Title 39 - Data Protection Act 2026 (DP)

Preamble:

A Bill to establish enforceable, proportionate and rights-respecting rules for the processing, security, retention and transfer of personal data; to provide individual rights and regulatory remedies; to protect children and special-category data; and to work in conjunction with the Online Safety and Digital Services Act 2025, the Digital Liberty and Algorithmic Rights Act 2025, the Unity and Equality Act 2025, the Consumer Fairness and Safety Act 2026, the National Secrets Protection and Official Secrecy Act 2025 and other relevant Acts. This Act is to be read alongside those Acts, preserving their wording and legal effect except where this Act expressly provides an additional and compatible protection.

Article 1: Purpose, Scope and Definitions

Section 1A — Purpose

(a) This Act establishes minimum standards for the lawful, fair, transparent and secure processing of personal data.

(b) This Act applies to public authorities, businesses, charities and other persons processing personal data in Links Land or offering services to persons in Links Land.

Section 1B — Definitions

(a) Personal data means information relating to an identified or identifiable living person.

(b) Processing includes collecting, recording, organising, storing, consulting, using, disclosing, transferring, restricting or deleting data.

(c) Controller means the person or body determining the purposes and means of processing. Processor means a person processing data on behalf of a controller.

(d) The Commissioner means the Data Protection Commissioner established under Article 8.

Article 2: Data Protection Principles

Section 2A — Principles

(a) Personal data must be processed lawfully, fairly and transparently.

(b) Personal data must be collected for specified, explicit and legitimate purposes and not processed incompatibly with those purposes.

(c) Personal data must be adequate, relevant and limited to what is necessary.

(d) Personal data must be accurate and corrected without undue delay when inaccurate.

(e) Personal data must not be retained longer than necessary for the stated purpose, subject to a lawful preservation duty.

(f) Personal data must be processed with appropriate security against unauthorised or unlawful processing, loss, destruction or damage.

(g) A controller must be able to demonstrate compliance with this Act.

Article 3: Lawful Bases and Special Data

Section 3A — Lawful Bases

(a) Processing is lawful only where it is based on consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a public task, or a legitimate interest that is proportionate and does not override the rights and freedoms of the person.

(b) Consent must be freely given, specific, informed and capable of withdrawal without unreasonable detriment.

Section 3B — Special-Category Data

(a) Special-category data includes health, genetic, biometric, religious, ethnic, trade-union, sexual-orientation, gender-identity and intersex-status data.

(b) Special-category data may be processed only with explicit consent or where strictly necessary for healthcare, public health, employment and social-protection duties, legal claims, protection of vital interests, or approved public-interest research with appropriate safeguards.

(c) A controller must use heightened security and access controls for special-category data.

Article 4: Rights of Individuals

Section 4A — Information and Access

(a) A controller must provide clear information about the purposes, lawful basis, retention period, recipients and rights connected with processing.

(b) A person may request confirmation of processing and a copy of their personal data. The controller must respond without undue delay and ordinarily within one month, subject to a proportionate extension for complex requests.

Section 4B — Correction, Erasure and Restriction

(a) A person may require inaccurate personal data to be corrected.

(b) A person may require deletion where the data is no longer necessary, consent has been withdrawn and no other lawful basis applies, or processing is otherwise unlawful.

(c) A controller may retain data where required by law, necessary for legal claims, public health, journalism, research or another lawful and proportionate public interest.

Section 4C — Portability, Objection and Human Review

(a) Where technically feasible, a person may receive data they provided in a structured, commonly used and machine-readable format and transmit it to another controller.

(b) A person may object to processing based on legitimate interests or direct marketing, subject to a controller demonstrating compelling lawful grounds where permitted by this Act.

(c) A person has the right to request meaningful human review of a solely automated decision producing legal or similarly significant effects, except where the decision is necessary for a contract, authorised by law with safeguards, or based on explicit consent.

Article 5: Children and Vulnerable Persons

Section 5A — Digital Consent

(a) For an online service offered directly to a child, consent is valid without parental authorisation only when the child is 16 or older.

(b) For a child under 16, the controller must take reasonable steps to obtain and verify parental or guardian authorisation.

(c) This section applies only to online services offered directly to children and does not displace healthcare competence, safeguarding duties or access to essential services under another Act.

Section 5B — Best Interests

(a) Processing concerning children must be designed and operated with particular regard to the child's safety, dignity and best interests.

Article 6: Organisational Duties and Breaches

Section 6A — Governance and Impact Assessments

(a) A public authority and an organisation processing data on a large scale or processing special-category data on a large scale must designate a suitably qualified data protection officer.

(b) A controller must complete and document a data-protection impact assessment before high-risk processing begins and must consult the Commissioner where substantial residual risk cannot be mitigated.

