Privacy and Personal Data Protection Bill

Chapter One
Introduction

Introduction and title

1. (a) This Act specifies the collection and regulation of private and personal data, the rights of those whose personal information is collected, and responsibilities of those who collect, manage and control such information, the rules upon which dissemination or utilisation of such data shall be regulated, and detail other relevant guidelines related to the protection of privacy and personal data.

(b) This Act shall be titled “Privacy and Personal Data Protection Act”.

Purpose

2. The purpose of this Act is to achieve the following objectives.

(a) Institutions shall protect individuals' rights in collecting, using, and disseminating private and personal information. The reasonable person standard must be utilised to determine the circumstances in which such information is collected, used, or disseminated.

Scope of the Act

3. (a) This Act shall apply to:

1. Processors and controllers of private and personal information, as referenced by this Act, include entities or institutions established or recognised by law. This includes parties based in the Maldives that utilise equipment to process personal information and parties responsible for offices, chapters, or agencies established in the Maldives; or

2. Processors and controllers of private information of data subjects, who were not established by law or recognised by law, including Maldivian citizens and residents based in the Maldives, regardless of whether the act was committed in the Maldives or abroad, the following shall be considered:

1. It is not required for data subjects to have paid for goods or services, provided that the processing of data is related to the provision of goods or services to data subjects based in the Maldives; or

2. Data processing is related to monitoring the activities or actions of a data subject in the Maldives.

(b) This Act shall not apply to the following parties

1. Agencies and parties working in the field of agencies working on collecting, using, and disseminating private information to fulfil their obligations or responsibilities are exempt from this Act. However, agencies carrying out functions specified in Chapter 5 (Protection of Private Information), Chapter 7 (Transfer of private information and/or processing of information by a third party), Chapter 8 (Investigation and Enforcement), and Chapter 9 (Cross Border Transfer) is not exempt from this Act;

2. Persons or parties working domestically in their individual capacities;

3. Institutions or part of institutions established

by the Regulation enacted by the Data Protection Commissioner of the Maldives or under a law of the Maldives delineating private information or classes of private information;

4. This Act shall not apply to private or personal information processed in exercising the right to freedom of expression, freedom of the media, and art and literature. However, the principles established by Chapter 5 (Protection of Private Information), Chapter 7 (Transfer of private information and/or processing of information by a third party), Chapter 8 (Investigation and Enforcement), and Chapter 9 (Cross Border Transfer) of this Act shall not be exempt;

5. Private information may be processed for public interest research, including historical, statistical, and scientific research. However, the principles established by Chapter 5 (Protection of Private Information), Chapter 7 (Transfer of private information and/or processing of information by a third party), Chapter 8 (Investigation and Enforcement), and Chapter 9 (Cross Border Transfer) of this Act shall not be exempt;

6. Information related to business transactions.

Prioritisation of law

4. Unless specified otherwise in this Act,

(a) Where a provision of this Act contravenes another law or regulation, that law or regulation shall be prioritised; and

(b) Where a provision of this Act obstructs a power, right, privilege, responsibility or restrictions imposed by another law, the legal privilege afforded shall not be impeded. However, responsibilities imposed by contractual obligations shall not be carried out in contravention of this Act.

Chapter Two
Implementation of the Act

Implementation and enforcement of the Act

5. (a) This Act shall be implemented by the Data Protection Office as specified.

(b) The Data Protection Office established as per subsection (a) of this Section refers to the "Information Commissioner's Office" established under the Right to Information Act (1/2014).

(c) The Data Protection Office referenced in subsection (a) of this Section shall function under the instruction of the Information Commissioner appointed under the Right to Information Act (1/2014).

Data Protection Office

6. (a) A Data Protection Commission shall be established to carry out the functions of the Data Protection Office.

(b) The Data Protection Commission shall comprise a maximum of 5 (Five) members.

(c) The Information Commissioner shall appoint and terminate the memberships of the members of the Data Protection Commission.

(d) The Information Commissioner has the authority to determine the remuneration of the members of the Data Protection Commission as advised by the

Minister of Finance.

(e) The Information Commissioner shall appoint the Data Protection Commission referenced in subsection (a) of this Section within 30 (Thirty) days from the date this Act enters into effect.

Requirements of Commission members

7. (a) Persons appointed to the Data Protection Commission shall have the educational qualifications and work experience within the following areas or related fields.

1. Privacy or data protection;
2. Information technology;
3. Information technology.

(b) Persons appointed as members of the Data Protection Commission shall meet the following requirements in addition to those stipulated in subsection (a) of this Section.

1. Shall possess the education qualification and expertise, as well as the work ethic required to fulfil their responsibilities as members of the Commission;
2. Shall not have been found guilty of a criminal offence within the past 5 (Five) years;
3. Shall not have been declared bankrupt;
4. Shall not occupy the post of Director or hold any other post at an institution which processes private and personal information;
5. Shall not have shares in their own name, under the name of a representative on their

behalf, or in the title of a company in which the person holds shares in an institution which processes private and personal information;

6. Shall not have been elected to a post through an election as stipulated by law.

(c) The term of membership for the Data Protection Commission is 5 (Five) years. Members not terminated, as stipulated in Section 9 of this Act, may be appointed for 2 (Two) additional terms.

(d) The Regulation made under this Act shall stipulate the procedure for appointing members to vacant membership posts.

Resignation of members of the Commission

8. Commission members may resign by submitting a letter to the Information Commissioner. The resignation becomes effective once the Commissioner receives the letter.

Termination of members of the Commission

9. (a) Members of the Data Protection Commission shall be terminated if they no longer meet the requirements stipulated by this Act.

10. (b) Notwithstanding subsection (a) of this Section, the Information Commissioner has the discretion to terminate members' membership where it is determined that they cannot carry out the responsibilities as mandated or where they are found to be in contravention of the Code of Conduct.

Conflict of interest

11. Where the Data Protection Commission is investigating a matter involving a member's interest, the member shall not be involved in the investigation or decision-making process to any extent. Where the interest, benefits, or role of a

member in a matter being investigated was unknown to the Commission, the member shall be excused from the investigation upon confirmation that they have a vested interest, benefit, or role in the matter being investigated.

