection of personal data for specific purpose.

32. A person who collects personal data shall collect the data for a lawful purpose which is specific, explicitly defined and is related to the functions or activities of a data controller or data processor.

Data protection impact assessment.

33. (1) A data controller or data processor shall, where the processing of data for lawful purposes is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment under subsection (1) shall be in such form as the Commission may prescribe and shall include –

- (a) a systematic description of the envisaged processing operations and the purposes of the processing including where applicable the legitimate interest pursued by the data controller or data processor;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risk to the rights and freedoms of data subjects;
- (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 Bill taking into account the rights and legitimate interests of data subjects and other persons concerned.

(3) A data controller or data processor shall, where a 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, submit the data impact assessment report to the Commission, **not later than 60 days prior to the processing of the data.**

Personal data relating to a child.

34. (1) A data controller or data processor shall not process personal data relating to a child unless –

- (a) consent is given by the child's parent or guardian; and
- (b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) For the purposes of subsection (1), verification of the age of a child shall be in accordance with prescribed standard procedure or mechanisms.

(3) Mechanisms contemplated under subsection (2) shall be determined on the basis of –

- (a) available technology;
- (b) volume of personal data processed;
- (c) proportion of personal data likely to be that of a child;
- (d) possibility of harm to a child arising out of processing of personal data; and
- (e) such other factors as may be specified by the Commission.

Processing of sensitive personal data.

35. (1) Subject to subsection (2), a data processor shall not process sensitive personal data of a data subject except in accordance with the following conditions -

- (a) the data subject has given his explicit consent to the processing of the personal data;
- (b) the processing is necessary –

- (i) for the purposes of exercising or performing a right or obligation which is conferred or imposed by law on the data controller or data processor in connection with employment;
 - (ii) in order to protect the vital interests of the data subject or another person in a case where consent cannot be given by or on behalf of the data subject or the data controller or data processor cannot reasonably be expected to obtain the consent of the data subject;
 - (iii) in order to protect the vital interests of another person in a case where consent by or on behalf of the data subject has been unreasonably withheld;
 - (iv) for medical purposes and is undertaken by a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health care professional;
 - (v) for the purpose of or in connection with legal proceedings;
 - (vi) for the purpose of obtaining legal advice;
 - (vii) for the purposes of establishing exercising or defending legal rights;
 - (viii) for the administration of justice;
 - (ix) for the exercise of a function conferred by or under any law; or
 - (x) for any other purposes as the Minister may by regulation prescribe.
- (c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

(2) The Minister may, by notice published in the Gazette, exclude the application of a subparagraph of paragraph (b) of subsection (1), where the condition stated shall not be regarded as satisfied unless further conditions are also satisfied

**Commercial
use of personal
data.**

36. (1) A person shall not use personal data obtained under this Act, for commercial purposes, unless the person –

- (a) has sought and obtained express consent from the data subject; or
- (b) is authorised to do so under a written law and the data subject has been informed of use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall where possible anonymise the data in such a manner as to ensure that the data subject is no longer identifiable

(3) The Commission may prescribe Code of Practice for commercial use of personal data under this Act.

**Consent
necessary for
processing
personal data.**

37. (1) Subject to subsection (2), a data controller or processor shall not process personal data unless consent is given by the data subject at the start of collecting the data.

(2) The consent of the data subject shall not be valid unless such consent is –

- (a) freely given;
- (b) informed, having regard to whether the data subject has been provided with the information required under [section 36](#);
- (c) specific, having regard to whether the data subject can determine the scope of consent in respect of the manner, time and purpose of processing;
- (d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given consent;
- (e) capable of being withdrawn except in the instance of completed civil registration process or by operation of law or by an order of court.

**Processing
personal data
without consent.**

38. Notwithstanding anything contained under [section 36](#), a data controller or data processor may collect or process personal data without obtaining the consent of the data subject if such collection or processing is necessary on the following grounds –

- (a) performance of a function of the State authorised by law;
- (b) the provision of a service or benefit to a data subject from the State;

- (c) the issuance of a certificate, licence or permit for an action or activity of a data subject by the State;
- (d) compliance with a law;
- (e) compliance with an order or judgment of a court or tribunal;
- (f) response to a medical emergency involving a threat to the life of a data subject;
- (g) undertaking of a legitimate measure to provide medical treatment to an individual during an epidemic, pandemic, outbreak of disease or any other threat to public health;
- (h) undertaking a measure to ensure safety of or provide assistance or service to a person during an emergency disaster or a breakdown of public order
- (i) recruitment or termination of employment of a data subject by a data controller or data processor;
- (j) provision of a service to or benefit sought by a data subject who is an employee of a data controller;
- (k) any other activity relating to the assessment of the performance of a data subject who is an employee of the data controller.

Use of data collected for specific purpose.

39. (1) Where a person holds personal data collected in connection with a specific purpose under **section 32**, further processing of the personal data shall only be for that specific purpose.

(2) A person who processes the personal data collected in connection with a specific purpose under subsection (1) shall take into account -

- (a) the relationship between the purpose of the intended further processing and the purpose for which the data was collected;
- (b) the nature of the data;
- (c) the manner in which the data has been collected;
- (d) the consequences that the further processing is likely to have for the data subject; and
- (e) the contractual rights and obligations between the data subject and the person who processes the data.

(3) The further processing of the data shall be considered to be compatible with the purpose of the collection where –

- (a) the data subject consents to the further processing of the information;
- (b) the personal data is publicly available or has been made public by the person concerned;
- (c) further processing is necessary for the prevention, detection, investigation, prosecution or punishment for an offence or breach of law;
- (d) processing is necessary for the enforcement of a law which imposes a pecuniary penalty;
- (e) processing is necessary for the enforcement of legislation relating to public revenue collection;
- (f) processing is necessary for the conduct of proceedings before a court or tribunal;
- (g) processing is necessary for the protection of national security;
- (h) processing is necessary to prevent or mitigate a serious and imminent threat to public health or safety or the life or health of the data subject or another individual;
- (i) the data is used for historical, statistical or research purposes and the person responsible for the processing ensure that –
 - (i) the further processing is carried out solely for the purpose for which the data was collected; and
 - (ii) the data is not published in a form likely to reveal the identity of the data subject.

