DATA PROTECTION ACT 2025

Arrangement of Sections

REPUBLIC OF KIRIBATI

(No. of 2025)

I assent

Beretitenti

18/9/2025

An Act

entitled

AN ACT TO PROVIDE AND REGULATE THE PROCESSING OF PERSONAL DATA, THE RIGHTS TO INDIVIDUALS RELATING TO PERSONAL DATA, THE BENEFICIAL USE OF PERSONAL DATA IN THE DIGITAL ECONOMY OF KIRIBATI AND FOR OTHER CONNECTED PURPOSES

Commencement date:

_____2025

MADE by the Maneaba ni Maungatabu and assented to by the Beretitenti

PART I – PRELIMINARY

1. Short title

This Act may be cited as the *Data Protection Act 2025.*

2. Commencement

This Act commences on a date that the Minister may by notice appoint.

3. Interpretation

In this Act unless the context otherwise requires:

"**consent**" means any freely given, specific, informed, and unambiguous indication of an individual's agreement;

"**controller**" means a person who or which, alone or together with others, determines the purposes and means of processing of personal data;

"**controller of major importance**" means a controller that is domiciled, resident or operating in Kiribati and currently processes, has processed in the last twelve months or expects to process in the next twelve months personal data relating to more than 10,000 data subjects who are within Kiribati;

"**data subject**" means an individual to whom personal data relates;

"**Director**" means the Director responsible for the DTO appointed under the Digital Government Act 2023;

"DTO" is the division responsible for information and communication established under the Digital Government Act 2023;

"**Ministry**" means the Ministry responsible for data protection;

"**Office**" means the Digital Transformation Office established under the Digital Government Act 2023;

"**person**" means an individual, private entity, public body, agency or any other body;

"**personal data**" means any data relating to an individual who can be identified or is identifiable, directly or indirectly by reference to such data, including without limitation a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual;

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

"**processing**" means the collection, recording, organisation, storage, alteration, disclosure by transmission, combination, restriction or destruction of personal data by electronic means;

"**public body**" means the Government's office including Island Councils, Judiciary, 'te Maneaba ni Maungatabu, statutory bodies and state-owned enterprises; and

"**Secretary**" means the Secretary of the Ministry.

4. Administration of this Act

(1) This Act shall be administered under the direction and control of the Secretary.

(2) The Secretary shall have power to delegate administration of this Act to officers within the Ministry.

5. Application

(1) Subject to Section 6, this Act applies to processing of personal data:

(a) within Kiribati; or

(b) outside Kiribati if the processing relates to the offering of goods or services to, or the monitoring of behaviour of, data subjects in Kiribati.

(2) For purposes of this Act, any processing of personal data carried out by a person on behalf of a controller including any downstream processing by other persons shall be considered processing of such personal data by such controller and such controller shall have liability under this Act therefor.

(3) This Act binds the Republic.

6. Exemptions and exclusions

(1) This Act does not apply to the processing of personal data solely for personal, recreational or household purposes.

(2) This Act does not apply to a person until the second anniversary of the date on which it comes into force if that person is domiciled, resident, or operating in Kiribati and is not a controller of major importance.

(3) The Minister may by regulation prescribe classes of persons or persons processing classes of personal data that are not excluded under subsection (2).

(4) This Act does not apply to processing of personal data:

(a) by legally authorised authorities for the purposes of the prevention, investigation, detection, prosecution or adjudication of criminal offences or the execution of criminal penalties;

(b) by legally authorised authorities for the purposes of prevention or control of a public health emergency;

(c) by legally authorised authorities as necessary for national security; or

(d) by any person as necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure;

provided that such processing uses reasonable, proportionate and effective measures to safeguard the fundamental rights and the interests of the data subject.

(5) Only to the extent that the obligations and rights in this Act would be incompatible with the purposes of journalistic, educational, artistic or literary expression, such obligations and rights shall not apply to processing carried out for such purposes.

7. Objectives

The objectives of this Act are to:

(a) protect data subjects from risks arising from the processing of personal data relating to them, including risks to their rights and liberties under the Constitution and laws of Kiribati;

(b) promote personal data processing practices that protect the security of personal data and privacy of data subjects;

(c) ensure that personal data are processed in a fair, lawful and transparent manner;

(d) promote secure and trusted processing of personal data for digital government services and enhance the welfare of the people of Kiribati; and

(e) increase the beneficial use of personal data in the digital economy of Kiribati and its participation in regional and global economies.

PART II – ADMINISTRATION

8. Mandate, powers and functions of the Office under this Act

(1) Without limiting any mandates, powers or functions granted under the Digital Government Act 2023 or other laws, the Office shall promote the protection of personal data, oversee the implementation of this Act and be responsible for its enforcement throughout Kiribati.