Facilitation of administration of the Data Protection Office

12. The Information Commissioner's Office shall make arrangements to facilitate the administration of the Data Protection Office.

Employees of the Data Protection Office

13. The Information Commissioner is required to appoint employees to the Data Protection Office as needed. The Commissioner may appoint additional employees and train and promote existing employees as facilitated by the annual budget approved by the Parliament for the Office.

Code of Conduct of employees

14. Employees of the Data Protection Office shall maintain the confidentiality of matters disclosed or discovered within the scope of their work. Such information shall not be disclosed to parties unless otherwise specified by law.

Legal protection

15. Employees of the Data Protection Office or persons acting on behalf of the Data Protection Office shall not be investigated or prosecuted for the work executed and not executed as mandated.

Carrying out responsibilities free from external influence

16. Employees or persons acting on behalf of the Data Protection Office shall perform their responsibilities and make decisions independently, impartially, free from external influence.

Financial matters

17 (a) The budget shall be disbursed to the Information Commissioner's Office, as approved by the Parliament for the Data Protection Office. The Information Commissioner shall request the Ministry of Finance to include the Data Protection

Office's budget in the State budget in line with the Public Finance Act and relevant regulations.

(b) A financial statement detailing the income, expenditure, assets, and financial responsibilities of the Data Protection Office shall be prepared in consultation with the Auditor General's Office and submitted to the Parliament.

Duties and obligations of the Data Protection Office

18. The Data Protection Office shall have the responsibility and authority to carry out the following duties and obligations:

(a) The formulation, revision, interpretation and implementation of the regulations, policies and guidelines required to implement this Act;

(b) Preparation of guidelines and provision of consultation services to protect administrative, physical and technical security for the protection of private and personal data;

(c) Formulation of data protection laws and regulations and amendment of existing laws to promote the protection of private and personal data;

(d) Participate in international and regional activities concerning the protection of private and personal data;

(e) Represent the Government of Maldives in technical meetings with agencies and international data protection institutions;

(f) Providing consultations and assistance to the State in determining matters related to the protection of private and personal data;

(g) Formulation and publication of policies relevant to

the protection of private and personal data, including the interpretation of relevant policies;

(h) Conducting awareness initiatives to carry out the responsibilities mandated by this Act to protect private and personal data;

(i) Protecting the rights of data subjects, conducting relevant research, promoting educational opportunities within the field, and collaborating with other relevant agencies;

(j) Ensure that data controllers and processors adhere to this Act as required;

(k) Ensure the privacy and protection of private and personal data by implementing cross-border obligations;

(l) Represent the government of Maldives in all matters related to privacy and personal data protection, participate in discussions with other countries, and formulate agreements and establish laws and regulations relevant to the protection of private and personal data;

(m) Receive and investigate grievances and complaints related to the protection of private and personal data;

(n) Enact a policy detailing the mechanism and procedure for filing and investigating grievances and complaints under this Act;

(o) To carry out functions as required for the implementation of this Act and to implement policies, orders, decrees and verdicts established within the sphere of private and personal data protection, in addition to implementing administrative penalties and fines.

Chapter Three

Guidelines on processing private and personal data

General guidelines on privacy

19. Private and personal information shall include:

(a) Data collected for a particular purpose, for which the purpose was ascertained before data collection, can only be used for predetermined purposes (“limited usage of data”);

(b) Data processed transparently for the benefit of the data subject, as detailed in Section 20 or 21 of this Act (“adherence to laws, equity and transparency”);

(c) Data collected for a particular purpose shall be appropriate for the purpose it was collected for and shall only be collected for that particular purpose (“limiting the amount and usage of data”);

(d) Data shall be up to date for the required purpose; the validity of private and personal data collected shall be ascertained, and data deemed expired or invalid shall be corrected, updated and discarded where necessary (“ascertaining validity”);

(e) Collected data shall be maintained for the duration of its use and shall be managed in a way that identifies the owner of the data, and such data should not be additionally protected (“Limitation of the duration for which data is protected”);

(f) Private and personal data shall be processed in a manner that ensures data protection and shall not be used in contravention of laws. Furthermore, private and personal data shall not be processed in a manner which results in losing, misplacing or destroying of data through technical, physical or administrative means (“Maintaining privacy and

integrity”);

Accountability 20 (a) Controllers are responsible for the data under their purview, including responsibility for data sent for processing or processed within the Maldives and data sent for processing or processed internationally.

(b) Controllers shall ascertain the protection and confidentiality of data when implementing the Act or carrying out responsibilities in line with the Act. Where third-party processors are contracted, controllers shall ensure adequate security and confidentiality of the information shared with processors.

(c) Controllers and processors shall determine the parties responsible for implementing and carrying out responsibilities in line with this Act.

(d) Data subjects shall be informed of the parties appointed as responsible person(s) under subsection (c) of this Section.

(e) Although specific persons responsible for ensuring compliance with this Act are determined under this Act as detailed in subsection (c) of this section, institutions shall remain accountable for ensuring their responsibilities are carried out as required.

Processing private information in adherence to this Act 21 Private information shall be considered processed in line with or in adherence to this Act where one of the following conditionalities are met:

(a) Where data subjects consent to the processing of their private or personal information for a specific purpose or purposes;

(b) Where information on a data subject is required to be processed before they enter into a contract, before obtaining a service, and for the completion of the terms of a contract or a service, as requested by the data subject;

(c) Where data is processed in fulfilling a legal obligation imposed on Controllers;

(d) Where data is processed to fulfil responsibilities imposed on controllers in carrying out their rights and obligations as per their employment;

(e) Where the data is processed in line with a law, regulation or policy, provided that the processed data includes private information detailed in public records for the purpose or related purposes for which the data was published;

(f) Where data is processed to ensure the lives, health and protection of a data subject or another person;

(g) Where data is processed to ensure public or national safety, public health or protection;

(h) Where data is processed for a credit reporting service of a credit bureau;

(i) Where data is processed in establishing a case, levying or imposing a charge, as a defence to a charge imposed, or for legal services;

(j) Where data is required to be processed to obtain information as required by a controller or a third party, provided that the purpose for which the data is processed does not infringe the privacy and fundamental rights and freedoms of the data subject, especially in cases where the data subject is a minor.

