Personal Data Protection Act

Personal Data Protection Act

Chapter I
Introduction

Introduction and Title

1. (a) An Act to protect the personal data by regulating the collection and processing of personal information; to stipulate the rights of the persons whose data is collected and the obligations of data Processors and data Controllers; to regulate the use or disclosure of personal information; and to provide for matters connected therewith or incidental thereto.

(b) This Act shall be cited as the "Personal Data Protection Act".

Purpose

2. The purpose of this Act is to govern the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their privacy and personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

Scope of Application

3. (a) This Act shall apply to:

(1) The processing of all types of personal data performed by a Controller or a Processor in both the public and private sectors within the Maldives, whether formed or recognized under the law of the Maldives, including the use of personal data processing equipment that are located in the

Maldives, or those who maintain an Authority, branch or agency in the Maldives; or

(2) The processing of personal data of data subjects located in the Maldives, including residents or citizens of Maldives, by a Controller or Processor not formed or recognized under the law of Maldives, regardless of whether the processing occurs outside of Maldives, where:

(i) The processing relates to the offering of goods or services to data subjects who are in the Maldives, regardless of whether payment is made by the data subject; or

(ii) The processing relates to the monitoring of data subjects' behaviour, where the behaviour takes place in the Maldives.

(b) This Act shall not apply to:

(1) Any public agency or an organization in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data pursuant to its legal mandated function. However, the non-applicability of the Act does not extend to public agencies with respect to the requirements set forth under Chapter IV (Rights of Data Subjects), Chapter V (Security of Personal Data), Chapter VI (Personal Data Breach Notification), Chapter VII (Personal Data Transfers to, and/or Processing By, Third Parties), Chapter VIII (Cross-Border Transfers) and Chapter IX (Investigation and Enforcement);

(2) Any natural person acting in a personal or domestic capacity;

(3) Any organizations, or classes of organizations prescribed by regulations issued by the Maldives

Data Protection Commission or by laws of Maldives, for the purposes of this provision in connection with personal data or classes of personal data.

(4) Personal data processed solely for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations. However, the non-applicability of the Act under this provision, does not extend to the requirements set forth under Chapter IV (Rights of Data Subjects), Chapter V (Security of Personal Data), Chapter VI (Personal Data Breach Notification), Chapter VII (Personal Data Transfers to, and/or Processing By, Third Parties), Chapter VIII (Cross-Border Transfers) and Chapter IX (Investigation and Enforcement);

(5) Personal data that will be processed for research, including historical, statistical, or scientific purposes intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards. However, the non-applicability of the Act under this provision, does not extend to the requirements set forth under Chapter IV (Rights of Data Subjects), Chapter V (Security of Personal Data), Chapter VI (Personal Data Breach Notification), Chapter VII (Personal Data Transfers to, and/or Processing By, Third Parties), Chapter VIII (Cross-Border Transfers) and Chapter IX (Investigation and Enforcement);

(6) Business contact information

Precedence over other laws

4. Unless otherwise stated in the Act;

(a) The provisions of this Act shall have effect notwithstanding anything to the contrary in any other written law, relating to the protection of personal data of data subjects; Provided however, where a public agency is governed by any other written law, it shall be lawful or such authority to carry out processing of personal data in accordance with the provisions of such written law, in so far as the protection of personal data of data subjects is consistent with this Act.

(b) In the event of any inconsistency between the provisions of this Act and the provisions of such written law, the provisions of this Act shall prevail.

(c) Nothing in this Act shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening this Act.

Chapter 2

Data Protection Authority

Data Protection Authority

5. (a) For the purpose of this Act, a "Data Protection Authority" is established on the date of the enforcement of this Act.

(c) The Data Protection Authority mentioned in sub-section (a) shall be regulated as a part of the National Center for Information Technology.

(d) The Minister shall be responsible to the People's Majlis regarding the matters of the Data Protection Authority.

(e) Data Protection Authority shall be responsible for the administration and enforcement of this Act.

Responsibilities of the Data Protection Authority

6. Pursuant to this Act, the Data Protection Authority shall have the following powers and responsibilities:

(a) Publish and review guidelines and regulation and procedures that is required to enforce the law;

(b) Offer advice regarding physical, administrative and technical security features that needs to be enforced to protect personal data and publish guidelines for such;

(c) Propose amendments to laws to protect personal information and bring amendments required for other laws to protect personal information;

(d) Take part in global and regional activities regarding privacy and personal information;

(e) Maintain technical relations with general agencies and global Data Protection Authorities and represent Maldives as such;

(f) Advice the government on matters relating to protecting privacy and personal data;

(g) Prepare and publish procedures and guidelines as advice with regard to interpreting the law and protecting privacy and personal data;

(h) Conduct public awareness to the law in respect to practicing the law and protecting privacy and personal data;

(i) Conduct research on protecting subjects' rights and participate and educate in activities related to data protection;

(j) Ensure that Controllers and Processors specified in the law abide by it;

(k) Carry out activities in enforcing the law across borders regarding privacy and personal data protection;

(l) Represent the government with regard to personal data privacy and negotiate and establish agreements across border;

(m) Receive complaints and investigate regarding privacy of personal data;

(n) Establish procedures with regard to filing complaints, investigation and breach of law;

(o)

Administrative arrangements of Data Protection Authority

7. National Center for Information Technology is responsible for making all administrative arrangements for Data Protection Authority. This includes coordinating and organizing the necessary administrative tasks and functions to ensure the smooth operation of the authority.

Staff of Data Protection Authority

8. (a) The staff of the Data Protection Authority are shall be civil service staff. Law No. 5/2007 (Maldives Civil Service Act) and the regulations made under the Act shall be applied to the staff.

(b) Within 6 (six) months of the commencement of this Act, the Data Protection Authority shall, on the advice of the Minister, prepare and submit to the Civil Service Commission an administrative structure of the technical and administrative staff of the Authority.

(c) The Civil Service Commission shall appoint and dismiss the employees required by the Authority in accordance with the structure formulated by the Authority under sub-section (b) of this Section.

conflicts of interest and ethics

9. (a) The employees of the Data Protection Authority shall act impartially and free from influence in carrying out all their responsibilities and in making decisions in the implementation of this Act.

(b) If the Data Protection Authority considers or decides whether any employee has a personal interest or benefit or role, such person shall not participate in the consideration or decision of such matter to any extent. The employee shall refrain from considering the matter or making any necessary decisions with respect to it upon becoming aware of such interest or benefit or role, even if there is no prior knowledge of the matter.

(c) No employee of the Data Protection Authority shall accept any gift or benefit of any kind in his own name or in the name of any person with whom he has a family or personal or business relationship in such a way as to rely on any person in the performance of his duties under this Act.

(d) Information received by the employees of the Data Protection Authority in their capacity shall be kept confidential. Such information shall not be disclosed to any person except to the person required to disclose it as permitted by law.

Protection by the law

10. An action taken or avoided by a staff of the Data Protection Authority or a person acting on behalf of the Authority, is done in good faith and within the bounds of the law, should not be subject to prosecution**.**

Influence /under duress/conflict of interest

11. A staff of a Data Protection Authority or any person acting on behalf of the Authority is required to perform their duties impartially and without being influenced by external pressures or coercion. They should not be under duress when carrying out their responsibilities.

Finances

12. (a) The funds required to perform the responsibilities of the Authority shall be included in the budget approved by the Parliament each year and shall be allocated to the Data Protection Authority by the Ministry of Finance.

(b) All accounts and all documents of the Data Protection Authority shall be kept in accordance with Law No. 2006-03 (Public Finance Act) and the regulations made thereunder.

(c) The financials of the Data Protection Authority should undergo auditing as instructed by the Auditor General. The Auditor General sets the regulations and guidelines for conducting the audit. Once the audit is completed, the

audited financial statements should be submitted to the People's Majlis.

Director General

13. (a) Director General is responsible for the day-to-day governance of the Data Protection Authority.

(b) The Director General shall work under the instruction of the Minister to implement the policies made by the Minister. The Director General shall be accountable to the Minister with regards to the matters relating to the Data Protection Authority.

(c) The Director General shall be appointed by the Civil Service Commission under the Law No. 5/2007 (Maldives Civil Service Act).

(d) A person appointed as the Director General must possess the following qualifications.

(1) Possess the necessary qualifications, expertise, and professional integrity to effectively discharge the duties of the Data Protection Authority;

(2) Possess at least 05 (years) of experience in the fields of personal data protection, information technology and cyber security;

(3) Should not have a criminal record for the past 5 (five) years;

Chapter 3

Principles Governing the Processing of Personal Data

General Principles

14. (a) Every controller shall process personal data in compliance with the obligations specified under this Act.

(b) Personal data shall be collected for specific, explicit and legitimate purposes declared before collection and not further processed in a manner that is incompatible with those purposes (purpose limitation).

(c) Personal data shall be processed lawfully in accordance with section 14 below, impartially and in a transparent

manner in relation to the data subject ('lawfulness, impartiality and transparency');

(d) Personal data that is processed be adequate, relevant and necessary data in relation to the declared, specific and legitimate purposes for which they are collected and processed ('data minimization or proportionality');

(e) Personal data that is processed shall be accurate and, where necessary, kept up to date and complete; reasonable steps must be taken to ensure that personal data that are inaccurate, outdated or incomplete, having regard to the purposes for which they are processed, are erased or rectified without delay ('ensure accuracy');

(f) Personal data that is processed shall be retained in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is collected and processed ('retention limitation');

(g) Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical, physical or organizational measures ('integrity and confidentiality').