(2) The Office shall exercise the powers set out in this Act and shall perform the following functions:

(a) promote public awareness of personal data protection, the risks relating to personal data and the rights granted and obligations imposed under this Act;

(b) encourage the introduction of technological and administrative measures to enhance personal data protection in accordance with recognised international standards and applicable international law;

(c) participate in international fora and engage with other national, regional and international authorities responsible for data protection with a view to developing consistent and efficient approaches to regulation of processing and transfers of personal data outside of Kiribati;

(d) advise the Secretary on policy issues relating to personal data protection;

(e) submit legislative proposals to the Secretary, including amending existing laws, with a view to strengthening personal data protection in Kiribati;

(f) receive complaints and investigate violations of this Act or regulations or other subsidiary legislation or notices hereunder;

(g) impose penalties in case of violations of this Act or regulations or other subsidiary legislation or notices hereunder;

(h) after consultation with Secretary, designate countries, regions, sectors, international organisations or measures as affording or not affording adequate protection for processing or transfers of personal data outside of Kiribati;

(i) advise the Secretary with respect to compliance by Kiribati with its international obligations relating to data protection;

(j) render technical assistance on data protection matters to the Secretary;

(k) submit proposals to the Secretary for regulations to be made under this Act;

(l) issue directives and opinions, make recommendations and publish guidance as required to give effect to and further specify the application of this Act; and

(m) generally, implement the provisions of this Act and do all such things as are necessary, incidental or conducive to the better carrying out of the functions of the Office under this Act.

9. Annual reporting

(1) The Director shall prepare, publish and submit to the Minister not later than twelve months after the end of each calendar year, an annual report which shall describe:

(a) the Office's activities relating to data protection in the prior calendar year;

(b) developments in Kiribati relating to personal data protection;

(c) a summary of any personal data breaches notified to the Office; and

(d) any other matter prescribed by the Minister in regulations.

(2) The annual report shall be published on the Ministry's and DTO's respective websites and shall remain available for at least 5 years.

PART III – PRINCIPLES GOVERNING PROCESSING OF PERSONAL DATA

10. Purpose specification, minimization, retention and quality

A controller shall ensure that personal data:

(a) are processed for a purpose that is explicit and not prohibited by law;

(b) are only further processed if for a purpose which is compatible with the original purpose of processing;

(c) are processed only to the extent necessary for the purposes of processing;

(d) are adequate and relevant, and kept accurate, complete, not misleading and up to date, to the extent required for the purposes of processing; and

(e) are not retained for longer than is necessary to achieve the purpose of processing, except where:

(i) such retention is required or authorised by law;

(ii) such retention is necessary for legitimate business purposes; or

(iii) the data subject has consented to such retention.

11. Lawfulness of processing of personal data

(1) A controller shall ensure that personal data are processed fairly and in a transparent manner.

(2) Subject to subsection (3), a controller shall not process personal data unless one of the following conditions has been met:

(a) the data subject has given consent to processing of the personal data for a specified purpose, subject to section 16(1)(a);

(b) the data subject has voluntarily provided the personal data for the purpose for which the personal data will be processed by or on behalf of the controller, subject to section 16(1)(b);

(c) the processing is necessary for the entering into or performance of a contract with the data subject;

(d) the processing is necessary for compliance with a legal obligation of the controller or a person processing personal data on the controller's behalf;

(e) the processing is necessary for the establishment, exercise or defence of a legal claim, obtaining legal advice or conduct of a legal proceeding by the controller or a person processing personal data on the controller's behalf;

(f) the processing is authorised by law and carried out by a legally authorised public authority;

(g) the processing is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the controller;

(h) the processing is necessary for responding to a medical emergency involving a threat to the life or immediate threat to the health of any person;

(i) the processing is necessary to respond to a specific public health or humanitarian emergency;

(j) the processing is necessary for the purposes of the legitimate interests of the controller or by a third party to whom or which the personal data are validly disclosed, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject;

(k) the processing is necessary for archiving purposes in the public interest, or for the purpose of historical, statistical or scientific research; or

(l) the data subject has intentionally made such personal data public.

(3) Upon satisfying subsection (2), a controller may further process such personal data in accordance with this Act for a purpose which is compatible with the original purpose for which such personal data was processed.

(4) Compatibility in subsection (3) shall be assessed in light of:

(a) the relationship between the original purpose and the purpose of the intended further processing;

(b) the consequences and risks of the further processing; and

(c) the application of appropriate safeguards to protect the privacy and security relating to such personal data.

