

DRAFTING NOTE

DATA PROTECTION AND PRIVACY ACT 2026

1. Status and purpose of this note

This drafting note is explanatory and is not part of the proposed Assembly Act. It identifies the legislative need, the relationship with earlier Eritrean law, the principal matters retained, the modernization choices made and the place of the draft within the emerging constitutional statute book. The instrument remains a consultation draft and should be finalized only after legal, institutional, fiscal and public review.

2. Legislative need and prior law

The supplied corpus contains no comprehensive modern data-protection statute, while digital government, banking, communications, health, employment and commercial services increasingly depend on personal information.

3. What the draft retains

The draft retains constitutional privacy, confidentiality, evidence, records and sector-specific professional duties.

4. What the draft updates and modernizes

It creates lawful-processing principles, rights of access and correction, security and breach duties, safeguards for sensitive data, children, biometrics and automated decisions, cross-border transfer rules, independent supervision and proportionate remedies.

5. Constitutional, code and treaty fit

The draft is framed under the Constitution of Eritrea 1997 and must be read with the Civil Code, Penal Code, Civil Procedure Code and Criminal Procedure Code of Eritrea 2015 where those Codes govern. It is also coordinated with the other institutional, financial, commercial, land, labour, administrative and sectoral drafts in this collection. References to international or regional standards guide compatibility and implementation; they do not bypass the Treaty-Making Act or convert an unincorporated instrument into domestic law.

6. Scope and organization

The principal divisions address preliminary provisions; principles and lawful processing; special protection; rights of data subjects; duties of controllers and processors; public administration and identification systems; law enforcement, security and surveillance; international transfers; data protection commission; complaints, remedies and enforcement; reconciliation with public interests and sectoral duties; regulations, transition and final provisions.

7. Transition, implementation and consultation

The draft preserves lawful accrued rights, completed transactions, pending proceedings and institutional continuity where appropriate, while preventing temporary savings from preserving unconstitutional coercion or indefinite executive discretion. Before enactment or issuance, authentic predecessor instruments and amendments should be verified, cross-references and fiscal capacity confirmed, implementing regulations and digital systems prepared, and affected institutions, professions, communities and the public given a practical opportunity to comment.

CONSULTATION DRAFT — NOT ENACTED LAW

ACT NO. ____/2026

DATA PROTECTION AND PRIVACY ACT 2026

(ACT)

AN ACT TO PROTECT PRIVACY AND PERSONAL DATA, REGULATE THE PROCESSING OF PERSONAL DATA, ESTABLISH AN INDEPENDENT DATA PROTECTION COMMISSION, AND PROVIDE FOR RELATED MATTERS.

PREAMBLE

WHEREAS Articles 16 and 18 of the Constitution of Eritrea protect human dignity and privacy, and Article 19 protects freedoms whose effective exercise increasingly depends upon secure and lawful communications;

WHEREAS digital government, electronic commerce, modern finance, health services and communications require public confidence that personal data will be collected and used lawfully, fairly, securely and only for legitimate purposes;

WHEREAS privacy must be protected without converting it into an excuse for official secrecy or an obstacle to freedom of expression, access to public information, research, innovation or the administration of justice;

WHEREAS Eritrean law should be interpreted consistently with the Constitution and with regional and international human-rights obligations lawfully binding upon Eritrea;

NOW, THEREFORE, the National Assembly of Eritrea enacts as follows:

CHAPTER I
PRELIMINARY PROVISIONS

Article 1 — Short title

This Act may be cited as the Data Protection and Privacy Act 2026.

Article 2 — Purposes

1. to give practical effect to the constitutional rights to dignity and privacy;
2. to permit responsible uses of personal data necessary for public administration, commerce, research and social development;
3. to confer enforceable rights upon data subjects and duties upon controllers and processors;
and
4. to establish independent, effective and proportionate supervision and remedies.

Article 3 — Application

1. This Act applies to processing by a controller or processor established in Eritrea, whether or not the processing occurs in Eritrea.
2. This Act applies to a controller or processor outside Eritrea that offers goods or services to persons in Eritrea or monitors their conduct in Eritrea.
3. This Act applies to public bodies, subject only to a specific limitation authorized by this Act or another Act consistent with the Constitution.

Article 4 — Excluded household activity

This Act does not apply to processing by a natural person exclusively for personal or household activity and without a commercial, professional, political-organizational or public purpose.