(h) Personal data shall be collected and processed in a manner that ensures data minimization, limiting the processing of personal data to what is necessary in relation to the purposes for which they are processed.

Principle of Accountability

15. (a) Each Controller is responsible for personal data under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(b) The Controller is accountable for complying with the requirements of this Act and shall use contractual or other

reasonable means to provide a comparable level of protection while the information is being processed by a third party on its behalf.

(c) Controllers and Processors shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. The designation of an individual by an organization hereunder shall not relieve the organization of any of its obligations under this Act.

(d) Each Controller or Processor should assign a person who is responsible to monitor if entities abide by the law.

(e) Data subjects should be notified about the person assigned under sub-section (c) of this section.

(f) Entities are not relieved from the responsibilities assigned to them under the law even if a person is assigned under sub-section (c) of this section.

Lawfulness of Processing Personal Data

16. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) The data subject has given consent prior to the processing of his/her personal data for one or more specific purposes;

(b) Processing is necessary for the performance and execution of a contract or service to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or service;

(c) Processing is necessary for compliance with a legal obligation to which the Controller is subject;

(d) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller in the field of employment.

(e) Processing relates to personal data which is part of public record pursuant to existing laws, rules and/or regulations,

provided that the purposes for the processing of such personal data is consistent with the purpose for its official publication;

(f) Processing is necessary in order to protect the vital interests of the data subject or of another natural person, including his or her life, health or safety;

(g) Processing is necessary for the performance of a task carried out in the public or national interest, including public health or safety;

(h) Processing is necessary for the provision by a credit bureau of credit reporting services;

(i) Processing is necessary for the establishment, exercise or defence of legal claims, including the provision of legal services;

(j) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Lawfulness of Processing Special Categories of Personal Data

17. The processing of special categories of personal data shall be prohibited except in the following instances:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller in the field of employment;

(c) Processing relates to personal data which is part of public record pursuant to existing laws, rules and/or regulations, provided that the purposes for the processing of such

personal data is consistent with the purpose for its official publication;

(d) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(e) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

(f) Processing is necessary for the performance of a task carried out in the public or national interest, or national security, including public health or safety where there is valid legal basis under applicable to laws, rules, or regulations of Maldives;

(g) Processing is necessary for the establishment, exercise, or defence of legal claims, including the provision of legal services;

Processing of personal data relating to criminal convictions and offences

18. Processing of personal data relating to criminal convictions and offences shall be carried out only under the control of public agency. Any comprehensive register of criminal convictions shall be kept only under the control of public agency.

Consent

19. (a) Where collection and processing is based on consent, the Controller must be able to demonstrate that the data subject has consented to the processing of his/her personal data. It must be time-bound in relation to the declared, specified and legitimate purpose provided to the data subject.

(b) Consent for the collection and processing of personal data shall not be considered valid under this Act unless the relevant data subject has been provided with the information required under Section 23 below prior to the

provision of such consent. Likewise, consent based on false or misleading information or deceptive practices shall not be considered valid.

(c) Consent for the collection and processing of personal data shall not be considered freely given where such consent is made a condition for the provision of a product or service, including the performance of a contract, in relation to personal data that is not reasonable and necessary for the provision of such product or service or the performance of such contract.

Consent by Minors

20. (a) The legal capacity of data subjects to validly provide consent under this Act shall follow existing laws and regulations of Maldives, defining the age of a minor including the lawful representation of minors.

(b) Before processing data of minors, the Controller should ensure that consent have been given as specified in sub-section (a) of this section.

Chapter 4

Rights of Data Subjects

General Provisions

21. (a) Facilitating the rights of data subjects defined in this chapter shall be carried out by the Controller.

(b) The Controller shall facilitate the exercise of data subject rights under this chapter. The Controller shall not refuse to take necessary action based on the request of a data subject for exercising his/her rights under this chapter except for the grounds provided hereunder and unless the Controller demonstrates that it is not in a position to identify the data subject.

(c) The Controller shall provide information on action taken on a request under this chapter to the data subject, including any legal consequences arising from such a

request, without delay and within a reasonable period of time.

(d) Where the Controller does not take necessary action based on the request of the data subject, the Controller shall inform the data subject without delay and within reasonable time, the possibility of lodging a complaint to the Data Protection Authority.

Right to Information

22. (a) Where personal data relating to a data subject are collected, at the time when personal data are obtained, the Controller shall provide the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, with all of the following information.

(1) Sources where personal data is obtained from, other than the data subject, the categories of personal data concerned, as well as the sources of such personal data;

(2) Purposes for which such personal data is to be processed as well as the lawful criteria for processing other than consent relied on by the Controller;

(3) Scope and method of the personal data processing;

(4) The existence of automated decision-making, including profiling, useful information about the meaning involved, as well as the significance and the envisaged consequences of such processing for the data subject;

(5) The recipients or categories of recipients to whom they are or may be disclosed, including whether or not cross-border transfers of personal data are involved;

(6) The identity and contact details of the Controller and the business contact information of at least one

of its designated representatives under Section 19 (c);

(7) The period for which the personal data will be stored; and

(8) The existence of their rights under this Act.

(b) Where the Controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the Controller shall provide the data subject prior to that further processing with information on that other purpose. In such cases, the data subject shall also be given an opportunity to withhold consent to the further processing of his/her personal data.

(c) Notification under this section shall not apply when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the Controller and the data subject, or when the information is being collected and processed as a result of legal obligation.

Right to access personal data

23. (a) The data subject has the right of reasonable access to, the following information upon a written request made by such data subject to the controller.

(1) Personal data about the data subject that is in the possession or under the control of the Controller;

(2) Sources from which personal data was obtained, other than the data subject;

(3) Purposes for which the personal data is collected and processed;

(4) Recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients located outside of Maldives, and the purposes for the disclosure;

(5) The period for which the personal data will be stored;

(6) Information on automated decision-making processes, including profiling, where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his/her personal information concerning the data subject were last accessed and modified;

(8) Information relating to policies and procedures;

(9) The identity and contact details of the Controller and its designated representative.

(b) The data subject's right to access shall cover information spanning at least 1 (one) year from the date of such request.

(c) The controller shall, upon receipt of a written request made by the data subject under the sub-section (a), provide the data subject with such information required to be provided.

(d) Controllers may deny a data subject's request for access under this section if the provision of that personal data or other information could reasonably be expected to:

(1) Threaten the safety or physical or mental health of a natural person other than the data subject who made the request;

(2) Cause immediate or severe harm to the safety or to the physical or mental health of the data subject who made the request;

(3) Reveal personal data about or identify another natural person and the said person does not consent to the disclosure of his identity; or

(4) Be contrary to the national interest or national security.

Right to Object

24. (a) Where the processing of personal data is based on grounds under section 20 , other than consent, the data subject shall have the right to object thereto at any time on substantial grounds. The Controller shall no longer process the personal data unless it is able to demonstrate that the grounds relied on to process personal data under sections 20 exist. Where an objection is denied under this section, the Controller shall document the nature of the objection and the reasons for the denial.

(b) Controllers may process personal data about a data subject collected before the effective date so long for the purposes for which the personal data was collected unless consent for such use is withdrawn in accordance with Section 27.

Right to Rectification

25. (a) The data subject shall, based on sufficient proof, have the right to dispute an inaccuracy, error or omission in the personal data and have the right to request a controller in writing to rectify the personal data relating to such data subject which is either inaccurate or incomplete.

(b) The controller shall, upon such a written request made by the data subject, rectify or complete the personal data without undue delay subject to sub-section (d) of this section.

(c) Where a correction has been made to the personal data under this section, the Controller shall notify and provide third parties to which such personal data was previously disclosed, the corrected personal data within a reasonable period.

(d) Controllers may deny a data subject's request to rectify personal data in respect of matters specified in schedule II. Where a request to rectify personal data has been denied, the Controller shall document the nature of the request and the reasons for the denial.

(d) Nothing in this section shall require a Controller to correct or otherwise alter an opinion, including a professional or an expert opinion.

Right to Withdraw Consent

26. (a) Where collection and processing are based solely on consent, the data subject shall have the right to withdraw his or her consent at any time.

(b) The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

(c) Where the data subject effectively withdraws consent, the Controller shall cease further processing of the personal data.

(d) In the event of withdrawal of consent as specified in sub-section (a) the Controller shall instruct third-party to stop processing related data.

(e) To ensure the right to transfer data, the Controller or a third-party should destroy or return back the data as preferred by the data subject.

Right to Restriction, Suspension or Blocking of Processing

27. (a) The data subject has the right to stop or suspend data processing based on the following:

(1) The accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data;

(2) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(3) The Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims;

(4) The data subject has objected to processing pursuant to Section 25 pending the verification

whether the legitimate grounds of the Controller override those of the data subject.

(b) Where processing has been restricted under paragraph subsection (a), such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. Where the exercise of the right is denied under this section, the Controller shall document the nature of the objection and the reasons for the denial.

(c) If the event that data subject request for the right stated in this article the Controller should record in writing, the nature of the rejection and the reason for the rejection by the data subject.

