
**INDEPENDENT STATE OF PAPUA NEW GUINEA**

**PROPOSED DRAFT 5th VERSION.**

***A BILL***

***For***

***AN ACT entitled***

***Data Governance and Data Protection Act 2026***

No. __ of 2026.

*Data Governance and Data Protection Act 2026.*

Certified on: __ / __ /2026.

**INDEPENDENT STATE OF PAPUA NEW GUINEA**

**Proposed Draft – 5th Version**

**No. ___ of 2026.**

# A BILL

For

AN ACT entitled

## Data Governance and Data Protection Act 2026.

Being an Act to provide for and relating —

(a) to the governance and protection of data and personal information in Papua New Guinea, structured around the data value lifecycle; and

(b) to deem NICTA to be the National Data Authority for the purposes of this Act; and

(c) to provide for the progressive establishment of the National Data Authority; and

(d) to protect the rights of individuals in relation to their personal data, including in relation to automated and artificial intelligence systems that affect them; and

(e) to regulate the cross-border transfer of personal data in a manner that safeguards national sovereignty; and

(f) to provide for a national data architecture and cross-border data transfer framework; and

(g) to capture the core principles for the responsible governance of artificial intelligence,

and for related purposes.

MADE by the National Parliament to come into operation in accordance with a Notice in the National Gazette by the Head of State, acting with, and in accordance with, the advice of the Minister.

## ARRANGEMENT OF SECTIONS.

**PART I. — PRELIMINARY.**

1. Compliance with Constitutional Requirements.
2. Commencement.
3. Interpretation.
4. Objects of Act.
5. Act implements national digital governance framework.
6. Reading with other digital laws.
7. Application.
8. Act binds the State.

**PART II. — NICTA DEEMED TO BE NATIONAL DATA AUTHORITY.**

***Division 1. — NICTA as National Data Authority.***

9. NICTA deemed to be Authority.
10. NICTA deemed to be NDA under digital governance laws.
11. Functions and powers of NICTA as Authority.
12. Relationship with ICT legislation.
13. Coordination with whole-of-government digital governance.
14. Coordination with the Digital Identity and Trust Services Regulator.

***Division 2. — Establishment of the National Data Authority.***

15. Establishment of NDA by NEC Decision.
16. Establishment of NDA.
17. Transfer of functions to NDA.
18. Functions of Authority.
19. Powers of Authority.
20. Independence of Authority.
21. Funding independence of Authority.
22. Ministerial directions.

**PART III. — GOVERNANCE OF THE AUTHORITY.**

***Division 1. — Board.***

23. Establishment and composition of Board.
24. Qualifications of Board members.
25. Tenure of members.
26. Vacation of office.
27. Meetings of Board.
28. Quorum and voting.
29. Disclosure of interests.
30. Committees of Board.

***Division 2. — Chief Executive Officer and Staff.***

31. Chief Executive Officer.
32. Functions of Chief Executive Officer.
33. Staff of Authority.
34. Delegation.

***Division 3. — Internal Units.***

35. Data Governance Committee.
36. National Cyber Security Unit.

**PART IV. — DATA GOVERNANCE PRINCIPLES AND THE DATA VALUE LIFECYCLE.**

***Division 1. — General Principles.***

37. Data governance principles.
38. Governance across the data value lifecycle.
39. Data classification framework.

***Division 2. — Lifecycle Stage Principles.***

40. Stage 1 — Create (collection).
41. Stage 2 — Store (storage).
42. Stage 3 — Use (processing).

43. Stage 4 — Share (transfer and disclosure).
44. Stage 5 — Archive (retention).
45. Stage 6 — Destroy (disposal and deletion).

***Division 3. — AI-Ready Data and Core Obligations.***

46. AI-ready data architecture and the FAIR-R principles.
47. Obligations of data controllers.
48. Obligations of data processors.
49. Data Processing Agreement.
50. Data Governance Officers.
51. Records of processing activities.
52. Transaction-level access and disclosure logs.
53. Data Protection Impact Assessment.
54. Privacy notices — language and accessibility.
55. Data security measures — technological, physical and organisational.

**PART V. — PERSONAL DATA PROTECTION.**

***Division 1. — Lawful Processing.***

56. Requirement for lawful basis.
57. Lawful bases for processing.
58. Consent.
59. Sensitive personal data.
60. Biometric data — heightened protection.
61. Children's personal data.

***Division 2. — Rights of Data Subjects.***

62. Right to be informed.
63. Right of access.
64. Right to rectification.
65. Right to erasure.
66. Right to restrict processing.
67. Right to data portability.
68. Right to object.
69. Prohibition on automated decisions affecting rights.
70. Right to human review of automated decisions.
71. Right to compensation.

**PART VI. — DATA BREACH AND INCIDENT MANAGEMENT.**

72. Notification of data breach to Authority.
73. Notification to data subjects.
74. Obligations of data processors on breach.
75. Emergency data breach response.

**PART VII. — GOVERNMENT DATA GOVERNANCE, NATIONAL DATA ARCHITECTURE AND CROSS-BORDER TRANSFERS.**

76. Government data governance obligations.
77. National data exchange and interoperability.
78. National Data Catalogue.
79. Data sharing between agencies.
80. Open government data.
81. Cross-border data transfer.
82. Sovereign hosting requirements.
83. Data localisation.
84. International cooperation and inter-authority consultation.
85. Cross-border suspension mechanism.
86. Emergency data sharing.

**PART VIII. — ARTIFICIAL INTELLIGENCE PRINCIPLES.**

87. Application and objects of this Part.
88. Responsible AI principles.
89. Risk-based AI governance.
90. Prohibited AI practices.

91. Obligations for AI systems affecting individuals.
92. AI systems to comply with data governance and data protection.
93. Authority's AI regulatory functions.

**PART IX. — COMPLAINTS, REMEDIES AND ENFORCEMENT.**

***Division 1. — Complaints and Non-Judicial Remedies.***

94. Complaints to Authority.
95. Non-judicial adjudication — conciliation and binding orders.
96. Investigation of complaints.

***Division 2. — Enforcement.***

97. Enforcement powers of Authority.
98. Compliance notices.
99. Administrative sanctions.
100. Compliance audits.
101. Offences — general.

***Division 3. — Judicial Remedies.***

102. Appeal to National Court.
103. Right of action for compensation.

**PART X. — FINANCIAL PROVISIONS.**

104. Funds of Authority.
105. Annual budget.
106. Application of Public Finance Management Act 1995.
107. Application of Audit Act 1989.

**PART XI. — REPORTING AND ACCOUNTABILITY.**

108. Annual report.
109. Tabling of annual report.
110. Public awareness and capacity building.

**PART XII. — MISCELLANEOUS AND SAVINGS.**

111. Protection from personal liability.
112. Confidentiality obligations.
113. Evidentiary provisions.
114. Collaboration and partnerships.
115. Review of Act.
116. Transitional provisions.
117. NDA transition savings.
118. Legislative coherence — reading with digital laws.
119. Savings — existing instruments and proceedings.

**PART XIII. — REGULATIONS.**

120. Regulations.

# PART I. — PRELIMINARY.

## 1. COMPLIANCE WITH CONSTITUTIONAL REQUIREMENTS.

(1) This Act, to the extent that it regulates or restricts a right or freedom referred to in Subdivision III.3.C. (qualified rights) of the Constitution, namely —

(a) the right to freedom from arbitrary search and entry conferred by Section 44; and

(b) the right to privacy conferred by Section 49; and

(c) the right to freedom of information conferred by Section 51; and

(d) the right to freedom of movement conferred by Section 52,

of the Constitution, is a law that is made for the purpose of giving effect to the public interest in public order and public welfare.

(2) The purposes of data protection, data governance and artificial intelligence governance under this Act are public purposes for the purpose of Section 53 (unjust deprivation of property) of the Constitution.

(3) Nothing in this Act is intended to be inconsistent with any Constitutional Law, and this Act must be construed accordingly.

## 2. COMMENCEMENT.

(1) Except for Part III, this Act comes into operation on the date of certification.

(2) Part III comes into operation on a day to be fixed by the Head of State, acting on advice, by notice published in the National Gazette, being a day not earlier than the date on which the National Executive Council makes a decision under Section 15.

(3) Parts IV to XIII may come into operation on different days for different Parts or for different provisions within a Part.

## 3. INTERPRETATION.

(1) In this Act, unless the contrary intention appears —

"AI system" means a machine-based system that uses models or algorithms, trained or derived from data, to generate outputs such as predictions, recommendations, decisions or content that can influence real or virtual environments, and that operates with varying degrees of autonomy;

"automated decision" means a decision based solely or substantially on automated processing of personal data, including by an AI system, that produces legal effects concerning a data subject or similarly significantly affects a data subject;

"Authority" means —

(a) during the interim period, NICTA acting as the National Data Authority in accordance with Division 1 of Part II; and

(b) after the establishment of the NDA, the National Data Authority established under Section 16;

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person that allows or confirms the unique identification of that person, including fingerprint, facial geometry, iris scan, voice print and gait data, and, where a national law on digital identity and trust services defines the term by reference to another instrument, the two definitions are to be read consistently;

"Board" means the Board of the Authority established under Section 23;

"Chief Executive Officer" means the Chief Executive Officer appointed under Section 31;

"child" means a person under the age of 18 years;

"consent" has the meaning given by Section 58;

"controlled data" has the meaning given by Section 39;

"data" has the same meaning as in the applicable national cybersecurity and electronic crimes legislation;

"data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"data controller" means a person or organisation that, alone or jointly with others, determines the purposes and means of processing personal data;

"Data Governance Officer" means an officer designated under Section 50;

"data lifecycle" or "data value lifecycle" means the stages through which data passes, namely create, store, use, share, archive and destroy, as provided for in Division 2 of Part IV;

"data processor" means a person or organisation that processes personal data on behalf of a data controller;

"data subject" means an identified or identifiable natural person to whom personal data relates;

"Digital Identity and Trust Services Regulator" means the body designated under a national law on digital identity and trust services as the regulator responsible for ICT and the digital economy in relation to digital identity, trust services and verifiable credentials;

"government agency" means a Department of State, a statutory authority, a provincial government, a local-level government, and any body or instrumentality of the State;

"interim period" means the period between the date of certification of this Act and the date on which the NDA is established under Section 16;

"Minister" means the Minister responsible for information and communications technology;

"National Data Catalogue" means the national inventory of government data assets maintained under Section 78;

"national data exchange platform" means a secure interoperability platform accredited as a Secure Digital Exchange or Interoperability Platform under any applicable national law on digital identity and trust services and designated by the Minister under Section 77 for cross-agency data exchange;

"NDA" means the National Data Authority, the body responsible for data governance and data protection matters under this Act;

"NEC Decision" means a formal decision of the National Executive Council published by notice in the National Gazette;

"NICT Act" means the National Information and Communications Technology Act 2009, as amended from time to time;

"NICTA" means the National Information and Communications Technology Authority established under the NICT Act;

"personal data" means any information relating to an identified or identifiable natural person; a person is identifiable if the person can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity;

"processing" means any operation or set of operations performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;

"public data" has the meaning given by Section 39;

"restricted data" has the meaning given by Section 39;

"sensitive personal data" has the meaning given by Section 59(1).

(2) A term used in this Act in the context of digital identity, trust services or verifiable credentials that is defined in a national law on digital identity and trust services has the same meaning as in that law.

### 4. OBJECTS OF ACT.

(1) The objects of this Act are to —

(a) protect the personal data and privacy of individuals in Papua New Guinea;

(b) establish a comprehensive data governance framework, structured around the data value lifecycle, applicable to government agencies and private sector entities;

(c) deem NICTA to be the National Data Authority and provide for the progressive establishment of the NDA as the single convergent data and digital economy regulator;

(d) provide effective rights to individuals in relation to their personal data, including rights in respect of automated and artificial intelligence systems that affect them;

(e) regulate the cross-border transfer of personal data in a manner that safeguards national sovereignty and gives effect to Papua New Guinea's obligations under applicable international data-sharing arrangements;

(f) establish a national data architecture supporting interoperability, sovereignty and AI-readiness;

(g) ensure that personal data processed within the national digital trust ecosystem established under any national law on digital identity and trust services is subject to this Act's data protection standards;

(h) capture the core principles for the responsible governance of artificial intelligence, including the prohibition of AI-only decisions affecting legal rights without human review;

(i) promote responsible data-driven innovation and a trusted digital economy;

(j) ensure consistency with international data protection standards including the APEC Cross-Border Privacy Rules and applicable protocol obligations; and

(k) give effect to the right to privacy under Section 49 of the Constitution.

