



**“AN ACT FOR THE COLLECTION, PROCESSING,
TRANSMISSION, STORAGE, PROTECTION, AND USE OF
PERSONAL INFORMATION IN LIBERIA”**

APPROVED: MARCH 9, 2026

**PUBLISHED BY AUTHORITY
MINISTRY OF FOREIGN AFFAIRS
MONROVIA, LIBERIA**

PRINTED: MARCH 23, 2026



**AN ACT FOR THE COLLECTION, PROCESSING,
TRANSMISSION, STORAGE, PROTECTION, AND USE OF
PERSONAL INFORMATION IN LIBERIA**

PREAMBLE

Whereas, the use of the internet and the physical collection of personal information everywhere has raised concerns about individuals' personal information protection and privacy;

Whereas, personal information protection and privacy safeguards individual's information from unauthorized access thereby safeguarding personal integrity;

Whereas, the Constitution of Liberia in Article 16 provides for a person's fundamental human right to privacy and interference thereto only through judicial orders;

Whereas, the regional body ECOWAS in 2010 adopted the *Supplementary Act on Personal Data Protection* that provides guidance on the content and obligations of member states, and to which Liberia signed unto;

Recognizing the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

Now, therefore, it is enacted by the Senate and House of Representatives of the Republic of Liberia in Legislature Assembled:

LIBERIA

Data Protection and Privacy Act of 2024

Chapter I – General Provisions

- Section 1: Title
- Section 2. Short Title
- Section 3. Objective
- Section 4. Definition of Terms
- Section 5. Scope
- Section 6. Application of the law related to the media and the protection of privacy
- Section 7. Extraterritorial Application

Chapter II – The Independent Information Commissioner

- Section 8. Functions of the Commissioner
- Section 9. Confidentiality
- Section 10. Working Structure of the Commissioner

Chapter III – Processing of Personal Information

- Section 11. General Data Privacy Principles
- Section 12. Criteria for Lawful Processing of Personal Information.
- Section 13. Sensitive Personal Information and Privileged Information
- Section 14. Subcontract of Personal Information
- Section 15. Extension of Privileged Communication

Chapter VI – Rights of The Data Subject

- Section 16. Rights of the Data Subject
- Section 17. Transmissibility of Rights of the Data Subjects
- Section 18. Right to Data Portability
- Section 19. Non-Applicability

Chapter V – Security of Personal Information

- Section 20. Security of Personal Information

Chapter VI – Accountability for Transfer of Personal Information

- Section 21. Principle of Accountability

Chapter VII – Security of Sensitive Personal Information in Government

- Section 22. Responsibility of Heads of Agencies
- Section 23. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information
- Section 24. Applicability to Government Contractors

Chapter VIII – Penalties

- Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information
- Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence
- Section 27. Improper Disposal of Personal Information and Sensitive Personal Information
- Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
- Section 29. Unauthorized Access or Intentional Breach
- Section 30. Concealment of Security Breaches Involving Sensitive Personal Information
- Section 31. Malicious Disclosure
- Section 32. Unauthorized Disclosure
- Section 33. Combination or Series of Acts
- Section 34. Extent of Liability
- Section 35. Large-Scale
- Section 36. Offense Committed by Public Officer
- Section 37. Restitution

Miscellaneous Provisions

- Section 38. Interpretation
- Section 39. Implementing Rules and Regulations (IRR)
- Section 40. Reports and Information
- Section 41. Transitory Provision
- Section 42. Separability Clause
- Section 43. Repealing Clause
- Section 44. Effectivity Clause

Chapter I

General Provisions

Section 1: Title

This Act shall be known as the Act for the Collection, Processing, Transmission, Storage, Protection, and use of Personal Information in Liberia

Section 2: Short Title.

This Act may be cited as the "Personal Data Protection and Privacy Act of 2024".

Section 3: Objective

The objectives of this Act are as follows:

- i. To provide the legal framework for the protection and privacy of information relating to the collection, processing, transmission, storage, and use of personal information without prejudice to the general interest of the State; and,
- ii. To provide the necessary penalties for the unauthorized access, processing and use, including concealment of breaches and other malicious disclosures of personal information data in the care of individuals and institutions that collect, hold, process, use, transfer or disclose such information.