Processing private and personal data of special categories in line with the law

22. Private and personal data of special categories shall not be processed unless specified otherwise below;

(a) Where consent is given by a data subject to process their private and personal data belonging to a special category for a specific purpose or purposes;

(b) Where the controller is required to process the data in carrying out the responsibilities and fulfilling rights as required by their employment;

(c) Where the private or personal data processed is published in public records as required by law, regulation or policy, provided that the data is processed for the purpose for which the data was collected;

(d) Where the data subject cannot actively or legally give consent to process the data in cases where the data is required to be processed for a special purpose related to the data subject or another person;

(e) Where data is processed for preventive or occupational health purposes, to assess the capabilities or capacity of an employee, for medical diagnostic purposes, to provide aid or treatment in line with health and public health and curative health systems, and for the management of these services and systems;

(f) Where data is processed to do that which is necessary to protect and ensure public health and national safety, as permitted and within the legal framework, in line with laws, regulations and policies;

(g) Where data is processed in establishing a case, levying or imposing a charge, as a defence to a charge imposed, or for legal services.

Data processed for criminal cases and penalties

23. A public authority's controller shall process data as necessary concerning criminal cases and penalties. Only a public authority shall maintain information on criminal offenders.

Consent

24. (a) Where data is collected or obtained with the consent of a data subject, the controller shall ascertain that the consent of the data subject was obtained. The duration in which the collected data, for the purpose for which data was collected, can be processed shall be ascribed.

(b) The consent of a data subject shall be considered to be obtained provided that the data subject is prior notified of the information contained in section 24 of this Act. As such, where incorrect information is shared with the data subject and consent is obtained unjustly, the obtained consent shall considered null.

(c) Data acquired from parties obtaining a good or service or from parties to a contract, including information or data related to the conditionalities of a good or service or the terms or conditions of a contract, shall not automatically be considered to have been obtained or processed with consent despite the inclusion of provisions which state that information which is not required for obtaining a good or service or adherence to a contract is being collected unless consent is expressly obtained.

Consent of minors

25. (a) In determining whether valid consent is obtained, laws shall be referenced to determine the age at which a person is no longer considered a minor.

Consent can be obtained with adherence to laws that stipulate the representation of minors and guidelines or policies on obtaining consent from minors.

(b) Before processing minors' data, the controller shall ascertain whether the minor's consent was obtained in accordance with subsection (a).

Chapter Four
Rights of Data Subjects

General Guidelines 26 (a) The controller shall ensure the rights of data subjects as stipulated by this Act.

(b) The controller shall comply with requests made by data subjects to invoke a right under this Act except in circumstances highlighted below or in situations where the controller is unable to verify the data subject's identity.

(c) The controller shall provide information on the follow-up actions taken following a request made by a data subject in line with this Act. The controller shall provide prompt and timely information, depending on its scope, difficulty in obtaining the information, and the legal consequences of requesting it.

(d) The controller shall inform the data subject of the opportunity to submit grievances without delay if the controller has not decided on a request made by the data subject.

Right to information 27 (a) The controller shall provide the following information to the data subject in a detailed, transparent, accessible and comprehensible manner where their private and personal data are

collected.

1) Where the data subject is not the direct source of private and personal information, the categories of private information and the entity through which the information is collected;

2) The need and requirement for processing private and personal information and circumstances allowing the processing of private and personal information without consent from the data subject;

3) The methodology and extent to which data can be processed;

4) Inform on the involvement of automated systems in data processing, details on what constitutes profiling, how such data shall be processed, and the benefits and expected results of this process in line with section 62 of this Act;

5) The recipients of the private and personal information or the information on the data categories and, when required, information of the data shared cross-border;

6) The details of the controller, phone number, and the information of assigned persons as detailed in section 19(c) of this Act.

(7) The duration for which private and personal data will be stored;

(8) The rights of the data subject as stipulated by this Act.

(b) The controller shall inform the data subject prior to

using the private and personal information for a purpose other than initially agreed. In such circumstances, the data subject can decline consent to process their private and personal information further.

(c) The controller is not obligated to inform the data subject where there is certainty in data collection and processing for a specific purpose, for instance, to fulfil contractual or service obligations, or association between employer and employee, controller and data subject, or to fulfil legal obligations under this section.

Right to Object

28 (a) The data subject has the right to object to collecting and processing private and personal information, as detailed in sections 20 and 21 of this Act, at any time for an acceptable reason. If the controller cannot justify data processing in compliance with sections 20 and 21, the processing of private and personal information shall be terminated. If an objection made under this section is not accepted, the type of objection and reason for rejection shall be recorded in writing.

(b) Prior to the enactment of this Act, all private and personal information collected from data subjects can be processed by the controller for data collection if the data subject has not withdrawn their consent.

Right to access information

29 (a) The data subject has the right to access the following information

(1) The private and personal information under the supervision of the data controller;

(2) Methodology of data collection where the information was sourced by a party other

than the data subject;

(3) Purpose of private and personal data collection and processing;

(4) The parties and persons with whom the information has been shared or will be shared, the data sharing categories, and the purpose of sharing private and personal information, including those residing outside the Maldives;

(5) The duration for which private and personal data will be stored;

(6) Information on the automated systems involved in data processing, including information on profiling and how data will be used to reach conclusions where the results may affect the data subject;

(7) The date on which private and personal information of the data subject was last used or revised;

(8) The information on the policies and guidelines formulated under section 36(b) of this Act;

(9) Information on the controller or the representative of the controller and their contact information.

(b) The data subject has the right to access private and personal information that predates a minimum of 1 (one) year.

(c) The controller has the right not to accept a request for private and personal information from the data subject if any of the following circumstances are

predicted to occur.

(1) For the protection of a party other than the data subject, or another party's mental and physical well-being is affected;

(2) For the data subject's protection or the data subject's mental and physical well-being is harmed;

(3) Private and personal data of another person are exposed, and the recipient does not consent to reveal particular information;

(4) The request affects or concerns national security.

Right to revise information

30 (a) The data subject has the right to revise inaccurate information or revise information that has been deducted, given that there is enough evidence to prove that the information has been changed.

(b) If a data subject requests to revise information under the right given to them under subsection(a) of this clause, the controller shall revise the information at the earliest.