**Retention
of records
of personal
data.**

40. (1) A person who collects personal data shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data is collected and processed unless the retention of the data is -

- (a) required or authorised by law;
- (b) necessary for a lawful purpose related to a function or activity for which the data is collected or processed;
- (c) required by a contract between the parties to the contract; or

- (d) done with the consent of the data subject.

(2) Subsection (1) shall not apply to personal data retained for –

- (a) the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
- (b) national security purposes;
- (c) enforcement of a law which imposes a pecuniary penalty;
- (d) enforcement of legislation relating to public revenue collection;
- (e) the conduct of proceedings before any court or tribunal; or
- (f) historical, statistical or research purposes.

(3) A person who uses personal data of a data subject to make a decision about the data subject shall –

- (a) retain the data for a period required or prescribed by law; or
- (b) where no retention period is required by law, retain the data for a period which shall afford the data subject an opportunity to request access to the data.

(4) Except provided by law, a data controller or data processor shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period.

**Processing
personal
data outside
Sierra Leone.**

41. Where a data processor based in Sierra Leone processes or stores personal data outside Sierra Leone, the data processor shall ensure that –

- (a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data, at least, equivalent to the protection provided for under this Act; and
- (b) the data subject has consented to processing or storing personal data outside Sierra Leone.

PART VII - RIGHTS OF DATA SUBJECT.

**Correction of
personal data.**

42. (1) A data subject may request a data controller or data processor to –

- (a) correct, deactivate, rectify, erase or delete personal data about the data subject processed by the data processor that is inaccurate,

irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

- (b) destroy or delete a record of personal data about the data subject processed by a data processor.

(2) A data controller or data processor shall, on receipt of a request under subsection (1) comply with the request.

(3) Where a data controller or data processor is not able to comply with the request under subsection (1), it shall inform the data subject and notify him in writing, stating the reasons for not complying.

(4) A data subject may appeal a decision of a data controller or data processor not to comply with his request to the Commission within 30 days of the date of the final decision of the data controller or data processor.

(5) A data controller or data processor shall, where it complies with the request by a data subject or the Commission, inform or update each person to whom the personal data has been disclosed, of the correction made.

(6) A data controller or data processor shall notify a data subject within a reasonable time of the action taken as a result of the request.

**Right to
access
personal
information.
controller or
data about that**

43. (1) A data subject who provides proof of identity may request a data controller or data processor to –

- (a) confirm whether or not the data processor holds personal data subject;
- (a) give a description of the personal data which is held by the data controller or data processor;
- (c) provide the identity of a third party or a category of third party who has or has had access to the personal data.

(2) A request under this section shall be made in such form as the Commission may prescribe.

(3) A data controller or data processor shall not comply with a request under this section –

- (a) unless he is given information that he may reasonably require to identify the person making the request and to locate the data requested by that person;
- (b) if the request cannot be complied with without disclosing data related to another data subject who may be identified from the information, unless-

- (i) the other data subject consents to the disclosure of the data;
- (ii) it is reasonable in all the circumstances to comply with the request without the consent of another data subject; or
- (iii) compelled by a court order.

(5) The inability of a data controller or data processor to comply with a request under subsection (1) shall not be an excuse for failing to communicate so much of the information sought that may be communicated without the disclosure of the identity of the data subject concerned.

(6) A data controller or data processor may, comply with a request under subsection (1) by omitting or deleting the name or other identifying particulars of another data subject.

(7) A data controller or data processor shall, for the purposes of determining whether it is reasonable to comply with a request under subsection (1) without the consent of another data subject, take into account –

- (a) the duty of confidentiality owed to the other data subject;
- (b) steps taken by the data controller or data processor to seek the consent of that other data subject;
- (c) whether the other data subject is capable of giving consent; and
- (d) an express refusal of consent by the other data subject.

Right to prevent processing of personal data.

44. (1) Subject to subsection (5), a data subject may, at any time by notice in writing, referred to as the data subject notice, to a data controller or data processor, require the data controller or data processor, at the end of such period as is reasonable in the circumstances, to cease the processing of his personal data or processing for a specified purpose or in a specified manner, based on the reasons to be stated in the notice, such as the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause –

- (a) substantial damage or substantial distress to him or to another person; and
- (b) damage or distress that is or would be unwarranted.

(2) A data controller or data processor shall, within 14 days from the date of receipt of a data subject notice under subsection (1), give the data subject a written notice stating -

- (a) that the notice has been complied with or is intended to be complied with; or
- (b) the reasons for regarding the notice as unjustified and the extent, if any, to which they have complied or intend to comply with.

(3) Where a data subject is dissatisfied with the failure of a data controller or data processor to comply with data subject notice, whether in whole or in part, the data subject may appeal within 30 days after the final decision of the data controller, to the Commission, requiring the data controller or data processor to comply with the notice.

(4) The Commission may, where it is satisfied that an appeal of a data subject under subsection (3) is justified or justified to an extent, require the data controller or data processor to take such steps to comply with the data subject notice.

(5) A data controller or data processor who fails to comply with the requirements of the Commission under subsection (4) commits an offence and is liable, on conviction, to a fine of not less than NLe. 20,000 but not exceeding NLe. 100,000.

(6) This section shall not apply where –

- (a) a data subject has given his consent;
- (b) the processing of personal data is necessary –
 - (i) for the performance of a contract to which the data subject is a party;
 - (ii) for the taking of steps, at the request of the data subject, with a view to entering a contract;
 - (iii) for compliance with a legal obligation to which the data controller or processor is the subject other than an obligation imposed by contract; or
 - (iv) in order to protect the vital interest of the data subject;
 - (v) in such other cases as the Minister may, by statutory instrument, prescribe.