**5. ACT IMPLEMENTS NATIONAL DIGITAL GOVERNANCE FRAMEWORK.**

(1) This Act implements the data governance, data protection and artificial intelligence governance components of Papua New Guinea's national digital economy and transformation framework.

(2) The Authority must, in performing its functions, have regard to the national digital economy framework and must coordinate with the apex whole-of-government digital governance body constituted under that framework.

(3) The Authority's Chief Executive Officer must, as directed by the Board, attend or provide written reports to the apex whole-of-government digital governance body on data governance matters.

**6. READING WITH OTHER DIGITAL LAWS.**

(1) This Act is to be read together with all other national laws relating to digital governance, digital economy, artificial intelligence, digital public infrastructure, cybersecurity, electronic transactions, and related matters.

(2) Where another national digital law makes provision for a matter also covered by this Act, this Act and that other law must be read as complementary and, so far as possible, as operating together without inconsistency.

(3) Without limiting Subsection (1) or (2) —

(a) where a national law on artificial intelligence governance is enacted, this Act is to be read consistently with that law and, in the event of inconsistency, the provisions of this Act relating to the data rights, data protection and individual rights of persons in relation to AI continue to apply; and

(b) where a national law on digital identity and trust services is enacted, that law governs the establishment, operation, accreditation and trust framework of the national digital trust ecosystem, and this Act applies to personal data processed within that ecosystem as the data protection law of general application; and

(c) where a national law on critical digital infrastructure investment is enacted, the data governance obligations of the Authority under this Act must be exercised in support of the objects of that law.

(4) Nothing in this Act limits the operation of any other national law relating to digital governance, and this Act does not, without prejudice, derogate from any obligation or right under any other applicable law.

**7. APPLICATION.**

(1) This Act applies throughout Papua New Guinea.

(2) This Act applies to the processing of personal data —

(a) by any person or organisation carrying on an activity in Papua New Guinea;

(b) by a data controller or data processor established in Papua New Guinea, regardless of where processing takes place; and

(c) relating to the offering of goods or services to persons in Papua New Guinea.

(3) This Act does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

**8. ACT BINDS THE STATE.**

(1) This Act binds the State.

# PART II. — NICTA DEEMED TO BE NATIONAL DATA AUTHORITY.

## Division 1. — NICTA as National Data Authority.

**9. NICTA DEEMED TO BE AUTHORITY.**

(1) NICTA is, for all purposes of this Act, deemed to be the National Data Authority.

(2) During the interim period, NICTA has all the functions, powers and responsibilities of the Authority under this Act.

(3) A reference in this Act to the Authority is, during the interim period, taken to be a reference to NICTA acting as the NDA under this Division.

(4) NICTA's assumption of the functions of the Authority under this section does not limit or affect any of NICTA's functions or powers under the NICT Act.

(5) NICTA must, in performing the functions of the Authority under this section, maintain clear internal separation between its functions under the NICT Act and its functions as the Authority under this Act, and must keep separate records and reporting for each.

**10. NICTA DEEMED TO BE NDA UNDER DIGITAL GOVERNANCE LAWS.**

(1) For the purposes of all national digital governance laws relating to data protection, data governance and artificial intelligence governance, NICTA is deemed to be the National Data Authority.

(2) A reference in any national digital governance law to the National Data Authority is, during the interim period, taken to be a reference to NICTA acting as the NDA in accordance with this Act.

(3) This section does not apply to any function assigned by a national law on digital identity and trust services to the Digital Identity and Trust Services Regulator; those functions are governed exclusively by that law, and the designation of the body to perform them is a matter for that law.

(4) This section applies without prejudice to any specific provision of another national digital law that assigns regulatory functions to a different body in respect of a matter not covered by this Act.

**11. FUNCTIONS AND POWERS OF NICTA AS AUTHORITY.**

(1) During the interim period, NICTA must, as the Authority —

(a) perform all functions of the Authority set out in Section 18;

(b) receive, consider and act on data breach and AI system incident notifications;

(c) receive and investigate complaints from individuals about the handling of their personal data and the use of AI systems;

(d) issue interim guidelines and standards on data protection, data governance and AI governance;

(e) administer the AI governance principles under Part VIII;

(f) coordinate with the Department responsible for information and communications technology on data system and AI system policy matters;

(g) liaise and coordinate with the Digital Identity and Trust Services Regulator on the data protection obligations attaching to identity data; and

(h) take all reasonable steps to prepare for the orderly transfer of functions, records and assets to the established NDA at the end of the interim period.

(2) An action taken, direction issued, standard made or decision given by NICTA under Subsection (1) has the same legal effect as if taken, issued, made or given by the established Authority.

(3) During the interim period, NICTA has the power to do all things necessary or convenient to be done for or in connection with the performance of its functions under this Act.

**12. RELATIONSHIP WITH ICT LEGISLATION.**

(1) This Act is the national law establishing the agency responsible for data protection, data governance and AI governance.

(2) In matters of data protection, the rights of data subjects and AI governance, this Act, as lex specialis, prevails over any general ICT legislation to the extent of any inconsistency.

(3) In matters of digital identity, trust services, verifiable credentials and the accreditation of trust service providers, any applicable national law on digital identity and trust services, as lex specialis for those matters, prevails over this Act to the extent of any inconsistency.

(4) In matters of ICT licensing, spectrum management, telecommunications and radiocommunications, the NICT Act prevails over this Act to the extent of any inconsistency.

(5) A direction, standard or guideline issued by NICTA under the NICT Act before the end of the interim period in relation to data protection or AI governance continues in force as if issued by the established Authority until replaced.

### 13. COORDINATION WITH WHOLE-OF-GOVERNMENT DIGITAL GOVERNANCE.

(1) The Authority must operate consistently with the whole-of-government digital governance architecture and the apex body responsible for approving major digital architecture standards under the national digital transformation framework.

(2) The Authority's data governance standards and policies must be consistent with standards approved by the apex whole-of-government digital governance body.

(3) After the end of the interim period, the established NDA and NICTA must —

(a) cooperate and coordinate to ensure a consistent regulatory environment;

(b) share relevant information on cybersecurity incidents, data breaches and compliance matters;

(c) develop joint protocols for cybersecurity incidents involving personal data breaches;

(d) avoid imposing duplicative or inconsistent requirements; and

(e) hold at least one joint coordination meeting in each calendar year.

(4) The NDA and NICTA must enter into a Memorandum of Understanding within 6 months of the end of the interim period, to be approved by the Minister, published in the National Gazette and tabled in Parliament.

### 14. COORDINATION WITH THE DIGITAL IDENTITY AND TRUST SERVICES REGULATOR.

(1) This section applies where a national law on digital identity and trust services designates a body as the Digital Identity and Trust Services Regulator.

(2) Where the same institution performs both the data protection mandate under this Act and the digital identity and trust services mandate under that law, the institution acts in different capacities under different statutory bases, and must maintain clear records identifying in which capacity each function, direction or determination is made.

(3) The Authority and the Digital Identity and Trust Services Regulator must —

(a) enter into a Memorandum of Understanding within 6 months of both this Act and the national law on digital identity and trust services commencing, to be tabled in Parliament, setting out coordination protocols, information sharing arrangements, and complaint referral mechanisms;

(b) coordinate the commencement of the data protection provisions of this Act with the operational commencement of the national digital trust ecosystem, so that personal data processed within that ecosystem is subject to the protections of this Act from the date of operational commencement;

(c) refer complaints to the appropriate regulator, so that identity and trust services complaints are handled by the Digital Identity and Trust Services Regulator and data protection complaints are handled by the Authority, and one complaint is not adjudicated under two regimes; and

(d) avoid imposing duplicative compliance obligations on entities operating under both laws.

(4) This Act applies to personal data processed within any national digital trust ecosystem as the data protection law of general application.

## Division 2. — Establishment of the National Data Authority.

### 15. ESTABLISHMENT OF NDA BY NEC DECISION.

(1) The National Executive Council shall, by NEC Decision, declare that the National Data Authority is established and operational from a day specified in the NEC Decision.

(2) The National Executive Council may make a decision under Subsection (1) when satisfied that —

(a) members of the Board have been or are ready to be appointed in accordance with Section 23;

(b) a Chief Executive Officer has been or is ready to be appointed in accordance with Section 31;

(c) adequate funding has been appropriated or secured for initial operations; and

(d) appropriate premises and administrative systems are in place.

(3) The Minister must publish the NEC Decision by notice in the National Gazette and must table the notice in Parliament within 30 days.

**16. ESTABLISHMENT OF NDA.**

(1) On the day specified in the NEC Decision under Section 15, the National Data Authority is established as a body corporate.

(2) The Authority —

(a) has perpetual succession; and

(b) shall have and may use a common seal; and

(c) may acquire, hold and dispose of real and personal property; and

(d) may sue and be sued in its corporate name; and

(e) may do and suffer all other things a body corporate may by law do and suffer.

(3) The Authority is a statutory authority of the National Government.

(4) On the establishment of the Authority —

(a) the interim period ends;

(b) NICTA ceases to be deemed to be the Authority under this Act; and

(c) the Authority assumes all functions, powers and responsibilities conferred by this Act.

**17. TRANSFER OF FUNCTIONS TO NDA.**

(1) On the establishment of the Authority under Section 16 —

(a) all assets, rights and liabilities of NICTA that relate to data governance, data protection and AI governance vest in the Authority;

(b) all personal data, records, databases, case files and documents held by NICTA in its capacity as the interim Authority are taken to be held by the Authority;

(c) all directions, standards and guidelines issued by NICTA in relation to data protection and AI governance continue in force as if issued by the Authority, until replaced;

(d) all complaints and investigations not finally determined are taken to have been lodged with the Authority;

(e) all pending proceedings by or against NICTA as interim Authority may be continued by or against the Authority; and

(f) any employee of NICTA whose principal duties related to data protection or AI governance may, with the agreement of the employee, NICTA and the Authority, be transferred to the Authority on terms no less favourable than those immediately before transfer.

(2) NICTA must, at least 60 days before the expected date of establishment, provide the Minister with a complete inventory of all assets, pending complaints and investigations, and all instruments to be transferred.

**18. FUNCTIONS OF AUTHORITY.**

(1) The functions of the Authority are to —

(a) administer and enforce this Act;

(b) protect and promote the rights of data subjects;

(c) regulate, supervise and oversee compliance with this Act by data controllers, data processors and operators of AI systems across the data value lifecycle;

(d) administer the AI governance principles under Part VIII;

(e) develop and issue codes of practice, standards and guidelines, including on data governance, the data value lifecycle and AI governance;

(f) receive, investigate and determine complaints from data subjects, including complaints relating to AI systems;

(g) conduct conciliation and non-judicial adjudication of data protection complaints under Section 95;

(h) conduct awareness and education programmes;

(i) conduct compliance audits;

(j) facilitate international data protection cooperation, including Papua New Guinea's participation in the APEC Cross-Border Privacy Rules and the implementation of obligations under applicable international data-sharing protocols;

(k) provide technical advice to government agencies on data governance and AI governance;

(l) maintain and administer the National Data Catalogue in coordination with government agencies;

(m) administer the national data exchange interoperability standards;

(n) coordinate with the Digital Identity and Trust Services Regulator on data protection matters arising in the digital trust ecosystem; and

(o) advise the Minister on data protection, governance and AI policy.

(2) The Authority may perform any act or do anything incidental or conducive to the performance of its functions.

**19. POWERS OF AUTHORITY.**

(1) The Authority has power to do all things necessary or convenient to be done for or in connection with the performance of its functions.