Section 4: Definition of Terms.

Whenever used in this Act, the following terms and phases shall have the respective meanings hereafter set forth:

- a. **"Data subject"** means an individual who is the subject of personal information processing;
- b. **"Consent of the data subject"** is any manifestation of specific, unequivocal, free, informed and expressed will by which the data subject or his legal, judicial or agreed representative accepts that his personal data be processed either manually or electronically;
- c. **"Personal data"** refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
- d. **"Direct marketing"** refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

- e. **"Recipient of personal data processing"** is any individual to whom the data may be disclosed, and who is not the data subject, the data controller, the data processor, or persons who by virtue of their functions are responsible for processing such data;
- f. **"Filing system"** refers to any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.
- g. **"Information and Communications System"** refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.
- h. **"Personal information controller"** refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:
 - 1. A person or organization who performs such functions as instructed by another person or organization; and
 - 2. An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family or household affairs.
- i. **"Personal information processor"** refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
- j. **"Processing"** refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.
- k. **"Privileged information"** refers to any and all forms of data which under any statute, law, regulations, directive or the Rules of Court and other pertinent laws constitute privileged communication.
- l. **"Sensitive data"** means personal data relating to an individual's religious, philosophical, political, trade union opinions or activities, to his sexual life, racial origin or health, relating to social measures, proceedings, and criminal or administrative sanctions;

m. **"Sensitive personal information"** refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to, national identification or social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an act of the Legislature or an executive order to be kept classified.

n. **"Health data"** means any information about the physical and mental health of the data subject, including the above-mentioned genetic data;

o. **"Direct prospecting"** means any message sent, on whatever medium and of whatever nature, in particular a commercial, political or charitable message, aimed at promoting, directly or indirectly, goods, services or the image of a person selling goods or providing services;

p. **"Code of conduct"** refers to the data-use charters drafted by the data controller in order to institute the rightful use of IT resources, the Internet, and electronic communications of the structure concerned, and which have been approved by the Independent Information Commissioner;

q. **"Authority of Protection"** refers to the Independent Information Commissioner responsible for ensuring that personal data is processed in compliance with the provisions of this Act.

r. **"Third party"** means any public or private individual or legal entity, body or association other than the data subject, the data controller, the data processor and any other persons placed under the direct authority of the data controller or the data processor, who is authorized to process data;

s. **"Personal data file"** means any structured set of data that is accessible according to defined criteria, whether the set is centralized, decentralized, or distributed functionally or geographically;

t. **"Combining personal data"** refers to any connection mechanism that consists of linking data processed for a given purpose with other data processed for a purpose that may or may not be identical, or that are linked by one or several data controllers;

u. **"Data controller"** means any public or private individual or legal entity, body or association who, alone or jointly with others, who collect and process personal data and determines the purposes for

which such data are processed;

Section 5. *Scope.*

This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing of residents of Liberia and the ECOWAS Region or beyond, including those personal information controllers and processors.

The following activities shall be subject to this Act:

- a. Collection, processing, transmission, storage, and use of personal data by any individual, by Government, local authorities, and public or private legal entities;
- b. Any processing of data related to public security, defense, investigation and prosecution of criminal offences or State security, subject to such exemptions as are defined by specific provisions stipulated in other legal texts in force.

This Act does not apply to the following:

(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

- (1) The fact that the individual is or was an officer or employee of the government institution;
- (2) The title, business address and office telephone number of the individual;
- (3) The classification, salary range and responsibilities of the position held by the individual; and
- (4) The name of the individual on a document prepared by the individual in the course of employment with the government;

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual or juridical person, including the name of the individual or juridical person and the exact nature of the benefit;

(d) Processing of personal data that is carried out for the purposes of journalism, research or artistic or literary expression shall be allowed when such processing is executed solely for the purposes of literary and artistic expression or in the exercise of the professional activity of journalist or researcher, in compliance with the ethical rules of these professions.

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority of the Republic.

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Republic.

Section 6. Application of the law related to the media and the protection of privacy

5. 1 Nothing in this Act shall be construed as to have amended or repealed the rights of the publishers, editors or reporters of any newspaper, magazine or periodical of general circulation or radio station and any other form of public information to be protected from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter, as established by national legislation and/or international and regional human rights standards.