Right to prevent processing of personal data for direct

45. (1) A data subject may at any time by notice in writing to a data controller or data processor, referred to as the data subject notice, require the data controller or data processor at the end of such period as is reasonable in the circumstances to cease processing the personal data for purposes of direct marketing.

marketing.

(2) Where a data subject is dissatisfied with the failure of a data controller or data processor to comply, whether in whole or in part, with a data subject notice, under subsection (1), within 21 days of the said notice, the data subject may appeal to the Commission, within 30 days of the final decision of the data controller or data processor, to require the data controller or data processor to comply with the data subject notice.

(3) The Commission may, where it is satisfied that the appeal of a data subject under subsection (2) is justified or justified to an extent, require the data controller or data processor to take such steps to comply with the data subject notice.

(4) A data controller or data processor who fails to comply with the requirements of the Commission under subsection (3) commits an offence and is liable, on conviction, to a fine of not less NLe. 20,000 but not exceeding NLe. 100,000.

(5) For the purposes of this section direct marketing means the communication, by whatever means, of an advertising or marketing material which is directed to a particular institution

**Rights in
relation to
automated
decision-taking.**

46. (1) A data subject may by notice in writing to a data controller or data processor, referred to as the data subject notice, require the data controller or data processor to ensure that a decision taken by or on behalf of the data controller or data processor which significantly affects that data subject is not based solely on the processing by automatic means of personal data in respect of that data subject.

(2) Without prejudice to subsection (1), where a decision which significantly affects a data subject is based solely on automated processing –

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

(3) A data controller or data processor shall within 14 days after receipt of a data subject notice, inform the data subject in writing of the steps that he has taken to comply with the notice.

(4) This section shall not apply to a decision made –

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

- (b) with a view to entering into a contract;
- (c) in the course of the performance of the contract; or
- (d) for a purpose authorised or required by or under any law.

(5) Where a data subject is not satisfied with the decision of a data controller or data processor under subsection (3), he shall appeal in writing to the Commission within 30 days after the final decision of the data controller or data processor.

(6) The Commission shall, where it is satisfied on a complaint by a data subject that a data controller or data processor has failed to comply, order the data controller or data processor to comply within 14 days.

**Right to
confirmation
and access.**

47. (1) A data subject shall have the right to request in writing the following from a data controller or data processor-

- (a) confirmation whether the data controller or data processor is processing or has processed personal data of the data subject;
- (b) the details or summary of the personal data of the data subject being processed or that has been processed by the data controller or data processor;
- (c) a brief summary of processing activities undertaken by the data controller or data processor regarding the personal data of the data subject including information requested under paragraph (a).

(2) A data controller or data processor shall, within 21 days after receipt of a request under subsection (1), respond, in writing, to the request of the data subject.

(3) Where the data controller or data processor refuses to respond to or grant the request of the data subject, the data subject shall appeal in writing to the Commission within 30 days after the final decision of the data controller or data processor.

(4) The Commission shall, where it is satisfied on a complaint by a data subject that a data controller or data processor has failed to comply, order the data controller or data processor to comply within 14 days.

**Right to
data portability.**

48. (1) Where data processing has been carried out through automated means the data subject shall have the right to –

- (a) receive the following personal data in a structured, commonly used and machine-readable format-
 - (i) the personal data provided to the data subject;
 - (ii) the data which has been generated in the course of provision of services or use of goods by the data controller or data processor; or
 - (iii) the data which forms part of a profile on the data subject or which the data controller or data processor has otherwise obtained; or
- (b) have the personal data transferred to another data controller or processor in a commonly used and machine-readable format.

(2) Subsection (1) shall not apply where –

- (a) processing is necessary for functions of the State or complying with a law or order of a court;
- (b) compliance with a request under subsection (1) would reveal a trade secret of a data controller or processor, or would not be technically feasible.

PART VIII - DATA CONTROLLER OR DATA PROCESSOR

Certificate of Registration.

49. (1) A person or entity, shall not operate as a data controller or data processor unless he is registered as such under this Act.

(2) An application for registration under subsection (1) shall contain the following information –

- (a) a description of the personal data to be processed by the data controller or data processor;
- (b) a description of the purpose for which the personal data is to be processed;
- (c) the category of the data subject to which the personal data relates;
- (d) contact details of the data controller or data processor;

- (f) contact details of a data protection officer of the data controller or processor;
- (e) a general description of the risks, safeguards, security measures and mechanism to ensure the protection of personal data;
- (f) any other measure as may be required by the Commission to protect the data subject from unlawful use of data by the data controller or data processor;
- (g) the privacy design policy and any other details as may be prescribed by the Commission.

(3) The Commission shall, on receipt of an application under subsection (1), issue a Certificate of Registration upon registration of a data controller or data processor.

(4) A data controller or data processor shall, where there is a change in the information supplied to the Commission under subsection (2), notify the Commission of such change.

(7) The Commission shall, on receipt of a notification under subsection (4), amend the registration accordingly.

(8) A data controller or data processor who –

- (a) knowingly supplies false or misleading information under subsection (3); or
- (b) fails to comply with any provision of this section,

commits an offence and is liable, on conviction, to a fine of not less than NLe. 10,000 but not exceeding NLe. 100,000.

Duration of Certificate of Registration.

50. A registration certificate issued under subsection (3) of section 47 shall be valid for a period of one year and may be renewed.

Cancellation or variation of Certificate of Registration.

51 The Commission may vary terms and conditions of a Certificate of Registration issued under subsection (3) of section 67 or cancel the registration where -

- (a) information given by an applicant is false or misleading;
- (b) the holder of the registration certificate fails to comply with a requirement of this Act.

**Compliance
and audit.**

52. The Commission may carry out periodical audits of the processes and systems of a data controller or data processor to ensure compliance with this Act.