(2) Without limiting Subsection (1), the Authority may —

(a) issue directions, guidelines and standards to data controllers, data processors and operators of AI systems;

(b) investigate suspected contraventions of this Act on its own initiative or on complaint;

(c) require the production of documents, records and information;

(d) enter and inspect premises where data processing is carried on, subject to any warrant required by law;

(e) impose administrative sanctions under Section 99;

(f) refer matters to appropriate law enforcement authorities for prosecution; and

(g) enter into memoranda of understanding with foreign data protection and AI governance authorities.

**20. INDEPENDENCE OF AUTHORITY.**

(1) In the performance of its functions and exercise of its powers, the Authority must act independently and in the public interest.

(2) The Authority must not be subject to direction or control of any Minister or government agency in the investigation or determination of a complaint, the conduct of an audit or enforcement action, or the exercise of its powers under Section 85, except as expressly provided in this Act.

(3) The independence of the Authority does not affect the obligation of the Board to report to the Minister under this Act.

(4) An appointed member of the Board must not be removed from office except for cause established under Section 26, and no member may be removed by reason of a decision made or position taken in good faith in the performance of the Authority's functions.

**21. FUNDING INDEPENDENCE OF AUTHORITY.**

(1) Parliament must appropriate funds to the Authority sufficient to enable the Authority to perform its functions independently and effectively.

(2) The Minister must, in preparing any budget submission relating to the Authority, consult the Chairperson of the Board and include the Board's funding assessment in the submission.

(3) The Authority may retain fees and charges collected under this Act and apply them toward its operating costs, subject to the Public Finance Management Act 1995.

(4) Where the Board is of the opinion that a proposed reduction in the Authority's funding would impair the Authority's ability to perform its enforcement functions independently, the Board must notify the Speaker of Parliament in writing, and the Speaker must cause the notification to be tabled in Parliament.

### 22. MINISTERIAL DIRECTIONS.

(1) The Minister may, by written notice, give directions to the Authority on matters of government policy relating to matters under this Act.

(2) A direction under Subsection (1) must not —

(a) require the Authority to make a particular decision in relation to a particular person; or

(b) direct the Authority in the investigation or determination of a specific complaint.

(3) The Authority must comply with a direction given under Subsection (1), in so far as it does not contradict any provision of this Act.

(4) The Minister must cause a copy of any direction given under Subsection (1) to be tabled in Parliament within 30 days.

## PART III. — GOVERNANCE OF THE AUTHORITY.

### Division 1. — Board.

### 23. ESTABLISHMENT AND COMPOSITION OF BOARD.

(1) The Authority has a Board of Directors.

(2) The Board consists of —

(a) a Chairperson, being a person with qualifications in law, public administration, information technology or a related field and at least 10 years of senior professional experience, appointed by the Head of State, acting on advice of the National Executive Council, on the recommendation of the Minister following a transparent, publicly advertised and merit-based selection process conducted by an independent selection panel;

(b) the Secretary of the Department responsible for information and communications technology, ex officio, or his or her nominee, who shall be the Deputy Chairperson;

(c) the Chief Executive Officer of the Authority, ex officio;

(d) a person with qualifications and experience in law, information technology, privacy or public administration;

(e) a person with qualifications in data privacy or information law;

(f) a person with qualifications in cybersecurity or information technology;

(g) a person representing civil society or consumer protection;

(h) a person with qualifications in finance, accounting or governance; and

(i) a person with experience in the digital private sector,

the members referred to in paragraphs (d) to (i) being appointed by the Head of State, acting on advice of the National Executive Council, on the recommendation of the Minister following a transparent and merit-based selection process.

(3) A person must not be appointed as a member of the Board under Subsection (2)(a) or (d) to (i) if the person is a member of Parliament or a serving public servant.

### 24. QUALIFICATIONS OF BOARD MEMBERS.

(1) An appointed member of the Board must be a person of good standing with relevant expertise in at least one of the following areas: law, information technology, cybersecurity, privacy and data protection, AI governance, public administration, consumer advocacy, finance or governance.

(2) A person is not eligible for appointment if the person —

(a) has been convicted of an indictable offence;

(b) is an undischarged bankrupt; or

(c) has a direct financial interest that would give rise to a systemic conflict with the functions of the Authority.

**25. TENURE OF MEMBERS.**

(1) An appointed member of the Board holds office for a term of 3 years and is eligible for reappointment for 1 further term only.

(2) A person must not hold office as an appointed member of the Board for more than 6 years in total.

(3) Despite Subsections (1) and (2), a member holds office until a successor is appointed, for a period not exceeding 3 months after the end of the member's term.

**26. VACATION OF OFFICE.**

(1) An appointed member of the Board vacates office if the member —

(a) dies; or

(b) resigns by written notice delivered to the Minister; or

(c) becomes permanently incapable of performing the duties of the office; or

(d) is convicted of an offence punishable by imprisonment; or

(e) becomes insolvent; or

(f) is absent from 3 consecutive meetings without the leave of the Chairperson; or

(g) fails to comply with Section 29; or

(h) ceases to hold the qualifications by reason of which the member was appointed.

(2) The National Executive Council must terminate the appointment of a member who has vacated office under Subsection (1).

**27. MEETINGS OF BOARD.**

(1) The Board must hold at least 4 meetings in each year.

(2) Meetings are to be held at the times and places the Chairperson determines.

(3) The Chairperson must convene a special meeting if requested in writing by at least 3 members.

(4) Meetings may be held using any appropriate communication technology.

(5) The Board must cause minutes of all meetings to be kept.

**28. QUORUM AND VOTING.**

(1) 5 members of the Board constitute a quorum.

(2) A question before the Board is decided by a majority of votes of members present and voting.

(3) The Chairperson has a deliberative vote and, in the event of an equality of votes, also has a casting vote.

**29. DISCLOSURE OF INTERESTS.**

(1) A member who has a material personal interest in a matter being considered by the Board must —

(a) disclose the nature of the interest to the Board as soon as practicable; and

(b) not take part in the consideration or decision of the matter; and

(c) not be present while the matter is being considered.

(2) A disclosure under Subsection (1) must be recorded in the minutes.

(3) A member who contravenes this section commits an offence.

**Penalty:** A fine not exceeding K20,000.

**30. COMMITTEES OF BOARD.**

(1) The Board may establish committees to advise on or assist with matters within the Board's functions, including a dedicated AI governance advisory committee.

(2) A committee may include persons who are not members of the Board.

(3) The Board must determine the functions and procedures of each committee.

## Division 2. — Chief Executive Officer and Staff.

**31. CHIEF EXECUTIVE OFFICER.**

(1) The Authority has a Chief Executive Officer.

(2) The Chief Executive Officer is appointed by the Board, on the recommendation of a selection committee, for a term of 4 years and is eligible for reappointment for 1 further term only.

(3) A person is not eligible for appointment unless the person has —

(a) a qualification in law, information technology, public administration or a related field; and

(b) at least 7 years of relevant professional experience.

(4) The terms and conditions of appointment shall be determined under the Salaries and Conditions Monitoring Committee Act 1988 and the Regulatory Statutory Authorities (Appointment to Certain Offices) Act 2004.

### 32. FUNCTIONS OF CHIEF EXECUTIVE OFFICER.

(1) The Chief Executive Officer is responsible for the day-to-day management and administration of the Authority in accordance with the policies and directions of the Board.

(2) The Chief Executive Officer must report quarterly to the Board on the Authority's performance and financial position.

(3) The Chief Executive Officer may, by written instrument approved by the Board, delegate to a staff member any power or function other than this power of delegation.

### 33. STAFF OF AUTHORITY.

(1) The Chief Executive Officer may appoint such employees as are necessary for the purposes of the Authority, within the limits of funds lawfully available.

(2) An employee must be appointed through an open and competitive process.

(3) Employees of the Authority are not public servants but are entitled to such terms and conditions as the Board determines, consistently with the Salaries and Conditions Monitoring Committee Act 1988.

### 34. DELEGATION.

(1) The Authority may, by written instrument, delegate to a person or class of persons any of the Authority's functions or powers, other than this power of delegation.

(2) A delegation does not prevent the Authority from exercising the delegated function or power.

## Division 3. — Internal Units.

### 35. DATA GOVERNANCE COMMITTEE.

(1) A committee to be known as the Data Governance Committee is established within the Authority.

(2) The Committee consists of the Chief Executive Officer (Chairperson) and the heads of the divisions responsible for data protection and compliance, cybersecurity, legal and policy, AI governance, and information systems.

(3) The functions of the Committee are to advise on data governance, data lifecycle and AI governance standards, oversee internal data management systems, and monitor the Authority's compliance performance.

(4) The Committee must meet at least once every 2 months.

### 36. NATIONAL CYBER SECURITY UNIT.

(1) A unit to be known as the National Cyber Security Unit is established within the Authority.

(2) The Unit is responsible for monitoring and responding to cybersecurity incidents, developing national cybersecurity standards, providing technical advice on cyber-risk management, and coordinating with regional and international cybersecurity agencies.

(3) The Unit must report annually to the Board on national cybersecurity readiness.

# PART IV. — DATA GOVERNANCE PRINCIPLES AND THE DATA VALUE LIFECYCLE.

## Division 1. — General Principles.

### 37. DATA GOVERNANCE PRINCIPLES.

(1) All data controllers, data processors and government agencies must, in processing personal data, comply with the following principles —

(a) Lawfulness and Fairness: data must be processed lawfully, fairly and in a manner that respects the rights and freedoms of individuals;

(b) Transparency: data subjects must be informed of how their personal data is collected, used, disclosed, stored and retained, and of their rights;

(c) Purpose Limitation: data must be collected for specified, explicit and lawful purposes and must not be further processed in a manner incompatible with those purposes;

(d) Data Minimisation: only the minimum amount of data necessary for the lawful purpose must be collected and retained, and data sought and processed must be relevant and not excessive;

(e) Accuracy and Completeness: data must be accurate, complete and, where necessary, kept up to date;

(f) Storage Limitation: data must not be retained for longer than is necessary, unless required by law, and retained data must be subject to periodic review;

(g) Integrity and Security: data must be protected by appropriate technological, physical and organisational measures against unauthorised or unlawful processing, accidental loss, destruction or damage;

(h) Accountability: a data controller is responsible for, and must be able to demonstrate compliance with, this section at every stage of the data value lifecycle;

(i) Data Sovereignty: data originating from within Papua New Guinea must be stored and managed in a manner that safeguards national sovereignty and jurisdictional control; and

(j) Ethical Use: all data governance decisions must take into account ethical considerations and the public interest.

(2) The Authority may issue guidelines, codes of practice and standards to give effect to the principles in Subsection (1).

### 38. GOVERNANCE ACROSS THE DATA VALUE LIFECYCLE.

(1) Data governance obligations under this Act apply at every stage of the data value lifecycle, and do not begin or end at the point of collection, but persist and evolve from creation to destruction.

(2) The data value lifecycle consists of the following 6 stages —

(a) Stage 1 — Create (collection), governed by Section 40;

(b) Stage 2 — Store (storage), governed by Section 41;

(c) Stage 3 — Use (processing), governed by Section 42;

(d) Stage 4 — Share (transfer and disclosure), governed by Section 43;

(e) Stage 5 — Archive (retention), governed by Section 44; and

(f) Stage 6 — Destroy (disposal and deletion), governed by Section 45.

(3) A data controller and a data processor must apply the stage-specific principles in Division 2 so that privacy is built in by design, accountability is clearly assigned at every stage, and personal data remains traceable, auditable and trustworthy throughout its lifecycle.

(4) The Authority must issue standards and guidance giving effect to the data value lifecycle principles and may require a data controller to demonstrate how each stage is governed.

### 39. DATA CLASSIFICATION FRAMEWORK.

(1) For the purposes of this Act, data is classified, at the point of creation, as follows —

(a) "public data" means information that may be freely accessed by the public without restriction;

(b) "controlled data" means information not intended for public disclosure, access to which is restricted to authorised persons;

(c) "restricted data" means information classified as highly sensitive, the disclosure of which may cause harm to national security, public safety, individual rights or organisational integrity; and

(d) "confidential data" means restricted data that is designated by the Minister as requiring the highest level of protection due to its strategic, security or sovereign significance.