Right to Erasure

28. (a) The data subject shall have the right to make a written request to the controller for the erasure, removal, or destruction of his or her personal data upon discovery and sufficient proof of any of the following:

(1) Where the processing is based on consent under sections 11 and 12, the data subject withdraws consent and there is no other legal ground for the processing;

(2) The data subject objects to the processing under Section 25, and there are no other legal grounds or overriding legitimate interests for the processing;

(3) The personal data is unlawfully obtained or unlawfully processed;

(4) The personal data is no longer necessary for the purposes for which they were collected; or

(5) The personal data is being used for purposes not authorized by the data subject.

(b) In the event of any state mentioned in sub-section (a) the Controller has the right to reject the request by the data subject to erase or destroy data.

(c) The Controller should keep record in writing the decisions made to reject the requests by the data subject for the requests stated in this article.

(d) The Controller may charge a reasonable fee for repetitive or technically excessive erasure requests.

(e) Retention requirements mandated by law for archiving, national interest, or national security shall take precedence over any erasure request.

Right to Data Portability

29. (a) Where data subject's personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject.

(b) Under this article if data transfer between controller is technically possible and does not require a huge spending by the controller, the data subject had the right to request such data transfer.

Chapter 5

Security of Personal Data

Data Privacy and Security of Personal Data

30. (a) To maintain integrity and secrecy of private data the Controller and Processor should implement reasonable administrative, physical and technical measures to prevent processing, destruction, change or disclosing unlawfully.

(b) The measures stated in sub-section (a) of this article should include preventive measures for data loss without negligence, damage by natural causes, or reaching the data unlawfully or gain access data by deceiving.

(c) In determining the standards for security, consideration shall be given to the type of personal data, potential threats

to individuals if data is compromised, the size and operational complexity of the entity, established best practices at the time, and the resources available for implementing security measures.

Organizational Security Measures

31. Data Protection Authority, may issue from time to time, the organizational measures to be implemented which must include, among others:

(a) The Controller and Processors should assign a data protection officer or compliance officer to ensure and monitor that entities follow the law to safeguard data privacy and security;

(b) To establish procedures of data privacy in entities, Controllers and Processors should prepare data protection process and standards;

(c) Controllers and Processors shall ensure that the processing of personal data adheres to the principles of 'privacy by design' and 'privacy by default', incorporating data protection measures into the design of processing systems and ensuring that, by default, only personal data necessary for each specific purpose are processed;

(d) The process and procedures stated in sub-section (b) of this section entities should include the following.

(1) The procedure of collecting personal data and instances where consent is required the procedures to be followed;

(2) The procedures that will be followed when a system issue or technical issues occur and access to systems;

(3) The process to be followed when requesting for the rights of data subject;

(4) Information storage, erasing of records or destruction time and criteria;

(5) To ensure the law is enforced;

(e) Clear defined activities carried out by the Controllers and Processors should be recorded and filed.

(f) For the record keeping specified in sub-section (e) by Controllers and Processors the following should be considered as minimum requirement

(1) the categories of personal data processed or obtained;

(2) Of the data processed or obtained as above the categories of data subject;

(3) Information about the individuals that the data was collected who the data would be shared. If the data is shared within other Controllers or Processors, if the data would be shared with cross border of the persons;

(4) The process of data collection, processing and retaining followed by the entity and the time frame of information flow in the event of data erase or destruction.

(g) The agents, representative or staff of that are involved in processing the data are when in service or after leaving the service bound by a strict agreement of confidentiality.

(h) Training the staff on process and procedures in protecting privacy is a responsibility of the Controller or Processors.

(i) The qualifications and the responsibilities of the data protection Officers assigned under sub-section (a) must be prescribed in a regulation made under this Act.

Physical Safety Measures

32. Where appropriate, Controllers and Processors shall comply with the following guidelines for physical safety:

(a) Policies and procedures shall be implemented to monitor and limit access to areas where personal data, in whatever media, is processed and stored;

(b) Office spaces and workstations shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

(c) The duties, responsibilities and schedule of personnel involved in the processing of personal data shall be clearly defined and restricted;

(d) Procedures and process implemented to prevent and safeguard damage files and resources

(e) The office environment that the data is processed are protected from natural incidents, power outage and cannot be accessed from outside.

Technical Security Measures

33. The following general technical security measures must be implemented by Controllers and Processors.

(a) An information security policy with respect to the processing of personal data;

(b) Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

(c) The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

(d) Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;

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

(f) A process for regularly testing, assessing, and evaluating the effectiveness of security measures;

(g) Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

Chapter 6

Personal Data Breach Notification

Data Breach Notification

34. (a) The Controller shall notify the I Data Protection Authority, and affected data subjects within seventy (72) hours upon knowledge of a reasonable belief that a personal data breach has occurred and that all of following elements are present: in the event of a personal data breach, a controller shall notify the Data Protection Authority, regarding such personal data breach within 72 (seventy-two) hours upon the receipt of knowledge of or a reasonable belief that a personal data breach has occurred.

(1) That personal data breach involves special categories of personal data or any personal data that may, under the circumstances, be used to enable identity theft or fraud;

(2) That the personal data may have been acquired by unauthorized persons; and

(3) That such unauthorized acquisition is likely to give rise to a real risk of serious harm to affected data subjects.

(b) Depending on the nature of the incident, or if there is delay or failure to notify, the Data Protection Authority, may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

(c) An investigation carried out as stated in sub-section (b) should include the systems in place at the entity and procedures that were followed.

Contents of Notification

35. The notice in regard to data loss should include the following as minimum;

(a) Type of damage,
(b) The type of personal data that was damaged,
(c) Steps taken to control the damage,
(d) Steps taken to minimise the damage or to prevent a bad outcome.

Procedure for Notification

36. The Data Protection Authority, shall issue guidelines covering the procedure for personal data breach management and notification, including additional qualifications requiring notification, grounds for delay in notification, and other reportorial requirements

Chapter 7

Personal Data Transfers To, And/Or Processing By Third Parties

Subcontracting of Personal Data Processing

37. (a) To gather or process information, a contractor can assign a Processor under an agreement.

(b) The Controller shall enter into a contract or agreement with the Processor referred to in sub-section (a) to ensure the confidentiality, security, and integrity of the data, prevent unauthorized use, and ensure compliance with this law, any other relevant laws concerning data privacy, and procedures issued by the Data Protection Authority.

Required Stipulations

38. (a) The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information Controller, and the geographic location of the processing under the subcontracting agreement.

(b) At the minimum, the contract or other legal act shall stipulate, in particular, that the Processor shall:

(1) Process the personal data only upon the documented instructions of the Controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;

(2) Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;

(3) Implement appropriate security measures and comply with this Act and other issuances of the Data Protection Authority;

(4) Not engage another Processor without prior instruction from the Controller: provided that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, considering the nature of the processing;

(5) Assist the Controller, by appropriate technical and organizational measures and to the extent possible, to fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;

(6) Assist the Controller in ensuring compliance with this Act, other relevant laws, and other issuances of the Data Protection Authority, considering the nature of processing and the information available to the personal information Processor;

(7) Notify the Controller regarding security incidents affecting personal data and where necessary, assist the Controller in complying with the requirements of personal data breach notification under this Act, other relevant laws, and other issuances Data

Protection Authority including providing relevant information and support.

(8) Undertake such steps as are reasonably required to mitigate the effects of any breach of privacy or security incident;

(9) At the choice of the Controller, delete or return all personal data to the personal information Controller after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law;

(10) Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information Controller or another auditor mandated by the latter; and

(11) Immediately inform the personal information Controller if in its opinion, an instruction infringes the Act, these rules, or any other issuance of the Data Protection Authority.

Duty of the Processor

39. The Processor shall comply with the requirements of the Act, other applicable laws, and other issuances of the Data Protection Authority, in addition to obligations provided in a contract, or other legal act with a Controller.

Data Sharing

40. (a) Data sharing shall be allowed when it is expressly authorized under sections 11 and 12 of this Act; provided that there are adequate safeguards for data privacy and security, and processing adheres to the principles of transparency, legitimate purpose and proportionality.

(b) Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement

which shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.

(c) The data subject shall be provided with the following information prior to collection or before data is shared:

(1) Identity of the personal information Controllers or personal information Processors that will be given access to the personal data;

(2) Purpose of data sharing;

(3) Categories of personal data concerned;

(4) Intended recipients or categories of recipients of the personal data;

(5) Existence of the rights of data subjects, including the right to access and correction, and the right to object;

(6) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

Guidelines for Data Sharing

41. The Data Protection Authority, shall issue guidelines covering the requirements for legitimate data sharing including the necessary safeguards for data privacy and security.

Transfer of Personal Data Outside Maldives

42. Controllers and Processors may only transfer personal data outside the Maldives if such transfer complies with this Act and the recipient ensures an adequate level of protection, as determined by the Data Protection Authority, based on factors such as the rule of law, respect for human rights, relevant data protection legislation, and the effectiveness of supervisory authorities.

Chapter 8

Cross-Border Transfers

General Principles of Transfers

43. (a) Cross-border data transfers by Controllers shall be carried out in accordance with the conditions specified in this Act.

(b) To ensure the safeguards mentioned in subsection (a), the following measures shall be implemented:

Transfers Subject to Appropriate Safeguards

44. (a) A Controller or Processor may transfer personal data to a jurisdiction outside of the Maldives only if the Controller or Processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(b) To implement the safeguards required in subsection (a), the following measures shall be taken:

(1) The corporate process stated in section 49 that could be implemented.

(2) The agreement signed with cross border entities should include the process of data protection endorsed by the Data Protection Authority.