**Register of
Data Controllers
and Data
Processors.**

53. (1) The Commission shall maintain a Register of Data Controllers and Data Processors.

(2) The Commission may, at the request of a data controller or data processor or of its own motion remove an entry in the register which has ceased to be applicable.

(3) A Register of Data Controllers and Data Processors under subsection (2), shall be a public document and shall be in either physical or digital form or both and available for public inspection.

PART IX - TRANSPARENCY, ACCOUNTABILITY MEASURES AND SECURITY OF DATA.

**Privacy
design
policy.**

54. (1) A data controller or data processor shall prepare a privacy design policy containing –

- (a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data subject;
- (b) the technology used in the processing of personal data in accordance with technically acceptable industry standards;
- (c) the legitimate business interests, including innovation achieved without compromising privacy interests;
- (d) the obligations of the data controller or processor;
- (e) the protection of privacy throughout processing from the point of collection to deletion or archiving of personal data.

(2) A data controller or data processor shall prepare and submit a privacy design policy under subsection (1) to the Commission for approval within such period as may be specified by the Commission.

(3) The Commission shall not approve a privacy design policy unless it is satisfied that it complies with the requirements set out in subsection (1).

(4) A data controller or data processor shall publish the approved privacy design policy on his website,

Technical and organisational measures.

55. (1) A data controller or data processor shall implement appropriate technical and organisational measures which are designed to -

- (a) implement the data protection principles in an effective manner;
- (b) integrate necessary safeguards into data processing.

(2) The duty of a data controller or data processor under subsection (1) shall apply at the time of –

- (a) the determination of the means of processing the data; and
- (b) the processing, and the manner or form of storage of personal data.

(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed taking into consideration the following –

- (a) the amount of personal data collected;
- (b) the extent to which personal data may be processed;
- (c) the manner, form, and period of its storage of personal data;
- (d) personal data accessibility; and
- (e) the cost of processing and storing data and the technologies and tools used.

(4) A data controller or data processor shall, for the purpose of giving effect to this section, consider measures to –

- (a) identify reasonably foreseeable internal and external risks to personal data under his possession or control;
- (b) establish and maintain appropriate safeguards against the identified risks;
- (c) undertake the pseudonymisation and encryption of personal data;
- (d) to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- (e) verify that the safeguards are effectively implemented and
- (f) ensure that the safeguards are continually updated in response to new risks of deficiencies.

Determining organisational measures.

56. (1) A data controller or data processor shall, in determining the appropriate technical and organisational measures under section 55, in particular where the processing involves the transmission of data over an information and communication network, have regard to the following –

- (a) the state of technological development available;
- (b) the cost of implementing any of the security measures;
- (c) the special risks that exist in the processing of the data; and
- (d) the nature of the data being processed.

(2) A data controller shall, where he is using the services of a data processor, –

- (a) opt for a data processor who provides sufficient guarantees in respect of organisational measures for the purpose of complying with subsection (1) of section 55; and
- (b) enter into a written contract with the data processor, which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller

(3) Where a data processor possesses personal data other than as instructed by the data controller, the data processor shall be deemed to be a data controller in respect of that processing.

(4) A data controller or data processor shall take all reasonable steps to ensure that a person employed by or acting under the authority of a data controller or data processor complies with the relevant security measures.

Transparency in personal data processing.

57. A data controller shall take necessary steps to maintain transparency in processing personal data and shall make the following information available –

- (a) the categories of personal data generally collected and the manner of such collection;

- (b) the purpose for which personal data is generally processed;
- (c) the categories of personal data processed in exceptional situations or exceptional purposes that create a risk of significant harm;
- (d) the existence of and the procedure in exercise of rights of the data subject;
- (e) the right of the data subject to file complaint against the data controller, or data processor, to the Commission;
- (f) any other information as may be prescribed.

Security measures relating to data processed by data processor.

58. (1) A data controller or data processor, shall ensure the integrity of personal data in the possession or control of a data controller or data processor by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage or unauthorised destruction and unlawful access to or unauthorised processing of the personal data.

(2) A data controller shall, for the purpose of subsection (1), take measures to –

- (a) identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;
- (b) establish and maintain appropriate safeguards against the identified risks;
- (c) regularly verify that the safeguards are effectively implemented; and
- (d) ensure that the safeguards are continually updated in response to new risks or deficiencies.

(3) A data controller shall observe generally accepted information security practices and procedures and specific industry or professional rules and regulations.

(4) A data controller shall not permit a data processor to process personal data for the data controller, unless the data processor establishes and complies with the security measures specified under this Act.

(5) A contract between a data controller and a data processor relating to processing of personal data, shall require the data processor to establish and

maintain the confidentiality and security measures necessary to protect the integrity of personal data.

**Data processed
by entity or
authorised
person.**

59. (1) A data processor, whether an entity or a natural person, who processes personal data on behalf of a data controller shall process the data only with the prior knowledge or authorisation of the data controller and shall treat the personal data which comes to their knowledge as confidential.

(2) A data processor shall not disclose data unless required by law or in the course of the discharge of a contractual duty.

**Notification
of breach.**

60. (1) A data controller shall, where personal data has been accessed or acquired by an unauthorised person or entity and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, –

- (a) notify the Commission without delay within 72 hours of becoming aware of such breach; and
- (b) subject to subsection (3) communicate to the data subject in written form within a reasonably practical period, unless the identity of the data subject cannot be established;

(2) Where a notification to the Commission under paragraph (a) is made after 72 hours, the notification shall be accompanied by reasons for the delay.

(3) A data processor shall, where he becomes aware of a personal data breach, notify the data controller without delay and where reasonably practicable within 48 hours of becoming aware of the breach.

(4) The data controller may delay or restrict communication under paragraphs (b) of subsection (1) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the relevant competent authority.

(5) A notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including –

- (a) description of the specific nature and extent of the personal data involved in the data breach;
- (b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;
- (c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

- (d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and
- (e) the name and contact details of contact point from whom information could be obtained.