(2) Classification at creation drives the controls applied at every subsequent stage of the data value lifecycle, and a data controller must establish and maintain a data classification framework in consultation with the Authority and ensure that appropriate access controls, encryption and security measures are applied to each classification tier.

(3) The Authority must issue and maintain the national data classification standards, which must be consistent with the classification framework in Subsection (1).

## Division 2. — Lifecycle Stage Principles.

### 40. STAGE 1 — CREATE (COLLECTION).

(1) A data controller must, before collecting or generating personal data, define and document why the data is being collected, and collection without a lawful basis or stated purpose is prohibited.

(2) At the create stage, the following principles apply —

(a) Lawfulness and Legitimacy: a lawful basis under Section 57 must exist before personal data is collected or generated;

(b) Purpose Specification: the purpose of the collection must be explicit, defined and documented prior to collection;

(c) Data Minimisation: only data that is adequate, relevant and necessary for the stated purpose may be collected;

(d) Transparency and Consent: the data subject must be informed and, where required, give freely given and informed consent in accordance with Section 58; and

(e) Data Classification: personal data must be classified by sensitivity at the point of creation under Section 39 to govern downstream controls.

### 41. STAGE 2 — STORE (STORAGE).

(1) A data controller must govern stored personal data through encryption at rest, clearly defined retention schedules, and role-based access controls, and retention must be tied to purpose and not to convenience.

(2) At the store stage, the following principles apply —

(a) Security and Confidentiality: personal data must be protected by appropriate technological, physical and organisational security measures;

(b) Data Accuracy and Quality: stored data must be accurate, complete and kept up to date, and inaccurate data must be corrected or deleted promptly;

(c) Storage Limitation: personal data must not be retained in identifiable form beyond the period necessary for its stated purpose; and

(d) Access Control: access to stored personal data must be role-based and limited to authorised personnel on a need-to-know basis.

### 42. STAGE 3 — USE (PROCESSING).

(1) A data controller must assign stewardship roles, record processing activities in records of processing activities under Section 51, and ensure that automated processing is subject to human review, and secondary use without a compatibility assessment is prohibited.

(2) At the use stage, the following principles apply —

(a) Purpose Compatibility: data may only be processed for purposes compatible with those for which it was originally collected;

(b) Accountability and Stewardship: designated data stewards and owners must be accountable for the lawful and ethical use of personal data;

(c) Integrity and Auditability: all processing activities must be logged, traceable and auditable through records of processing activities and the transaction-level logs under Section 52; and

(d) Automated Decision-Making Safeguards: where data is used in automated or AI-driven decisions, human oversight and the right to contest must be guaranteed in accordance with Sections 69 and 70.

**43. STAGE 4 — SHARE (TRANSFER AND DISCLOSURE).**

(1) A data controller must ensure that every sharing relationship is governed by a written agreement, that cross-border transfers occur only under an adequacy decision or approved safeguards, and that data subjects can exercise their rights regardless of where data has been shared.

(2) At the share stage, the following principles apply —

(a) Data Subject Rights: data subjects retain the right to access, rectify, object to and port their personal data at any stage of sharing;

(b) Third-Party Accountability: data processors and third parties must be bound by agreements ensuring equivalent protection standards, and onward sharing or onward transfer by a recipient is subject to the same controls as the original disclosure;

(c) Cross-Border Transfer Controls: personal data must not be transferred to a jurisdiction without an adequate level of protection unless approved safeguards under Section 81 are in place; and

(d) Need-to-Share Principle: data may only be shared where there is a legitimate, documented need, and sharing must not exceed what is necessary.

**44. STAGE 5 — ARCHIVE (RETENTION).**

(1) The archiving of personal data does not suspend governance obligations, and a data controller remains legally liable for archived personal data, which must be de-identified, access-restricted and subject to regular review.

(2) At the archive stage, the following principles apply —

(a) Proportionality of Retention: archived data must serve a legitimate legal, historical, statistical or public interest purpose, and indefinite retention is prohibited;

(b) De-identification and Pseudonymisation: where data is archived beyond its primary purpose period, it must be anonymised or pseudonymised to the extent practicable;

(c) Restricted Access to Archives: access to archived personal data must be strictly limited, and archived data must not re-enter active use without a fresh governance review; and

(d) Periodic Review and Audit: archived datasets must be subject to scheduled review to assess continued necessity, accuracy and compliance.

**45. STAGE 6 — DESTROY (DISPOSAL AND DELETION).**

(1) The destruction of personal data is a governance obligation and not an operational option, and a failure to destroy data that has reached the end of its life creates ongoing legal and security liability.

(2) At the destroy stage, the following principles apply —

(a) Right to Erasure: a data subject may request deletion of their personal data in accordance with Section 65;

(b) Secure and Verified Destruction: destruction must render data permanently unrecoverable using approved methods, including cryptographic erasure, physical destruction or certified wiping;

(c) Completeness of Destruction: destruction must cover all copies, including backups, test environments, logs and third-party processor copies; and

(d) Record-Keeping of Destruction: a data controller must maintain documented evidence of destruction, including the method used, the date, the data categories and the authorising officer.

(3) A data controller who fails to comply with this section commits an offence.

**Penalty:** A fine not exceeding K10,000 in the case of a natural person; a fine not exceeding K80,000 in the case of a body corporate.

## Division 3. — AI-Ready Data and Core Obligations.

**46. AI-READY DATA ARCHITECTURE AND THE FAIR-R PRINCIPLES.**

(1) All government agencies and all data controllers operating data management systems used for or connected with the delivery of government services must apply the following AI-ready data architecture principles —

(a) Interoperability by Design: data systems must adopt open standards to enable interoperability across government and with approved national digital infrastructure;

(b) Sovereignty by Design: critical government data must remain subject to national sovereign control, including control over storage, access, processing and cross-border transfer;

(c) Resilience and Continuity by Design: data systems must support redundancy, disaster recovery and operational continuity;

(d) Privacy, Security and Trust by Design: data protection and security must be embedded in the design and architecture of systems, not added as an afterthought;

(e) Modularity and Reuse: data systems must be designed to enable reuse of components and integration with national digital public infrastructure without duplication; and

(f) Inclusion by Design: data systems and the services they support must be accessible in Tok Pisin and, where feasible, other local languages, and must support low-connectivity environments.

(2) Datasets prepared for use in artificial intelligence and machine learning must be prepared in accordance with the FAIR-R principles, namely —

(a) Findability: datasets must be discoverable, searchable and easily located through robust metadata, unique identifiers and well-organised repositories;

(b) Accessibility: clear documentation and provenance metadata must ensure that data is understandable and accessible to both humans and machines;

(c) Interoperability: standardised formats and metadata must facilitate seamless integration and sharing of data across systems and platforms;

(d) Reusability: datasets must be formatted for downstream applications, including AI and machine learning workflows; and

(e) Readiness for AI: datasets must be structured to meet the quality requirements of AI applications, including labelled data for supervised learning and comprehensive coverage for unsupervised learning.

(3) The Authority may, in consultation with the apex whole-of-government digital governance body, issue standards giving effect to the principles in this section.

**47. OBLIGATIONS OF DATA CONTROLLERS.**

(1) A data controller must —

(a) ensure that all collection, processing, storage, sharing, archiving and disposal of personal data is lawful, fair and transparent;

(b) collect only data adequate, relevant and limited to what is necessary for the lawful purpose;

(c) implement appropriate technological, physical and organisational measures to ensure data security across the data value lifecycle;

(d) maintain records of processing activities under Section 51;

(e) maintain transaction-level access and disclosure logs under Section 52;

(f) ensure that all persons handling personal data are trained in data protection obligations;

(g) designate a Data Governance Officer as required by Section 50;

(h) conduct a Data Protection Impact Assessment as required by Section 53; and

(i) cooperate with the Authority in the exercise of its functions.

(2) A data controller must report to the Authority any data breach within 72 hours of becoming aware, in accordance with Section 72.

(3) A data controller who contravenes Subsection (1) or (2) commits an offence.

**Penalty:** A fine not exceeding K50,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

**48. OBLIGATIONS OF DATA PROCESSORS.**

(1) A data processor must —

(a) process personal data only on the documented instructions of the data controller;

(b) ensure that persons authorised to process personal data are bound by appropriate confidentiality obligations;

(c) implement the technological, physical and organisational measures required under Section 55;

(d) not engage a sub-processor without the prior written consent of the data controller;

(e) notify the data controller immediately of any data breach, loss or unauthorised access;

(f) maintain records of all processing activities under Section 51 and transaction-level logs under Section 52; and

(g) assist the data controller in responding to data subject rights requests and in complying with Sections 53 and 55.

(2) A data processor who engages a sub-processor remains liable for that sub-processor's acts and omissions.

(3) A data processor who contravenes this section commits an offence.

**Penalty:** A fine not exceeding K30,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K250,000 in the case of a body corporate.

**49. DATA PROCESSING AGREEMENT.**

(1) A data controller must not engage a data processor to process personal data unless the engagement is governed by a written Data Processing Agreement.

(2) A Data Processing Agreement must set out the subject matter, duration, nature and purpose of the processing, the categories of personal data and data subjects, the obligations and rights of the data controller, and the security and confidentiality obligations of the data processor.

(3) A data controller or data processor who enters into a processing arrangement without a Data Processing Agreement commits an offence.

**Penalty:** A fine not exceeding K20,000 in the case of a natural person; a fine not exceeding K100,000 in the case of a body corporate.

**50. DATA GOVERNANCE OFFICERS.**

(1) The following must designate a qualified Data Governance Officer —

(a) every government agency;

(b) every data controller that, as a core activity, carries out large-scale processing of sensitive personal data; and

(c) every data controller or data processor that carries out large-scale systematic monitoring of individuals or operates an AI system that materially affects individuals.

(2) A Data Governance Officer must —

(a) inform and advise the data controller or government agency and staff of obligations under this Act;

(b) monitor compliance with this Act across the data value lifecycle, including compliance with the AI principles under Part VIII;

(c) maintain an inventory of AI systems used by the entity;

(d) provide advice on Data Protection Impact Assessments; and

(e) act as the point of contact with the Authority.

(3) A Data Governance Officer must be given the resources, access and independence necessary to perform the functions of the office and must not be penalised, dismissed or otherwise disadvantaged for performing those functions.

(4) A data controller, data processor or government agency must notify the Authority of the identity and contact details of the Data Governance Officer within 30 days of designation.

**51. RECORDS OF PROCESSING ACTIVITIES.**

(1) Every data controller must maintain a written record of processing activities containing —

(a) the identity and contact details of the data controller;

(b) the purposes of the processing;

(c) the categories of data subjects and personal data;

(d) the categories of recipients, including recipients in foreign countries;

(e) information about cross-border transfers, including the safeguards in place;

(f) retention periods for each category of personal data;

(g) a description of the technological, physical and organisational security measures applied; and

(h) where applicable, a record of all AI systems used in processing.

(2) Every data processor must maintain a record of all categories of processing activities carried out on behalf of each data controller.

(3) Records under this section must be made available to the Authority on request.

**52. TRANSACTION-LEVEL ACCESS AND DISCLOSURE LOGS.**

(1) Every data controller and every data processor must maintain transaction-level logs recording, for each instance of access to or disclosure of personal data —

(a) the identity or role of the person who accessed or disclosed the data;

(b) the date and time of the access or disclosure;

(c) the category or categories of personal data accessed or disclosed;

(d) the purpose of the access or disclosure; and

(e) where data was disclosed to a third party, the identity of the recipient and the legal basis for the disclosure.

(2) Logs maintained under Subsection (1) must be retained for a minimum of 5 years and must be protected against tampering and unauthorised deletion.

(3) A data subject has the right to request information from the data controller about access to or disclosure of the data subject's personal data, and the data controller must respond within 30 days.

(4) Logs under this section must be made available to the Authority on request and must be provided to the Authority without undue delay in the event of a data breach investigation.

(5) The Authority may, by notice in the National Gazette, exempt classes of small data controllers from this section where the volume and sensitivity of processing does not justify the compliance burden.