(c) In data protection referred in sub-section (b) (2) to ensure safety of data should include sections which can be applicable to safeguard the rights of data subjects.

(d) The Data Protection Authority should formulate and implement the process through a regulation made under this Act.

Binding Corporate Rules

45. (a) The Data Protection Authority, may approve binding corporate rules submitted by Controllers or Processors provided such rules:

(1) The structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(2) The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(3) Their legally binding nature, both internally and externally;

(4) The application of the general data protection principles found in Section 9 of this Act, and the requirements in respect of onward transfers to Controllers or Processors bodies not bound by the binding corporate rules under Chapter VII of this Act and Section 50 above;

(5) The rights of data subjects in regard to processing and the means to exercise those rights, including the right to lodge a complaint with the Data Protection Authority, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(6) The acceptance by the Controller or Processor established in the Maldives of liability for any breaches of the binding corporate rules by any member concerned not established or found in the Maldives. Such Controller or the Processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(7) How the information on the binding corporate rules, in particular on the provisions referred to in points (iv) to (vi), of this paragraph is provided to the data subjects in addition to section 17;

(8) The tasks of any Data Protection Officer designated in accordance with this Act or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(9) The complaint procedures;

(10) The mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (viii) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the Data Protection Authority,

(11) The mechanisms for reporting and recording changes to the rules and reporting those changes to the I Data Protection Authority;

(12) The cooperation mechanism with the Data Protection Authority, to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the Data Protection Authority, the results of verifications of the measures referred to in point (viii);

(13) The mechanisms for reporting to the Data Protection Authority, any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(14) The appropriate data protection training to personnel having permanent or regular access to

personal data. The Data Protection Authority, may specify the format and procedures for the exchange of information between the Data Protection Authority for binding corporate rules within the meaning of this Article.

Chapter 9

Investigation and Enforcement

The Right to Complain

46. (a) Any person has the right to lodge a complaint with the Data Protection Authority regarding any alleged infringement of their rights under this Act.

(b) Procedures and process should be defined in the regulation formulated under this Act.

The Right to Investigate

47. (a) If a complaint is filed at Data Protection Authority against an entity or would want to ensure an entity is following the law Data Protection Authority has the right to investigate.

(b) The Data Protection Authority may halt, suspend, or decline to investigate a complaint under the following circumstances:

(1) If an entity is able to prove that it is following the law and directions by the Data Protection Authority;

(2) If both parties of conflict agree to amicably resolve the issue;

(3) If Data Protection Authority establishes that the matter should be investigated by other institutions;

(4) If the complaint is baseless, or a harassment or not in goodwill.

(c) All records related to an investigation carried out should be retained for at least 5 (five) years.

(d) Data Protection Authority have the following rights on investigation carried out

(1) Enter premises to do searches;

(2) Search documents of the entity and make copies of documents ;

(3) Make copies of part or entire document;

(4) Interview personal during search and keep record of the interviews;

(5) Including electronic devices to operate devices within the area of search;

(6) Take pictures and videos of the searched area.

(e) Even if it is stated in sub-section (d) if the owner of the premises refused to be searched such a search should be carried out with a court order.

Power to Review

48. (a) On the application of a complainant, the Data Protection Authority, may review

(1) A refusal to provide access to personal data requested by the complainant, or a failure to provide such access within a reasonable time;

(2) A refusal to correct data or a data is not corrected within reasonable time;

(b) After review as stated in sub-section (a) Data Protection Authority shall make a decision as follows;

(1) The request was declined correctly;

(2) If the request was wrongfully declined, instruct the entity to provide information in a time frame specified by Data Protection Authority.

Power to instruct

49. (a) If in an investigation it is determined that an entity is not following the law Data Protection Authority have the right to instruct the entity to abide by the law

(b) Data Protection Authority has the right to instruct the entity to do the following :

(1) Stop collecting, using or publicizing personal data unlawfully;

(2) Destroy all data gathered unlawfully;

(3) Instruct the entity to follow instruction given to the entity by the Data Protection Authority or explain that the entity has followed the instructions.

(c) Data Protection Authority have the right to publish information about the entities that do not follow instructions given.

Review instructions

50. (a) If an entity or an individual is not happy with the instruction given, they could request in writing to the Minister within 30 (thirty)days of issuing the instruction, to review such instruction.

(b) Procedures and process for such review should be included in a regulation made under this Act.

Correctional powers

51. The following are correctional powers entitled to the Data Protection Authority:

(a) Warn the Controller or Processor if the action carried out is against the law;

(b) Take necessary action if the activity done by the Controller or Processor contradicts, the law;

(c) Instruct the Controller or Processor to abide if a data subject request for a right specified in the law;

(d) Instruct the Controller or Processor to carry out activities within the law and specified time frame;

(e) Instruct the Controller or Processor to inform a data subject if there is a danger to personal information;

(f) Any other situation in addition to what is stated in this article.

The right to issue order

52. If the Data Protection Authority determines that sharing personal data across border is a threat to national security or stability of the society, Data Protection Authority have the right to issue an order to temporarily or permanently stop the data processing.

Power to exemption

53. The Data Protection Authority has the right to exempt an individual or entity or a category from some part of the law on the following situations:

(a) The employees working on an entity

(b) The financials of the entity

(c) Amount of data processed by the entity

Administrative Actions

54. (a) The Data Protection Authority, shall impose administrative penalties, including fines, in addition to any other sanctions prescribed under this chapter. In determining the appropriate fine, the following factors shall be taken into account:

(1) The nature and scope of the unlawful conduct, including the duration of the breach, the extent of data processing, and the harm caused to the data subjects;

(2) Whether the violation was intentional, negligent, or the result of a failure to implement appropriate safeguards;

(3) The steps taken by the Controller or Processor to mitigate the harm suffered by the data subjects as a result of the violation;

(4) The level of responsibility assumed by the Controller or Processor, including any technical and organizational measures;

(5) Any prior breaches of this Act or related regulations by the Controller or Processor;

(6) The degree of cooperation provided by the Controller or Processor to the Data Protection Authority in addressing the breach and minimizing further damage

(7) The category of personal data and the specific groups of data subjects affected by the breach;

(8) The timeliness, accuracy, and completeness of the notifications made by the Controller or Processor to the Data Protection Authority, and the actions taken to remedy the breach;

(9) Whether the Controller or Processor has previously been subject to enforcement action under this chapter, and the extent to which corrective measures from prior enforcement have been implemented;

(10) The financial impact of the breach, including any financial gain realized by the Controller or Processor or the extent of financial damage mitigated by the Controller or Processor following the breach.

(b) If a Controller or Processor violates their obligations under Chapter 5, Chapter 6 (, or Chapter 7, the Data Protection Authority, in addition to administrative measures under sub-section (a), may impose a fine not exceeding MVR 500,000 or up to 4% of the total annual revenue or financial benefit derived from the unlawful conduct, whichever is greater.

(c) For breaches of the following provisions, the Data Protection Authority, in addition to administrative measures under sub-section (a), may impose a fine not exceeding MVR 250,000 or up to 2% of the total annual revenue or financial benefit derived from the unlawful conduct, whichever is greater:

(1) The basic requirements for processing personal data, including consent;

(2) The rights of data subjects;

(3) The requirements for cross-border transfers of personal data,.

(d) Any failure to comply with an order issued by the Data Protection Authority under Article 53, including an order to perform a specific act or to temporarily halt data processing, or any failure to comply with orders issued under Chapter 9, or the failure to adhere to the processes

related to complaint resolution, investigation, or dispute resolution, shall result in additional penalties as prescribed by this chapter.

The right for compensation

55. (a) Every person has the right for compensation for damage caused due to breach of law.

(b) A Controller or a Processor must bear responsibility for any damage caused due to breach of law by them.

(c) A Processor has to take responsibility for unlawful processing done under this law or a regulation of this law or for damage caused due to disobeying instructions given by a Controller.

(d) A Controller or a Processor will only be exempted to take responsibility under sub-section (a) or (b) if they can prove they do not have to responsibility .

(e) Compensation shall be given through the judicial system through the courts.

Chapter 10

Miscellaneous Provisions

Technological Neutrality and Adaptability

56. (a) This Act shall be interpreted and applied in a technologically neutral manner, focusing on the purposes, principles, and outcomes of data protection rather than specific technological means or implementations.

(b) The provisions of this Act shall apply equally to existing and future technologies, processing methods, and data formats, without imposing undue restrictions on technological innovation or advancements in data processing.

(c) The Data Protection Authority shall, at intervals not exceeding three years, review and assess the Act's applicability to emerging technologies and data processing methods, and may issue guidelines or

recommend amendments as necessary to maintain the Act's effectiveness and technological neutrality.

(d) In applying this Act, particular regard shall be given to encouraging the development and use of privacy-enhancing technologies and privacy by design principles, facilitating data protection in all states of data (including but not limited to data at rest, in transit, and in use), and promoting innovative approaches to achieving compliance with the principles set forth in this Act.

Power to Make Regulations

57. Unless otherwise stated, all regulations to be made under this Act shall be made by the Data Protection Authority within 6 (six) months of the commencement of this Act.

Effective Date

58. This Act shall take effect on the date of its publication in the Government Gazette.

Interpretation

59. Unless otherwise stated, in this Act:

(a) **"Automated Decision-Making"** means decisions based solely on automated processing, including profiling, which produces legal effects concerning a data subject or significantly affects the data subject.