(6) The communication of a breach to a data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data. (7) Where and to the extent that it is not possible to provide all the information referred to under subsection (5) at the same time, the information may be provided in phases, providing reasons and without undue delay.

(8) A data controller or data processor shall keep detailed records of all data breaches, regardless of whether they are reported to the Commission or the data subject and failure to keep these records and produce on an annual basis will result in such administrative fines as may be prescribed by the Commission.

PART X–THE RIGHT TO ACCESS INFORMATION

Access to information.

61. (1) A person has the right to access information held by or is under the control of –

- (a) a public authority;
- (b) a private body,

where that information is necessary for the enforcement or protection of a right.

(2) Nothing in this Act limits or otherwise restricts the disclosure of or the right to access, information pursuant to any other enactment, policy or practice.

(3) A person making a request for information to a public authority shall be entitled–

- (a) to have the public authority confirm or deny whether it holds information of the description specified in the request; and
- (b) where the public authority holds information of the description specified in the request, to have the information communicated to him.

(4) A public authority shall be deemed to have complied with subsection (3) if it has communicated the information to an applicant.

(5) In this Act, the duty of a public authority to comply with paragraph (a) of subsection (3) shall be referred to as “the duty to confirm or deny”.

**Submission
and form of
application.**

62. (1) An application to access information shall -

- (a) be made in writing;
- (b) describe the information requested; and
- (c) provide an address, which may be an email address, for purposes of correspondence.

(2) For the purposes of paragraph (a) of subsection (1), an application for information shall be deemed to be made in writing where the text of the request—

- (a) is transmitted by electronic means;
- (b) is received in legible form; and
- (c) is capable of being used for subsequent reference.

(3) An application to access information shall be made by email, fax, post, telephone or by any other medium provided that the applicant provides—

- (a) contact details; and
- (b) sufficient particulars for the public information officer or any other official to understand what information is requested.

(4) A public information officer who receives an oral application to access information shall put the application in writing, including the public information officer's name and designation and give a copy thereof to the applicant.

(5) A public information officer who receives an application to access information shall, where the application does not comply with subsection (3), render such reasonable assistance, free of charge, as may be necessary to enable the application to comply with that subsection.

(6) A public authority which receives an application to access information shall provide the applicant with a receipt documenting the application.

(7) A public authority shall record and maintain records of all applications to access information.

**Time limit
for compliance.**

63. (1) A public information officer who receives an application to access information shall dispose of the application as soon as possible, and in any event, not later than 15 working days of receipt of an application.

(2) Notwithstanding subsection (1), where an application to access information concerns the life or liberty of a person, application to access information shall be disposed of not later than 48 hours of receipt of the application.

(3) A public authority may, where an application to access information is complex or relates to a large volume of information, make an

application to the Commission for an extension of time not exceeding 15 working days.

(4) A failure to conform to the timelines set out in this section shall be deemed to be a refusal of an application to access information.

Transfer of application.

64. (1) Where a public authority does not hold information which is responsive to an application to access information or part of the application, that application or any relevant part of it may, not later than 3 days from the date of its receipt, be transferred to another public authority if the information is held by that other public authority.

(2) Where an application is transferred under subsection (1), the applicant shall be informed of the transfer immediately, and in any event not later than 3 working days from the date of the transfer.

(3) A public authority to which an application is transferred under subsection (1) shall decide the application to access information in accordance with the time limit set out in section 8, to run from the day upon which the public authority receives the transferred request.

Fee notice.

65. (1) A public authority to which an application to access information is made may, within the time limit for compliance specified in section 63, give the applicant a fee notice, stating that a fee of an amount specified in the notice is to be charged by the public authority for disposing of the application to access information.

(2) A public authority shall, where a fee notice under subsection (1), has been given to an applicant, not be obliged to comply with section 63 unless the fee is paid within the period of 3 months beginning on the day on which the fee notice is given to the applicant.

(3) A fee under this section shall –

- (a) not exceed the reasonable, cost-based amount for reproducing and sending the information to the applicant; and
- (b) be in accordance with Regulations made under this Act.

(4) Regulations made under paragraph (b) of subsection (3) may, in particular, provide that no fee shall be payable under this section in the following cases, where –

- (a) the applicant falls below a certain income level;
- (b) the application to access information is for personal information relating to the applicant; or
- (c) the application to access information is in the public interest, for example because the applicant intends to make the information public.

**Application
expressing
preference.**

66. (1) A public authority shall, where in an application to access information, the applicant expresses a preference for communication by any of the following means –

- (a) providing the applicant with a copy, certified or otherwise, of the information in permanent form or in another form acceptable to the applicant, such as an electronic form;
- (b) giving the applicant a reasonable opportunity to inspect a record containing the information;
- (c) providing the applicant with a digest or summary of the information in permanent form or in another form acceptable to the applicant; or
- (d) allowing the applicant to take notes, extracts and samples of a material,

so far as is reasonable, give effect to that preference.

(2) A public authority shall not be required to comply with subsection (1) where to do so would–

- (a) be detrimental to the preservation of the record;
- (b) unduly divert the resources of the public authority; or
- (c) breach a copyright not held by the public authority.

(3) Where a public authority does not, pursuant to subsection (2), comply with a preference expressed by an applicant in communicating the information, it shall–

- (a) notify the applicant of the reasons for his non-compliance; and
- (b) communicate the information to the applicant by any means reasonable in the circumstances.