(6) A data controller or data processor who fails to maintain logs as required commits an offence.

**Penalty:** A fine not exceeding K20,000 in the case of a natural person; a fine not exceeding K150,000 in the case of a body corporate.

**53. DATA PROTECTION IMPACT ASSESSMENT.**

(1) A data controller must conduct a Data Protection Impact Assessment before commencing any processing that is likely to result in a high risk to the rights and freedoms of data subjects, including —

(a) large-scale processing of sensitive personal data;

(b) systematic profiling;

(c) processing biometric data;

(d) processing children's personal data at scale; and

(e) deployment of any AI system that processes personal data or materially influences decisions affecting individuals.

(2) A Data Protection Impact Assessment must assess the nature, scope, context and purpose of the processing; the necessity and proportionality; the risks to rights and freedoms; and the measures to address those risks.

(3) Where a Data Protection Impact Assessment indicates a high residual risk, the data controller must consult the Authority before commencing processing.

(4) A data controller who fails to conduct a required Assessment commits an offence.

**Penalty:** A fine not exceeding K20,000 in the case of a natural person; a fine not exceeding K150,000 in the case of a body corporate.

**54. PRIVACY NOTICES — LANGUAGE AND ACCESSIBILITY.**

(1) A data controller must, at or before the time of collecting personal data, provide the data subject with clear and accessible notice containing —

(a) the identity and contact details of the data controller and Data Governance Officer;

(b) the purpose and lawful basis for processing;

(c) any intended disclosure to third parties;

(d) information about any cross-border transfer and safeguards in place;

(e) the retention period;

(f) the data subject's rights under Sections 62 to 71; and

(g) the right to lodge a complaint with the Authority under Section 94.

(2) Where personal data is not collected directly from the data subject, notice must be provided within 30 days of obtaining the data.

(3) A data controller providing services to persons in Papua New Guinea must —

(a) make privacy notices available in Tok Pisin and, where feasible, in other local languages used by data subjects; and

(b) ensure that consent forms and data subject rights information are accessible in a form suitable for persons with low digital literacy.

(4) A data controller who fails to comply with this section commits an offence.

**Penalty:** A fine not exceeding K10,000 in the case of a natural person; a fine not exceeding K80,000 in the case of a body corporate.

### 55. DATA SECURITY MEASURES — TECHNOLOGICAL, PHYSICAL AND ORGANISATIONAL.

(1) A data controller and a data processor must implement and maintain appropriate technological, physical and organisational measures to ensure the security, integrity and confidentiality of personal data at every stage of the data value lifecycle, having regard to the risks presented by the processing and the nature of the data.

(2) Technological measures under Subsection (1) must include —

(a) encryption of personal data in storage and in transmission;

(b) network security protocols and firewalls;

(c) role-based access controls and, for systems holding sensitive personal data, multi-factor authentication;

(d) procedures for regular testing, assessment and evaluation of technical security measures; and

(e) incident response and recovery systems.

(3) Physical measures under Subsection (1) must include —

(a) secure access controls for premises and server rooms where personal data is stored or processed;

(b) visitor management and physical access records for data processing facilities;

(c) secure storage and certified destruction of physical media and paper records containing personal data;

(d) clean desk and clear screen practices for staff handling personal data; and

(e) equipment security measures to prevent theft or loss of devices containing personal data.

(4) Organisational measures under Subsection (1) must include —

(a) documented data protection policies and procedures;

(b) mandatory data protection training for all staff who handle personal data;

(c) confidentiality obligations for all staff and contractors with access to personal data;

(d) a data breach response plan tested at least annually; and

(e) regular internal audits of data security compliance.

(5) A data controller and a data processor must continuously monitor their systems for unauthorised access or data breaches and report incidents to the Authority without undue delay in accordance with Section 72.

(6) A data controller or data processor who fails to comply with this section commits an offence.

**Penalty:** A fine not exceeding K30,000 in the case of a natural person; a fine not exceeding K300,000 in the case of a body corporate.

## PART V. — PERSONAL DATA PROTECTION.

### Division 1. — Lawful Processing.

**56. REQUIREMENT FOR LAWFUL BASIS.**

(1) A data controller must not process personal data unless the processing is based on one of the lawful bases set out in Section 57.

(2) Where an AI system is used to process personal data, the AI system and its use of personal data must be based on a lawful basis under Section 57 and must comply with Part VIII.

(3) A data controller who processes personal data without a lawful basis commits an offence.

**Penalty:** A fine not exceeding K30,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K300,000 in the case of a body corporate.

**57. LAWFUL BASES FOR PROCESSING.**

(1) Processing of personal data is lawful if —

(a) Consent: the data subject has given consent for one or more specified purposes;

(b) Contract: the processing is necessary for the performance of a contract with the data subject, or to take pre-contractual steps at the data subject's request;

(c) Legal obligation: the processing is necessary for compliance with a legal obligation;

(d) Vital interests: the processing is necessary to protect the vital interests of the data subject or another person;

(e) Public task: the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

(f) Legitimate interests: the processing is necessary for the legitimate interests of the data controller or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

(2) Subsection (1)(f) does not apply to processing carried out by a government agency in the performance of its functions.

**58. CONSENT.**

(1) Where the lawful basis is consent, consent must be freely given, specific, informed and unambiguous, given by a clear affirmative act, and capable of being demonstrated by the data controller.

(2) Consent is not freely given if the provision of a service is made conditional on consent to processing that is not necessary for that service, or if there is a clear power imbalance between the data subject and the data controller.

(3) A data subject may withdraw consent at any time, and withdrawal does not affect the lawfulness of processing before withdrawal.

(4) When consent is withdrawn, the data controller must cease processing within 14 days unless otherwise authorised under Section 57.

**59. SENSITIVE PERSONAL DATA.**

(1) In this Act, "sensitive personal data" means personal data revealing or relating to —

(a) racial or ethnic origin;

(b) political opinions;

(c) religious or philosophical beliefs;

(d) trade union membership;

(e) genetic data;

(f) biometric data, where processed for the purpose of uniquely identifying a natural person;

(g) health or medical data;

(h) data concerning sexual orientation or sex life; or

(i) financial account information and banking credentials.

(2) The processing of sensitive personal data is prohibited unless —

(a) the data subject has given explicit consent for one or more specified purposes;

(b) the processing is necessary for obligations in the field of employment, social security or social protection law;

(c) the processing is necessary to protect vital interests where the data subject is incapable of giving consent;

(d) the processing relates to data manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims;

(f) the processing is necessary for reasons of substantial public interest, on the basis of law, and is proportionate; or

(g) the processing is necessary for the purposes of preventive medicine, medical diagnosis, or the provision of health or social care.

(3) A data controller who processes sensitive personal data in contravention of this section commits an offence.

**Penalty:** A fine not exceeding K50,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

**60. BIOMETRIC DATA — HEIGHTENED PROTECTION.**

(1) Biometric data is sensitive personal data for all purposes of this Act and must be afforded the highest available level of protection, wherever and by whomever it is collected or processed.

(2) A person or organisation must not —

(a) collect or use biometric data for any purpose other than a purpose expressly authorised by law or by the explicit consent of the data subject;

(b) sell, lease, profit from or otherwise commercially exploit biometric data;

(c) share biometric data with a third party except as required by law or expressly authorised by the data subject; or

(d) retain biometric data for longer than is necessary for the purpose for which it was collected.

(3) Biometric data must be encrypted at the point of collection and must remain encrypted at all times except during active verification processing.

(4) Biometric raw data, being the unprocessed or minimally processed biometric capture before template extraction, and root cryptographic key material used to secure any system processing biometric data, must not be stored or processed outside Papua New Guinea under any circumstances, including under an arrangement approved under Section 82.

(5) A Data Protection Impact Assessment under Section 53 is mandatory before any system processing biometric data is deployed, regardless of scale.

(6) This section applies to biometric data collected or processed in any context, including by providers accredited under any national law on digital identity and trust services.

(7) A person or organisation that contravenes Subsection (2) commits an offence.

**Penalty:** A fine not exceeding K100,000 or imprisonment for a term not exceeding 5 years, or both, in the case of a natural person; a fine not exceeding K1,000,000 in the case of a body corporate.

**61. CHILDREN'S PERSONAL DATA.**

(1) A child must not be the subject of a data collection, processing or profiling activity without —

(a) the explicit consent of the child's parent or guardian, if the child is under 13 years; or

(b) the consent of the child, if the child is 13 years or over.

(2) A data controller collecting personal data from or about a child must provide a privacy notice in language that is clear and appropriate for the child's age and must make that notice available in Tok Pisin where the child is in Papua New Guinea.

(3) A data controller must not process a child's personal data for the purpose of profiling or behavioural advertising, or to influence or manipulate the child, including through AI systems.

(4) Where a data controller becomes aware that it has collected personal data from a child without the required consent, it must delete that data within 7 days.

(5) A data controller who contravenes this section commits an offence.

**Penalty:** A fine not exceeding K50,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

## Division 2. — Rights of Data Subjects.

### 62. RIGHT TO BE INFORMED.

(1) A data subject has the right to receive a privacy notice that complies with Section 54.

### 63. RIGHT OF ACCESS.

(1) A data subject has the right to obtain from the data controller confirmation of whether or not personal data relating to the data subject is being processed, and if so, access to that data and information about the purpose, categories, recipients and retention period.

(2) A data controller must respond to a request under Subsection (1) within 30 days of receipt.

(3) A data controller who fails to comply commits an offence.

**Penalty:** A fine not exceeding K10,000 in the case of a natural person; a fine not exceeding K80,000 in the case of a body corporate.

### 64. RIGHT TO RECTIFICATION.

(1) A data subject has the right to obtain from the data controller, without undue delay, the rectification of inaccurate or incomplete personal data.

(2) A data controller must rectify inaccurate or incomplete personal data within 14 days of a request.

(3) A data controller who fails to comply commits an offence.

**Penalty:** A fine not exceeding K10,000 in the case of a natural person; a fine not exceeding K80,000 in the case of a body corporate.

### 65. RIGHT TO ERASURE.

(1) A data subject has the right to obtain erasure of personal data where the data is no longer necessary for the purpose collected; consent is withdrawn; the data subject objects under Section 68 and there are no overriding grounds; the data has been unlawfully processed; or erasure is required for compliance with a legal obligation.

(2) A data controller must erase personal data within 30 days of receiving a valid erasure request.

(3) This section does not apply where processing is necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

(4) A data controller who fails to comply commits an offence.

**Penalty:** A fine not exceeding K10,000 in the case of a natural person; a fine not exceeding K80,000 in the case of a body corporate.

### 66. RIGHT TO RESTRICT PROCESSING.

(1) A data subject has the right to obtain restriction of processing where the accuracy of the data is contested; the processing is unlawful and the data subject opposes erasure; the data controller no longer needs the data but the data subject requires it for legal claims; or the data subject has objected to processing pending verification.

(2) Where processing has been restricted, the data may only be stored, or processed with the data subject's consent or for legal claims.

### 67. RIGHT TO DATA PORTABILITY.

(1) A data subject has the right to receive personal data in a structured, commonly used and machine-readable format where the processing is based on consent or contract and is carried out by automated means.

(2) Where technically feasible, a data subject may request that personal data be transmitted directly from one data controller to another.

(3) This section does not apply where the processing is necessary for the performance of a public task.

### 68. RIGHT TO OBJECT.

(1) A data subject has the right to object, on grounds relating to the data subject's particular situation, to the processing of personal data based on a public task or legitimate interests.

(2) A data controller must cease processing unless compelling legitimate grounds for processing override the interests, rights and freedoms of the data subject, or the processing is for legal claims.

(3) A data subject has the right to object at any time to processing for direct marketing.

### 69. PROHIBITION ON AUTOMATED DECISIONS AFFECTING RIGHTS.

(1) No public body may make a decision solely by automated means, including by an AI system, in any matter that —

(a) affects a person's legal rights, entitlements, penalties or access to significant public services; or

(b) determines or materially influences a person's eligibility, benefits, obligations or outcomes in relation to a government service or program,

without providing for meaningful human review of that decision.

