



PUBLIC CONSULTATION

DATA GOVERNANCE AND DATA PROTECTION BILL 2026

Introductory Statement and Matters for Stakeholder Comment

The Government of Papua New Guinea invites public authorities, regulated industries, professional bodies, civil society organisations, academic institutions, development partners and members of the public to comment on the proposed Data Governance and Data Protection Bill 2026.

The Bill is being developed to give legislative effect to the National Data Governance and Data Protection Policy 2024 and to establish a coherent national framework for the responsible collection, use, protection, sharing and management of data. It is also intended to provide a legal foundation for trusted digital government, secure data exchange, digital identity services and the responsible use of emerging technologies.

This introductory statement identifies the principal matters on which feedback is sought. It should be read with the draft Bill and the Revised Detailed Drafting Instructions. Stakeholders are encouraged to address the practical effect of the proposed provisions, including their suitability for Papua New Guinea's legal, institutional, economic and technical circumstances.

Purpose and policy setting

The National Data Governance and Data Protection Policy 2024 recognises data as a strategic national resource. Properly governed data can improve public administration and service delivery, support research and innovation, strengthen the digital economy and enable more effective planning and decision-making. Those benefits depend on public confidence that information will be handled lawfully, securely and for legitimate purposes.

The same growth in data collection and digital processing creates material risks. These include unauthorised access or disclosure, misuse of personal information, inconsistent sharing practices, poor data quality, fragmented government systems, excessive retention, discriminatory processing and decisions made without adequate transparency or human accountability. The proposed Bill responds to those risks by establishing enforceable rights, duties, safeguards and oversight arrangements across the data lifecycle.

The proposed framework treats data governance, data protection and privacy as connected but distinct concerns. Data governance addresses the stewardship, quality, classification, sharing and value of data. Data protection establishes controls against loss, misuse and unauthorised processing. Privacy protects the dignity and legitimate expectations of individuals in relation to information about them. The Bill must accommodate each of these concerns while permitting necessary and

proportionate uses of data for government administration, health, education, research, public safety, commerce and innovation.

Proposed legislative framework

The Bill is intended to apply across public and private sector settings and to regulate handing of data by persons and organizations that determine the purposes of processing or process data on behalf of others. Subject to clearly defined exceptions, it would establish lawful processing requirements; safeguards for sensitive information and children's data; security, retention and breach-notification duties; and mechanisms for complaints, investigation, audit, enforcement and redress.

Individuals would have rights to receive clear information about processing and, where applicable, to access, correct, restrict, erase or object to the use of their personal data. The framework also contemplates data portability, meaningful human review of certain automated decisions and compensation where loss or damage results from a contravention. The practical scope, limitations and enforcement of those rights are important matters for consultation.

For government data, the proposed approach includes common rules for classification, quality, interoperability, data sharing, enterprise architecture and registration of datasets through a National Data Catalogue. It also provides for a designated national data exchange platform and enhanced controls for restricted, confidential and strategically significant information.

The drafting approach further addresses cross-border transfers and sovereign hosting, digital identity and trust services, and an interim risk-based framework for artificial intelligence. The AI provisions include controls for prohibited practices and high-risk systems, impact assessment, bias testing, audit records, transparency, human oversight and review of decisions that materially affect rights or access to significant public services.

Implementation is expected to be staged. Transitional periods, guidance, sector-specific instruments and capacity development will be required so that obligations can be introduced in a manner that is credible, proportionate and capable of enforcement.

Matters for stakeholder feedback

Stakeholders are invited to comment on the following matters and to identify any provisions that are unclear, disproportionate, impracticable or likely to create unintended consequences.

1. Scope and application

Does the proposed scope appropriately cover government agencies, State bodies, private organisations, contractors, service providers and relevant foreign entities that process data concerning persons in Papua New Guinea? Feedback is also sought on the territorial reach of the Bill and on whether any exclusions or exemptions are necessary and sufficiently confined.

2. Individual rights and organisational duties

Are the proposed rights of information, access, correction, erasure, restriction, objection, portability, human review and compensation clear and workable? Do the duties imposed on controllers and processors provide an appropriate level of accountability, including for consent, lawful processing, data minimisation, accuracy, security, retention and disposal?

Stakeholders should indicate where a right may require a carefully defined limitation for public administration, law enforcement, national security, public health, research or another legitimate public interest, and what safeguards should apply to any such limitation.

3. Government data governance and interoperability

Do the proposed requirements for data classification, data quality, sharing, interoperability, enterprise architecture and dataset registration provide a workable basis for coordinated digital government? Comment is sought on the role of the designated national data exchange platform, the National Data Catalogue, responsibility of agency heads and the time required for agencies to comply.

4. Sovereign hosting and cross-border transfers

Do the proposed controls adequately protect personal data and nationally significant government information while allowing the use of secure regional or international services where appropriate safeguards exist? Stakeholders are invited to address transfer mechanisms, approved sovereign environments, localisation requirements and any sector-specific operational implications.

