TITLE 6 - PUBLIC PROCEEDINGS AND RECORDS
CHAPTER 4 - PERSONAL DATA PROTECTION ACT 2025

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

PERSONAL DATA PROTECTION ACT 2025

Index

Section **Page**

§401. Short title. 3
§402. Purpose. 3
§103. Application. 4
§404. Exclusions. 4
§405. Interpretation. 4
PART II –COMPETENT AUTHORITY FOR PERSONAL DATA PROTECTION 6
§406. Administration 6
§407. Duties and powers. 6
§408. Duty to maintain confidentiality. 7
PART III –PERSONAL DATA PROTECTION PRINCIPLES 7
§409. Personal data protection principles. 7
PART IV –COMPLAINTS, REMEDIES, AND COMPLIANCE 8
§410. Private right of action. 8
§411. Remedies 9
§412. Reports. 9
§413. Compliance 9
§414. Complaints process. 10
PART V – MISCELLANEOUS 11
§415. Data sharing among ministries and agencies. 11
§416. Guidance and internal policies. 11
§417. Regulations. 11
§418. Effective date. 12

TITLE 6 - PUBLIC PROCEEDINGS AND RECORDS
CHAPTER 4 - PERSONAL DATA PROTECTION ACT 2025

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

PERSONAL DATA PROTECTION ACT 2025

AN ACT to promote the protection of personal data of natural persons in the Republic of the Marshall Islands by core Government ministries and agencies.

Commencement : *October 7, 2025*
Source : *P.L. 2025-43*

§401. Short title.

This Chapter may be cited as the Personal Data Protection Act 2025.

§402. Purpose.

The purpose of this Chapter is to:

(a) establish an enabling legal framework to protect the personal data and privacy of natural persons in the Republic in a manner that is consistent with the right to privacy enshrined in the Constitution and the needs of the people of the Republic;

(b) provide guidance to natural persons, public bodies, and private bodies on the collection, use, storage, processing, disclosure, transfer, and deletion of personal data among core Government ministries and agencies;

(c) facilitate transparency and legal certainty regarding the safeguarding and sharing of personal data;

(d) identify the competent authority to administer this Chapter; and

(e) promote public confidence and trust in the collection, use, storage, processing, disclosure, and transfer of personal data of natural persons in the Republic.

§103. Application.

This Chapter applies to core Government ministries and agencies that may collect, use, store, process, disclose, or transfer personal data of natural persons in the Republic.

§404. Exclusions.

This Chapter does not apply:

(a) where the collection, use, storage, processing, disclosure, or transfer of personal data is for:

(i) purposes of law enforcement; or

(ii) national intelligence or national security purposes;

(b) to non-personal data; or

(c) to publicly available information that is:

(i) lawfully made available from Government records;

(ii) lawfully made available by a natural person about whom the personal data relate and that person has not restricted the information to a specific audience; or

(iii) lawfully obtained, truthful, and is a matter of public concern.

§405. Interpretation.

In this Chapter, unless context otherwise requires:

(a) 'collection' means buying, renting, gathering, obtaining, receiving, or accessing any personal data pertaining to a natural person by any means. This includes receiving information from the natural person, whether directly or indirectly, or by observing the natural person's behavior;

(b) 'competent authority' means the authority designated to administer this Chapter in accordance with section 106;

(c) 'core Government ministries and agencies' mean national executive branch ministries, departments, divisions, bureaus, offices, and any

other agency of the Republic, created by the Constitution, statute, treaty, regulation, or executive order, but does not include:

(i) national State-Owned Enterprises Act, 2015; and

(ii) such other agencies as may be determined by the President from time to time;

(d) 'data controller' means the core Government ministry or agency, or any third party acting on behalf of the core Government ministry or agency, which alone or jointly with others, determines the purposes and means of the processing of personal data;

(e) 'data processor' means the core Government ministry or agency, or third party acting on behalf of the core Government ministry or agency, which processes personal data on behalf of the data controller;

(f) 'data subject' means an identified or identifiable natural person about whom personal data directly or indirectly relates;

(g) 'disclosure' means sharing, releasing, or otherwise making personal data available or accessible to a third party, which may be a natural or legal person, public body, or other organization other than the data subject, data controller, or data processor;

(h) 'Government' means the national Government of the Republic of the Marshall Islands;

(i) 'non-personal data' means any information that is not personal data;