(2) A public body that deploys an AI system for a purpose described in Subsection (1) must —

(a) ensure that a qualified human officer reviews and takes responsibility for each decision before it is communicated as final; and

(b) document and retain a record of the human review for audit purposes.

(3) A public body that contravenes Subsection (1) commits a contravention of this Act and the impugned decision is voidable at the election of the affected person.

### 70. RIGHT TO HUMAN REVIEW OF AUTOMATED DECISIONS.

(1) A data subject has the right to request human review of any decision that —

(a) was made wholly or substantially by an AI system or automated process; and

(b) adversely affects the data subject's legal rights, benefits, entitlements, or access to significant public services.

(2) A data controller or government agency that makes a decision to which Subsection (1) applies must —

(a) inform the data subject, at the time the decision is communicated, of the right to request human review;

(b) provide clear information on how to exercise that right; and

(c) ensure that such information is available in Tok Pisin.

(3) Upon receiving a request for human review, a data controller or government agency must —

(a) assign the review to a suitably qualified human officer who was not involved in the original automated decision;

(b) give the data subject the opportunity to present relevant information or to contest the automated decision; and

(c) provide the data subject with written reasons for the outcome of the review within 30 days.

(4) A data controller or government agency who fails to comply with this section commits an offence.

**Penalty:** A fine not exceeding K30,000 in the case of a natural person; a fine not exceeding K200,000 in the case of a body corporate.

### 71. RIGHT TO COMPENSATION.

(1) A person who suffers material or non-material damage as a result of a contravention of this Act is entitled to receive compensation from the responsible data controller, data processor or government agency.

(2) A claim for compensation may be pursued —

(a) as a civil claim before the National Court under Section 103; or

(b) through the Authority's non-judicial adjudication process under Section 95, where a binding remedial order may include compensation.

(3) A data controller or data processor is not liable if it proves that it was not in any way responsible for the contravention.

## PART VI. — DATA BREACH AND INCIDENT MANAGEMENT.

### 72. NOTIFICATION OF DATA BREACH TO AUTHORITY.

(1) A data controller who becomes aware of a personal data breach must notify the Authority without undue delay and, where feasible, within 72 hours of becoming aware.

(2) The notification must include —

(a) a description of the nature of the breach;

(b) the name and contact details of the Data Governance Officer;

(c) the likely consequences of the breach; and

(d) the measures taken or proposed to address the breach.

(3) Where notification cannot be provided within 72 hours, the data controller must provide it in phases, giving reasons for the delay.

(4) A data controller who fails to notify as required commits an offence.

**Penalty:** A fine not exceeding K30,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K300,000 in the case of a body corporate.

### 73. NOTIFICATION TO DATA SUBJECTS.

(1) Where a breach is likely to result in a high risk to the rights and freedoms of data subjects, the data controller must notify the affected data subjects without undue delay.

(2) The notification must describe in plain language the nature of the breach, the likely consequences, and the measures taken, together with advice on steps data subjects may take to protect themselves, and where data subjects are in Papua New Guinea, the notification must be provided in Tok Pisin.

(3) Notification is not required where the data was protected by measures rendering it unintelligible; subsequent measures have ensured the high risk is no longer likely; or notification would involve disproportionate effort, in which case a public notice must be published.

(4) A data controller who fails to notify as required commits an offence.

**Penalty:** A fine not exceeding K20,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K200,000 in the case of a body corporate.

### 74. OBLIGATIONS OF DATA PROCESSORS ON BREACH.

(1) A data processor who becomes aware of a personal data breach must notify the data controller immediately and in any event within 24 hours of becoming aware.

(2) A data processor who fails to notify as required commits an offence.

**Penalty:** A fine not exceeding K10,000 in the case of a natural person; a fine not exceeding K100,000 in the case of a body corporate.

### 75. EMERGENCY DATA BREACH RESPONSE.

(1) Where the Authority is satisfied that a data breach or AI system incident poses a serious and immediate threat to a large number of persons, the Authority may —

(a) issue an emergency directive requiring immediate action to contain the breach or incident;

(b) direct the suspension of processing operations or of an AI system;

(c) coordinate a public notification; and

(d) engage the National Cyber Security Unit.

(2) A data controller or AI system deployer must comply with an emergency directive immediately.

(3) A person who fails to comply commits an offence.

**Penalty:** A fine not exceeding K50,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

## PART VII. — GOVERNMENT DATA GOVERNANCE, NATIONAL DATA ARCHITECTURE AND CROSS-BORDER TRANSFERS.

### 76. GOVERNMENT DATA GOVERNANCE OBLIGATIONS.

(1) Every government agency must —

(a) designate a Data Governance Officer under Section 50;

(b) develop and maintain a data governance policy consistent with this Act and the data value lifecycle;

(c) publish and maintain a data asset register in the National Data Catalogue under Section 78;

(d) implement data classification as required by Section 39;

(e) ensure any system processing personal data complies with this Act before deployment;

(f) ensure any AI system used in government operations complies with Part VIII;

(g) use the national data exchange platform designated under Section 77 for cross-agency data exchange; and

(h) submit an annual data governance report to the Authority.

(2) A government agency must ensure that any data management system or data exchange platform it procures or deploys is certified as compliant with the national enterprise architecture standards before it may be used to process personal data or government data.

(3) The Head of a government agency is personally responsible for ensuring the agency complies with this section.

**77. NATIONAL DATA EXCHANGE AND INTEROPERABILITY.**

(1) The Minister may, by notice in the National Gazette, designate an accredited Secure Digital Exchange or Interoperability Platform as the national data exchange platform for cross-agency data exchange.

(2) A platform designated under Subsection (1) must be accredited under any applicable national law on digital identity and trust services or, pending the commencement of such a law, must meet the technical standards issued by the Authority.

(3) A government agency must use the designated national data exchange platform for the electronic exchange of government data with other government agencies, unless the Authority has expressly approved an alternative arrangement.

(4) The Authority must develop and maintain the data governance conditions applicable to data exchanged through the designated platform, consistent with the national enterprise architecture and the principles in Section 46.

(5) Private sector entities processing government data under contract with a government agency must, where directed by the Authority, integrate with the designated national data exchange platform.

(6) This section governs the legal basis, purpose limitation and data sharing conditions applicable to data exchanged through a designated platform; the accreditation, technical standards and operation of the platform itself are governed by any applicable national law on digital identity and trust services.

**78. NATIONAL DATA CATALOGUE.**

(1) The Authority must establish and maintain a National Data Catalogue as a register of government data assets held by government agencies.

(2) A government agency must register in the National Data Catalogue —

(a) all datasets it holds or processes;

(b) the classification of each dataset under Section 39;

(c) the purpose for which each dataset is held; and

(d) any AI systems used to process each dataset.

(3) A government agency must update its registration in the National Data Catalogue within 30 days of creating or acquiring a new dataset or deploying a new AI system.

(4) The Authority must make the National Data Catalogue publicly accessible in a machine-readable format, subject to the exclusion of restricted and confidential data.

(5) Data registered in the National Data Catalogue must comply with the national data quality, lineage and documentation standards issued by the Authority.

**79. DATA SHARING BETWEEN AGENCIES.**

(1) A government agency must not share personal data with another entity unless the sharing is authorised by law or by the data subject's consent, and the receiving entity has adequate safeguards.

(2) A government agency sharing personal data with another government agency must —

(a) notify the Authority before sharing, unless authorised by regulation; and

(b) use the designated national data exchange platform under Section 77.

(3) The Authority may issue binding guidelines on inter-agency data sharing protocols, including controls on onward sharing by a receiving agency.

(4) A person who shares personal data in contravention of this section commits an offence.

**Penalty:** A fine not exceeding K20,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K150,000 in the case of a body corporate.

### 80. OPEN GOVERNMENT DATA.

(1) The Minister, in consultation with the Authority, may by notice in the National Gazette declare categories of government data to be open data that must be made publicly available.

(2) Open data must be made available in a machine-readable format under an open data licence approved by the Authority.

(3) Open data must not include personal data unless it has been anonymised in a manner approved by the Authority.

(4) An open data declaration must be consistent with the data classification framework in Section 39 and must not include restricted or confidential data.

### 81. CROSS-BORDER DATA TRANSFER.

(1) A data controller or data processor must not transfer personal data outside Papua New Guinea unless —

(a) the recipient country or jurisdiction ensures an adequate level of protection as determined by the Authority;

(b) the transfer is authorised by the Authority with appropriate safeguards, including standard contractual clauses prescribed under Subsection (2);

(c) the data subject has expressly consented after being informed of the risks; or

(d) the transfer is necessary for the performance of a contract with the data subject.

(2) The Authority may by notice in the National Gazette prescribe countries providing adequate protection and standard contractual clauses for use in cross-border transfers.

(3) The adequacy assessment under Subsection (1)(a) must include an assessment of sovereign hosting requirements in accordance with Section 82 and, where Papua New Guinea is a party to an applicable international data-sharing protocol, whether the recipient jurisdiction provides protections consistent with that protocol.

(4) A recipient of personal data transferred under this section must not make an onward transfer of that data to a third jurisdiction unless the onward transfer itself satisfies Subsection (1).

(5) A data controller or data processor who transfers personal data in contravention of this section commits an offence.

**Penalty:** A fine not exceeding K30,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K300,000 in the case of a body corporate.

### 82. SOVEREIGN HOSTING REQUIREMENTS.

(1) The following data must be stored and processed within Papua New Guinea or within sovereign environments approved by the Minister under Subsection (2) —

(a) government data classified as restricted or confidential under Section 39;

(b) data relating to nationally significant digital public infrastructure systems; and

(c) data assets designated as of strategic significance by the Minister by notice in the National Gazette.

(2) The Minister may, on the advice of the Authority, approve a sovereign hosting arrangement with a foreign jurisdiction or cloud infrastructure provider that —

(a) provides contractual safeguards ensuring Papua New Guinea's jurisdictional control;

(b) includes data portability and exit rights;

(c) is subject to Papua New Guinea cybersecurity oversight; and

(d) meets the sovereign hosting standards issued by the Authority.

(3) A government agency must not enter into an arrangement for the offshore hosting or processing of data described in Subsection (1) without the approval of the Minister on the advice of the Authority.

(4) Despite any other provision of this section, biometric raw data and root cryptographic key material described in Section 60(4) must not be hosted, stored or processed offshore under any circumstances.

(5) A government agency that contravenes this section commits a contravention of this Act.

**83. DATA LOCALISATION.**

(1) A government agency must store and process all restricted data and personal data of citizens within Papua New Guinea, except where authorised under Section 81 or Section 82.

(2) A data controller that stores or processes personal data outside Papua New Guinea must notify the Authority of the location and ensure that the foreign data centre provides protections consistent with this Act.

(3) The Authority may, in consultation with the Department responsible for information and communications technology, issue standards for data localisation.

**84. INTERNATIONAL COOPERATION AND INTER-AUTHORITY CONSULTATION.**

(1) The Authority may, with the approval of the Minister, enter into arrangements with foreign data protection and AI governance authorities for information sharing, technical assistance and coordination of enforcement.

(2) The Authority may apply for Papua New Guinea's participation in the APEC Cross-Border Privacy Rules System and may represent Papua New Guinea in international data protection forums.

(3) The Minister may recommend to the National Executive Council that Papua New Guinea accede to international treaties or conventions relating to data protection and privacy.

(4) Where Papua New Guinea is a party to an international data-sharing protocol that requires personal data received under the protocol to be subject to specified data protection standards, the Authority must —

(a) monitor compliance with the protocol's data protection requirements by data controllers and data processors who receive personal data under the protocol; and

(b) on receiving a request for consultation from a foreign authority under such a protocol, respond within 30 days and cooperate fully in the consultation process.

(5) A data controller who receives personal data under an applicable international data-sharing protocol must comply with the data protection conditions specified in that protocol in addition to the requirements of this Act.

**85. CROSS-BORDER SUSPENSION MECHANISM.**

(1) The Authority may, by written notice to the Minister, recommend suspension or restriction of the transfer of personal data to a foreign jurisdiction where —

(a) the Authority determines that the jurisdiction no longer provides an adequate level of protection, notwithstanding a prior adequacy determination under Section 81;

(b) a pattern of serious or systematic breaches of data protection obligations has been identified in relation to personal data transferred to that jurisdiction; or

(c) a foreign data protection authority has notified the Authority of a serious or systematic breach involving personal data originating from Papua New Guinea.