(b) **"Business"** includes the activity of any organization, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity;

(c) **"Business contact information"** means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes;

(d) **"Commercial"** means any activity, transaction, act or conduct or any regular course of conduct that is of a commercial character;

(e) **"Controller"** means any individual, company, association, or body, whether corporate or unincorporated, that alone or jointly with others determines the purposes and means of processing personal data;

(f) **"Consent"** refers to any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, through a statement or a clear affirmative action, signify agreement to the processing of personal data relating to them. Consent may be provided by a lawful representative or agent with the authority to act on behalf of the data subject;

(g) **"Credit bureau"** means an individual or organization which provides credit reports for gain or profit; or Provides credit reports on a routine, non-profit basis as an ancillary part of a business carried on for gain or profit;

(h) **"Credit report"** means a communication, whether in written, oral or other form, provided to an organization to assess the creditworthiness of an individual in relation to a transaction between the organization and the individual;

(i) "**Data sharing"** is the sharing, disclosure, or transfer to a third party of personal data under the custody of a Controller to one or more other Controller/s;

(j) **"Data Sharing Agreement" or "DSA"** refers to a legally binding document or contract between personal data Controllers, outlining the obligations, responsibilities, and liabilities of the parties involved in the transfer of personal data, including provisions for adequate safeguards to protect data privacy and security;

(k) **"Data subject"** means an individual whose personal data is processed;

(l) **"Document"** includes information recorded in any form;

(m) **"Domestic"** means related to home or family;

(n) **"Education institution"** means any organization that provides education, including instruction, training or teaching;

(o **"Employment"** includes working under an unpaid volunteer work relationship;

(p) **"Individual"** means a natural person;

(q) **"Investigation"** means an investigation relating to —

(1) a breach of an agreement;

(2) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(3) a circumstance or conduct that may result in a remedy or relief being available under any law;

(r) **"Minister"** means the Minister responsible for Information Technology, unless the context otherwise requires;

(s) **"National interest"** includes national defence, national security, public security, the maintenance of essential services and the conduct of international affairs;

(t) **"Personal data"** means any information, whether in a material form or otherwise, that can directly or indirectly, used in combination with other information, identify or identifiable identity of an individual (data subject);

(u) **"Personal data breach"** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

(v) **"Processor"** includes any natural person, company, association or body of persons, corporate or unincorporated, which processes personal data on behalf of the Controller;

(w) **"Processing"** means the carrying out of any operation or set of operations which is performed on personal data, whether or not by automated means, and includes any of the following:

(1) Collection
(2) Recording;
(3) Storage or holding;
(4) Organization, adaptation or alteration;
(5) Use
(6) Retrieval;
(7) Combination;
(8) Disclosure, dissemination or transmission; or
(9) Erasure or destruction;

(x) **"Profiling"** means any automated processing of personal data to evaluate, analyse or predict aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(y) **"Public agency"** means

(1) The Government of Maldives, including any Ministry, department, agency, or other institution or instrumentality;
(2) Any tribunal appointed under any written law; or
(3) Any other statutory body;

~~(z)~~ **"Special Categories of Personal Data"** includes personal data revealing racial or ethnic origin, political opinions or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation.

(aa) **"Tribunal"** includes a judicial or quasi-judicial body or a disciplinary, an arbitral or a mediatory body.

National Cyber Security Bill

National Cyber Security Bill

Chapter I

Introduction

Introduction and Title

1. (a) This Act provides for a framework to promote the security and resilience of people, processes, technology, and critical infrastructure in the Maldives against cyber threats. It establishes measures to prevent, detect, respond to, and recover from cyber security incidents, while safeguarding the confidentiality, integrity, and availability of critical data and services.

(b) This Act may be cited as the "National Cyber Security Act".

Objective

2. The main objectives of this Act are as follows.

(a) To establish and maintain a comprehensive national cyber security framework for the Maldives, adhering to internationally recognized standards and best practices, in order to protect critical infrastructure, enhance cyber resilience, and support secure digital transformation;

(b) To create and empower the National Cyber Security Agency as the central authority responsible for coordinating and implementing national cyber security initiatives, including the development of national capabilities, promotion of cyber awareness, and fostering of public-private collaboration; and

(c) To facilitate the Maldives' participation in international cyber security efforts and implementation of relevant conventions, while preserving national sovereignty and

independence, thereby enhancing the country's cyber security posture and supporting economic growth and national development.

Scope of application

3. (a) This act applies to cyber security activities in the country.

(b) Chapter 3 applies to any critical infrastructure located wholly or partly in Maldives.

Administration and Enforcement

4. This Act shall be administered and enforced as set out in this Act.

Chapter II
NATIONAL CYBER SECURITY AGENCY

National Cyber Security Agency

5. (a) The National Cyber Security Agency hereinafter referred as "the Agency") is established upon commencement of this Act. Agency is a legal entity, able to sue and be sued, having the right to acquire and own property, to deal in credit, and to obtain proceeds from such properties, and which will determine procedures and policies for planning and organizing all matters relating to securing of cyberspaces in the Maldives, and will do everything necessary to enforce all matters in this Act.

(b) the Agency is not part of the Maldives Civil Service.

(c) the Agency shall be governed under the supervision of the Minister.

(d) The Ministry responsible for finance shall provide the Agency with additional funds from the annual budget approved by the People's Majlis in order for the CEO to undertake the functions and responsibilities set forth herein.

(e) To allocate additional funds to the Agency in the state budget, as per clause (d), the CEO shall submit the details to the Ministry of Finance in accordance with the Financial Act and its Regulation,.

(f) The salary, benefits, and other allowances to such employees of Agency and its supporting committees shall be determined by the Ministry of Finance with the counsel of the CEO.

(g) Upon the establishment of the Agency under this Act, and prior to commencement of this Act, all property and utilities which were designated to, the budget allocated by the Parliament to, all responsibilities, obligations, rights and benefits incurred under law

and agreements by, and the staff of the National Centre for Information Technology's Security Operations Centre and any other national cyber security related function, shall be transferred to the Agency.

Functions of the Agency

6. The objectives of the Agency are to:

(a) Develop and implement cyber security policies, regulations, and standards across all sectors in the Maldives.

(b) Establish and maintain national capabilities for cyber incident detection, prevention, response, and recovery.

(c) Oversee the implementation of cyber security measures by operators of critical infrastructure and cyber security service providers.

(d) Foster the development of a resilient national cyber security ecosystem and digital economy, including promotion of research and innovation.

(e) Establish mechanisms for cross-sector engagement on matters of cyber security for effective co-ordination and co-operation between key public institutions and the private sector.

(f) Improve cyber security awareness on cyber security matters among the public and private sectors as well as citizens;

(g) To lead collaboration with international agencies and establish cooperation for the promotion of cyber security and/or other relevant fields for the country; and

(h) To provide expert advice to the government on cyber security strategies and policies to safeguard national interests in cyberspace, including the development and maintenance of a national cyber security strategy.

Responsibilities of the Agency

7. the Agency shall execute the following responsibilities.

(a) Provide policy and technical guidance and support to the government and other public entities on all issues pertaining to national cyber security.

(b) Increase the security of the nation's computer networks, computers and data by empowering owners and operators.

(c) Operate a National Security Operations Centre (SOC) and Cyber Security Incident Response Team (CSIRT) to monitor and respond to cyber security threats within and outside the country.

(d) Establish cyber security codes of practice and standards for cyber security and keep track of how owners of critical infrastructure and services in the public and private sectors are adhering to them.

(e) Establish standards for certifying cyber security products or services.

(f) Take measures in response to cyber security incidents that occur within and outside the country which may threaten

(1) National security.

(2) The economy of the country.

(3) International relations between the State and other countries.

(4) Health of the public.

(5) The safety of life and property; and

(6) any other sectors of the country likely to be affected by a cyber security incident.

(g) Identify and designate critical infrastructure and services and advise the Minister on the regulation of owners of critical infrastructure to protect the critical infrastructure of the country and services, in accordance with national objectives and consistent with international best practices.

(h) Supplying technical assistance to law enforcement and security organizations in their pursuit of cyber offenders.

(i) Promote the protection of people, process and technology their by promoting a culture of responsible digital citizenship.

(j) Issue licenses and establish standards for the provision of cyber security services.

(k) Support technological advancements and research and development in cyber security to ensure a resilient and sustainable digital ecosystem.

(l) Deploy strategies to implement research findings towards promoting the country's cyber security.

(m) Establish and maintain a framework for disseminating information on cyber security.

(n) Submit periodic reports on the state of cyber security in the country to the Minister.

(o) Educate the public on matters related to cybercrime and cyber security.

(p) Build the capacity of people in the public or private sector in matters related to cyber security.

(q) Collaborate with law enforcement agencies to intercept or disable a digital technology service or product whose operation undermines the cyber security of the country within the national legal framework.

(r) Establish and maintain a national register of the following;

(1) Identified potential risks.

(2) the levels and impact of risks.

(3) owners of critical infrastructure; and

(4) any other persons licensed or accredited to carry out cyber security activities.

(s) Perform any other functions which are ancillary to the objects of the Agency.

conflicts of interest and ethics

8. (a) The members of the Board and staff of The Agency shall, shall act impartially and free from influence in carrying out all their responsibilities and in making decisions in the implementation of this Act.