(j) 'personal data' means any information relating to an identified or identifiable natural person that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, whether directly or indirectly, with a particular natural person, including by reference to an identifier, such as name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

(k) 'processing' means any action performed on personal data, whether or not by automated means, and includes any operation or set of operations performed on personal data or a set of personal data, such as collection; recording; organization; structuring; storage; adaptation; alteration; retrieval; consultation; use; alignment; combination; transfer, transmission, dissemination, disclosure, sharing, or otherwise making available; restriction; erasure; or destruction; and

(l) 'Republic' means the Republic of the Marshall Islands;

(m) 'safe harbor' means protection from legal liability or other penalty when the conditions specified in section 415 are met; and

(n) 'sensitive personal data' means a special category of personal data that relates to fundamental rights and freedoms of natural persons, such as information that reveals racial or ethnic origin, political views, religious or philosophical beliefs, genetic or biometric data, health-related data, financial data, or data concerning a person's sexual orientation.

PART II –COMPETENT AUTHORITY FOR PERSONAL DATA PROTECTION

§406. Administration.

(1) The Economic Policy, Planning and Statistics Office (EPSSO) shall be the competent authority responsible for administering this Chapter.

§407. Duties and powers.

The competent authority shall have the following duties and powers under this Chapter:

(a) develop and implement education, guidance and capacity-building initiatives for core Government ministries and agencies regarding application, interpretation, and compliance with this Chapter;

(b) develop and implement education, guidance, and awareness-raising initiatives for natural persons and other entities and organizations regarding the objectives, protections, functions, and implementation of this Chapter;

(c) coordinate and consult with core Government ministries and agencies to facilitate data sharing among government ministries and agencies and ensure that personal data are adequately protected;

(d) engage and enter into agreements for capacity building and coordination to support effective implementation of this Chapter;

(e) require information from core Government ministries and agencies as needed to comply with this Chapter, including section 412;

(f) make any rules or regulations required to implement this Chapter, including but not limited to, minimum standards and requirements regarding sharing of personal data among core Government ministries and agencies; and

(g) undertake any other actions as required or that in the opinion of the competent authority are necessary to effectively implement this Chapter.

§408. Duty to maintain confidentiality.

Any director, employee, consultant, or other legal or natural person engaged by the competent authority under this Chapter must maintain confidentiality of personal data obtained in the performance of their duties.

PART III –PERSONAL DATA PROTECTION PRINCIPLES

§409. Personal data protection principles.

The following personal data protection principles apply to core Government ministries and agencies:

(a) legitimate purpose principle, which requires personal data to:

(i) be collected for specified and legitimate purposes;

(ii) be processed lawfully, fairly, and transparently in relation to the data subject; and

(iii) not be further processed in a manner that is incompatible with the specified purposes;

(b) data minimization principle, which requires personal data to be collected:

(i) by lawful and fair means; and

(ii) in a manner that is relevant and limited to what is necessary to fulfill the purpose for which the personal data is processed;

(c) accuracy principle, which requires:

(i) personal data to be accurate and kept up to date, as necessary; and

(ii) for reasonable steps to be taken to ensure that inaccurate personal data are corrected or deleted without delay;

(d) retention principle, which requires personal data to be retained or stored in a manner that permits identification of data subjects only as long as necessary to fulfill the purposes for which the personal data were collected and processes;

(e) integrity and security principle, which requires personal data to be stored or processed in a manner that adequately secures the information using appropriate technical or organizational measures, including:

(i) protection against unauthorized or unlawful processing and against unintentional loss, destruction, or damage of the personal data; and

(ii) measures to limit access to personal data by any director, staff, consultant, or other legal or natural person except as necessary to fulfill their professional duties and responsibilities; and

(f) accountability principle, which requires the data controller to be responsible for, and demonstrate compliance with, the personal data protection principles specified in this part.

PART IV –COMPLAINTS, REMEDIES, AND COMPLIANCE

§410. Private right of action.

(1) A natural person residing in the Republic who suffers an injury arising from alleged improper administration of this Chapter by a core Government ministry or agency may bring suit in accordance with section 411 against such core Government ministry or agency alleged to have caused the injury.