(2) Before making a recommendation under Subsection (1), the Authority must consult the relevant foreign authority and give the foreign jurisdiction a reasonable opportunity to respond.

(3) Where the Minister accepts the recommendation, the Minister may, by notice in the National Gazette, suspend or restrict data transfers to the relevant jurisdiction for a specified period, pending remediation.

(4) Where a foreign authority notifies the Authority that data controllers in Papua New Guinea are in serious or systematic breach of an applicable protocol or treaty obligation, the Authority must —

(a) investigate the notified breach within 60 days;

(b) report the outcome to the Minister and to the foreign authority; and

(c) where the breach is substantiated, take proportionate enforcement action to remedy the breach and prevent recurrence.

(5) A data controller or data processor who transfers personal data to a jurisdiction in contravention of a suspension notice under Subsection (3) commits an offence.

**Penalty:** A fine not exceeding K50,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

### 86. EMERGENCY DATA SHARING.

(1) Despite any other provision of this Act, a data controller may share personal data without prior consent if sharing is necessary to protect the life, health or safety of a person who is incapable of giving consent; is directed by a court order or law enforcement authority; or a state of emergency has been declared under the Constitution and sharing is necessary for emergency response.

(2) A data controller relying on Subsection (1) must limit sharing to what is strictly necessary, record the grounds, and notify the Authority within 7 days.

## PART VIII. — ARTIFICIAL INTELLIGENCE PRINCIPLES.

### 87. APPLICATION AND OBJECTS OF THIS PART.

(1) This Part applies to all persons and government agencies that develop, deploy or operate AI systems in Papua New Guinea or that use AI systems to deliver goods or services to persons in Papua New Guinea, regardless of where the AI system is hosted or developed, provided its outputs affect persons in Papua New Guinea.

(2) The objects of this Part are to capture the core principles for the responsible governance of AI in Papua New Guinea, to protect individuals from harm caused by AI systems, and to ensure that, until a dedicated national AI law is enacted, AI systems that process personal data or affect individuals are subject to the data protection and data governance protections of this Act.

(3) Where a dedicated national AI law is enacted, that law and this Part must be read consistently, and where there is an irreconcilable inconsistency the dedicated national AI law prevails, except to the extent that this Part deals with the data protection rights of individuals and the data governance obligations of data controllers, in which case this Part continues to apply.

### 88. RESPONSIBLE AI PRINCIPLES.

(1) A person who develops, deploys or operates an AI system must apply the following responsible AI principles —

(a) Human oversight: an AI system that affects individuals must remain subject to meaningful human oversight, and a qualified human officer must be able to intervene, suspend or override the system;

(b) Transparency: affected persons must be informed, in plain language and where applicable in Tok Pisin, that an AI system is being used in a process or decision that affects them;

(c) Explainability: a meaningful explanation of the factors leading to a decision must be available on request;

(d) Fairness and non-discrimination: an AI system must be assessed for bias and must not produce unfair or discriminatory outcomes;

(e) Accountability and auditability: the deployer of an AI system must maintain auditable records of the system's operation and remain accountable for its outcomes;

(f) Safety and security: an AI system must be secure, robust and tested before deployment; and

(g) Data governance: an AI system must comply with the data governance and data protection requirements of this Act.

### 89. RISK-BASED AI GOVERNANCE.

(1) The Authority must establish, maintain and publish a risk-based framework that classifies AI systems according to the level of risk they pose to individuals and to society, distinguishing at least between prohibited practices, high-risk AI systems, and other AI systems.

(2) A person who deploys a high-risk AI system, being an AI system that materially influences a decision affecting an individual's legal rights, entitlements or access to significant public services, or that performs biometric identification, must —

(a) conduct a Data Protection Impact Assessment under Section 53 before deployment;

(b) implement human oversight and maintain auditable records of the system's operation;

(c) assess the system for bias before deployment and periodically thereafter; and

(d) provide transparency to affected persons in accordance with Section 88.

(3) A government agency must not deploy a high-risk AI system unless human oversight mechanisms are documented and operational, auditable records are maintained, and the agency's Data Governance Officer has reported the system to the Authority.

(4) The Authority may issue standards and guidelines giving effect to the risk-based framework, including registration requirements for high-risk AI systems.

**90. PROHIBITED AI PRACTICES.**

(1) The following AI practices are prohibited in Papua New Guinea —

(a) AI systems that use subliminal techniques operating below a person's conscious awareness to influence behaviour in a manner that causes or is likely to cause harm;

(b) AI systems that exploit the vulnerabilities of a specific group of persons due to their age, disability, or social or economic situation, in a manner that causes or is likely to cause harm;

(c) AI systems used by a government agency for social scoring of individuals based on their social behaviour or personal characteristics for the purpose of imposing detriments unrelated to the context in which the data was originally produced;

(d) AI systems that perform real-time remote biometric identification of individuals in publicly accessible spaces for law enforcement purposes, except where expressly authorised by the National Court in respect of a specific investigation and for a limited period; and

(e) AI systems that generate or amplify deceptive content designed to manipulate electoral or judicial processes.

(2) A person who develops, deploys or operates a prohibited AI practice commits an offence.

**Penalty:** A fine not exceeding K500,000 or imprisonment for a term not exceeding 7 years, or both, in the case of a natural person; a fine not exceeding K5,000,000 in the case of a body corporate.

**91. OBLIGATIONS FOR AI SYSTEMS AFFECTING INDIVIDUALS.**

(1) A person who deploys an AI system that interacts directly with persons, including a chatbot or virtual assistant, must disclose to the person that they are interacting with an AI system and must not mislead the person about the nature of the interaction.

(2) A government agency that deploys an AI system to autonomously initiate, process, decide upon or communicate government service transactions must ensure that the system operates within pre-approved workflows, maintains auditable logs, provides a clear pathway to human assistance, and does not make a decision affecting a person's legal rights or access to significant public services without human review in accordance with Section 69.

(3) A person who fails to comply with Subsection (1) commits an offence.

**Penalty:** A fine not exceeding K20,000 in the case of a natural person; a fine not exceeding K100,000 in the case of a body corporate.

**92. AI SYSTEMS TO COMPLY WITH DATA GOVERNANCE AND DATA PROTECTION.**

(1) Any AI system that processes personal data must —

(a) comply with the lawful basis requirements under Sections 56 and 57;

(b) comply with all data governance obligations under Part IV, including the data value lifecycle principles;

(c) comply with the data subject rights under Part V, including the prohibition on automated decisions affecting rights under Section 69 and the right to human review under Section 70; and

(d) not use personal data in a manner incompatible with the purpose for which it was collected.

(2) The data governance obligations of Part IV apply to all AI workflows, including data collection for AI training, AI processing of personal data, and AI-generated outputs that contain or are derived from personal data.

### 93. AUTHORITY'S AI REGULATORY FUNCTIONS.

(1) The Authority must —

(a) maintain and publish the risk-based AI framework under Section 89;

(b) receive and act on AI system incident notifications and complaints relating to AI systems;

(c) conduct compliance audits of AI systems;

(d) issue guidelines and standards giving effect to the AI principles in this Part; and

(e) advise the Minister on AI governance policy, including on the need for a dedicated national AI law.

(2) The Authority may issue interim AI governance standards pending the enactment of dedicated national AI legislation.

(3) A person who deploys an AI system in contravention of a directive of the Authority commits an offence.

**Penalty:** A fine not exceeding K50,000 in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

## PART IX. — COMPLAINTS, REMEDIES AND ENFORCEMENT.

### Division 1. — Complaints and Non-Judicial Remedies.

### 94. COMPLAINTS TO AUTHORITY.

(1) A data subject who believes that a data controller or data processor has contravened this Act in relation to their personal data, or in relation to an AI system that processes their personal data or makes or materially influences a decision affecting them, may lodge a written complaint with the Authority.

(2) A complaint must identify the data controller or data processor; describe the conduct alleged to contravene this Act; and be lodged within 12 months of the data subject becoming aware of the alleged contravention, or within such longer period as the Authority permits.

(3) The Authority must acknowledge receipt of a complaint within 14 days.

(4) The Authority may decline to investigate a complaint that is frivolous, vexatious or lacks sufficient substance, and where a complaint discloses a systemic issue the Authority may initiate an investigation on its own initiative.

(5) Where a complaint relates to digital identity, trust services or verifiable credentials and falls within the mandate of the Digital Identity and Trust Services Regulator, the Authority must refer the complaint to that Regulator under the referral mechanism in Section 14(3)(c), and must notify the complainant of the referral.

### 95. NON-JUDICIAL ADJUDICATION — CONCILIATION AND BINDING ORDERS.

(1) On receiving a complaint, the Authority must first offer the parties a conciliation process, being a voluntary process in which the Authority assists the parties to reach a mutually acceptable resolution.

(2) Where conciliation results in an agreement, the terms of the agreement must be recorded in writing, signed by both parties, and a copy provided to the Authority. A conciliation agreement is binding on the parties and may be enforced as a contract.

(3) Where conciliation does not result in an agreement within 30 days of being offered, or where a party declines to participate, the Authority must proceed to investigation under Section 96.

(4) Following investigation, the Authority may, in addition to any other enforcement action, issue a binding remedial order requiring a data controller or data processor to —

(a) cease the contravening conduct;

(b) take specified action to remedy the contravention, including rectifying, erasing or providing access to personal data;

(c) pay compensation to the complainant for material or non-material damage suffered, not exceeding K100,000; or

(d) implement specified data protection measures within a stated period.

(5) A binding remedial order under Subsection (4) constitutes a non-judicial remedy, and is available in addition to, and without limiting, the judicial remedies under Division 3.

(6) A person who fails to comply with a binding remedial order commits an offence.

**Penalty:** A fine not exceeding K30,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K300,000 in the case of a body corporate.

(7) A party dissatisfied with a binding remedial order may appeal to the National Court under Section 102.

### 96. INVESTIGATION OF COMPLAINTS.

(1) On proceeding to investigation, the Authority must notify the data controller or data processor named in the complaint, investigate the complaint and determine whether a contravention has occurred.

(2) The Authority must complete an investigation within 60 days of commencing it, or within such further time as is reasonable in the circumstances.

(3) The Authority must give written notice of its determination, including the outcome, the reasons, and the rights of the parties to appeal, to the complainant and to the data controller or data processor within 14 days of making the determination.

## Division 2. — Enforcement.

### 97. ENFORCEMENT POWERS OF AUTHORITY.

(1) The Authority may investigate suspected contraventions on its own initiative or on complaint; enter and inspect premises where data processing is carried on, subject to any warrant required by law; require the production of documents, records and information, including transaction-level logs under Section 52; interview persons and take evidence on oath or affirmation; issue compliance notices under Section 98; impose administrative sanctions under Section 99; issue binding remedial orders under Section 95; and refer matters to appropriate law enforcement authorities for prosecution.

### 98. COMPLIANCE NOTICES.

(1) Where the Authority determines that a person or organisation has contravened or is likely to contravene this Act, the Authority may issue a compliance notice requiring the person or organisation to take specified steps to remedy the contravention or to cease or modify specified data processing or AI system activities.

(2) A compliance notice must specify the contravention or likely contravention; specify the action required; specify the period within which the action must be taken; and state the right to appeal.

(3) A person or organisation that fails to comply with a compliance notice commits an offence.

**Penalty:** A fine not exceeding K20,000 or imprisonment for a term not exceeding 12 months, or both, in the case of a natural person; a fine not exceeding K200,000 in the case of a body corporate.

### 99. ADMINISTRATIVE SANCTIONS.

(1) Where the Authority determines that a person or organisation has contravened this Act and that the contravention does not warrant criminal prosecution, the Authority may impose an administrative sanction.

(2) Administrative sanctions may include a written warning or reprimand; a direction to cease or modify specified data processing or AI system activities; a requirement to undertake corrective measures or training; or a monetary penalty not exceeding K100,000 for a natural person or K1,000,000 for a body corporate.