Article 5 — Definitions

1. “automated decision” means a decision based solely or substantially on automated processing that produces a legal or similarly significant effect upon a person;
2. “biometric data” means personal data resulting from technical processing of physical, physiological or behavioural characteristics that permits or confirms unique identification;
3. “Commission” means the Data Protection Commission established by this Act;
4. “consent” means a freely given, specific, informed and unambiguous indication of agreement by a clear affirmative act;
5. “controller” means a person or public body that determines the purposes and essential means of processing;
6. “data subject” means an identified or identifiable natural person to whom personal data relates;
7. “personal data” means information relating to an identified or reasonably identifiable natural person;
8. “processing” includes collecting, recording, organizing, storing, altering, retrieving, consulting, using, disclosing, combining, restricting, erasing or destroying personal data;
9. “processor” means a person that processes personal data for a controller;
10. “profiling” means automated processing used to evaluate or predict personal characteristics, conduct, interests, reliability, location or movements;
11. “public body” has the meaning assigned by the law governing access to public information; and
12. “special-category data” means data revealing racial or ethnic origin, political opinion, religion, trade-union membership, health, disability, sex life or sexual orientation, genetic or biometric identity, or criminal accusation or conviction.

Article 6 — Relationship with the Constitution and other laws

1. This Act shall be interpreted to advance the Constitution and shall not authorize conduct prohibited by it.

2. The Civil Code governs personality rights, delictual responsibility and civil remedies except where this Act supplies a more specific protection.
3. The Penal Code determines criminal offences and punishments; nothing in this Act creates criminal liability by implication.
4. The Civil Procedure Code and Criminal Procedure Code govern judicial process, warrants, evidence and remedies except where this Act expressly provides otherwise.
5. The Commercial Code governs commercial transactions and electronic commerce, subject to the personal-data protections of this Act.

Article 7 — No implied executive exemption

A ministry, security body, defence body, police service, public enterprise or other executive institution is not exempt merely because it performs a public, security or governmental function.

CHAPTER II PRINCIPLES AND LAWFUL PROCESSING

Article 8 — General principles

1. Personal data shall be processed lawfully, fairly and transparently.
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed incompatibly with those purposes.
3. Personal data shall be adequate, relevant and limited to what is necessary.
4. Personal data shall be accurate and, where necessary, kept current.
5. Personal data shall not be retained in identifiable form longer than necessary.
6. Personal data shall be protected by appropriate technical and organizational security.

Article 9 — Accountability

1. A controller is responsible for compliance and must be able to demonstrate it.
2. Allocation of work to a processor does not relieve the controller of responsibility.

Article 10 — Lawful bases

1. Processing is lawful only if necessary for performance of a contract with the data subject, compliance with a legal obligation, protection of vital interests, performance of a function expressly assigned by law, or a legitimate interest not overridden by the data subject's rights.
2. Processing is also lawful on valid consent, but a public body shall not rely on consent where refusal would expose the person to disadvantage in obtaining a legally available service.

Article 11 — Consent

1. A request for consent shall be intelligible, accessible and distinguishable from unrelated terms.
2. The controller bears the burden of proving consent and must make withdrawal as easy as giving consent.
3. Consent obtained through deception, coercion, bundled conditions or an abuse of power is invalid.

Article 12 — Change of purpose

1. Before using data for a materially different purpose, a controller shall determine its compatibility with the original purpose, the context of collection, the nature of the data, foreseeable consequences and available safeguards.
2. Incompatible processing requires a separate lawful basis and fresh notice, unless expressly required by an Act.

Article 13 — Data minimization by public bodies

A public body shall not require a person to disclose personal data merely because the data may be convenient or potentially useful; it shall identify the statutory function for which each material category is necessary.

Article 14 — Accuracy

1. A controller shall take reasonable steps to ensure that data used for a decision affecting a person is accurate, complete and current.
2. Disputed data shall be marked as disputed until the dispute is resolved.

Article 15 — Retention and disposal

1. A controller shall establish and publish or internally maintain a retention schedule appropriate to its functions.
2. Data no longer lawfully required shall be securely erased, anonymized or transferred to a lawful public archive.

CHAPTER III SPECIAL PROTECTION

Article 16 — Special-category data

1. Processing special-category data is prohibited unless strictly necessary under an Act, required for employment or social protection, necessary for health care or substantial public interest, or based on explicit consent that is genuinely free.
2. The controller shall document necessity, proportionality, access limits and additional security before processing begins.