12. Children or individuals lacking capacity

(1) Where a data subject is under the age of eighteen or otherwise lacks legal capacity:

(a) for purposes of satisfying Sections 10(e)(iii), 17(c), 11(2)(a) or 24(a), consent shall be obtained from a parent or legal guardian or other appropriate legal representative, respectively;

(b) for purposes of satisfying Sections 11(2)(b) or 24(b), voluntary provision of personal data shall be made by a parent or legal guardian or other appropriate legal representative, respectively; and

(c) for purposes of exercising any rights under Part IV or lodging a complaint under Section 26, such rights shall be exercised or complaints lodged on the data subject's behalf by a parent or legal guardian or other appropriate legal representative, respectively.

(2) Subsection (1)(a) shall not apply where the processing:

(a) is carried out for purposes of education, medical, or social care, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality;

(b) is necessary for proceedings before a court relating to the individual; or

(c) concerns personal data relating to a child thirteen years of age or older in relation to the provision of information and services by electronic means at the specific request of the child.

13. Provision of information to a data subject

(1) Prior to collection of personal data from a data subject, a controller shall ensure that a data subject is informed of:

(a) the identity of, and means of contacting, the controller;

(b) the purpose or purposes of the processing;

(c) the means of exercising the data subjects' rights under Part IV; and

(d) the right to lodge complaints with the Office in accordance with Section 26.

(2) Where the information provided for in subsection (1) was not provided to the data subject before collection, the controller shall ensure that it is provided as soon thereafter as possible.

(3) This section shall not apply to the extent that compliance would be impossible or would involve a disproportionate effort or expense.

14. Engagement of persons to process personal data on a controller's behalf

(1) A controller shall take reasonable measures to ensure that any person that processes personal data on the controller's behalf (including any person engaging in downstream processing of such personal data) carries out such processing in a manner that ensures compliance of such person and the controller with this Act, including without limitation:

(a) providing all notifications, information and assistance to the controller reasonably required for the controller to comply and demonstrate compliance with this Act; and

(b) complying with the requirements under Part V.

(2) Reasonable measures under this section include a written agreement between the controller and each person that processes personal data on the controller's behalf, including a contractual requirement in that agreement that such person enter into a similar written agreement with any other person it engages to perform downstream processing on such personal data.

PART IV – RIGHTS OF A DATA SUBJECT

15. Rights of confirmation, access, correction and deletion

(1) Subject to subsections (2) and (4), a data subject has the right to obtain from a controller for reasonable purposes, at no expense and without unreasonable delay:

(a) confirmation as to whether or not the controller is processing, or a person is processing on behalf of the controller, personal data relating to the data subject and, if so, the source of such personal data;

(b) a copy of such personal data in a commonly used electronic format;

(c) correction, or if correction is not feasible or suitable, deletion of any such personal data that are inaccurate, out of date, incomplete or misleading; and

(d) deletion of any such personal data which the controller is not entitled to retain.

(2) If a data subject's request under subsection (1) is manifestly unfounded or excessive, in particular because of its repetitive character, a controller may charge a data subject a reasonable fee in relation to a request or refuse the request.

(3) Prior to making any correction under subsection (1)(c), a controller may require sufficient evidence of the accuracy of such correction.

(4) A controller may impose a fee for receipt of a copy of personal data under subsection (1)(b) to the extent such fee is otherwise prescribed under applicable law.

(5) Any fee under subsection (2) shall be set taking into account the administrative costs of providing the information or communication or taking the action requested.

(6) The right to receive a copy of personal data under subsection (1)(b) may be limited by applicable law that sets limitations on the frequency of a data subject's right to receive copies of data from a service provider.

16. Right to withdraw consent or express a lack of consent to processing

(1) A data subject has the right to:

(a) withdraw consent to processing previously given to a controller under Sections 10(e)(iii), 17(c), 11(2)(a) or 24(a) or

(b) object to processing where no lawful basis of processing applies under Sections 11(2)(b) or 24(b).

(2) A controller shall ensure that it is as easy for the data subject to exercise the rights under subsection (1) as to give consent or voluntarily provide the personal data, and that he or she is informed of the consequences of doing so upon expressing a desire to exercise the right.

(3) When a data subject exercises the rights under subsection (1), the controller shall promptly cease any processing to the extent that it relies solely on the applicable sections of this Act.

17. Right not to be subject to a decision based solely on automated processing

A data subject has the right not to be subject to a decision based solely on automated processing of personal data which produces legal or similar significant effects concerning such data subject, except where such decisions are:

(a) necessary for entering into, or performance of, a contract between the data subject and a controller;

(b) authorised by a written law which establishes suitable measures to safeguard the fundamental rights and the interests of the data subject; or

(c) authorised by the consent of the data subject.