5.2 The provisions of this Act shall not preclude the enforcement of legal provisions relating to the protection of privacy as provided for in the Penal Code.

Section 7. *Extraterritorial Application.*

This Act applies to an act done or practice engaged in and outside of the Republic and ECOWAS Region by an entity or individual if:

(a) The act, practice or processing relates to personal information about Liberian resident or ECOWAS Region;

(b) The entity has a link with the Liberian government or ECOWAS Region, and the entity is processing personal information in the Republic or ECOWAS Region or even if the processing is outside the Republic or ECOWAS Region as long as it is about Liberian or ECOWAS residents such as, but not limited to, the following:

- (1) A contract is entered in the Republic or ECOWAS Region;
- (2) A juridical entity unincorporated in the Republic or ECOWAS Region but has central management and control in the country; and
- (3) An entity that has a branch, agency, office or subsidiary in the Republic or ECOWAS Region and the parent or affiliate of the Liberian or ECOWAS entity has access to personal information; and

(c) The entity has other links in the Republic or ECOWAS Region such as, but not limited to:

- (1) The entity carries on business in the Republic or ECOWAS Region; and
- (2) The personal information was collected or held by an entity in the Republic or ECOWAS Region

Chapter II

The Independent Information Commissioner

Section 8: *Functions of the Independent Information Commissioner.*

To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards and best practice set for data protection and privacy, there is hereby amended the Freedom of Information Act of 2010 to confer on the Independent Information Commissioner, an independent oversight body of the Government of Liberia created by the Freedom of Information Act of 2010 which shall have the following additional functions:

- (a) Ensure compliance of personal information controllers with the provisions of this Act;
- (b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided*, that in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commissioner shall act as a collegial body. For this purpose, the Commissioner may be given access to personal information that is subject of any complaint and to collect the information necessary to perform his/her functions under this Act;
- (c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;
- (d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data protection and privacy;
- (e) Monitor the compliance of other government ministries, agencies or instrumentalities on their security and technical measures in place to protect personal data and recommend the necessary action in order to meet minimum standards pursuant to this Act;
- (f) Coordinate with other government ministries and agencies and the private sector, including civil society, the media and academic institutions on efforts to formulate and implement plans and policies to strengthen the protection of personal data in the country;
- (g) Issue regulation(s) to guide the implementation of data protection, retention and disposal pursuant to the objectives of this Act;
- (h) Publish a compilation of agency system of records and notices, including index and other finding aids;
- (i) Recommend to the Ministry of Justice (MOJ) the prosecution of violations as specified in this Act;

(j) Review, approve, reject, or require modification of privacy codes voluntarily adhered to by personal information controllers; *provided*, that the privacy codes shall adhere to the underlying data privacy principles embodied in this Act; *provided, further*, that such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commissioner shall consult with the relevant regulatory agencies and stakeholders in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: *Provided, finally*, that the Commissioner may review such privacy codes and require changes thereto for purposes of complying with this Act;

(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(l) Comment on the implication on data protection and privacy of proposed statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws and regulations;

(m) Make suggestions as to the simplification and improvement of the legislative and regulatory framework governing data processing;

(n) Participate in international fora or negotiations concerning the protection of personal information;

(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Liberian companies doing business abroad to respond to foreign privacy or data protection laws and regulations;

(q) Ensure that ICTs do not constitute a threat to public liberties and privacy by performing the following:

- i) inform data subjects and data controllers of their rights and obligations.
- ii) respond to all requests for an opinion relating to processing of personal data.
- iii) examine the prerequisite conditions for implementing personal data processing
- iv) receive claims, petitions, and complaints relating to processing of personal data and inform the affected party of action taken on such matters.
- v) immediately inform the Ministry of Justice of certain types of offences of which it may gain knowledge to act as needed.
- vi) carry out verifications of any processing of personal data, using sworn officials.
- vii) impose administrative and financial sanctions on data controllers;
- viii) update a register of personal data processing and make it available to the public;
- ix) authorize trans-border transfers of personal data;
- x) make suggestions as to the simplification and improvement of the legislative and regulatory framework governing data processing;
- xi) set up mechanisms for cooperation with personal data protection authorities of third countries;
- xii) Submit annual activity report with focus on personal data protection to the President and the National Legislature.

xiii) In compliance with the provisions of this Act, sworn personnel of the Technical Secretariat may be called upon to participate in carrying out verification missions.