Article 17 — Children

1. The best interests, evolving capacities and safety of the child shall be a primary consideration.
2. Information addressed to a child shall be clear and age appropriate, and commercial profiling of children shall be strictly limited.
3. Consent of a parent or guardian shall not validate processing contrary to the child's rights or best interests.

Article 18 — Biometric and genetic data

1. Biometric or genetic identification shall be used only where authorized by law and demonstrably necessary for a specified purpose that cannot reasonably be achieved by a less intrusive means.
2. Centralized biometric databases, facial-recognition surveillance in public space and population-wide genetic databases require express authorization by an Act and independent safeguards.

Article 19 — Political, religious and associational data

1. No public body shall create or maintain a register of persons based on lawful political opinion, religion, association, peaceful assembly, journalism or human-rights activity.
2. Incidental collection shall be deleted unless retention is specifically authorized by law and necessary to investigate a particular offence or protect an identified person from a concrete threat.

Article 20 — Data relating to criminal matters

1. Processing concerning accusation, arrest, conviction or sentence requires legal authority and safeguards against stigma, inaccuracy and indefinite retention.
2. A person shall not be represented as convicted where proceedings ended without conviction or the conviction was lawfully expunged.

Article 21 — De-identification

1. A controller relying on anonymization shall use measures reasonably resistant to re-identification in light of available technology and other accessible data.
2. Pseudonymized data remains personal data where re-identification is reasonably possible.

CHAPTER IV

RIGHTS OF DATA SUBJECTS

Article 22 — Transparent notice

1. At or before collection, the controller shall identify itself, the purposes and lawful bases, recipients, retention period, transfers, rights and means of complaint.
2. Where data is obtained elsewhere, notice shall be given within a reasonable period and before first material use or disclosure, unless the person already has the information or an Act narrowly provides otherwise.

Article 23 — Right of access

1. A person may obtain confirmation whether personal data is processed and receive an intelligible copy with information concerning source, purpose, recipients, retention and automated processing.
2. The first copy shall ordinarily be free, and a response shall be made within thirty days unless complexity justifies one notified extension not exceeding thirty days.

Article 24 — Correction

1. A person may require inaccurate data to be corrected and incomplete data to be completed.
2. The controller shall notify material recipients of the correction unless impossible or disproportionate.

Article 25 — Erasure

1. A person may require erasure where data is no longer necessary, consent is withdrawn without another basis, processing is unlawful, or erasure is required by law.
2. Erasure may be refused only to the extent necessary for freedom of expression, compliance with law, public health, lawful archiving or research, or the establishment or defence of a legal claim.

Article 26 — Restriction

1. A person may require temporary restriction while accuracy, lawfulness or an objection is being determined.
2. Restricted data may be stored but otherwise processed only with consent, for legal claims, to protect another person, or for an overriding public interest established by law.

Article 27 — Data portability

1. Where processing is automated and based on consent or contract, a person may receive data supplied by that person in a structured, commonly used and machine-readable format.
2. Where technically feasible and lawful, the person may require direct transmission to another controller.

Article 28 — Objection

1. A person may object on grounds relating to that person's situation to processing based on public function or legitimate interest.
2. Processing shall cease unless the controller proves compelling lawful grounds overriding the person's interests or necessity for a legal claim.
3. An objection to direct marketing shall be honoured without balancing or delay.

Article 29 — Automated decisions

1. A person has the right not to be subject to a solely automated decision producing a legal or similarly significant effect, unless expressly authorized by law or necessary for a contract and accompanied by safeguards.
2. Safeguards include meaningful information about the principal logic, an opportunity to present the person's position, and prompt review by a competent human decision-maker empowered to change the result.

Article 30 — Exercise through a representative

A right under this Chapter may be exercised by an authorized representative, parent, guardian, personal representative or other person recognized by law, subject to verification and the interests of the data subject.

Article 31 — Limits upon rights

1. A limitation must be provided by an Act, pursue a legitimate constitutional purpose, and be necessary and proportionate in a democratic society.
2. A limitation shall be specific in scope and duration, preserve the essence of the right, and provide independent oversight and an effective remedy.
3. Administrative convenience, embarrassment, avoidance of accountability or a general reference to national security is insufficient.