PART V – DATA SECURITY AND PERSONAL DATA IMPACT ASSESSMENTS

18. Security, integrity and confidentiality of personal data

(1) A person processing personal data shall implement, and ensure any other person processing data on its behalf (including any person engaging in downstream processing of such personal data) implements, appropriate technical and organisational measures to ensure the security, integrity and confidentiality of the personal data including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access.

(2) In implementing measures under subsection (1), a person shall take into account:

(a) the amount of the personal data;

(b) the nature, degree and likelihood of harm to data subjects that could result from the loss, disclosure or other misuse of the personal data;

(c) the extent of the processing;

(d) the period of data retention; and

(e) the availability and cost of any technologies, tools or other measures to be implemented.

(3) Measures implemented under subsection (1) may include:

(a) de-identification of personal data;

(b) encryption of personal data;

(c) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services;

(d) processes to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) periodic assessments of risks to processing systems, services and transmission over electronic communications networks;

(f) regular testing, assessing and evaluation of the effectiveness of the measures implemented against current and evolving risks identified; and

(g) regular updating of the measures and introduction of new measures to address shortcomings in effectiveness and accommodate evolving risks.

19. Personal data breaches

(1) Each person processing personal data on behalf of another person shall inform the controller or such other person who or which has engaged it as soon as practicable after having become aware of it:

(a) when a personal data breach has occurred, regardless of whether it requires notification under Section 20; or

(b) when it receives a notification under this subsection from any person it has engaged to process personal data on its behalf.

(2) The information provided under subsection (1) shall include the information required to be included in a notification under Section 20(5), to the extent known and applicable.

(3) Each person shall keep a record of any personal data breach with respect to personal data processed by it, regardless of whether it requires notification under Section 20, including the facts relating to the personal data breach, its effects and the remedial action taken in a manner that enables the Office to verify compliance with this Part.

(4) For each personal data breach with respect to personal data processed by it, a controller shall determine whether such breach meets the requirements of Section 20(1), keep a written record of its analysis of the factors set out in Section 20(1) and make such record available to the Office upon request.

20. Harmful personal data breaches

(1) This section applies to any personal data breach that has resulted in, or is likely to result in, significant harm to affected data subjects, taking into account:

(a) whether the personal data are protected by encryption, methods of de-identification, or other security measures that may reduce the risk of harm to affected data subjects;

(b) the nature of the harm that has resulted or is likely to result to affected individuals;

(c) any action taken or expected to be taken to reduce the harm or risk of harm following the breach;

(d) in the case of unauthorised access to or disclosure of personal data, how the data might be used by any person having such access or to which disclosure may be made;

(e) in the case of loss, destruction or alteration of personal data, whether the personal data has been recovered and the impact on the processing; and

(f) any other factors relevant to assessing the harm or risk of harm, or mitigation thereof, to affected data subjects.

(2) When a personal data breach has occurred, the relevant controller shall, as soon as practicable after having become aware of the breach, notify:

(a) the Office; and

(b) each affected data subject.

(3) If a direct notification to each affected data subject under subsection (2) would involve disproportionate effort or expense or is otherwise not feasible, the controller may instead notify data subjects by public notification through one or more widely used media sources.

(4) The Office may at any time make a public notification about a personal data breach if it considers the public notification made by a controller to data subjects under subsection (2) inadequate.

(5) The notifications under subsections (2) or (3) shall:

(a) set out the nature of the personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned;

(b) communicate the name and contact details of a point of contact of the controller where more information can be obtained;

(c) describe the likely consequences to affected data subjects of the personal data breach;

(d) describe the measures taken or expected to be taken by the controller, or any other person processing the personal data on the controller's behalf, to address the personal data breach, including any measures to mitigate its possible adverse effects; and

(e) in the case of a notification made directly to affected data subjects or a public notification, provide advice about measures the affected data subjects could take to mitigate effectively the possible adverse effects of the personal data breach.

(6) To the extent that it is not possible to provide information under subsection (5) at the same time, the information may be provided in phases without undue further delay.

21. Data protection impact assessments

(1) Where processing by a controller of major importance is likely to expose 10,000 or more data subjects to a high risk of significant harm by virtue of the nature, scope, context and purposes of such processing, such controller shall, prior to the processing:

(a) carry out a data protection impact assessment; and

(b) submit a data protection impact assessment report to the Office.

(2) For purposes of this section, a "data protection impact assessment" is an assessment of the impact of the envisaged processing on the protection of personal data comprising:

(a) a systematic description of the envisaged processing, its purpose, and the lawful basis of processing under Section 11;

(b) an assessment of the necessity of the processing in relation to the purposes for which the personal data would be processed;

(c) an assessment of the risks of harm to data subjects; and

(d) an evaluation of the likely effectiveness of the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act.