**Proactive
publication.**

67. (1) The following classes of information form the core proactive publication obligations for every public authority –

- (a) the particulars of its organisation, functions and duties;
- (b) the powers and duties of its officers and employees;
- (c) the procedure followed in the decision-making process, including channels of supervision and accountability;
- (d) the norms set by it for the discharge of its functions;

- (e) any guidance used by the public authority in relation to its dealings with the public or with corporate bodies, including the rules, instructions, manuals and records, held by it or under its control or used by its employees for discharging its functions;
- (f) a guide sufficient to enable a person wishing to apply for information under this Act to identify the classes of information held by it, the subjects to which they relate or the location of an index to be consulted by a person;
- (g) the particulars of an arrangement that exists for consultation with or representation by, the members of the public in relation to the formulation of its policy or implementation thereof;
- (h) a statement of the boards, councils, committees and other bodies consisting of 2 or more persons constituted as its part or for the purpose of advising it with information as to whether meetings of those boards, councils, committees and other bodies are open to the public, or the minutes of the meetings are accessible to the public;
- (i) a directory of its officers and employees;
- (j) the monthly remuneration received by each of its officers and employees, including the system of compensation;
- (k) the budget allocated to each of its agencies, including the particulars of all plans, proposed expenditures and reports on disbursements made;
- (l) the manner of execution of subsidy programmes, including the amounts allocated and the details of beneficiaries of such programmes;
- (m) particulars of concessions, permits or authorisations granted by it;
- (n) details in respect of the information available to or held by it, in an electronic form;
- (o) the particulars of facilities available to citizens for obtaining information, including the working hours of a library or reading room, if maintained for public use;
- (p) the names, designation, contact details of its public information officers, appellate authorities

and the particulars and contact details of the Commission;

- (q) a list of applications under this Act received by the public authority, including an indexed register containing copies of records released in response to requests made under this Act other than records relating to the personal affairs of the applicant.

(2) A public authority shall adopt and disseminate widely, including on its website, a publication scheme approved by the Commission.

(3) A publication scheme under subsection (2), shall set out–

- (a) the classes of records that the public authority will publish on a proactive basis; and
- (b) the manner in which it will publish these records.

(4) A public authority shall, in adopting a publication scheme under subsection (2), have regard to the public interest in –

- (a) allowing access to the information it holds; and
- (b) making information available proactively so as to minimise the need for individuals to make an application to access information.

(5) A public authority shall publish information in accordance with its publication scheme.

(6) A publication scheme shall, within 7 years of the adoption of the first publication scheme by a public authority, cover all of the core proactive publication obligations set out in subsection (1).

(7) A person may institute proceedings in a court to compel the head of a public authority, to comply with this section.

Approval of publication scheme.

68. (1) The Commission may, when approving a publication scheme, provide that the approval shall expire at a certain time.

(2) The Commission shall, when refusing to approve a publication scheme, give reasons and provide reasonable direction to the public authority as to how it may amend the publication scheme so as to obtain approval.

(3) The Commission may, upon giving 6 months' notice with reasons, withdraw its approval of a publication scheme.

Model publication scheme.

69. (1) The Commission may adopt or approve a model publication scheme for different classes of public authorities.

(2) Where a public authority in a certain class adopts a model publication scheme which applies to that class of public authorities, it shall not require further approval from the Commission, but it shall inform the Commission that it is applying that model publication scheme.

**Other
proactive
schemes.**

(3) The Commission may put a time limit on the validity of a model publication scheme or, upon giving 6 months' notice to all public authorities using it, terminate the validity of a publication scheme.

70. (1) A public authority shall, in addition to the items listed in its publication scheme, also—

- (a) publish all relevant facts while formulating important policies or announcing the decisions which affect the public;
- (b) provide to a person the reasons for a decision taken by it in relation to that person;
- (c) before initiating a project or formulating a policy, scheme, programme or law, publish or communicate to the public in general or to the persons likely to be affected by it in particular, the facts available to it or to which it has reasonable access which in its opinion should be known to them in the best interests of natural justice and promotion of democratic principles;
- (d) unless there are good reasons to the contrary, allow members of the public to attend its meetings at which decisions affecting them are made and shall give adequate notice of the meetings;
- (e) upon signing a contract shall publish it in the Gazette, detailing at a minimum for each contract—
 - (i) the public works, goods acquired or rented, and the contracted service, including any sketches, scopes of service and terms of reference;
 - (ii) the contract sum;
 - (iii) the name of the provider, contractor or individual to whom the contract has been granted;
 - (iv) the periods within which the contract shall be completed.

(2) A public authority shall take steps in accordance with its publication scheme and the requirements of subsection (1) to provide information proactively to the public at regular intervals through various media of communication.

(3) A material shall be disseminated taking into consideration the need to reach persons with disability, the cost, local language and the most effective method of communication in that local area; and the information

should be easily accessible and be available free or at cost, taking into account the medium used.

(4) At a minimum, the material referred to in subsection (1) shall be made available—

- (a) for inspection without charge;
- (b) by supplying a copy on request for which a reasonable charge to cover the costs of copying and supplying them may be made; and
- (c) on the internet, provided that the materials are held by the public authority in electronic format.

PART XI – EXEMPT INFORMATION

Exempt information.

71. (1) Information is exempt information if its disclosure by a public authority is exempted under this Act.

(2) Notwithstanding subsection (1), information shall not be exempt where the public interest in accessing the information out-weighs the harm which the exemption seeks to prevent.

Notice of exempt information.

72. A public authority shall, where in relation to an application to access information, it is relying on a claim that the information is exempt information, within the time limits for complying under section 63, notify the applicant in writing stating—

- (a) that the information is exempt;
- (b) the specific exemption in question; and
- (c) why the exemption applies.

Information accessible by other means.

73. (1) The duty to disclose information shall not apply if, or to the extent that, compliance with section 63 would involve the disclosure of information which is reasonably accessible to an applicant.