(c) The controller shall provide the revised information to third-party recipients of this data as stipulated in this clause

(d) The controller shall record in writing any decisions made not to accept requests to revise information.

(e) The controller is not obliged to make revisions to the information suggested by professionals and parties.

Right to revoke consent.

31 (a) Where data can be processed with the data subject's consent, the data subject has the right to

revoke that consent at any time.

(b) The data processed before the revokement will be legally valid where the consent is revoked.

(c) The controller shall stop processing private and personal data on a data subject from the moment they revoke their consent.

(d) The controller shall inform third-party data processors to stop all activities to process private and personal information of data subjects that have revoked their consent under section (a) of this clause.

(e) Where the controller or a third party mentioned in this clause revokes their consent to send or transfer data as requested by the data subject under section 33 of this Act, the private and personal information shall be destroyed or returned.

Right to Prohibit, Suspend, or Terminate data processing

32 (a) The data subject has the right to prohibit, suspend, or terminate data processing in the following situations.

(1) Where the data subject questions the validity of the private and personal information, the period it takes for the controller to establish the validity of the data;

(2) Where private and personal information was processed in contravention of the law, the data subject refused to erase it and requested that the use of private and personal information be prohibited;

(3) Where the controller does not require

private and personal information for data processing, but the data is used by the data subject in establishing a case, levying or imposing a charge, defending a charge imposed, and for legal services;

(4) Where the data subject objects to the use of private and personal information under section 27 of this Act, and the rights of the controller override the rights of the data subject.

(b) where data processing is prohibited under subsection (a) of this clause, the data shall be processed with the consent of the data subject only to establish a case, levy or impose a charge, defend a charge imposed, and protect the vested interest of an individual, legal entity, or community.

(c) The controller shall record in writing any situation in which the data subject wishes to assert a right as described in this section, where their request was denied, including details of the type of objection they had and the reason for refusal.

Right to request erasure of information or data

33 (a) The data subject has the right to request the erasure and destruction of information and private data in the following situations, provided that there is enough evidence to support the request.

(1) Where the data was processed according to sections 20 and 21 of this Act with the data subject's consent, and provided the data subject revoked the consent, where there are no other means to process the data;

(2) Where the data subject objects to data processing under section 27 of this Act, where there is no other means to process

data, and there is no situation that can override the rights of the data subject;

(3) Where the data is collected and processed in contravention of the law;

(4) Where the purpose for which the data was collected is no longer valid or exists;

(5) Where the information was used for a purpose other than what was consented by the data subject.

(b) The data controller has the discretion not to accept requests made by the data subject to erase or destroy the data as stipulated by subsection (a) of this section.

(c) The controller shall record in writing any decisions made not to accept requests made by the data subject under this section.

Right to transfer data

34 (a) If a data subject's private and personal information is shared electronically on a public platform, the data subject has the right to obtain a copy of the private data in an electronic or standard format from the data controller and to use the data further.

(b) If the data subject’s private and personal data can be transmitted from one controller to another, and if such a transfer is technically possible without any additional financial charges, the data subject has the right to request data transfer and to use the right to transfer data under this section.

Chapter Five
Protection of private and personal information

Privacy of data and

35. (a) Administrative, physical, and technical security

protection of personal information

measures shall be imposed and implemented to monitor how the controller and processor handle private information, ensure the maintenance of integrity and confidentiality in carrying out their obligations, prevent discarding information in contravention of the law, modify or disclose information, or process information in any other manner or form in contravention of the law.

(b) Administrative, physical and technical security measures imposed as required by subsection (a) shall account for circumstances where private or personal data may be lost or destroyed faultlessly due to natural occurrences, as well as circumstances where private or personal data may be lost or destroyed due to fault of a person(s) in contravention of the law, usage, contamination or modifying of data in contravention of the law. The imposed measures shall provide ways in which this can be prevented, and data shall be protected.

(c) Security measures imposed as required by this section shall account for ways in which data can be processed, measures to be imposed to protect data in the process, the category or type of data that must be protected, dangers that persons could face due to processing of data, the capacity of the institution and the difficulty of the work carried out by the institution, best practices related to data privacy, and the expenses to be incurred in establishing security measures.

Security measures of institutions

36. Institutions shall impose security measures in line with the policies enacted by the Data Protection Office and established by this Act as follows:

(a) Controllers and processors shall appoint a Data Protection Officer or a Compliance Officer to

ensure data privacy and security and guarantee institutions' adherence to this Act. Data Protection or Compliance Officers are required to be answerable as such.

(b) The controller and processor shall establish data protection policies and guidelines to ensure adherence to the privacy policies stipulated by this Act.

(c) The adequate security measures imposed by design and by default (privacy by design and by default) shall be adequate to ensure that data is processed for the purpose for which it was collected.

(d) The policies and guidelines established under subsection (b) shall contain the following:

1. The manner in which private information shall be collected and how consent shall be obtained from data subjects;

2. Potential issues or technical problems that could occur in systems handling private information, guidelines to be followed in such circumstances, system monitoring and entry and exit from the systems;

3. The manner in which the rights of the data subject shall be ascertained as per section 26 of this Act;

4. Timeline and conditionalities for data protection and erasure of data;

5. Ensure compliance with this Act;

(e) Actions undertaken by processors and controllers shall be recorded and maintained adequately.

(f) In compliance with subsection (e), controllers and processors shall, at minimum, record the following information.

1. Categories of private and personal information collected and processed;

2. Categories of data subjects from which personal and private data are collected and processed;

3. Details of parties from which information was collected, parties to which such information can be disseminated, and where controllers and/or processors are included shall be stipulated whether the information may be shared with international parties as per section 19 (c) of this Act.

4. The manner in which information is collected, processed and retained in an institution, including the time at which the data can be discarded or destroyed and the circulation of data

(g) Controllers and processors shall ascertain that the employees, agents, or representatives involved in processing private and personal data shall be bound by strict confidentiality even after their employment ends.

(h) The controller and processor shall be responsible for training employees, agents, and representatives to familiarise themselves with the guidelines on maintaining privacy and protecting private and personal data.

Protection measures 37. Controllers and processors shall take the following

steps to protect private and personal information.