(3) If notwithstanding the measures envisaged under subsection (2)(d), the data protection impact assessment indicates that the processing has a high risk of significant harm to data subjects, the controller of major importance shall proceed with such processing only upon approval of, and subject to any conditions imposed by, the Office .

(4) This section shall not apply until the second anniversary of the date on which this Act enters into force.

22. Guidance on compliance

The Office may issue guidance on the steps to be taken by persons to comply with the personal data breach and data protection impact assessment obligations in this Part.

PART VI – PROCESSING AND TRANSFERS OUTSIDE KIRIBATI

23. Adequate protection of personal data processed or transferred outside Kiribati

(1) Except as permitted in Section 24, a person that processes personal data outside Kiribati or transfers personal data to a person outside Kiribati shall take reasonable steps to verify or ensure, as applicable, that there is adequate protection with respect to the personal data.

(2) For purposes of this section, there is "adequate protection" with respect to personal data processed or transferred outside Kiribati if:

(a) the person processing or receiving the personal data is subject to restrictions and obligations substantially similar to those set forth in Parts III and V;

(b) the data subject has rights substantially similar to those found in Part IV; and

(c) such restrictions, obligations and rights are substantially enforceable.

(3) Adequate protection may be afforded by any one or combination of the following:

(a) the laws of the jurisdiction in which the processing occurs or to which the personal data are transferred or may be subsequently transferred;

(b) binding corporate rules, contractual clauses, a code of conduct, certification mechanism or other measures; or

(c) if the person processing or receiving the personal data outside Kiribati is an international organisation, the policies and administrative and technical measures of such organisation.

(4) The Office may:

(a) issue guidelines with respect to the assessment of whether there is adequate protection; or

(b) designate any international organisation, country, region or specified sector within a country, law, binding corporate rules, contractual clauses, code of conduct, certification mechanism or other measures as affording or not affording adequate protection under this Part.

(5) The absence of any guideline or designation by the Office under subsection (4) with respect to any country, region or specified sector within a country, international organization or measure shall not imply that it does or does not afford adequate protection under this Part.

(6) The Office may prohibit processing or transfer of personal data or specified categories of personal data outside Kiribati to a specified jurisdiction, a specified organisation or under specified measures:

(a) on the basis that the personal data will not be afforded adequate protection; or

(b) for reasons of national security.

(7) The reasonableness of steps under subsection (1) shall be assessed taking into account the factors referred to in Section 18(2).

(8) Notwithstanding Section 5(2), for purposes of this section, a "transfer" of personal data by a person includes any transfer to a second person processing such personal data on the first person's behalf.

24. Other bases for processing and transfer of personal data outside Kiribati

A person may process personal data outside Kiribati or transfer personal data to a person outside Kiribati if:

(a) the data subject has given and not withdrawn consent to such processing or transfer after having been informed of the possible risks of such processing or transfer to the data subject due to the possible absence of an adequate level of protection;

(b) the data subject has voluntarily provided personal data to the controller, or a person processing personal data on such controller's behalf, for the specified purpose of such processing or transfer, and the data subject has not indicated that he or she does not consent to such processing;

(c) the processing is necessary for the entering into or performance of a contract with the data subject;

(d) the processing is necessary for responding to a medical emergency involving a threat to the life or immediate threat to the health of any person;

(e) the transfer is for the benefit of the data subject and:

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would likely give it; or

(f) the processing involves transfer of personal data pursuant to an order or decision of a court, tribunal or administrative authority of a third country based on an international agreement, such as a mutual legal assistance treaty, in force between the third country and Kiribati.

25. Documentation and recordkeeping

A person processing or transferring personal data outside Kiribati shall keep a written record of the reasonable steps taken under Section 23(1) or the bases relied on under Section 24, and shall make such record available to the Office upon request.

PART VII – ENFORCEMENT

26. Complaints

(1) A data subject who is aggrieved by any act or omission of a person resulting in a violation of this Act or any regulations or other subsidiary legislation may lodge a complaint with the Office.

(2) The Office shall admit any complaint referred to it where it appears to the Office that:

(a) the complainant has an interest in the matter to which the complaint relates; and

(b) the complaint is not frivolous or vexatious.

27. Investigations

(1) The Office may initiate an investigation pursuant to a complaint it has admitted or of its own accord where it has reason to believe a person has violated or is likely to violate this Act or any regulations or other subsidiary legislation or notices hereunder.

(2) The Office may, for the purpose of an investigation, issue a notice to any person to:

(a) attend at a specific time and place for the purpose of being examined orally in relation to a complaint;

(b) produce such document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other written law from disclosing; or

(c) furnish a statement in writing made under oath or an affirmation setting out all information which may be required under the notice.