(2) For the purposes of subsection (1) information is reasonably accessible, if it is information that –

- (a) is accessible only on payment, as long as the payment does not exceed the fees that would be applicable under this Act;
- (b) the public authority or any other person is bound by law to communicate;
- (c) is held by a public authority is not regarded as reasonably accessible merely because the information is available from the public authority itself on request, unless the information is made available in accordance with the **publication scheme referred to in section 68.**

**Non-application
of duty to
disclose
information.**

74. The duty to disclose information shall not apply if, or to the extent that, -

The duty to disclose information shall not apply if, or to the

- (a) compliance with section 63 would reasonably be expected to seriously prejudice national security and the defence of Sierra Leone;
- (b) compliance with section 63 would, or could reasonably be expected to seriously prejudice relations between Sierra Leone and any other state or inter-governmental body;
- (c) compliance with section 63 would, or could reasonably be expected to seriously prejudice the ability of the Government to manage the economy;
- (d) compliance with section 63 would, or could reasonably be expected to cause serious prejudice to—
 - (i) the prevention and detection of crime;
 - (ii) the apprehension and prosecution of offenders; or
 - (iii) matters that are *subjudice*.
- (e) compliance with section 63 would, in relation to information obtained by the public authority from a third party, would or could reasonably be expected to constitute a breach of confidence actionable by that third party.
- (f) compliance with section 63 would involve a breach of the rules governing legally privileged information.
- (g) compliance with section 63 would involve the unreasonable disclosure of personal information concerning an individual:

Provided that disclosure is not unreasonable if—

- (i) the individual to whom the information relates gives prior consent;
- (ii) the disclosure is required to promote public health or public safety;
- (iii) the disclosure is necessary in order to subject public authorities and private bodies to public scrutiny;

- (iv) the disclosure is made to the individual to whom the information relates;
 - (v) the disclosure can reasonably be expected not to have an adverse effect on the affairs of a person or prejudice the future supply of the information;
 - (vi) the information is already available to the public;
 - (vii) the individual to whom the information relates was informed or made aware prior to supplying the information that the information belongs to a class of information that will or might be made available to the public;
 - (viii) in the case of a deceased person, the applicant is the next-of-kin or represents the next-of-kin of the deceased;
 - (ix) the third party has been deceased for more than 20 years.
- (h) compliance with section 63, in relation to information obtained by a public authority from a third party, would divulge a trade secret or would or could really be expected to seriously prejudice a commercial interest of that third party;
 - (i) compliance with section 63 would or could reasonably be expected to seriously prejudice the commercial interests of a public authority;
 - (j) relates to a matter concerning the traditional rites or customary usages of a group of people in Sierra Leone.

Historical records.

75. Access to a historical record shall not be denied under this Part unless the Commission certifies that there is an ongoing need for it to be kept confidential.

Severability.

76. Where a request for information relates to a record containing information which falls within the scope of an exception in this Part, an information in the record which is not subject to an exception shall, to the extent it may reasonably be severed from the rest of the information, be provided to the applicant.

PART XII –MEASURES TO PROMOTE OPENNESS

Development of information communication facilities.

77. A public authority shall develop, for the purposes of this Act, information communication technology units in accordance with the national information communication technology policy of Sierra Leone, to—

- (a) facilitate access to information;
- (b) ensure transparency and accountability;
- (c) improve record keeping.

Maintenance of records.

78. A public authority shall record and maintain records of its activities in a manner that facilitates the right to information, in accordance with this Act and the Code of Practice under section 87.

Code of Practice.

79. The Commission shall, after consultation with other stakeholders issue and from time to time update a Code of Practice relating to the keeping, management and disposal of records, as well as the transfer of records to public archives.

PART XIII–OFFENCES AND PENALTIES

Denying or obstructing access to record or information.

80. (1) A person shall not –

- (a) deny or obstruct the access of another person to a record or information contrary to this Act;
- (b) obstruct compliance by a public authority of any of its obligations under this Act;
- (c) interfere with the work of the Commission or an officer of the Commission;
- (d) destroy a record with intent to deny access to a request made under this Act; or
- (e) deliberately conceal or falsify a record or provide false, misleading, incomplete or inaccurate information in response to a request made under this Act,

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to, in the case of –

- (a) an individual to a fine not exceeding NLe. 20,000 or to a term of imprisonment not exceeding one year to both the fine and imprisonment;
- (b) a body corporate to a fine not exceeding NLe. 200,000.

**Failure to
supply
information
requested.**

81. (1) A person shall not, without reasonable excuse, fail to supply information requested under this Act, within the period specified in this Act.

(2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to, in the case of –

- (a) an individual to a fine not exceeding NLe. 20,000 or to a term of imprisonment not exceeding one year to both the fine and imprisonment;
- (b) a body corporate to a fine not exceeding NLe. 200,000.

**Unauthorised
disclosure or
storage of
personal data.**

82. (1) A data controller shall not disclose or store personal data in a manner that is incompatible with the purpose for which such data has been collected.

(2) A data processor shall not process sensitive personal data of a data subject without the explicit consent of the data subject and the processing is necessary.

(3) A data processor shall not disclose or store personal data processed by him without the prior authority of the data controller.

(4) A person shall not, -

- (a) obtain access to personal data or information constituting such data, without prior authority of the data controller or data processor by whom the data is kept; or
- (b) disclose personal data to a third party:

Provided that this subsection shall not apply to a person who is an employee or agent of a data controller or data processor acting within the scope of such mandate.

(5) A person shall not offer to sell personal data where such personal data has been obtained in breach of subsection (1).

(6) A person who contravenes a provision under this section commits an offence and is liable, on conviction, to a fine not less than NLe. 20,000 but not exceeding NLe. 100,000.

**Offence by
corporation.**

83. Where an offence under this Act is committed by a corporation, the corporation and every officer of the corporation who knowingly and wilfully authorises or permits the contravention shall be liable on conviction to pay a fine of not less than NLe. 20,000 Leones and not exceeding NLe. 100,000.

General penalty.

84. (1) A person who commits an offence under this Act, for which a specific penalty is not provided, shall, on conviction, be liable to a fine not less than NLe. 20,000 and not exceeding NLe. 100,000.

(2) The court may in addition to the penalty referred to under subsection (1) –

- (a) order the forfeiture of an equipment or an article used or connected in any way with the commission of an offence under this Act; or
- (b) order or prohibit the doing of an act to stop a continuing contravention.