(a) Guidelines and policies shall be established to monitor entry and exit into places where private and personal data is processed;

(b) Privacy shall be afforded to those who process private and personal data, with account for the environment in which the work is carried out;

(c) The obligation and responsibilities of persons responsible for processing data must be considered, and timelines for processing private and personal data shall be established;

(d) Establish guidelines and procedures detailing protection measures to ensure files and equipment remain safeguarded from harm;

(e) Ensure that the offices or environments in which private and personal data are processed are protected from natural disasters, continuously supplied with electricity, and restricted in entry, in addition to protecting the office environment from other potential dangers.

Technical security measures

38. Controllers and processors shall establish the following technical and security measures at institutions;

(a) The information security policy for protecting private and personal information;

(b) Prevent accidental or intentional utilisation or access into computer networks, and ensure data is protected from modification or misuse by establishing protection measures;

(c) Establish measures to ensure confidentiality, integrity and resilience of the established systems;

(d) Routinely monitor security breaches, identify potential issues with the computer networks, and identify measures that can be taken to prevent modification or harm to private and personal information by taking the necessary and adequate measures;

(e) Establish measures to recover and access private and personal information during or after physical or technical incidents;

(f) Ensure that the imposed security measures work effectively by routinely testing and verifying the imposed measures;

(g) Encrypt private and personal information to protect such information during the transfer of such information, establish an authentication process to limit the usage of private and personal information, and establish other technical security measures.

Chapter Six
Notification of breach caused to private and personal data

Notification of breach caused to private and personal data

39 (a) Where private or personal information is breached, or it is speculated that harm may be caused to such information, and one of the scenarios, as stipulated below, occurs, the Controller shall notify the Data Protection office and the data subject to whom harm may be caused because of the breach within 72 (hours).

1. Where the data breached consists of information belonging to a special category, and such data may be used deceptively or maliciously to commit identity theft;

2. Where private or personal information was

collected or accessed by an unauthorised party;

3. Where private or personal information was collected or accessed by an unauthorised party, as a result of which the data subject may be exposed to harm or danger.

(b) Where the circumstances in which the data was breached or the parties required to be notified of the breach were not informed within the stipulated time, the Data Protection Office is required to investigate such cases.

(c) Investigations carried out under subsection (b) shall account for the institution's system, policies, and procedures.

Details to be included in the notification

40. Notifications of breach of data shall contain the following information.

(a) Type of breach;

(b) The type of information that was breached;

(c) Actions carried out to remedy the breach;

(d) Actions carried out to mitigate the harm caused by the breach;

(e) The contact information through which the controller may contact the relevant employee and the contact information for data subjects to acquire additional information;

(f) Details of assistance that can be provided to data subjects harmed by the breach;

Guidelines for sending the

41 The Data Protection Office shall formulate a policy detailing the management of breach of data,

notification			notification of data breach, additional information that shall be included in the notification of breach, and guidelines on reporting the breach.

Chapter Seven
Sharing of private and personal information with third parties and processing of private and personal information by third parties

Subcontracts for processing private and personal information	42	(a)	Third-party processors may be contracted to process private and personal information.
		(b)	In adherence with subsection (a), the controller and third-party processor shall sign a contract to the effect detailing protection of the information, confidentiality in dealing with the information, integrity in ascertaining that the information is not used for any other purpose than that which is specified, and adherence to this Act, other laws detailing protection of private and personal data, policies and guidelines enacted by the Data Protection Office.
Conditions	43.	(a)	The contract shall cite the purpose for which the contract is formulated, the timeline during which the information shall be processed, the type of processing required, the purpose for processing the information, types of private information, categories of data subjects, rights and responsibilities of the Controller, and information regarding the place at which the data shall be processed.
		(b)	The contract shall stipulate that the processor shall undertake the following responsibilities.

1. Private and personal information shall be processed as instructed by the controller, whereby private and personal information may be transferred to international institutions as authorised by the law or as agreed upon in writing;

2. Ensure confidentiality is maintained by processors permitted to process private and personal information;

3. Establish necessary security measures in line with this Act and policies and guidelines established by the Data Protection Office;

4. Additional parties shall not be involved in processing private and personal information unless the controller permits. In such instances, the terms indicating responsibilities and obligations shall apply to the additional parties involved;

5. The processor shall assist the controller in ensuring that the rights of data subjects are upheld and in answering queries that may be posed;

6. Accounting for the type of processing required and the nature of private and personal data being processed, the processor shall assist the controller in complying with this Act and other relevant laws and policies formulated by the Data Protection Office;

7. The processor shall notify the controller of incidents which may impact the security of private and personal information and assist the controller in notifying the relevant

parties as required by this Act, other relevant laws, and policies enacted by the Data Protection Office;

8. Take action as required to mitigate harm caused by privacy breaches or security incidents;

9. Upon conclusion of processing data, private and personal data shall returned or erased as required by this Act and other relevant laws, as instructed by the controller;

10. Provide information to the controller in performing the responsibilities and obligations imposed under this Act and assist in auditing and inspections as required;

11. Immediately inform the controller of occurrences which contravene this Act and other relevant laws or policies and regulations formulated by the Data Protection Office.

Responsibilities of processors

44. Processors must comply with this Act, other relevant laws, policies and guidelines formulated by the Data Protection Office, and the contract with the Controller.

Sharing of information

45. (a) Information shall be shared in adherence to sections 20 and 21 of this Act by fulfilling the security measures, ensuring privacy, and transparency in processing data for the purpose for which the data was collected.

(b) Where information is shared for commercial purposes such as marketing, an agreement must

be entered between the parties specifying the security and privacy of the information shared and the rights of the data subject(s).

(c) The following information shall be shared with data subjects before collecting or disclosing information.

1. Information on the controller and processor of private information;
2. The purpose for which the information is shared;
3. Categories of private information shared;
4. Parties or categories of parties with which the information shall be shared;
5. The rights of data subjects, including the right to acquire and amend information and the right to refuse;
6. The extent to which private information is shared and information regarding how data is processed;

Guidelines for sharing information

46. The Data Protection Office shall formulate policies and guidelines detailing the procedure to share information and ensure privacy.

Sharing information with international parties

47. Information shall only be shared with international parties after ascertaining that the parties have taken the required steps to protect private and personal information per this Act.