(b) If the Agency considers or decides whether any member or employee has a personal interest or benefit or role, such person shall not participate in the consideration or decision of such matter to any extent. The member or employee shall refrain from considering the matter or making any necessary decisions with respect to it upon becoming aware of such interest or benefit or role, even if there is no prior knowledge of the matter.

(c) No board member or employee of the Agency shall accept any gift or benefit of any kind in his own name or in the name of any person with whom he has a family or personal or business relationship in such a way as to rely on any person in the performance of his duties under this Act.

(d) Information received by the board members and employees of the Agency in their capacity shall be kept confidential. Such information shall not be disclosed to any person except to the person required to disclose it as permitted by law.

Immunity from Civil Liability for Actions Taken in Good Faith

9. A member of the Board or an employee of The Agency shall enjoy immunity from civil liability for actions taken or omitted to be taken in good faith in the performance of the functions of The Agency.

Agency's board

10. (a) The Agency shall be governed by a board consisting of the following members appointed by the President.

(1) The Minister responsible for the Ministry mandated with the functions relating to the technology;

(2) The Minister responsible for Ministry mandated with the functions of homeland security;

(3) The Minister responsible for the Ministry mandated with national defence force and national security;

(4) National Security Advisor;

(5) Chief of Defence Force;

(6) Commissioner of Police;

(7) Attorney General.

(b) The President shall appoint the Minister responsible for the Agency as the chairperson of the Board.

Functions of the Board

11. The Board shall, subject to the provisions of this Act,

(a) Have strategic oversight responsibility for The Agency;

(b) Ensure the Agency's activities align with national priorities and international best practices;

(c) Endorse the annual budget and approve significant regulations, investments and expenditures as defined in the Agency's financial policy;

(d) Provide strategic guidance on matters of national security and national interest.

Tenure of office for the members of the Board

12. (a) A member of the Board shall hold office for a period of 5 (five) years and is eligible for re-appointment.

(b) Subsection (a) does not apply to the CEO.

(c) A member of the Board, may, at any time, resign from office in writing addressed to the President.

(d) The President may, by a letter addressed to a member, revoke the appointment of the member.

(e) Where a member of the Board is, for a sufficient reason, unable to act as a member, the Minister shall determine whether the inability may result in the declaration of a vacancy.

(f) Where there is a vacancy, due to any of the reasons stated below, the Minister shall notify the President of the vacancy and the President shall, subject to section 10, appoint a person to fill the vacancy for the unexpired term.

(1) as a result of a declaration under subsection; or

(2) by reason of the death of a member.

Meetings of the Board

13. (a) The Board shall meet quarterly for the conduct of business at a time and place determined by the chairperson.

(b) The chairperson shall, at the request in writing of not less than one-third of the membership of the Board, convene an extraordinary meeting of the Board, at a time and place determined by the chairperson.

(c) The chairperson shall preside over meetings of the Board and in the absence of the chairperson, a member of the Board, other than the CEO, elected by the members present from among their number shall preside.

(d) Matters before the Board shall be decided by the majority of the members present and voting and in the event of an equality of votes, the person presiding shall have a casting vote.

(e) The Board may co-opt a person to attend a meeting of the Board, but that person shall not vote on any matter for decision at the meeting.

(f) The validity of any proceedings of the Board shall not be affected by a vacancy among the members of the

Board or by a defect in the appointment or qualification of a member.

(g) The Board shall, subject to this section, formulate a regulation stipulating the procedure to be followed in conducting board meetings, the secretariat of the board and other administrative matters including meeting invitations, notification of absence and minutes of the meeting.

Granting of Leave

14. (a) Under a policy determined by the Board, the Minister shall grant leave to the CEO.

(b) Under a policy determined by the Board, the Chair shall grant leave to other members of the Board.

Disclosure of Interest

15. (a) A member of the Board who has an interest in a matter for consideration by the Board

(1) shall disclose in writing the nature of that interest and the disclosure shall form part of the record of the consideration of the matter; and

(2) is disqualified from being present at or participating in the deliberations of the Board in respect of that matter.

(b) Where a member contravenes subsection (a), the chairperson shall inform the President in writing to revoke the appointment of the member.

(c) Without limiting any further cause of action that may be instituted against the member, the Board shall recover any benefit derived by a member who contravenes subsection (a).

Allowances

16. (a) The salary and other allowances of the Chair and the members of the board shall be determined by the President.

(b) The salary and other allowances provided to the employees of the Agency shall be determined by the Ministry of Finance and Treasury with the counsel of the CEO.

Appointment of Chief Executive Officer (CEO)

17. (a) The President shall appoint a CEO for The Agency, with the recommendation of the board.

(b) The CEO will be appointed for a period of 5 (five) years. The President may renew the tenure of the CEO for an additional 5 (five) years.

(c) The CEO shall hold office on the terms and conditions specified in the letter of appointment.

(d) A person is qualified for appointment as a CEO if that person is/has

(1) a Maldivian citizen not holding a dual passport;

(2) attained the age of 35;

(3) possession of a Master's Degree in Information Technology or a related field with a minimum of 10 (ten) years of experience in digital leadership roles;

(OR)

possession of a Doctor of Philosophy (PhD) related to cyber security and a minimum of 5 years of experience in digital leadership roles;

(e) Prior to appointment, the CEO will undergo a process of security clearance from both Maldives Police Service and the Maldives National Defence Force.

(f) The CEO will be a accountable to the Minister.

Functions of the Chief Executive Officer (CEO)

18. (a) The CEO is responsible for the day-to-day administration and management of The Agency and is answerable to the Board in the performance of functions under this Act.

(b) The CEO is responsible for the implementation of the decisions of the Board.

(c) The CEO may delegate a function to an officer of The Agency but shall not be relieved of the ultimate

responsibility for the performance of the delegated function.

(d) The CEO may appoint a secretary to the board to

(1) Arrange the business of the board

(2) Keep the minutes of the meetings and decisions of the Board in the form required by the Board.

(3) Perform any other functions that the Board or the CEO may direct.

(e) The CEO may, by legislative instrument, make Regulations to provide for:

(1) the forms for applications;

(2) authorizations and licenses;

(3) the use of equipment to intercept or disable a digital technology service or product by authorized persons to execute an interception warrant;

(4) accreditation of cyber security professionals and practitioners;

(5) the operationalization of a platform for cross-sector engagement on matters of cyber security for effective co-ordination and cooperation between key public institutions and the private sector;

(6) the promotion and development of cyber security to ensure a secured and resilient digital ecosystem;

(7) certification of cyber security products and technology solutions;

(8) implementation of early warning system;

(9) receipt of complaints by the National Cyber Incident Response Team from Sectoral Computer Emergency Response Focal Points, citizens, and other similar international bodies;

(10) the modalities for

(a) the preservation of data; and

(b) the retention of data.

(11) dispute resolution.

(12) any other matters necessary for the effective implementation of this Act.

Vacancy of Office of the CEO

19. The office of the CEO may be considered vacant solely for cause, following 3 (three) consecutive unapproved absences from Board meetings, contingent upon a fair and transparent inquiry conducted by the Board, with the President making the final decision based exclusively on the inquiry's documented findings and confirmation that due process has been fully observed.

Administrative penalties for contraventions

20. (a) The Agency shall, for the purpose of imposing an administrative penalty under this Act, take into account:

(1) the size of the service provider concerned.

(2) the criticality of the sector.

(3) the impact of the contravention; and

(4) any other relevant criterion determined by the Board

(b) The imposition by the Agency, of a fine stipulated in this Act for an offence specified herein, shall not bar the imposition of additional criminal penalties under the Maldives Penal Code for acts which constitute criminal offences under the Maldives Penal Code.

Accounts and Audit

21. (a) The Agency shall keep books, records, returns and other documents relevant to the accounts in the form approved by the Auditor- General.

(b) The Board shall submit the accounts of The Agency to the Auditor-General for audit at the end of the financial year.

(c) The Auditor-General shall, within six months after the end of the immediately preceding financial year,

audit the accounts and forward a copy each of the audit report to the Minister and the Board.

(d) The financial year of The Agency is the same as the financial year of Government.

Annual Report and other reports

22. (a) The Board shall, within thirty days after the receipt of the audit report, submit an annual report to the Minister covering the activities and operations of The Agency for the year to which the annual report relates.

(b) The annual report shall include:

(1) the report of the Auditor-General.

(2) a list of entities granted licenses and accreditation in the year to which the annual report relates.

(3) the number and outcome of production orders and interception warrants issued under this Act in the year to which the annual report relates; and

(4) the report of the Chief Cyber Security Officer attached as a separate report.

(c) The Minister shall, within thirty days after the receipt of the annual report, submit the report to Parliament with a statement that the Minister considers necessary.

(d) The Board shall submit to the Minister any other report which the Minister may require in writing.

International Cooperation

23. (a) The Agency shall in the performance of the functions of The Agency, lead the promotion of the security of cyberspace through international co-operation.

(b) All bilateral agreements relating to cyber security shall be endorsed by the Board of the Agency.

(c) The Agency shall implement relevant measures for the effective implementation and enforcement of international treaties on cybercrime and cyber security, of which Maldives is a signatory.

(d) For the purposes of international co-operation, The Agency shall designate and maintain a 24/7 contact point as defined in subsection (36)(a).

(e) The 24/7 contact point shall provide assistance in respect of

(1) technical advice to other contact points.

(2) the expeditious preservation of data and evidence.