PART XIV – MISCELLANEOUS

**Appeal
mechanism.**

85. (1) The Commission may create an internal appeal mechanism which requesters may use, if they wish to complain that their rights under this Act have been violated.

**Complaints
against breach
or non-compliance.**

86. (1) A person or a data subject who believes that his rights under this Act has been infringed or violated, may make a complaint in the prescribed to the internal appeal mechanism under section 8.

(2) The internal appeal mechanism shall, on receipt of a complaint under subsection (1), review of the complaint to ascertain whether the Commission failed to comply with an obligation under this Act, including–

- (a) refusing to indicate whether or not it holds a record, or to provide access to information, contrary to section 61;
- (b) failing to respond to a request for information within the time limits established in section 63;
- (c) failing to communicate information in the form requested under this Act;
- (d) charging an excessive fee, contrary to section 65;
- (e) refusing to accept an application requesting access to information;
- (f) personal data has been disclosed or stored in a manner that is incompatible with the purpose for which such data has been collected;
- (g) any other matter relating to a request for access to information or data protection under this Act.

**Code of
Practice.**

87. (1) The Commission may, by statutory instrument, make regulation specifying the Code of Practice to promote good practices of data protection and facilitate compliance with the obligations under this Act.

(2) The Code of Practice referred to under subsection (1) may include the following –

- (a) requirements for notice referred to under the Act;
- (b) measures for ensuring quality of personal data processed;
- (c) measures pertaining to the retention of personal data;
- (d) manner for obtaining a valid consent from a data subject;
- (e) measures pertaining to processing of personal data;
- (f) measures pertaining to processing of sensitive data;
- (g) processing of personal data under any other ground for processing including processing of personal data of children
- (h) exercise of any right by a data controller or data processor;
- (i) the standard and means by which a data controller or data processor may avail the right to data portability;
- (j) transparency and accountability measures including the standards to be maintained by data controllers and data processors;
- (k) standards for safeguards to be maintained by the data controller and data processor;
- (l) method of deletion or erasure of personal data when required under the Act;
- (m) appropriate action to be taken by the data controller or data processor in response to a personal data breach;
- (o) manner in which data protection impact assessment may be carried out by the data controller or a class of data controllers;
- (p) transfer of personal data out of Sierra Leone;
- (q) processing of any personal data or sensitive personal data to carry out any activity

necessary for research archiving or statistical purposes;

- (r) any other matter which in the view of the Commission may be necessary to be included in the code of practice.

(3) A person who contravenes a Code of Practice under this section commits an offence and is liable, on conviction, to a fine not less than NLe. 20,000 but not exceeding NLe. 100,000.

Compensation for failure to comply with Act.

88. Where a data subject suffers damage or distress through the contravention by a data controller, data processor, or data collector of the requirements of this Act, the data subject is entitled to apply to a court for compensation from the data collector, data processor or data controller for the damage or distress.

Regulation.

89. The Minister may, by statutory instrument, after consultation with the Commission, make regulations for any matter which is necessary to give effect to this Act.

Transitional provisions.

90. On the commencement of this Act, assets, including funds and administrative records which, immediately before the commencement of this Act, were vested in the Right to Access Information Commission shall be vested in the Data Protection and Right to Access Information Regulatory Commission.

Repeal and savings.

91. (1) The Right to Access to Information Act, 2013 (Act No. 2 of 2013) is hereby repealed.

(2) Notwithstanding subsection (1), a regulation, order or other statutory instrument made under Right to Access to Information Act, 2013 and in force immediately before the commencement of this Act shall remain in force until their expiration or are expressly repealed.

MEMORANDUM OF OBJECTS AND REASONS

The object of this Bill is to provide for the establishment, functions and powers of the Data Protection and the Right to Access to Information Regulatory Commission and to provide for other related matters.

The Bill is divided into 14 parts -

PART I- deals with Preliminary and includes Interpretation, Application and exemption provisions.

PART II- deals with the Data Protection and Right to Access Information Regulatory Commission including composition, meetings, disclosure of interest, immunity, committees of Board, etc.

PART III – deals with the functions and powers of the Commission.

PART IV – deals with administrative provisions including Executive-Chairman, Data Protection Commissioner, Access to Information Commissioner, other staff and directorates.

PART V – deals with financial provisions including funds of Commission, accounts and audit, financial year and annual report.

PART VI– deals with principles of data protection including collecting, processing, holding or use of personal data, restriction on processing, prohibition of collecting and processing of sensitive personal data, protection of privacy, collection of data from data subject etc.

PART VII – deals with the rights of data subject including correction of personal data, right to access personal information, right to prevent processing of personal data, right to prevent processing of personal data for direct marketing, rights in relation to automated decision-taking etc.

PART VIII – deals with data controller or data processor including certificate of registration, duration of certificate of registration, cancellation or variation of certificate of registration, compliance and audit etc.

PART IX – deals with transparency, accountability measures and security of data including privacy design policy, technical and organisational measures, determining organisational measures, transparency in personal data processing, security measures relating to data processed by data processor etc.

PART X – deals with the right to access information including access to information, submission and form of application, time limit for compliance, transfer of application, fee notice, application expressing preference etc.

PART XI– deals with exempt information including notice of exempt information, information accessible by other means, non-application of duty to disclose information etc.

PART XII– deals with measures to promote openness including development of information communication facilities, maintenance of records and code of practice.

PART XIII – deals with offences and penalties including denying or obstructing access to record or information, failure to supply information requested, unauthorised disclosure of storage of personal data, offence by corporation and general penalty.

PART XIV – deals with miscellaneous including appeal mechanism, complaints against breach or non-compliance, code of practice, compensation for failure to comply with Act, regulation etc.

MADE this day of , 2025.

Chernor Bah
Minister of Information and Communications

Freetown,
Sierra Leone.