Chapter Eight
Cross-border sharing of information

Guidelines on data sharing

48. (a) The controller and processor shall send information cross-border, outside the jurisdiction of the

Maldives, in accordance with this Act's conditionalities and this chapter's specificities.

(b) All provisions of this chapter shall be adhered to when sharing data cross-border to ensure the protection of persons.

Ascertaining protection in sharing information

49 (a) The processor and controller shall share information with persons outside the jurisdiction of the Maldives after ensuring the fulfilment of conditionalities to ensure protection by guaranteeing the rights of data subjects and that legal remedies are afforded to subjects.

(b) The conditionalities to ensure protection specified in subsection (a) shall be considered fulfilled, provided that the following criteria are met.

1. Ensuring enforceability of corporate policies as specified in section 49 of this Act; or

2. Ensuring that the provisions as required by the Data Protection Office are included in agreements with parties outside the jurisdiction of the Maldives.

(c) Enforcement provisions shall be included in the agreements as specified in subsection (b) (2) to ensure that the rights of data subjects are protected.

(d) The Data Protection Office is required to establish and adhere to guidelines to ensure compliance with this section.

Enforcement of commercial policies

50. (a) The Data Protection Office shall enact the commercial policies submitted by the controller and processor, provided the following requirements are met.

1. The policy includes provisions which can be enforced or applied to commercial businesses, groups, members and their employees;

2. The policy includes the rights of data subjects, which can be enforced; and

3. The requirements set forth by subsection (b) are met.

(b) The enforcement of commercial policies, as referenced in subsection (a) shall include the following:

1. Information on the mandate or purview of the commercial businesses and groups, including information on contact numbers of members;

2. Information regarding the sharing of data and datasets, categories of private and personal data, types of processes, the purpose for which the data is processed, the concerned data subject, and the country or countries involved;

3. The manner in which parties will be legally bound to policies enacted;

4. The application of the general principles of data protection referenced in Section 18 of this Act, enforcement of corporate policies as per Chapter 8 of this Act, and the requirements to be fulfilled to complete onward transfers by controllers and processors exempt from section 48 of this Act;

5. Rights of data subjects which must be ensured in processing data, the manner in which these rights will be ensured, the procedure for filing complaints with the Data Protection Office, remedies for complaints, and compensation for breach of commercial policies;

6. Where parties established outside the jurisdiction of Maldives contravene commercial policies, the Controller or Processor established in the Maldives shall be responsible for their infringement. However, where it is proven that the damages incurred occurred without fthe ault of the member(s), the controller or processor shall be exempt from responsibility as such;

7. The manner in which information regarding commercial policies shall be shared with the data subjects as per Section 27 of this Act and subsection (4) to (6) of this Section;

8. The party or institution responsible for ensuring that the Data Protection Officers appointed by this Act carry out their responsibilities, monitoring of adherence to commercial policies by commercial businesses and groups, training, and investigation of complaints and grievances submitted;

9. The procedure for submitting complaints and grievances;

10. Internal policies shall be formulated to ensure compliance of commercial

businesses, enterprises and groups with the commercial policies. This policy shall include information on data protection audits, corrective actions to ensure that the rights of data subjects are guaranteed, and monitoring of adherence to this Act. The outcome of this policy shall be communicated to the parties referenced in subsection (9) of this section, as well as the boards of commercial enterprises and groups. This information shall be shared with the Data Protection Office upon request;

11. Recording changes to the policy, informing the Data Protection Office of changes to the policy and reporting mechanisms;

12. The result shall be communicated or shared with the Data Protection Office after fulfilling the obligations detailed in subsection (8) of this Section. A mechanism shall be established to cooperate with the Data Protection Office to ensure compliance with the commercial policies by members of commercial enterprises and groups;

13. Where an incident occurs in a third country which negatively impacts the guarantee provided by commercial policies enforced upon members of commercial enterprises or groups, the manner in which this shall be reported to the Data Protection Office;

14. The Information Commissioner has the discretion to decide the format and procedure for sharing information by and between the Controller and Processor and

the Data Protection Office and how training shall be provided to parties that permanently or generally handle private and personal information.

Chapter Nine
Investigation and Enforcement

Right to submit grievances

51 (a) All persons are entitled to submit grievances to the Data Protection Office regarding any right stated in this Act.

(b) The procedures and guidelines for submitting grievances to the Data Protection Office, as stated in subsection(a) of this clause, shall be formulated as part of the regulations developed under this Act.

Authority to investigate

52 (a) The Data Protection Office has the authority to investigate if a complaint is submitted to the Data Protection Office regarding any institution or if there is a need to ensure institutions' compliance with this Act.

(b) Investigations carried out by the Data Protection Office shall be suspended, terminated or refused in the following circumstances.

(1) Confirming that the institutions are operating as per the directions of the Data Protection Office as per clause 9 of this Act;

(2) Arriving at a joint agreement by two parties involved in the disagreement or issue;

(3) The Data Protection Office shall transfer investigations to another institution if it is deemed more appropriate to undertake the investigation;

(4) If the grievance submitted to the Data Protection Office has no basis, is submitted for inconvenience, or has no good intentions of submitting the complaint.

(c) The Data Protection Office shall store records of the investigations carried out up to 1 (One) year following the completion of the investigation or as per the written directions issued by the Data Protection Office for the notified duration.

(d) The Data Protection Office has the authority to carry out the following actions in investigations.

1. Entering and searching premises;
2. Inspecting, copying required documents and carrying copies of documents;
3. Copying documents or part of documents;
4. Interviewing persons working at the premises and recording the interviews;
5. Operating equipment at the premises, including any electronic equipment;
6. Photography, videography and recording.

(e) If the owner or operator of a private property does not permit the Data Protection Office to enter the premises for investigation, the Office can enter the property after obtaining a court order to fulfil its duties under this Act.

Authority to Revise 53 (a) The Data Protection Office has the authority to carry out the following actions where a grievance has been submitted.

1. Amend the decision to refuse the provision of information or provision of information

within an acceptable duration for information requests submitted to the Data Protection Office as per section 26 of this Act;

2. Amend the decision to accept a request to revise private and personal information as per section 29 of this Act or proceed with a revision within an acceptable duration.