5. Artificial intelligence and automated decision-making

Is the proposed interim, risk-based framework sufficiently clear and proportionate? Feedback is sought on prohibited practices, the definition and registration of high-risk systems, impact assessment, bias testing, audit logging, biometric systems, transparency and meaningful human oversight. Particular attention is invited to decisions that affect legal rights, eligibility for public services or other significant interests.

6. Compliance, enforcement and implementation

Are the proposed powers to receive complaints, investigate, audit, issue directions, impose sanctions and provide remedies suitable and enforceable? Comment is also sought on staged commencement, transitional periods, guidance, sector codes, public awareness and the institutional and technical capacity required for effective compliance.

Central governance question

A principal matter for consultation is the institutional arrangement through which the proposed legislation would be administered, regulated and enforced.

The Revised Detailed Drafting Instructions propose a phased model. Under that model, the National Information and Communications Technology Authority (NICTA) would initially perform the functions of the National Digital Economy Authority for the purposes of the Bill and related national digital laws. During the transitional period, NICTA would exercise the relevant data governance, data protection, digital identity and interim AI governance functions.

A separate National Digital Economy Authority may subsequently be constituted following an Executive Government decision and confirmation that the necessary governance, leadership, funding, premises, systems and institutional capacity are in place. The relevant functions, records, complaints, instruments, staff arrangements, rights and liabilities would then transfer to the constituted Authority.

CONSULTATION QUESTION

Does the proposed phased governance model provide an appropriate, independent, and sustainable mechanism for administering data protection, data governance, digital identity and interim artificial intelligence regulation in Papua New Guinea?

In responding to this question, stakeholders are asked to consider whether NICTA should perform the functions during the interim period or whether a standalone authority should be established at commencement; the safeguards required for independent complaints, investigations and enforcement; and the appropriate separation of policy, regulatory and operational responsibilities.

Views are also sought on accountability to the Minister, Parliament and the public; separate records, accounts, staffing and decision-making arrangements during the interim period; the conditions that should be met before the standalone Authority is constituted; whether transition should occur after a fixed period or following an assessment of readiness; and coordination with bodies responsible for cybersecurity, digital government, competition, consumer protection, financial regulation and national security.

Stakeholders may also comment on the proposed composition and appointment of the governing Board, including whether it provides sufficient expertise and representation in law, privacy, cybersecurity, artificial intelligence, public administration, civil society and the digital private sector.

Form of submissions

Submissions should identify the provision or subject addressed, state the stakeholder's position and, where possible, explain the likely practical effect of the proposal. Alternative wording, implementation options and evidence from relevant sectors are welcome. Stakeholders should clearly identify any information they consider confidential and provide reasons for that request.

The consultation is intended to test both the substance of the proposed legal framework and the suitability of the governance arrangements required to administer it. Feedback will inform further refinement of the Bill so that it protects individual rights, supports trusted digital transformation and establishes a workable basis for responsible data use across government, industry and society.

Policy and drafting basis

This notice has been prepared with reference to the National Data Governance and Data Protection Policy 2024 and the Revised Detailed Drafting Instructions for the Data Governance and Data Protection Bill 2026.

Submissions and Enquiries

A joint Technical Working Group has been established by the Department of Information and Communications Technology (DICT) and the National Information and Communications Technology

Authority (NICTA) to assess, review, and develop the policies, strategies, legislation and regulatory instruments required to support the broader ICT sector reform programme.

The current legislative review and drafting process is being coordinated through the Technical Working Group. Government agencies, industry participants, civil society organisations, professional bodies, academic institutions, and members of the public are invited to provide written comments, submissions, and recommendations on the proposed legislative framework.

Submissions should clearly identify the relevant provision, issue or policy area being addressed and, where possible, include the reasons for the proposed position and any recommended alternative wording or implementation approach.

All submissions, enquiries and requests for clarification should be directed through the following channels:

ICT Legislative Review Submission Portal

Or Email Submissions and Enquiries

Email: ictsector_reset@nicta.gov.pg

NICTA Contact

Ms Lillian Smith

Manager, Research and Emerging Technology

Email: lsmith@nicta.gov.pg

Department of ICT Contact

Mr Thomson Simon

Manager, Policy Development

Email: thomson.simon@ict.gov.pg

Mr Pokana Nouari

Manager, Policy Planning and Implementation

Email: pokana.nouari@ict.gov.pg

Submissions should include the name of the individual or organisation making the submission, relevant contact details and an indication of whether the submission may be published or referenced as part of the consultation process.

Unless confidentiality is specifically requested and accepted, submissions may be treated as public consultation material and may be summarized, published, or referred to in the final consultation report.

Closing Date for Submissions: 19th, August, 2026

Reference: Data Governance and Data Protection Bill 2026 Consultati