CHAPTER V DUTIES OF CONTROLLERS AND PROCESSORS

Article 32 — Privacy by design and default

1. A controller shall integrate privacy, security and minimization into the design, procurement and operation of systems.
2. Default settings shall collect, disclose and retain no more data than necessary for the service chosen by the person.

Article 33 — Records of processing

1. A controller and processor shall maintain accurate records of purposes, categories, recipients, transfers, retention, security and responsible officers.
2. The Commission may exempt genuinely small, low-risk processing but not systematic, special-category or public-sector processing.

Article 34 — Data protection impact assessment

1. Before high-risk processing, the controller shall assess necessity, proportionality, risks, alternatives and safeguards in consultation with affected interests where practicable.
2. High-risk processing includes large-scale surveillance, biometrics, sensitive profiling, automated allocation of essential services and systematic monitoring of children or workers.

Article 35 — Prior consultation

Where an impact assessment reveals a high residual risk, processing shall not begin until the controller has consulted the Commission and addressed its lawful directions.

Article 36 — Data protection officer

1. Every public body and every controller engaged in systematic high-risk or large-scale special-category processing shall appoint an independent and adequately resourced data protection officer.
2. The officer shall advise, monitor compliance, facilitate rights, cooperate with the Commission and report serious unresolved risks to the highest governing authority.

Article 37 — Processor contract

1. A processor may act only on documented lawful instructions under a written contract addressing confidentiality, security, subcontracting, assistance, return or deletion and audit.
2. A processor that determines an unauthorized purpose becomes a controller for that processing.

Article 38 — Confidentiality

1. A person with access to personal data shall process it only as authorized and shall remain bound by confidentiality after employment or engagement ends.
2. Confidentiality does not prevent a protected disclosure of wrongdoing made under law.

Article 39 — Security

1. Controllers and processors shall use security appropriate to sensitivity, scale, context, available technology and foreseeable harm.

2. Measures shall include access control, encryption where appropriate, resilient backups, logging, testing, incident response and secure disposal.

Article 40 — Personal-data breach

1. A processor shall notify the controller without undue delay after discovering a breach.
2. A controller shall notify the Commission within seventy-two hours where feasible unless the breach is unlikely to risk a person's rights.
3. Where a high risk is likely, affected persons shall be informed promptly in clear language unless effective measures have removed that risk.

Article 41 — Joint controllers

Persons jointly determining purposes and essential means shall transparently allocate duties, remain jointly responsible to the data subject, and make the essential allocation available.

Article 42 — Audit and certification

1. A controller shall periodically audit compliance in proportion to risk and preserve evidence of corrective action.
2. The Commission may approve voluntary certification schemes, but certification does not eliminate legal responsibility.

CHAPTER VI PUBLIC ADMINISTRATION AND IDENTIFICATION SYSTEMS

Article 43 — Legal authority for public processing

1. A public body shall identify the constitutional or statutory function requiring processing and shall not infer coercive data powers from a general administrative mandate.
2. A regulation may prescribe implementation details but shall not create a new compulsory database, surveillance power or material limitation of a right without authority in an Act.

Article 44 — Digital public services

1. Digital services shall use interoperable, secure and accessible systems while collecting only data necessary for each service.
2. A person shall not be denied an essential service solely because that person lacks a device, connectivity, digital literacy or biometric enrolment, unless an Act provides a necessary and proportionate requirement.

Article 45 — Data sharing among public bodies

1. Sharing requires a documented legal basis, specified purpose, necessary fields, responsible recipients, retention limit and security arrangements.

2. A general request for all available data, continuous unrestricted access or data fishing is prohibited.

Article 46 — National identification systems

1. A national identification system requires an Act specifying purposes, governance, data fields, permitted linkages, rights, security and independent oversight.
2. An identifier shall not become a universal key joining unrelated databases unless the National Assembly expressly authorizes each necessary class of linkage with safeguards.

Article 47 — Registers and population databases

1. Public registers shall disclose only information that an Act makes public and only to the extent necessary for the register's purpose.
2. Bulk extraction, unrestricted reuse or commercial profiling from a public register may be restricted to protect rights and the integrity of the register.

Article 48 — Public records and archives

1. Records of enduring historical, legal or democratic value may be preserved by a lawful public archive with access safeguards.
2. Archival preservation shall not be used to maintain operational intelligence files or evade an erasure duty.