(3) information on the detection of suspects and related matters

(4) the immediate transmission of legal requests in accordance with applicable laws and treaties; and

(5) any other matter related to paragraphs (1) to (4).

Establishment of Committees

24. (a) The Board may establish committees consisting of members of the Board and non-members or both, to perform a function of the Board.

(b) A committee of the Board composed of members and non-members shall be chaired by a member of the Board.

(c) A committee of the Board composed of non-members only shall be advisory.

(d) Section 15 applies to a member of a committee of the Board.

Divisions of the Agency

25. (a) The Board shall establish divisions of The Agency that are necessary for the efficient and effective performance of the functions of the Agency.

CHAPTER III

NATIONAL CYBER SECURITY INCIDENT RESPONSE TEAM (MV-CSIRT)

Establishment of the Maldives Cyber Security Incident Response Team (MV-CSIRT)

26. The Agency shall establish The Maldives Cyber Security Incident Response Team (MV-CSIRT) as a division of the Agency.

Functions of Maldives Cyber Security Incident Response Team (MV-CSIRT)

27. The functions of the Maldives Cyber Security Incident Response Team (MV-CSIRT) include the following:

(1) responding to and managing cyber security incidents;

(2) co-coordinating responses to cyber security incidents amongst public institutions, private institutions and international bodies;

(3) conducting thorough analyses to understand the incident's cause, impact, and effectiveness of the response;

(4) raising awareness about cyber security best practices and providing training to government employees, enhancing aspect of cyber defence;

(5) overseeing the Sectoral Computer Emergency Response Focal Point established under section 29.

Responsibility of The Agency relating to response to cyber security incidents

28. (a) The Agency shall implement the relevant technical measures to ensure an effective cyber security incident monitoring and response system.

(a) Without limiting subsection (b), a technical measure aimed at ensuring an effective cyber security incident monitoring and response system shall include an interception

capability to execute an interception warrant authorized by a Court.

(b) For the purposes of subsection (c), The Agency shall intercept, disable or take-down a digital technology, digital service or a digital product that is likely to undermine the cyber security of the country.

Sectoral Cyber Emergency Response Focal Point (SCERFP)

29. (a) For the purposes of achieving an effective cyber security incident co-ordination, The Agency shall, by notice published in the Gazette, establish Sectoral Computer Emergency Response Focal Points to

(1) collect and collate cyber security incidents; and

(2) co-ordinate responses to cyber security incidents within the sectors.

(b) The Agency shall, in establishing a Sectoral Computer Emergency Response Focal Point, take into account factors including

(1) the needs and criticality of a sector; and

(2) developments in respect of cyber security in the country.

(c) The Agency shall accredit and oversee the operation of Sectoral Computer Emergency Response Focal Points.

(d) A Sectoral Computer Emergency Response Focal Point shall submit to The Agency, through the administrative head of that Sectoral Computer Emergency Response Focal Point, a monthly report covering the operations of that Sectoral Computer Emergency Response Focal Point based on a reporting template determined by The Agency.

(e) A notice published under subsection (a) shall state the relevant requirements including the

(1) reporting obligation of the Sectoral Computer Emergency Response Focal Point concerned and the penalty for non-compliance; and

(2) adherence to risk management protocols.

(f) For the purposes of this section, "sector" includes the

(1) Banking, Finance & Production;

(2) Utilities & Public Infrastructure;

(3) Health & Education; and

(4) any other sector determined by The Agency.

Duty to report cyber security incidents

30. (a) A person in charge of an institution shall report a cyber security incident or event having an actual adverse effect on the security of network and information system to the relevant Sectoral Computer Emergency Response Focal Point or the National Cyber Incident Response Team within a period of not more than twenty-four hours after the incident is detected.

(b) A Sectoral Computer Emergency Response Focal Point shall report a cyber security incident to the National Cyber Incident Response Team.

(c) An institution or an individual licensed by the Agency to provide cyber security services shall report a cyber security incident to the relevant Sectoral Computer Emergency Response Focal Point or the Cyber Security Incident Response Team

within a period of not more than twenty-four hours after the incident is detected.

(d)

Cyber Security incident point of contact

31. (a) The Agency shall, establish a cyber security incident point of contact to facilitate

(1) reporting of a cyber security incident by the general public; and

(2) international co-operation in cyber security matters.

(b) An institution that is not affiliated to a designated Sectoral Computer Emergency Response Focal Point, shall report a cyber security incident to the National Cyber Incident Response Team through the cyber security incident point of contact established under subsection (a).

(c) An individual may report a cyber security incident to the National Cyber Incident Response Team through the cyber security incident point of contact established under subsection (a).

CHAPTER IV

CRITICAL INFRASTRUCTURE

Designation of Critical Infrastructure

32. (a) The Agency shall designate a computer system or computer network as a critical infrastructure if the Agency considers that the computer system or computer network is essential for

(1) national security, or

(2) The continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Maldives.

(3) The economic and social well-being of citizens.

(b) Where the Agency designates a computer system or computer network as a critical infrastructure, the Agency shall publish the designation in the Gazette.

(c) The Agency shall, in making a determination under subsection (a), consider if the computer system or computer network is necessary for

(1) The security, defence or international relations of the country.

(2) The production, preservation or identity of a confidential source of information related to the enforcement of criminal law.

(3) The provision of services directly related to

(1) Communications and telecommunications infrastructure;

(2) Banking and financial services.;

(3) Public utilities;

(4) Public transportation;

(5) Public key infrastructure; and

(6) Any other systems or assets designated by the Agency as critical due to their essential role in sustaining national and societal functions.

(4) The protection of public safety and public health, including systems related to essential emergency services.

(5) an international business or communication affecting a citizen of Maldives or any other international business in which a citizen of Maldives or the Government has an interest; or

(6) the Legislature, Executive, Judiciary, Public Services or security agencies.

(d) The Agency shall, lay down the procedure for the regulation of a critical infrastructure, in the regulation made under this Act.

Registration of critical infrastructure

33. (a) The Agency shall maintain a register of critical infrastructures designated under section 32 of this Act.

(b) The Agency shall, stipulate the following in the regulation made under this Act.

(1) the requirements for the registration of a critical infrastructure;

(2) the procedure for the registration of a critical infrastructure; and

(3) any other matter relating to the registration of a critical infrastructure.

(c) Where there is any change in the legal ownership of a registered critical infrastructure, the owner of the registered critical infrastructure shall, within 30 (thirty days) after the change, inform The Agency of the change in ownership.

Withdrawal of designation of critical infrastructure

34. The Agency may, with the counsel of the Board and by informing the designated owner of the critical infrastructure, withdraw the designation of a critical infrastructure at any time if the Agency considers that

the computer system or computer network no longer satisfies the criteria of a critical infrastructure.

Management and compliance audit of critical infrastructure

35. (a) The Agency shall with the counsel of the Board, prescribe minimum standards for prohibitions in respect of the general management of a critical infrastructure that the Minister considers necessary for the protection of national security.

(b) The Agency shall mandate regular security audits on critical infrastructure, to be conducted by certified third-party cybersecurity firms accredited and licensed by the Agency.

Duty of owner of critical infrastructure

36. (a) An owner of a critical infrastructure shall

(1) report a cyber security incident to the relevant Sectoral Computer Emergency Response Focal Point or the National Cyber Incident Response Team, in the case of a critical infrastructure that does not belong to a Sectoral Computer Emergency Response Focal Point, within 24 (twenty-four) hours after the incident is detected;

(2) cause an audit to be performed on a critical infrastructure; and

(3) submit a copy of the audit report to The Agency.

(b) An owner of a critical infrastructure who contravenes clause (a) of this section, shall , based on the severity of the violation, be subject to corrective measures imposed by The Agency, this may include,

administrative corrective directives, financial penalties, or referral for criminal investigation. The Agency shall determine the appropriate course of action, considering the impact of the non-compliance on national security, public welfare, and the integrity of critical infrastructure.

Unauthorised access to critical infrastructure

37. (a) A person shall not without authorization, secure access, or attempt to secure access to a computer system or a computer network designated as a critical infrastructure.

Guidelines

38. The Agency shall publish guidelines that the Agency considers necessary for

(a) the identification of critical infrastructure.

(b) the registration of critical infrastructure.

(c) the protection of critical infrastructure.

(d) the management of critical infrastructure.

(e) access to, transfer and control of data in critical infrastructure.

(f) the storage or archiving of data or information in critical infrastructure.

(g) reporting incidents involving critical infrastructure; and

(h) any other matter required for the adequate protection of critical infrastructure.

Directives relating to Critical Infrastructure

39. (a) The Agency may issue directives to an owner of a critical infrastructure, a cyber security service provider or service provider for the purpose of ensuring the cyber security of the country.

CHAPTER V

CYBER SECURITY STANDARDS

Licensing Cyber Security Service Providers

40. (a) The Agency shall issue licenses to cyber security service providers in the Maldives.

(b) The requirements for the licensing shall be laid down in the regulation made under this Act.

Application for Cyber Security Service Provider License

40. (a) Cyber security service providers shall apply to the Agency for license.

(b) The application shall be made in the prescribed form and accompanied by the

(1) supporting documentation, and

(2) prescribed fee, that The Agency may determine.

(c) The Agency shall within 14 (fourteen) days of receipt of an application, acknowledge receipt of the application.

Grant of license

41. (a) The Agency must ensure the following:

(1) the applicant meets the requirements of The Agency for the grant of a license, and

(2) the grant of a license is not against public interest.