(b) The Data Protection Office can inform to carry out the below actions following a revision made under subsection (a) of this section.

1. Notify that the decision to reject the request for information was correct or instruct to provide the requested information within a specified duration by the Data Protection Office.

2. Notify that the decision to reject the revision of information was correct or instruct to revise the information accordingly.

Authority to command

54 (a) Where other institutions are found to be acting in contravention of this Act during investigations undertaken by the Data Protection Office, as per section 51, the Data Protection Office has the authority to command other institutions to adhere to this Act.

(b) The Data Protection Office has the authority to command institutions to carry out the following actions as per subsection (a) of this section.

1. Command institutions to terminate the collection, usage, or publishing of private and personal information in contravention of this Act;

2. Command institutions to destroy private and personal information collected in contravention of this Act;

3. Command institutions to provide details if actions have been undertaken to abide by the directions provided by the Information Commissioner Office or to take necessary measures to adhere to the directions.

(c) The Data Protection Office has the authority to publish information on institutions that do not abide by the commands issued under this clause.

Revision of commands

55 (a) Institutions or individuals with grievances related to commands issued by the Data Protection Office under section 53 of this Act shall submit a written request to revise the command within 30 (Thirty) days from its issuance.

(b) The regulations formulated under this Act shall include procedures and guidelines for submitting requests to revise the commands under subsection (a) of this section.

(c) Where a request to revise a guidance is submitted, the Information Commissioner shall ensure the following.

1. Revision of the guidance;

2. Where the Information Commissioner considers that no revisions are required to the guidance, the decision shall be informed, or the guidance shall be either rejected or changed;

3. Inform the decision to the applicant in writing.

Authority to take corrective measures.

56 The Information Commissioner, through the Data Protection Office, has the authority to take the following corrective measures.

(a) Warn data controllers and/or processors where the data processing works are contravening with this Act.

(b) Take action where the data processing works carried out by the controllers and/or processors contravene this Act.

(c) Command the data controller and/or processor to ensure the data subject's rights where such a request is submitted.

(d) Command data controllers and/or processors to conduct data processing works in adherence to this Act and carry out works in a specific manner within a particular duration.

(e) Command data controller to inform of any risks to the private and personal data of the data subject.

(f) Command persons with whom data was shared to terminate revising, erasure, or processing of private and personal data.

(g) In addition to the provisions of this Section, penalties may be imposed as detailed in Section 58 of this Act instead of the penalties stipulated by this Section concerning each incident or circumstance.

Authority to issue orders

57 The Data Protection Office has the authority to issue an injunction, either permanently or temporarily, to prohibit the processing of personal data to protect the rights of the data subjects or if the Data Protection Office determines that the transmission of data to locations beyond the Maldivian jurisdiction may harm the public interest.

Power of exemption 58 The Information Commissioner has the discretion to grant exemptions to specific individuals, institutions or classes of individuals or institutions as detailed in this Act based on the following provisions.

(a) The total workforce of the institution.

(b) Revenue of the institution.

(c) The volume of data processed.

Administrative measures 59 (a) After assessing the circumstances of each matter, the Information Commissioner's Office shall take executive and administrative measures and impose fines in addition to those stated under this Chapter through the Data Protection Office.T o determine the sum of the fine imposed under executive measures, the following factors shall be considered:

1. The action taken in contravention to the law, its seriousness, duration, reason for processing that data, damages to the data subjects and the extent of these damages;
2. Action taken in contravention to the laws, either intentionally or due to negligence;
3. Actions taken by the data controller or processor to minimise damages to the data subjects;
4. Responsibility taken by the data controller or processor and the measures implemented to protect the personal data specified under Chapter Five of this Act;
5. Actions taken by the data controller or processor in contravention of laws;

6. Cooperation was provided to the actions taken by the Information Commissioners Office to resolve or minimise the damages resulting from the action taken in contravention of laws;

7. The categories of the data affected by the action taken in contravention of laws;

8. The manner in which the Information Commissioner's Office became aware of the action taken in contravention of laws and the extent to which the data controller or processor attempted to notify the Information Commissioner's Office thereof;

9. Whether the data controller or processor has been ordered or if it is determined that the data controller or processor had previously been ordered in relation to a similar matter under this Chapter (Investigation and Implementation). Or whether an investigation has been conducted to determine if the data controller or processor was acting in compliance with Chapter Nine of this Act;

10. Financial gains or reduced financial damages through direct or indirect measures taken in order to minimise damages due to an action taken in contravention of laws;

(b) In the event that the controller and/or the processor acts in contravention of Chapters Five (Protection of private and personal information), Six (Notification of breach caused to private and personal data) and Seven (Sharing of private and

personal information with third parties and processing of private and personal information by third parties) of this Act, under section (a) of this provision, take administrative action may be taken either by imposing a fine of no more than MVR …. or if the controller or processor engages in a particular course of action, by deducting no more than …% of the profit of the next fiscal year. The measure resulting in a greater sum shall be taken.

(c) In an event where an action is taken in contravention to the following provisions, administrative action may be taken under section (a) of this provision, either by imposing a fine of no more than MVR …. or if the controller or processor engages in a particular course of action, by deducting no more than …% of the profit of the next fiscal year. The measure resulting in a greater sum shall be taken.

11. The fundamental conditions regarding processing and the conditions pertaining to consent under Chapter Three (Guidelines on processing private and personal data) of this Act.

12. Rights under Chapter Four (Rights of the Data Subject) of this Act;

13. Policies related to the sharing of data cross-border as specified in Chapter Eight (Cross-border sharing of information) of this Act;

(d) Acting in contravention to an injunction, specific performance order or an order issued by the Data Protection Office pursuant to section 53 of this Act, mandating the destruction of processing of personal data, whether permanently or temporarily,

			or an order or notice issued under Chapter Nine of this Act, and contravention of policies about the grievance process, investigation and resolution.
Right to compensation for damages	60	(a)	An individual has the right to receive damages resulting from harm caused by an action taken in contravention of the law.
		(b)	The data controller is liable for any damages arising from harm caused by processing carried out in contravention of the Act.
		(c)	The data processor shall only be liable for damages under this provision if they acted in contravention of the policies under the relevant regulations of this Act during processing or where actions were taken in direct contravention of the instructions issued by the data controller.
		(d)	The controller or processor shall bear the burden of proving that they are not liable for the damages incurred and shall be exempt from liability under sections (b) and (c) of this provision.
		(e)	Damages under this provision must be sought by filing a claim before the court.
Certificate of National Interest	61		For the purpose of this Act, a certificate signed by the Minister responsible for national security and interest shall be provided as evidence in circumstances where action is required or where there is any doubt regarding a situation that may disrupt the national interest.