CHAPTER VII LAW ENFORCEMENT, SECURITY AND SURVEILLANCE

Article 49 — Application to security processing

Processing for policing, defence, intelligence, border control or national security remains subject to this Act except to the precise extent that another Act establishes a necessary, proportionate and independently supervised rule.

Article 50 — Targeted authority

1. Covert collection, interception, location tracking, device access or systematic surveillance requires specific statutory authority and, except in a narrowly defined emergency, prior judicial authorization.
2. An application shall identify the person, facility or place, facts establishing necessity, data sought, method, duration, minimization and handling of incidental data.

Article 51 — Prohibition of indiscriminate surveillance

1. No authority shall conduct generalized surveillance of the population or indiscriminately retain communications content, traffic, location or biometric data.

2. A programme affecting a class of persons must be defined by objective risk-related criteria and remain subject to judicial and independent institutional review.

Article 52 — Emergency access

1. Where delay creates an imminent threat of death or serious bodily harm, an authorized officer may obtain strictly necessary data without prior authorization.
2. The officer shall record reasons immediately and seek judicial confirmation within forty-eight hours; unconfirmed data shall be sealed and deleted except as a court orders to protect a person.

Article 53 — Confidential professions and sources

1. Surveillance affecting lawyer-client communication, medical confidentiality, journalistic sources, legislators or judges requires heightened necessity and safeguards appropriate to the protected function.
2. Privileged or unrelated material shall be segregated, independently reviewed and destroyed unless a court lawfully orders otherwise.

Article 54 — Notice after surveillance

1. A person subjected to covert surveillance shall be notified after the legitimate need for secrecy ends, sufficiently to seek a remedy.
2. A court may postpone notice for a defined period upon proof that notice would create a concrete and substantial risk to an ongoing lawful investigation or identified person.

Article 55 — Oversight reports

1. Each surveillance authority shall report annually to the Commission and the National Assembly on applications, approvals, refusals, emergencies, breaches and remedial action, without compromising particular lawful operations.
2. The Commission shall publish aggregated findings and may submit a confidential annex to the appropriate Assembly committee.

CHAPTER VIII INTERNATIONAL TRANSFERS

Article 56 — General rule for transfer

1. Personal data may be transferred outside Eritrea only where rights and effective remedies remain substantially protected.
2. A controller remains accountable for selecting the transfer mechanism, minimizing the data and responding to foreseeable foreign-government access.

Article 57 — Adequacy determination

1. The Commission may determine that a country, territory, sector or international organization affords adequate protection after assessing law, practice, independent supervision, remedies and international commitments.
2. A determination shall be reasoned, published, periodically reviewed and suspended where protection materially deteriorates.

Article 58 — Appropriate safeguards

1. Absent adequacy, transfer may rely on binding and enforceable contractual clauses, approved group rules, a treaty arrangement or another mechanism approved by the Commission.
2. Safeguards shall grant enforceable rights and effective remedies to the data subject.

Article 59 — Limited derogations

1. An occasional transfer may occur with explicit informed consent, for a necessary contract, vital interests, an important public interest established by law, or a legal claim.
2. A derogation shall not justify repetitive, structural or large-scale transfer and shall be interpreted narrowly.

Article 60 — Foreign demands

1. An order of a foreign authority demanding personal data is enforceable only through a treaty, court process or other lawful cooperation mechanism consistent with constitutional rights.
2. A controller shall challenge a manifestly unlawful or disproportionate demand and notify the Commission unless lawfully prohibited.

CHAPTER IX DATA PROTECTION COMMISSION

Article 61 — Establishment and independence

1. The Data Protection Commission is established as an independent public institution accountable to the Constitution and the National Assembly.
2. The Commission shall not seek or accept direction from the President, a ministry, security body, regulated entity or private interest in deciding a matter.

Article 62 — Composition

1. The Commission consists of a Commissioner and two Deputy Commissioners selected through an open, merit-based process and appointed in the manner prescribed by an Act governing independent constitutional or statutory offices.

2. The membership shall collectively possess expertise in law, technology, public administration, human rights, cybersecurity and regulation.

Article 63 — Qualification and disqualification

1. A member shall be an Eritrean citizen of integrity with at least ten years of relevant professional experience.
2. A serving political party officer, elected official, minister, security commander, regulated-entity director or person with a disqualifying conflict may not serve.