(2) Nothing in this Chapter shall be interpreted to preclude or in any way limit a natural person from bringing suit under law, including for compensatory damages, against an employee of the public service in their personal capacity for willful or grossly negligent conduct that results in a breach of this Chapter and an injury arising from alleged improper administration of this Chapter., provided that such compensatory relief shall be imposed against a core ministry or agency pursuant to section 411(2).

§411. Remedies.

(1) Pursuant to section 410(1), the remedies that a court may impose on a core Government ministry or agency that has been found in contravention of this Chapter include:

(a) injunction;

(b) mandamus;

(c) other order requiring the relevant core Government ministry or agency to:

(i) correct or delete inaccurate information;

(ii) amend the relevant core Government ministry or agency policies on the overall management of personal data, including the collection, use, storage, processing, disclosure, and transfer of personal data; and/or

(d) issue a public statement regarding the contravention and the actions taken or to be taken to remedy the contravention.

(2) A court may not impose compensatory relief for damages suffered by a natural person for contravention under this Chapter by a core Government ministry or agency.

§412. Reports.

(1) The competent authority shall, on a yearly basis, or when so directed by the Minister, make a report to the Minister for presentation to the Nitijela, regarding the implementation of this Chapter.

(2) To fulfill this requirement, the competent authority is empowered to undertake surveys, studies, and other actions to obtain information relating to the implementation of this Chapter.

§413. Compliance.

(1) Core Government ministries and agencies shall compile and record the following information and actions for each calendar year:

(a) policies, decisions, and actions taken to implement this Chapter during the reporting period; and

(b) complaints received in relation to the application of this Chapter during the reporting period, including the:

(i) number of complaints received;

(ii) personal data protection principle(s) alleged to have been contravened in the complaints;

(iii) manner in which the complaints were resolved or handled, including any decisions and actions taken; and

(iv) any other information that the competent authority may request or the core Government ministries and agencies deem relevant and related to actions taken to the implement this Chapter.

(2) Core Government ministries and agencies must inform the competent authority on a yearly basis, by July 1 of each year, regarding all information and actions specified in subsection (1).

(3) The information and actions that core Government ministries and agencies provide to the competent authority in accordance with subsection (2) must be anonymized and used by the competent authority for statistical purposes and Nitijela reporting only.

§414. Complaints process.

(1) Core Government ministries and agencies must establish a process for natural persons residing in the Republic to submit complaints to the relevant core Government ministry or agency regarding alleged violations of the personal data protection principles set forth in this Chapter.

(2) The processes established in accordance with subsection (1) must be consistent with any guidance or policies adopted by the competent authority under this Act.

(3) Should a core Government ministry or agency fail to adopt such dispute resolution process, a natural person residing in the Republic who suffers an alleged injury arising from alleged improper administration of this Chapter may file a complaint with such relevant Government ministry or agency using any dispute process adopted by the competent authority.

(4) Core Government ministries and agencies must retain records on submitted complaints and any determination adopted or action taken on matters that do not arise to complaints, to be used for submission of annual reports to the competent authority, pursuant to section 413.

PART V – MISCELLANEOUS

§415. Data sharing among ministries and agencies.

(1) Core Government ministries or agencies may voluntarily share personal data between or among each other based on safe harbor protections, provided that such sharing:

(a) serves a legitimate function of each such core Government ministry or agency that discloses or receives such personal data; and

(b) comports with the personal data protection principles set out in section 409 of this Chapter.

(2) The competent authority may make rules or regulations establishing the standards or provisions of agreements between or among core Government ministries or agencies to facilitate information sharing of personal data, provided that such standards or provisions comport with the personal data protection principles under section 409 of this Chapter.

(3) Any absence of regulation pursuant to subsection (2) above, shall not limit the ability for core Government ministries or agencies to rely on the safe harbor established in subsection (1).

§416. Guidance and internal policies.

(1) The competent authority is directed to issue guidance and adopt policies to implement, interpret, and clarify the provisions of this Chapter, including in relation to the complaints process.

(2) Core Government ministries and agencies my adopt internal data protection policies consistent with this Act, the personal data protection principles, and any guidance, policies, rules, or regulations adopted by the competent authority in accordance with this Chapter.

§417. Regulations.

The competent authority may, with Cabinet approval., make regulations for the effective performance of its function pursuant to the Marshall Islands Administrative Procedure Act 1979.

§418. Effective date.

This Chapter will take effect twelve (12) months after the date of certification in accordance with Article IV, section 21 of the Constitution.