(r) Generally, perform such acts as may be necessary to facilitate cross-border enforcement of data privacy and protection.

(s) Organize routine public awareness activities and programs nationwide to inform institutions and the general public about the importance of safeguarding individuals' personal information, privacy and integrity, and about the risk and abuse unauthorized access poses to people's confidential information.

2) The Independent Information Commissioner (IIC) may issue the following notices:

- i) a warning to a data controller who does not comply with the obligations enshrined in this Act;
- ii) A formal demand to desist from the violations within a time stipulated by the IIC not to exceed 14 calendar days.

3) In case of emergency, when processing and use of personal data may lead to a violation of rights and liberties, the IIC may decide:

- i) To suspend the processing;
- ii) To block certain personal data processed;
- iii) To temporarily or permanently prohibit any processing that is contrary to the provisions of this Act.

Section 9. *Confidentiality.*

The Commissioner shall always ensure that personal data is protected and processed confidentially, in particular when processing includes transmission of personal data on a network or transfer of personal data for external use.

Section 10. *Working Structure of the Commissioner.*

The working structure of the Commissioner shall remain consistent with the operational structure as provided for within the Freedom of Information Act of 2010, except that for the purpose of this Act, the Commissioner shall have data protection and monitoring responsibilities as part of his/her function.

Chapter III

Processing of Personal Information

Section 11. *General Data Privacy Principles.*

The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal data must, be:

- (a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
- (b) Processed fairly and lawfully;
- (c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information or data, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
- (d) Adequate and not excessive in relation to the purposes for which they are collected and processed;
- (e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise, or defense of legal claims, or for legitimate business purposes, or as provided by law; and
- (f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided*, that personal information collected for other purposes may be processed for historical, statistical or scientific purposes, and shall remain private, undisclosed and protected.

The personal information controller must ensure implementation of personal data processing principles set out herein.

Section. 12. *Criteria for Lawful Processing of Personal Information.*

The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which requires protection under the Constitution of Liberia.

Section 13. *Sensitive Personal Information and Privileged Information.*

The processing of sensitive personal data and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: *Provided*, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further*, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided*, that such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further*, That the sensitive personal information are not transferred to third parties: *Provided, finally*, That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority.

Section 14. *Subcontract of Personal Information.*

A personal information controller may subcontract the processing of personal information: *Provided*, that the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

Chapter IV **Rights of The Data Subject**

Section 16. *Rights of the Data Subject.*

The data subject is entitled to:

- (a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;
- (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
 - (1) Description of the personal information to be entered into the system;
 - (2) Purposes for which they are being or are to be processed;
 - (3) Scope and method of the personal information processing;
 - (4) The recipients or classes of recipients to whom they are or may be disclosed;
 - (5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
 - (6) The identity and contact details of the personal information controller or its representative;
 - (7) The period for which the information will be stored; and
 - (8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint, first with the Independent Information Commissioner and thereafter seek remedial redress in keeping with the process established under the Freedom of information Act of 2010.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided*, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena* or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

(c) Reasonable access to, upon demand, the following:

- (1) Contents of his or her personal information that were processed;
- (2) Sources from which personal information were obtained;
- (3) Names and addresses of recipients of the personal information;
- (4) Manner by which such data were processed;
- (5) Reasons for the disclosure of the personal information to recipients;
- (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
- (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
- (8) The designation, or name or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly unless the request is vexatious or otherwise unreasonable. If the personal information has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided*, That the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, and false, unlawfully obtained or unauthorized use of personal information.

Access to Information Commission and subsequent judicial oversight for the protection of his right.

Section 17. *Transmissibility of Rights of the Data Subject.*

The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

Section 18. *Right to Data Portability.*

The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data

undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commissioner may specify the electronic format referred to above, as well as the technical standards, modalities, and procedures for their transfer.