Article 64 — Tenure and removal

1. A member serves one non-renewable term of six years on protected remuneration.
2. Removal is permitted only for incapacity, serious misconduct, incompetence or material breach of duty after fair independent inquiry and approval by the National Assembly.

Article 65 — Functions

1. The Commission shall supervise compliance, investigate complaints and systemic risks, issue lawful orders, advise public institutions and educate the public.
2. It shall review high-risk systems, approve transfer and certification mechanisms, cooperate with independent regulators and report to the National Assembly.

Article 66 — Powers

1. The Commission may require information, inspect systems and premises under lawful safeguards, summon testimony, commission technical tests and obtain a judicial warrant where entry or access is resisted.
2. It may warn, reprimand, order compliance, suspend processing, require deletion or correction, restrict transfers and impose an administrative penalty under this Act.

Article 67 — Procedural fairness

1. Before an adverse order, the Commission shall give adequate notice of the case, access to material relied upon and a reasonable opportunity to respond.
2. An urgent interim order may be made to prevent serious harm, but expires within fourteen days unless confirmed after an expedited hearing.

Article 68 — Confidentiality and openness

1. The Commission shall protect confidential personal, commercial and security information obtained in its work.
2. It shall publish decisions, guidance, registers and statistics with necessary redactions, because regulatory confidentiality shall not become institutional secrecy.

Article 69 — Annual report

1. Within four months after each financial year, the Commission shall submit to the National Assembly a report on activities, resources, systemic risks, public-body compliance, surveillance oversight and recommended reforms.
2. The report shall be public, subject only to narrow redaction demonstrably required by law.

CHAPTER X COMPLAINTS, REMEDIES AND ENFORCEMENT

Article 70 — Complaint

1. A data subject, representative or public-interest organization with a sufficient connection may complain to the Commission without fee.
2. The Commission shall provide accessible procedures, assistance to vulnerable persons and reasons for declining or resolving a complaint.

Article 71 — Investigation

1. The Commission may investigate a complaint or act on its own initiative where information suggests material or systemic non-compliance.
2. Investigations shall be proportionate, timely and respectful of privilege, due process and legitimate confidentiality.

Article 72 — Corrective orders

1. An order may require a controller or processor to answer a request, correct or erase data, notify persons, improve security, alter a system, suspend processing or cease an unlawful practice.
2. An order shall state reasons, compliance time, consequences and the right of appeal.

Article 73 — Administrative penalties

1. For a serious or repeated contravention, the Commission may impose a proportionate administrative penalty only where an Assembly Act defines the contravention and liable person and enacts the applicable maximum.
2. In setting the amount, it shall consider gravity, duration, affected persons, sensitivity, intention, mitigation, cooperation, prior history, financial capacity and public interest.
3. No monetary penalty may be imposed until those statutory elements are in force, and a public body's penalty shall not be paid from funds needed for an essential service where an effective personal, managerial or corrective measure is more appropriate.

Article 74 — Civil remedy

1. A person suffering material or non-material harm from a contravention may seek compensation, declaration, injunction, correction, erasure or another appropriate remedy in a competent court.
2. The remedies under this Act supplement, and do not diminish, remedies under the Civil Code or Constitution.

Article 75 — Representative and collective proceedings

1. A qualified public-interest organization may represent consenting data subjects or, with leave of court, seek prospective relief against a systemic practice affecting a defined class.
2. The court shall protect class members from conflicting settlements and ensure that any relief is fair and effective.

Article 76 — Appeal and judicial review

1. A person materially affected by a final Commission decision may appeal to the competent court within thirty days.
2. An appeal does not automatically suspend protective action, but the court may grant a stay on just terms after considering rights, harm and public interest.

Article 77 — Obstruction and referral

1. The Commission may refer suspected offences, corruption or professional misconduct to the competent authority while preserving its regulatory jurisdiction.
2. Criminal responsibility arises only under an express offence in the Penal Code or another Act and shall be determined with full procedural guarantees.

Article 78 — Protection against retaliation

1. No person shall dismiss, penalize, threaten or disadvantage another for exercising a right, making a good-faith complaint, assisting the Commission or reporting a breach.
2. A court or tribunal may order reinstatement, compensation, protective relief and another remedy available under labour or civil law.