Chapter Ten
General Provisions

Power to formulate Regulations	62	(a)	The Data Protection Office shall formulate and enforce the regulations necessary to implement the

provisions of this Act according to its objectives.

(b) Regulations under this Act can be formulated in a manner that varies according to institutions, individuals or the classes of these institutions or individuals.

Enforcement Date of the Act 63 This Act shall enter into force upon its passage and assent by the Parliament of the Maldives and its publication in the Government Gazette.

Definitions 64 In this Act, unless stated otherwise:

(a) “Automated Systems” shall refer to the process of making decisions based on data that can be processed automatically, where such decisions have legal effects on the data subject.

(b) “Beneficial Plan” shall refer to an insurance policy, pension policy, annuity or other similar plan.

(c) “Business” shall refer to an office that operates on an ongoing basis regardless of whether it is for profit and is not operated by a person acting in their capacity.

(d) “Business-related Information” shall refer to the name, status, and position of the person connected to the business. In addition, the business's phone number, address, email or fax number, and any other relevant information must be provided.

(e) “Commercial” shall mean the activities, transactions, and other customary activities associated with the business.

(f) “Commission” shall refer to the Data Protection Commission of Maldives

(g) “Controller” shall refer to individuals, companies,

associations, bodies, corporate or unincorporated groups, and individuals acting alone or jointly responsible for determining the purposes and means of processing personal data.

(h) “Consent” refers to the clear approval provided by the data subject without coercion to gather and process personal data. The approval must be recorded in writing, electronically or otherwise. This approval can be provided by an agent or person appointed to act on behalf of the data subject.

(i) “Credit Bureau” shall refer to any entity that provides Credit Reports for remuneration or establishments operating as a business for profit that provide Credit Reports regularly without charge.

(j) “Credit Report” shall mean a report, provided either orally or in writing, that assesses the capability of individuals engaged in transactions with any institution to repay a loan.

(k) “Data Sharing” shall mean the sharing of information that is under the supervision of a controller to another controller or controllers.

(l) “Data Sharing Agreement” or “D.S.A” shall mean an agreement or contract formulated between the controllers to transfer personal data, outlining actions to be taken to ensure the privacy and protection of the data, safeguard the rights of the data subjects, and define the controllers' responsibilities and liabilities.

(m) “Data Subject” shall mean the individual to which the personal data belongs.

(n) “Document” shall refer to information protected

through various means.

(o) “Domestic” shall refer to matters pertaining to family.

(p) “Educational Centre” shall refer to education, training and teaching facilities.

(q) “Enforcement Date of the Act” shall refer to the date the law shall enter into force.

(r) “Employment” shall include voluntary work.

(s) “Need for assessment” shall refer to;

1. Assessing the capacity and suitability of the person in relation to the information in the following areas;
    a. To hire for employment or appoint for a position.
    b. To grant promotions and to retain their position.
    c. To terminate employment.
    d. To enrol in an educational centre.
    e. To provide contracts, awards, scholarships, bursaries, titles, and other prizes.
    f. To select for involvement in sports or artistic activities.
    g. To provide health-related services in relation to schemes provided by public agencies and to offer financial and social assistance.
2. Assessing whether any contract, award, scholarship, bursary, or title should be maintained, modified, or terminated;
3. To provide insurance for a person or an

asset, maintain an existing insurance policy or establish a new policy;

4. And other purposes;

(t) “Individual” refers to private persons.

(u) “Investigation” refers to investigations taking place under the following circumstances.

1. Due to breach of contract

2. Due to a breach of policies established by regulatory authorities constituted under an Act or due to a breach of other relevant policies.

3. Due to the occurrence of an incident or action subject to a remedy or resolution under the law.

(v) “Minister”, unless otherwise specified, refers to the Minister responsible for technology-related matters.

(w) “National Interest” includes the national defence mechanism, national security, public safety, fundamental services, and the management of internal affairs within the country.

(x) “Personal Information” refers to information, in any form, that, alone or combined with other information, can directly or indirectly be used to identify an individual (data subject).

(y) “Losing Personal Information” refers to information transmitted, protected, or processed being destroyed, lost, altered, or released in contravention of the laws due to a security breach.

(z) “Healthcare Body” refers to the healthcare body

appointed by the Minister of Health.

(aa) “Law Enforcement Agency” refers to an authority designated by the Minister amongst those responsible for criminal investigation and prosecuting offenders.

(bb) “Private Trust” refers to a trust established for the benefit of a specific individual or individuals.

(cc) “Continuation of proceedings” refers to a claim, whether it is civil, criminal or administrative, that is ongoing before the courts, tribunals or regulatory authorities for the following reasons;

1. Due to the breach of contract.

2. Due to a breach of policies established by regulatory authorities constituted under an Act or due to a breach of other relevant policies;
   Due to the occurrence of an incident or action that is subject to a remedy or resolution under the law.

(dd) “Processor” refers to individuals, companies, associations, bodies, corporations, or unincorporated groups responsible for processing information on behalf of the controller.

(ee) “Processing” refers to work carried out in connection with operations or operational sectors involving personal data, whether automated or manual, carried out including the following.

1. Gathering;

2. Recording;

3. Protection or safeguarding;

4. Arrangement, modification or composition;

5. Use;

6. Discovery;

7. Merging;

8. Publication, transmission and dissemination;

9. Erasing or destroying;

(ff) “Determination” refers to matters established under the laws and regulations.

(gg) “General Agency” includes the following;

1. The Government of Maldives, including its ministries, departments, agencies, and other government institutions;

2. Tribunals constituted under laws;

3. Other governmental bodies;

(hh) “Tribunal” refers to any entity with judicial or court-like authority and those performing restorative, arbitral, or mediation functions.