Section 6B — Security and Breach Notification

(a) A controller must implement technical and organisational measures appropriate to the risk, including access control, resilience, testing and staff training.

(b) A controller must notify the Commissioner without undue delay and, where practicable, within 72 hours after becoming aware of a breach likely to create a risk to individuals.

(c) A controller must notify affected individuals without undue delay where a breach is likely to create a high risk, unless effective measures have made the data unintelligible or another lawful exception applies.

Section 6C — International Transfers

(a) Personal data may be transferred outside Links Land only where the recipient jurisdiction or arrangement provides protection substantially equivalent to this Act, or where approved contractual safeguards, an adequacy decision or a necessary and proportionate statutory exception applies.

Article 7: Exemptions and Relationship with Other Law

Section 7A — Exemptions

(a) This Act does not prevent processing strictly necessary for national security under the National Secrets Protection and Official Secrecy Act 2025, subject to that Act and applicable constitutional safeguards.

(b) Police and courts may obtain personal data through a judicial order, except in a genuine emergency where immediate action is necessary to prevent serious harm and subsequent judicial review is obtained as soon as practicable.

(c) Processing for journalism, literary expression, academic research or artistic expression is exempt only to the extent necessary to protect freedom of expression and a free press under the Constitution.

(d) Processing by an individual solely for household, personal or domestic activity is outside the scope of this Act.

Section 7B — Specialist Legislation

(a) This Act works in conjunction with specialist legislation concerning health, banking, children, consumer fairness, online safety, algorithmic rights, equality, national secrets and criminal procedure.

(b) A specialist Act may provide stricter protection or more specific duties, but may not be interpreted to remove a protection in this Act unless Parliament expressly passes a later amend or repeal Act.

Section 7C — Non-Duplication

(a) The Commissioner must not impose a second administrative penalty on the same person for the same conduct where another competent authority has already imposed a penalty for that conduct, but may coordinate investigations and impose a separate penalty for distinct unlawful conduct.

Article 8: Data Protection Commissioner

Section 8A — Establishment and Independence

(a) There is established a Data Protection Commissioner within the Linkslandic Digital Rights Commission for administrative support.

(b) The Commissioner exercises operational, investigative and enforcement functions independently and must not receive direction concerning an individual case.

(c) The Commissioner must publish enforcement guidance, maintain accessible complaint procedures and report annually to Parliament on activities, costs, penalties, compliance and complaint outcomes.

Section 8B — Powers

(a) The Commissioner may investigate complaints, require information, inspect relevant systems on lawful notice, issue compliance orders, require deletion or correction, restrict processing and refer suspected criminal conduct to the appropriate authority.

(b) An inspection of a private dwelling or privileged legal material requires judicial authorisation.

(c) The Commissioner must use the least intrusive effective measure and must give reasons for a material decision.

Article 9: Remedies, Penalties and Appeals

Section 9A — Complaints and Compensation

(a) A person may complain to the Commissioner without charge and may bring a civil claim for material or non-material damage caused by a breach of this Act.

(b) The court may order compliance, correction, deletion, restriction, compensation and reasonable costs.

Section 9B — Administrative Penalties

(a) For a lower-tier breach, the Commissioner may impose a penalty of up to 500,000 Dimes.

(b) For a serious or repeated breach, the Commissioner may impose a penalty of up to 1 million Dimes or four percent of annual worldwide turnover, whichever is higher, subject to proportionality and the safeguards in this section.

(c) Before imposing a penalty, the Commissioner must consider culpability, duration, harm, mitigation, cooperation, previous compliance, financial capacity and whether another penalty has been imposed for the same conduct.

(d) A small organisation should ordinarily receive guidance and a warning before a penalty, except in cases of fraud, deliberate misuse, repeated non-compliance or serious risk to health or safety.

Section 9C — Appeals

(a) A person subject to an enforcement notice or administrative penalty may appeal to the competent court within 28 days.

(b) An appeal must provide a full review of the legality, facts and proportionality of the decision, and the court may confirm, vary or quash it.

Article C: Constitutional Compliance

Section C1 — Rights and Proportionality

(a) This Act must be interpreted consistently with constitutional dignity, equality, healthcare, speech, press freedom, fair-trial and due-process rights.

(b) Any restriction on processing, expression, access to information or public administration must be lawful, necessary and proportionate to a legitimate public interest.

Section C2 — Review

(a) The Commissioner must conduct a statutory review after three years, including consultation with civil society, public authorities, businesses and children's representatives, and must report recommended changes to Parliament.

(b) Nothing in this Act removes the jurisdiction of the courts or the constitutional responsibility of Parliament to review the operation of data-protection law.