CHAPTER XI

RECONCILIATION WITH PUBLIC INTERESTS AND SECTORAL DUTIES

Article 79 — Access to public information

1. This Act shall not be used to withhold information concerning public functions, expenditure, contracts, official decisions, qualifications, conflicts of interest, corruption, abuse or other matters of legitimate public concern where disclosure is required by law.

2. A public body shall balance privacy and access by considering public interest, official responsibility, sensitivity, foreseeable harm, passage of time, redaction and partial disclosure.

Article 80 — Expression, journalism and artistic work

1. Processing for journalism, literature, art or public-interest expression is protected to the extent necessary to reconcile privacy with freedom of expression and access to information.
2. Relevant considerations include truth-seeking, public interest, the person's public role, methods of collection, vulnerability, accuracy and severity of intrusion.

Article 81 — Research and statistics

1. Research or statistical processing may receive proportionate adaptations where it serves a legitimate public interest and uses minimization, ethics review, security and publication controls.
2. Identifiable results shall not be published unless lawful, necessary and accompanied by appropriate protection.

Article 82 — Health and social services

1. Health and social-service data shall be accessible only to persons who need it for care, administration authorized by law, safety, payment or approved research.
2. A person shall receive meaningful information about record access and may obtain an audit history where reasonably available.

Article 83 — Employment

1. An employer may process worker data only as necessary for lawful employment purposes and shall not demand access to private accounts, communications, genetic data or irrelevant medical information.
2. Workplace monitoring must be transparent, necessary, proportionate and designed to avoid continuous or intimate surveillance.

Article 84 — Credit, insurance and essential services

1. A provider using personal data to determine eligibility, price or risk shall ensure accuracy, relevance, explainability and a meaningful opportunity to contest adverse information.
2. Special-category data and proxies producing unjustified discrimination shall not be used.

Article 85 — Direct marketing and communications

1. Electronic direct marketing requires consent or a narrowly related existing-customer basis with a clear, free and immediate means to opt out.

2. A person who objects shall be placed on a suppression list used solely to respect that objection.

CHAPTER XII

REGULATIONS, TRANSITION AND FINAL PROVISIONS

Article 86 — Regulations

1. The Commission may, after public consultation, propose regulations necessary to implement technical, procedural, transfer, breach, certification and fee provisions of this Act.
2. Regulations shall be made by the authority designated by the Constitution or an Assembly Act, remain within delegated power, and be published before taking effect.

Article 87 — Codes of practice

1. The Commission may approve sector codes developed transparently with data subjects, civil society, professional bodies, industry and relevant regulators.
2. A code may guide compliance but shall not reduce a right, create an exemption or displace this Act.

Article 88 — Transitional compliance

1. Within six months after commencement, each public body and high-risk controller shall appoint a responsible officer, inventory processing and report its compliance plan to the Commission.
2. Within twelve months, controllers and processors shall bring existing systems, contracts, notices, retention schedules and security measures into compliance.
3. The Commission may grant a reasoned extension not exceeding six months where immediate compliance is genuinely impracticable and rights remain adequately protected.

Article 89 — Existing databases

1. The existence of a database before commencement does not establish its lawfulness.
2. The responsible body shall identify legal authority, necessity, accuracy, retention and safeguards, and shall discontinue, delete or regularize unlawful processing within the transitional period.

Article 90 — Review of surveillance laws

1. Within twelve months, the Advocate General shall present to the National Assembly a review of laws authorizing interception, surveillance, identification and security databases for consistency with the Constitution and this Act.
2. The review shall identify powers lacking judicial authorization, necessity tests, retention limits, notice, independent oversight or effective remedy.

Article 91 — Effect on more protective rules

1. A sector law, professional duty or contract providing greater protection continues to apply.
2. A contract may not waive or reduce a data subject's minimum rights under this Act.

Article 92 — Periodic legislative review

1. The National Assembly shall review this Act within five years after commencement and at intervals not exceeding five years thereafter.
2. The review shall consider technological change, enforcement evidence, effects upon expression and access to information, public-sector surveillance, artificial intelligence and regional and international developments.

Article 93 — Commencement

1. Chapters I, IX and XII commence on publication in the Gazette.
2. The remaining provisions commence six months after publication, unless the National Assembly by law appoints an earlier date for a specified provision.

Made at Asmara, this ____ day of _____ 2026.

THE NATIONAL ASSEMBLY OF ERITREA