(3) Upon approval from the Secretary, the Director may appoint one or more officers with the powers to do all or any of the following in carrying out an investigation by the Office under this section:

(a) interview a person where the officer believes, on reasonable grounds, that he has knowledge or information regarding non-compliance with this Act or any regulations or other subsidiary legislation or notices hereunder;

(b) require a person to provide information pertaining to non-compliance with this Act or any regulations or other subsidiary legislation or notices hereunder; or

(c) upon obtaining a warrant from the appropriate court after demonstrating reasonable grounds to suspect a violation of this Act or any regulations or other subsidiary legislation or notices hereunder and the necessity of a search or seizure to ascertain whether such a violation has occurred or is occurring, and in the company of a law enforcement officer:

(i) enter and search relevant premises or computer systems; or

(ii) seize any items related to a suspected violation.

(4) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Office may require the person named to produce or give access to it in a form in which it is visible and legible in a structured, commonly used and machine-readable format.

28. Notices of the Office

(1) If the Office, after completing an investigation under Section 27, is satisfied that a person has violated any provision of this Act, or any regulation or other subsidiary legislation hereunder, it may issue a notice requiring the person to within a specified period of time:

(a) stop or refrain from doing an act which is in violation of this Act, including stopping or refraining from processing that is the subject of the notice;

(b) take reasonable action to compel a second person processing personal data on the first person's behalf to stop or refrain from processing as required to ensure the first person's compliance;

(c) remedy the violation, including providing compensation to an affected data subject; or

(d) pay an administrative penalty not exceeding $100,000.

(2) Any administrative penalty under subsection (1)(d) shall be proportionate to and shall take into account:

(a) the gravity of the violation and its repetitive nature;

(b) the controller's efforts to comply and provide information to the Office and data subjects;

(c) the extent of any profits made by the person as a result of the violation; and

(d) the nature and degree of resulting harm or risk of harm to the affected data subjects.

29. Offences

(1) A person who fails to comply with any notice issued under Sections 27 or 28 that is not the subject of a duly made and ongoing appeal under Section 30 commits an offence for which such person is liable to a fine not exceeding $100,000 and to a term of imprisonment not exceeding 10 years or both.

(2) Liability for a fine under subsection (1) does not release or reduce any liability arising from a notice made under Section 28.

30. Appeal of a notice of the Office

An affected data subject, a person who is the subject of a notice under Section 28 or another interested person who is not satisfied with a notice under Section 28 may apply to the appropriate court within thirty days after the date the notice was made for judicial review thereof.

31. Civil remedies

(1) A data subject who suffers injury, loss or harm as a result of a violation of this Act by a person processing personal data, or a consumer organisation acting on behalf of such a data subject or multiple data subjects, may recover damages by way of civil proceedings in the appropriate court from such person.

(2) The remedies under subsection (1) shall not be duplicative of any remedies requiring compensation to a data subject under a notice under Section 28.

PART VIII – MISCELLANEOUS

32. Regulations

The Minister has the power to make regulations for the implementation of this Act, including and without limitation setting out methods for service of notices issued by the Office.

33. No limitation of obligations and rights

Nothing in this Act shall be interpreted to limit any obligations on any person processing personal data or the rights of any data subject granted otherwise under the laws of Kiribati.

CONSEQUENTIAL AMENDMENTS

34. The following legislative provisions are hereby amended;

(1) Digital Government Act 2023

(a) Section 4 of the Digital Government Act 2023 is amended by inserting after the definition of "open data" the definition of "personal data" as follows:

> "personal data" means any data relating to an individual who can be identified or is identifiable, directly or indirectly by reference to such data, including without limitation a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual;

(b) Section 29(2)(b) of the Digital Government Act 2023 is amended by repealing and replacing the subsection as follows:

> "in the case of personal data, in addition to permission under paragraph (a), the access is not in violation of the Data Protection Act 2025."

(c) Section 34(1)(h) of the Digital Government Act 2023 is amended by repealing and replacing the subsection as follows:

> "compliance with obligations on the disclosure and other processing of personal data under the Data Protection Act 2025 and other applicable standards of security and privacy for individuals, national security and commercial confidentiality"

(d) Section 47(2) of the Digital Government Act 2023 is amended by inserting the words "and the Data Protection Act 2025" after the word "Act".

(e) Section 47(3)(b) of the Digital Government Act 2023 is amended by repealing and replacing the subsection as follows:

> "in the case of personal data, in addition to permission under paragraph (a), the access is not in violation of the Data Protection Act 2025."

(f) Section 47(3)(c) of the Digital Government Act 2023 is amended by repealing the subsection.