Section 19. *Non-Applicability.*

The immediately preceding sections are not applicable if the processed personal information is used only for the needs of scientific and statistical research and, based on such, no activities are carried out and no decisions are taken regarding the data subject: *Provided*, That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

Chapter V

Security of Personal Information

Section 20. *Security of Personal Information.* –

(a) The personal information controller must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

(c) The determination of the appropriate level of security under this section must consider the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. The measures implemented must include:

- (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
- (2) A security policy with respect to the processing of personal information;
- (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
- (4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information is not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller believes, such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the Commissioner may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.

(2) The Commissioner may exempt a personal information controller from notification where, in his/her reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commissioner may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Chapter VI

Accountability for Transfer of Personal Information

Section 21. Principle of Accountability.

Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

Chapter VII

Security of Sensitive Personal Information in Government

Section 22. Responsibility of Heads of Agencies.

All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein and is required to monitor the compliance and may recommend the necessary action to satisfy the minimum standards.

Section 23. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.

(a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commissioner, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-site Access – Unless otherwise provided in this Act, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:

- (1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;
- (2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and
- (3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured using the most secure encryption standard.

Section 24. Applicability to Government Contractors.

In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the agency in accordance with this Act and to comply with the other provisions of this Act in the same manner as agencies and government employees comply with such requirements.

Chapter VIII

Penalties

Section 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. –

The unauthorized processing of personal information shall be penalized by imprisonment for a period of one (1) year and a fine of not less than Twenty Five Thousand Liberian Dollars (L\$25,000.00) shall be imposed on the person who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

Section 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence.

Accessing personal information due to negligence shall be penalized by imprisonment for a period of two (2) years and a fine of Thirty Thousand Liberia Dollars (L\$30,000.00) shall be imposed on a person who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

Section 27. Improper Disposal of Personal Information and Sensitive Personal Information. –

The improper disposal of personal information shall be penalized by imprisonment for a period of one (1) year and a fine of not less than Ten Thousand Liberia Dollars (L\$10,000.00) shall be imposed on a person who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

Section 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.

The processing of personal information for unauthorized purposes shall be penalized by imprisonment for a period of three (3) years and a fine of not less than Thirty Thousand Liberian Dollars (L\$30,000.00) shall be imposed on a person processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

Section. 29. Unauthorized Access or Intentional Breach.

The penalty of imprisonment ranging from five (5) years to ten (10) years and a fine of not less than Fifteen Thousand Liberian Dollars (L\$15,000.00) but not more than Thirty Thousand Liberian Dollars (L\$ 30,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

Section 30. Concealment of Security Breaches Involving Sensitive Personal Information.

The penalty of imprisonment of two (2) years and a fine of not less than Fifteen Thousand Liberia (L\$15,000.00) but not more than Thirty Thousand Liberian Dollars (L\$30,000.00) shall be imposed on person who, after having knowledge of a security breach and of the obligation to notify the appropriate authority, intentionally or by omission conceals the fact of such security breach.

Section 31. *Malicious Disclosure.*

Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Fifteen Thousand Liberian Dollars (L\$15,000.00) but not more than Thirty Thousand Liberia Dollars (L\$30,000.00).

Section 32. *Unauthorized Disclosure.*

Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third-party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Fifteen Thousand Liberian Dollars (L\$15,000.00) but not more than Thirty Thousand Liberia Dollars (L\$30,000.00).

Section 33. *Combination or Series of Acts.*

Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than Twenty-five Thousand Liberian (L\$25,000.00) but not more than Fifty Thousand Liberian Dollars (L\$50,000.00).

Section 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or he/she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, shall suffer a year's suspension from the job without pay.

Section 35. *Large-Scale.*

The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least fifty (50) persons are harmed, affected or involved as the result of the above-mentioned actions.

Section 36. *Offense Committed by Public Officer.*

When the offender or the person responsible for the offense is a public officer in the exercise of his or her duties, and where he/she is found guilty of acts penalized under Section 28 of this Act, the penalty of imprisonment of four (4) years and a fine of not less than Thirty Thousand Liberia (L30,000.00) but not more than Sixty Thousand Liberian Dollars (L\$60,000.00) shall be imposed.

Chapter IX

Miscellaneous Provisions

Section 38. Interpretation.

Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

Section 39. Implementing Rules and Regulations (IRR).

Within twenty-four (24) months from the effectivity of this Act, the Independent Information Commissioner shall promulgate the rules and regulations to effectively implement the provisions of this Act.