(3) In determining an administrative sanction, the Authority must have regard to the nature, gravity and duration of the contravention; the degree of responsibility and any previous contraventions; the categories and number of data subjects affected; any action taken to mitigate the harm; the size and turnover of the entity; and the level of cooperation with the Authority.

### 100. COMPLIANCE AUDITS.

(1) The Authority may conduct compliance audits of any person or organisation that collects, processes or stores personal data or deploys an AI system.

(2) An audit may be initiated on a routine basis; following a complaint, data breach notification or AI system incident notification; or where the Authority has reasonable grounds to suspect non-compliance.

(3) The Authority must provide written notice of an audit specifying the date, scope and purpose.

(4) The audited entity must cooperate with the audit, provide access to facilities, systems, data, AI systems and records, and implement recommendations within the period specified by the Authority.

(5) Failure to cooperate with an audit or implement required recommendations is a contravention of this Act.

### 101. OFFENCES — GENERAL.

(1) A person or organisation must not obstruct, hinder or interfere with the Authority in the lawful performance of its functions; knowingly give false or misleading information to the Authority; fail to comply with a lawful direction, order or notice issued by the Authority; or process, disclose or transfer personal data in contravention of this Act.

(2) A person or organisation that contravenes Subsection (1) commits an offence.

**Penalty:** A fine not exceeding K50,000 or imprisonment for a term not exceeding 2 years, or both, in the case of a natural person; a fine not exceeding K500,000 in the case of a body corporate.

(3) Where an offence under this Act is committed by a body corporate, every director, officer or manager who consented to or connived in the commission of the offence also commits an offence and is liable to the same penalty.

## Division 3. — Judicial Remedies.

### 102. APPEAL TO NATIONAL COURT.

(1) A person aggrieved by a determination, compliance notice, binding remedial order or administrative sanction of the Authority may appeal to the National Court within 30 days of being notified of the decision.

(2) The National Court may, on appeal —

(a) confirm, vary or set aside the decision of the Authority;

(b) remit the matter to the Authority for reconsideration; or

(c) make such other order as is just and equitable.

(3) An appeal does not automatically stay the decision of the Authority unless the National Court orders otherwise.

### 103. RIGHT OF ACTION FOR COMPENSATION.

(1) A person who suffers material or non-material damage as a result of a contravention of this Act may bring a civil claim for compensation before the National Court, in addition to any complaint to the Authority.

(2) In awarding compensation, the National Court may have regard to —

(a) the nature and gravity of the contravention;

(b) any distress, inconvenience or harm suffered by the claimant;

(c) any financial loss suffered; and

(d) whether the respondent took reasonable steps to prevent the contravention.

(3) A data controller or data processor is not liable under this section if it proves that it was not in any way responsible for the contravention.

(4) A person must not recover compensation both under this section and under a binding remedial order under Section 95(4)(c) in respect of the same damage.

## PART X. — FINANCIAL PROVISIONS.

### 104. FUNDS OF AUTHORITY.

(1) The funds of the Authority consist of —

(a) moneys appropriated by the Parliament for the purposes of the Authority;

(b) fees and charges collected by the Authority under this Act;

(c) grants and donations received with the approval of the Minister; and

(d) any other moneys lawfully received by the Authority.

(2) The funds of the Authority must be applied only for the purposes of this Act.

### 105. ANNUAL BUDGET.

(1) Before the start of each financial year, the Board must prepare and submit to the Minister a budget setting out estimated revenue and expenditure and proposed capital expenditure.

(2) The Minister may approve the budget with or without amendment, subject to Section 21.

### 106. APPLICATION OF PUBLIC FINANCE MANAGEMENT ACT 1995.

(1) The Authority is subject to the Public Finance Management Act 1995.

### 107. APPLICATION OF AUDIT ACT 1989.

(1) The accounts of the Authority are subject to inspection and audit by the Auditor-General under the Audit Act 1989.

## PART XI. — REPORTING AND ACCOUNTABILITY.

### 108. ANNUAL REPORT.

(1) The Authority must, within 3 months after the end of each financial year, prepare and submit to the Minister an annual report including —

(a) a report on the performance of the Authority's functions;

(b) statistics on complaints received, conciliations conducted, binding remedial orders issued, investigations completed and enforcement actions taken;

(c) a report on AI governance activities, including the number of high-risk AI systems registered and audited;

(d) a report on cross-border data transfer activities, including adequacy determinations made and any suspension action taken under Section 85;

(e) a report on coordination with the Digital Identity and Trust Services Regulator; and

(f) audited financial statements.

### 109. TABLING OF ANNUAL REPORT.

(1) The Minister must table a copy of the annual report in the National Parliament within 30 days of receiving it.

### 110. PUBLIC AWARENESS AND CAPACITY BUILDING.

(1) The Authority may develop and implement programmes to raise public awareness about data governance, the data value lifecycle, data protection rights and responsible AI.

(2) The Authority must ensure that awareness programmes and materials are available in Tok Pisin and are accessible to persons in rural and remote areas and to persons with low digital literacy.

(3) The Authority may collaborate with public bodies, private sector organisations, academic institutions, civil society organisations and media organisations for the purposes of this section.

## PART XII. — MISCELLANEOUS AND SAVINGS.

### 111. PROTECTION FROM PERSONAL LIABILITY.

(1) A member of the Board or an officer of the Authority is not personally liable for anything done or omitted in good faith in the exercise or purported exercise of a power, or the performance or purported performance of a function, under this Act.

**112. CONFIDENTIALITY OBLIGATIONS.**

(1) A member of the Board, an officer of the Authority, or any person engaged by the Authority must not disclose any information obtained in the course of performing functions under this Act, except in the course of performing those functions; with the consent of the person to whom the information relates; as required or authorised by law; or to the extent necessary for the administration of this Act.

(2) A person who contravenes Subsection (1) commits an offence.

**Penalty:** A fine not exceeding K20,000 or imprisonment for a term not exceeding 12 months, or both.

**113. EVIDENTIARY PROVISIONS.**

(1) In any proceedings under this Act, a certificate signed by the Chief Executive Officer certifying the content of any register or record maintained by the Authority under this Act at a specified time is evidence of the fact certified; and a document purporting to be signed by the Chairperson of the Board is, without proof of signature, admissible as evidence of its contents.

**114. COLLABORATION AND PARTNERSHIPS.**

(1) All public bodies, private organisations and stakeholders must cooperate with the Authority in carrying out this Act.

(2) The Authority may enter into memoranda of understanding or partnership arrangements for information sharing and technical assistance with national, regional or international organisations.

**115. REVIEW OF ACT.**

(1) The Minister must cause this Act to be reviewed 3 years after its commencement to assess whether its objects are being achieved and whether any amendments are required.

(2) The review must assess, in particular —

(a) the operation of the data value lifecycle provisions in Part IV;

(b) the adequacy of the AI principles in Part VIII and whether a dedicated national AI law is required;

(c) the effectiveness of the non-judicial remedy mechanism under Section 95;

(d) the effectiveness of the cross-border suspension mechanism under Section 85; and

(e) the effectiveness of coordination with the Digital Identity and Trust Services Regulator under Section 14.

(3) The Minister must table a report on the review in the Parliament within 3 months of the review being completed.

**116. TRANSITIONAL PROVISIONS.**

(1) Data controllers and data processors must comply with Parts IV and V within 12 months of those Parts coming into operation.

(2) Government agencies must comply with Sections 76, 77 and 78 within 18 months of those sections coming into operation.

(3) Deployers of existing high-risk AI systems must comply with Part VIII within 18 months of that Part coming into operation.

(4) A data controller operating without a Data Processing Agreement before commencement must enter into a Data Processing Agreement complying with Section 49 within 6 months of that section coming into operation.

(5) Data controllers and data processors must establish the transaction-level logs required by Section 52 within 12 months of that section coming into operation.

(6) All policies, standards and guidelines issued before commencement by the Department responsible for information and communications technology or by NICTA in relation to data governance, data

protection or AI governance continue in force and are taken to have been issued by the Authority under this Act until replaced.

### 117. NDA TRANSITION SAVINGS.

(1) On the establishment of the NDA under Section 16 —

(a) all references in this Act and in any other national law to NICTA in its capacity as the Authority or as the NDA are taken to be references to the established NDA;

(b) all standards, guidelines, directions and instruments issued by NICTA as the interim Authority continue in force as instruments of the NDA until replaced;

(c) all complaints, investigations and proceedings before the interim Authority are taken to be before the NDA and must be continued and determined accordingly;

(d) all rights and obligations of NICTA in its capacity as the interim Authority vest in the NDA; and

(e) any reference in any contract, agreement, licence or instrument to NICTA acting in its capacity as the interim Authority is to be read as a reference to the NDA.

(2) NICTA continues to perform its functions under the NICT Act after the establishment of the NDA, and nothing in this Act affects those functions.

### 118. LEGISLATIVE COHERENCE — READING WITH DIGITAL LAWS.

(1) This Act must be read together with all national laws relating to digital governance, digital economy, artificial intelligence, digital identity, cybersecurity, electronic transactions, critical digital infrastructure and related matters, as those laws are enacted or amended from time to time.

(2) Where a national digital law addresses a matter also addressed by this Act, the Authority must exercise its functions consistently with both laws.

(3) Where a national law on artificial intelligence governance is enacted, the data protection rights of data subjects and the data governance obligations of data controllers under this Act continue to apply in relation to AI systems, and all standards and enforcement actions issued by the Authority under Part VIII that are not inconsistent with that law continue in force.

(4) Where a national law on digital identity and trust services is enacted, that law governs digital identity, trust services and verifiable credentials, and this Act applies as the data protection law of general application to personal data processed within the digital trust ecosystem; the Authority and the Digital Identity and Trust Services Regulator must coordinate under Section 14 to avoid duplicative regulation.

(5) Where a national law on critical digital infrastructure investment is enacted, the data governance obligations and sovereign hosting requirements under this Act must be exercised consistently with the objects of that law.

(6) The Authority must, in performing its functions, have regard to the whole digital legislative framework of Papua New Guinea and must exercise its functions in a manner that supports coherent and integrated digital governance.

### 119. SAVINGS — EXISTING INSTRUMENTS AND PROCEEDINGS.

(1) All policies, standards and guidelines referred to in Section 116(6) continue in force until replaced by an instrument of the Authority under this Act.

(2) A legal proceeding commenced before commencement of this Act that relates to a matter covered by this Act may be continued as if this Act had not been enacted.

## PART XIII. — REGULATIONS.

### 120. REGULATIONS.

(1) The Head of State, acting on advice, may make regulations, not inconsistent with this Act, prescribing all matters that are required or permitted to be prescribed or that are necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Without limiting Subsection (1), regulations may prescribe —

(a) technological and organisational standards for data protection and data security at each stage of the data value lifecycle;

(b) physical security standards for premises and facilities where personal data is stored or processed;

(c) procedures for data breach notification and reporting;

(d) criteria for determining adequacy of data protection in foreign countries for cross-border transfers, including consistency with applicable international data-sharing protocols;

(e) national data classification standards;

(f) national data quality, metadata and lineage standards consistent with the National Data Catalogue;

(g) data lifecycle governance, archiving and secure destruction standards;

(h) data retention requirements;

(i) the form, content and retention of transaction-level access and disclosure logs under Section 52, and classes of data controllers exempt from that section;

(j) qualifications, appointment and responsibilities of Data Governance Officers;

(k) procedures for conciliation and non-judicial adjudication under Section 95;

(l) AI risk classification criteria and registration requirements for high-risk AI systems;

(m) AI impact and bias assessment procedures and standards;

(n) open data release frameworks;

(o) data localisation and sovereign hosting requirements;

(p) data governance conditions for the use of designated data exchange platforms under Section 77;

(q) criteria for administrative penalties and sanctions;

(r) fees and charges payable under this Act; and

(s) any forms required for the administration of this Act.

(3) Regulations must be published in the National Gazette and take effect on the date of publication or a later date specified in the regulation.

(4) A regulation may prescribe penalties not exceeding K10,000 for offences against the regulation.