(g) Section 47(6) of the Digital Government Act 2023 is amended by repealing and replacing the subsection as follows:

"Nothing in this section prevents or limits an individual from exercising any rights granted under the Data Protection Act 2025."

(2) Business Names Act 2021

Section 7(2) of the Business Names Act 2021 is amended by adding the following to the end of the subsection:

"to the extent in compliance with the Data Protection Act 2025."

(3) Companies Act 2021

Section 160(b) of the Companies Act 2021 is amended by repealing and replacing the subsection as follows:

"the disclosure of the information would or would be likely to prejudice the commercial position of any other person, whether or not that person supplied the information to the company, or constitute a violation of the Data Protection Act 2025;"

EXPLANATORY MEMORANDUM

BACKGROUND

With the increasing digitalization of services and the growing importance of data in the modern economy, there is a pressing need to ensure adequate protection of personal data while fostering innovation and economic growth. The Data Protection Act 2025 (Act) sets out a comprehensive framework to govern the processing of personal data in Kiribati that is consistent with international standards. It ensures that personal data processing is subject to appropriate safeguards, grants rights to individuals concerning their personal data, and promotes the beneficial use of personal data in the digital economy.

PART I – PRELIMINARY

Part I specifies the name of the Act as the Data Protection Act 2025, indicates that it commences on a date to be appointed by the Secretary and sets out a list of defined terms that include critical data protection concepts. It also names the Secretary as responsible for the administration of the Act, permitting delegation of this function to officers in the Ministry.

This part defines the scope of application of the Act to include processing of personal data within Kiribati and in limited circumstances outside Kiribati and specifies that the Act binds the Republic. It also sets out exemptions and exclusions from the application of the Act, including the processing of personal data for personal, recreational or household purposes or the exercise or defence of legal claims, certain actions taken by legally authorised authorities relating to national security, law enforcement, and public health emergencies, and processing for journalistic, educational, artistic or literary expression.

This part also sets out the objectives of the Act, which include the protection of individuals from risks arising for the processing of personal data, promotion of practices to protect personal data and ensure it is processed fairly, lawfully and in a transparent manner, and advancement of digital government services and the use of personal data in the digital economy.

PART II – ADMINISTRATION

Part II designates the Digital Transformation Office (the Office) as responsible for the enforcement of the Act. It sets out the functions of the Office under the Act, including promoting awareness of personal data protection, receiving complaints of and investigating potential violations of the Act, imposing penalties in case of such violations, designating counties as affording adequate personal data protection, submitting proposals to the Secretary for regulations to be made under the Act, and generally implementing the provisions of the Act. This part also requires the Director to prepare and submit annual reports describing the Office's activities and developments in relation to data protection in the prior year.

PART III – PRINCIPLES GOVERNING PROCESSING OF PERSONAL DATA

Part III sets out the principles governing the processing of personal data applicable to controllers under the Act. It requires that any processing of personal data be for an explicit purpose, not exceed that purpose, be limited to the extent necessary to achieve such purpose, be adequate, relevant and

kept accurate to the extent required by such purpose, and not be retained for longer than necessary to achieve such purpose, subject to certain exceptions.

This part requires controllers to process personal data fairly and in a transparent manner. Processing is not permitted unless one of twelve conditions is met, including individual consent to such processing, compliance with a controller's legal obligations, authorisation by law, various emergency situations and the public nature of the personal data. Further processing is also permitted when it is compatible with the original purpose for which the personal data was processed. This part also clarifies the ability of a legal guardian or other appropriate legal representative to give consent to processing on behalf of children or other individuals lacking capacity, respectively.

This part sets out mandatory disclosures that must be made to individuals when a controller collects personal data, subject to certain exceptions. It also requires controllers to take reasonable measures to ensure that any person that processes personal data the controller's behalf does so in a manner that ensures compliance with the Act. Such reasonable measures include a written agreement between the controller and such person which satisfies certain requirements.

PART IV – RIGHTS OF A DATA SUBJECT

Part IV grants rights to individuals relating to the processing of their personal data. These rights comprise the rights to know whether or not a controller is processing the individual's personal data, receive a copy of any such personal data, correct any such personal data that are inaccurate, out of date, incomplete or misleading, and have the controller delete any such personal data it is not entitled to retain. It also grants individuals the right to withdraw any consent given under the Act relating to processing of personal data and the right not to be subject to a decision based solely on automated processing.

PART V – DATA SECURITY AND PERSONAL DATA IMPACT ASSESSMENTS

Part V sets out obligations on any person processing personal data to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal such personal data, including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access. The appropriateness of such measures can be determined with respect to factors such as the amount of the personal data and the risks of harm to individuals. Such measures may include de-identification and encryption of the personal data.