Section 40. Reports and Information.

Each public ministry and agency shall annually report to the Independent Information Commissioner on its activities in carrying out the provisions of this Act. The agency shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities. The Independent Information Commissioner shall annually submit a report on the implementation of this Act to the National Legislature.

Section 41. Transitory Provision.

Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transitory period from the effective date on which this Act comes into force to comply with the requirements of this Act.

Section 42. Separability Clause.

If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise be affected shall remain valid and subsisting.

Section 43. Repealing Clause.

Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

Section 44. Effectivity Clause.

This Act shall take effect upon publication into handbills.

-2025-

SECOND SESSION OF THE FIFTY-FIFTH LEGISLATURE OF
THE REPUBLIC OF LIBERIA

HOUSE'S ENGROSSED BILL NO. 21 ENTITLED:

“AN ACT FOR THE COLLECTION, PROCESSING,
TRANSMISSION, STORAGE, PROTECTION, AND USE OF
PERSONAL INFORMATION IN LIBERIA”

On motion, the Bill was read. On motion, the Bill was adopted
on its first reading and sent to Committee Room on Tuesday,
June 10, 2025 at the hour of 12:32 GMT

On Motion, the Bill was taken from the Committee Room for
its second reading. On motion, under the suspension of the
rule, the second reading of the Bill constituted its third and
final reading and the Bill was adopted, passed into the full
force of the law and order engrossed today, Thursday, July 10,
2025 at the hour of 14:44 GMT



CHIEF CLERK, HOUSE OF REPRESENTATIVES, R.L.

-2026-

THIRD SESSION OF THE FIFTY-FIFTH LEGISLATURE
OF THE REPUBLIC OF LIBERIA

SENATE'S ENDORSEMENT TO HOUSE'S ENGROSSED BILL
NO. 21 ENTITLED:

“AN ACT FOR THE COLLECTION, PROCESSING,
TRANSMISSION, STORAGE, PROTECTION, AND USE OF
PERSONAL INFORMATION IN LIBERIA”

On motion, Bill read on its 1st reading, Tuesday,
November 4, 2025 @ 13:20 GMT. On motion, Bill read
on its second reading, adopted and sent to the
Committee Room on Thursday, November 6, 2025 at
14:30 GMT.

On motion, Bill taken from the Committee Room. On
Motion, the third reading of the Bill constituted the third
and final reading and the Bill was adopted, passed into
the full force of the Law and order engrossed today,
Thursday, December 18, 2025 @ 16:45 GMT



SECRETARY OF THE SENATE, R.L.

-2026-

ATTESTATION

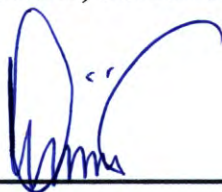
**“AN ACT FOR THE COLLECTION, PROCESSING,
TRANSMISSION, STORAGE, PROTECTION, AND USE OF
PERSONAL INFORMATION IN LIBERIA”**



**VICE PRESIDENT OF THE REPUBLIC OF LIBERIA/PRESIDENT OF
THE SENATE R.L.**



THE SECRETARY, LIBERIA SENATE R.L.



THE SPEAKER, HOUSE OF REPRESENTATIVES R.L.



THE CHIEF CLERK, HOUSE OF REPRESENTATIVES, R.L.



THE HONORABLE HOUSE OF REPRESENTATIVES

Capitol Building
P.O. Box 9005
Monrovia, Liberia
Website: www.legislature.gov.lr



Office of the Chief Clerk

-2026-

THIRD SESSION OF THE FIFTY-FIFTH LEGISLATURE OF THE REPUBLIC OF LIBERIA

SCHEDULE OF HOUSE'S ENROLLED BILL NO 6 ENTITLED:

“AN ACT FOR THE COLLECTION, PROCESSING, TRANSMISSION,
STORAGE, PROTECTION, AND USE OF PERSONAL INFORMATION IN
LIBERIA”

PRESENTED TO THE PRESIDENT OF THE REPUBLIC OF LIBERIA
FOR EXECUTIVE APPROVAL.

APPROVED: 9th DAY OF March A.D. 2026

AT THE HOUR OF 11:30 a.m


THE PRESIDENT OF THE REPUBLIC OF LIBERIA