(b) the Agency shall, within 30 (thirty) days of receipt of an application for a license, inform the applicant in writing of the decision of the Agency.

(c) A license granted by The Agency is subject to the terms and conditions specified in the license.

(d) Where The Agency refuses to grant a license, The Agency shall within 28 (twenty-eight) days after the refusal communicate in writing the reason for the refusal to grant the license.

(e) The Agency shall publish the grant of a license under this section in the Gazette.

Non transferability of license

42. (a) An entity granted a license shall not transfer that license to another entity..

Validity and duration of license

43. (a) A license granted under this Act is valid for 2 (two) years from the date that the license is granted.

(b) A licensed cyber security service provider who intends to continue operations as a cyber security service provider shall, not later than one month before the expiration of the license, apply in writing to The Agency for a renewal of the license.

Suspension of license

44. (a) The Agency may suspend a license issued under this Act for a period of not more than 6 (six) months where:

(1) the licensee fails to renew the license not later than one month before the expiration of the license; or

(2) the licensee fails to comply with a condition specified in the license.

(b) The Agency shall, before exercising the power of suspension under this section,

give the licensee 30 (thirty) days' notice in writing of the intention to do so, and

specify in the notice the grounds on which The Agency intends to suspend the license.

(c) Where The Agency decides to suspend a license, The Agency shall give the licensee the opportunity

to submit to The Agency, within the time specified by The Agency, a written statement of objections, if any, to the suspension of the license; and

to remedy, within the time specified by The Agency, the breach which has

occasioned the decision to suspend the license.

(d) The Agency shall, within 28 (twenty-eight) days of the suspension of a license, notify the cyber security service provider concerned of the suspension.

Revocation of license

45. (a) The Agency may revoke a license issued under this Act if The Agency considers that

(1) the license has been obtained by fraud or misrepresentation.

(2) the licensee has ceased to carry on the business for which the licensee is licensed.

(3) a circumstance existed at the time the license was granted or renewed that The Agency was unaware of, which would have prevented The Agency from granting or renewing the license of the licensee if The Agency had been aware of the circumstance at that time.

(4) the licensee has been declared bankrupt or has gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction.

(5) the licensee no longer meets the requirements for holding the license; or

(6) it is not in the public interest for the licensee to continue to carry on the business of a licensee.

(b) Subsections (c) and (d) of section 44 apply to revocation of a license.

(c) The Agency shall publish the revocation of a license under this section in the Gazette.

Accreditation of cyber security professionals and practitioners

46. The Agency shall establish a mechanism for the accreditation of cyber security professionals and practitioners.

Certification of cyber security products and technology solutions

47. The Agency shall establish a mechanism for the certification of cyber security products and technology solutions.

Review of decisions of the National Cyber Security Agency

48. (a) A person aggrieved by a decision of The Agency may, within 28 (twenty-eight) days of receipt of the decision, submit a complaint in writing to the Board for a review of the decision.

(b) A person dissatisfied with the decision of the Board may, within 28 (twenty-eight) days after the date of receipt of the decision, submit a complaint in writing to the Minister for a review of the decision of the Board.

(c) A person dissatisfied with the decision of the Minister may, within 28 (twenty-eight) days after the date of receipt of the decision, seek redress in a court of competent jurisdiction.

Cyber Security Risk Register

49. (a) The Agency shall establish and maintain an electronic Cyber security Risk Register for the country.

(b) The Register shall contain details of the

(1) Name and contact information of the entity that manages the critical infrastructure.

(2) identified and potential risks; and

(3) Level of impact of risk.

(c) Information contained in the Register shall not be disclosed to any person other than an employee of The Agency who is responsible for keeping the Register.

(d) Despite subsection (c), The Agency may disclose information contained in the Register if required by law.

Cyber Security Standards and Enforcement

50. (a) The Agency shall without imposing or discriminating in favour of the use of a particular type of technology, encourage, develop, establish and adopt standards for cyber security in :

(1) Education and skills development.

(2) Hardware and software engineering.

(3) Governance and risk management.

(4) Research and development; and

(5) Practitioners in any other relevant area that The Agency may determine in accordance with international best practice.

(b) The Agency shall publish on the website of The Agency, the standards developed and promote the adoption of the standards by a Sectoral Computer Emergency Response Focal Point, a licensed service provider, an institution or any other relevant person.

(c) The Agency shall take the necessary measures to enforce the cyber security standards adopted and monitor compliance by the public and private sectors with the cyber security standards.

Research and development program

51. (a) The Agency shall

(1) develop and implement a research and development program to promote the development of cyber security in the country.

(2) develop a qualification and competency framework for

(a) persons offering training in cyber security programs; and

(b) educational institutions offering cyber security programs.

(3) develop or implement technology solutions to mitigate existing and emerging cyber security threats and vulnerabilities to ensure the cyber security of the country; and

(4) collaborate with academic research centers and other relevant institutions within and outside the country, for the development and implementation of cyber security research and development programs for the country.

(b) Contents of research and development of cyber security comprise:

(1) Establishment of systems of cyber security protective software and equipment.

(2) Methods of evaluating whether cyber security software and equipment satisfy standards, and minimizing the existence of security vulnerabilities or weaknesses, and malware.

(3) Methods of checking whether the hardware and software which is provided in fact functions properly.

(4) Methods of protecting State secrets, work-related secrets, business secrets, personal secrets, family secrets and private life [personal privacy], and the capability of maintaining confidentiality when

transmitting information in cyberspace.

(5) Determination of the sources of information transmitted in cyberspace.

(6) Resolution of cyber security threats.

(7) Establishment of the network range and the cyber security testing environment.

(8) Technical initiatives increasing cyber security awareness and skills.

(9) Cyber security forecasts.

(10) Practical research and theoretical development of cyber security.

(c) Relevant agencies, organizations and individuals have the right to research and develop cyber security.

Chapter VI

Miscellaneous

Commencement

52. This Act shall come into effect, on the date of publication in the Government Gazette.

Definitions

53. Unless there is any other interpretation of the declaration or otherwise in this Act, the following terms are defined as the following.

(a) "Agency" means, the National Cyber Security Agency established under this section (6) of this Act.

(b) "Minister" means the minister responsible for the Ministry mandated with the functions relating to the ICT.

(c) "Board" means, the Agency's governing board established under section (11) of this Act.

(d) "Chair" means, the Board's Chair or anyone temporarily performing the responsibilities of

the Chair appointed under section (11) of this Act.

(e) "CEO" means, the Agency's CEO or anyone working in that capacity appointed under.

(f) "Content data" means the communication content of the communication, that is, the meaning or purport of the communication, or the message or information being conveyed by the communication other than traffic data.

(g) "Cyberspace" refers to the global, interconnected domain consisting of digital infrastructures, including but not limited to the internet, telecommunications networks, computer systems, embedded processors, control systems, and databases. It encompasses the interactions between individuals, organizations, and automated entities facilitated by software, services, and devices, in a virtual environment not constrained by physical boundaries, where social, economic, and operational activities are conducted.

(h) "Traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication or the type of underlying service;

(i) "Service Provider" includes

(1) a public or private entity that provides users of the service of the entity, the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and

(2) an entity that processes or stores computer data on behalf of a communication service or a user of a communication service;

(3) an entity that provides services including data and content delivered or executed in full by a technical system involving

i. computer time;

ii. computer output;

iii. data processing and;

iv. the storage or retrieval of a program or data through multiple platforms and devices such as web or a mobile device;

(j) "Subscriber" means a customer or a user of an electronic communications network, electronic communications service or broadcasting service;

(k) "Subscriber Information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of the services of a service provider other than traffic or content data and by which may be established

(1) the type of communication service used, the technical provisions taken in respect of the communication service and the period of service;

(2) the identity, postal or geographic address, telephone and other access number of the subscriber, billing and payment information available on the basis of the service agreement or arrangement; and

(3) any other information on the site of the installation of a communication equipment, available on the basis of the service agreement or arrangement;

(l) "Child" refers to a child as defined in Article 4 of the Child Protection Act

(m) "Network and Information System" means:

(1) an electronic communications network, which includes transmission systems and, where applicable, switching or routing equipment and other resources that permit the conveyance of signals by wire, radio, optical, or other electromagnetic means. This includes satellite networks, fixed networks (circuit-switched and packet-switched, including the Internet), mobile terrestrial networks, electricity cable systems used for transmitting signals, and networks used for radio, television broadcasting, and cable television, regardless of the type of information conveyed; or

(2) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(3) digital data stored, processed, retrieved or transmitted by elements covered under points (1) and (2) for the purposes of their operation, use, protection and maintenance;

(n) "Cyber threat" means: any potential circumstance or event, including but not limited to actions by individuals, groups, or entities, that may exploit vulnerabilities in information systems or networks to cause harm or disruption by compromising the confidentiality, integrity, or availability of data or systems, whether through deliberate malicious acts or unintentional incidents.

(o) “Critical Infrastructure” means: the systems, networks, assets, and services, whether physical, digital, or hybrid, that are indispensable for the national security, economic stability, public health, or safety of a nation. This includes, but is not limited to, sectors such as energy, water, healthcare, transportation, finance, communications, and government operations. CI also encompasses future technologies and evolving systems. Any disruption, failure, or compromise of such infrastructure would result in significant detrimental effects on the functioning of society, with particular emphasis on cross-sector dependencies and the need for resilience across these essential services.