This part also addresses actions to be taken upon the occurrence of personal data breaches. Any person processing personal data on behalf of a controller must report all such breaches to the person who engaged it and keep records of the facts of such breach. In addition, controllers are required to notify the Office and each affected individual when a personal data breach results in, or is likely to result in, significant harm to affected individuals. This part sets out factors to take into consideration in determining whether this threshold is met, including whether the personal data are protected by encryption, pseudonymisation or other methods of de-identification, or other security measures that may reduce the risk of harm, and mitigating action taken or expected to be taken. If a direct notification to each affected individual would involve disproportionate effort or expense or is otherwise not feasible, the controller may instead make a public notification through one or more widely used media sources.

When certain controllers plan to engage in processing that is likely to expose 10,000 or more data subjects to a high risk of significant harm by virtue of the nature, scope, context and purposes of such processing, such controllers must carry out a data protection impact assessment and submit it to the Office prior to the processing. This assessment must describe the processing, assess its necessity and the risk of harm to individuals and evaluate the effectiveness measures envisaged to address such harm. If such harms cannot be effectively mitigated, then such processing may only proceed with the approval of the Office. These requirements do not apply until the [first/second] anniversary of the date on which the Act enters into force.

PART VI – PROCESSING AND TRANSFERS OUTSIDE KIRIBATI

Part VI governs processing and transfers of personal data outside Kiribati. In general, a person may engage in such extraterritorial processing or transfers only if the person can verify that adequate protections are in place. Adequate protection means that key protections under the Act would continue to apply outside Kiribati. Such protection could be achieved if the extraterritorial jurisdiction has sufficient laws in place or the processing is protected through binding corporate rules, contractual clauses, a code of conduct, certification mechanism or other measures. The Office may designate certain jurisdictions or measures as providing or not providing adequate protection and may prohibit any extraterritorial processing or transfers of certain categories of personal data on the basis of national security.

This part also provides a list of alternative bases for extraterritorial processing and transfers of personal data. These include consent of the individual, actions taken in response to certain medical emergencies and compliance with obligations under international agreements with third countries, such as those governing mutual legal assistance.

Under this part, any person processing or transferring personal outside Kiribati must keep a written record of its compliance with this part and make such record available to the Office upon request.

PART VII – ENFORCEMENT

Part VII governs enforcement of the Act. It permits any individual who is aggrieved by any act or omission of a person resulting in a violation of the Act to lodge a complaint with the Office.

The Office may initiate an investigation on the basis of a complaint or of its own accord where it has reason to believe a person has violated or is likely to violate the Act. This part grants the Office certain powers necessary to conduct investigations, including the appointment of officers, upon approval of the Secretary, to conduct interviews, require provision of information and conduct searches and seizures pursuant to a court-issued warrant.

Upon completing an investigation and finding that a person has violated the Act, the Office may issue a notice to such person to take or refrain from action, remedy the violation or pay an administrative penalty. Affected individuals and persons who are the subject of a notice of the Office may apply to the appropriate court within thirty days after the notice was issued for judicial review. Failure to comply with a notice issued by the Office is considered a criminal offence for which such person is liable to a fine.

In addition, this part grants individuals who suffer injury, loss or harm as a result of a violation of the Act by a person processing personal data the ability to recover damages by way of civil proceedings in the appropriate court from such person.

PART VIII – MISCELLANEOUS

Part VIII grants the Minister the power to make regulations for the implementation of the Act. It also specifies that the Act should not be interpreted to limit obligations imposed on any person processing personal data or the rights of any data subject granted otherwise under other laws.

CONSEQUENTIAL AMENDMENTS

The Act sets out amendments to the Digital Government Act 2023, Business Names Act 2021, and the Companies Act 2021 to harmonise them with the terminology and requirements under the Act.

HON ALEXANDER TEABO
MINISTER FOR INFORMATION, COMMUNICATION AND TRANSPORT

LEGAL REPORT

I hereby certify my opinion that none of the provisions of the above Act conflict with the Constitution and that the Beretitenti may properly assent to the Act.

MS PAULINE BEIATAU
ATTORNEY GENERAL

CERTIFICATE OF THE CLERK OF THE MANEABA NI MAUNGATABU

This printed impression of the Data Protection Act 2025 has been carefully examined by me with the Bill which passed the Maneaba ni Maungatabu on the 18th August 2025 and is found by me to be a true and correctly printed copy of the said Bill.

.....

Eni Tekanene
Clerk of the Maneaba ni Maungatabu

Published by exhibition at the Maneaba ni Maungatabu this 18th day of September 2025.

.....

Eni Tekanene
Clerk of the Maneaba ni Maungatabu