PARLIAMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

PERSONAL DATA PROTECTION ACT, No. 9 OF 2022

[Certified on 19th of March, 2022]

Printed on the Order of Government

Published as a Supplement to Part II of the **Gazette of the Democratic Socialist Republic of Sri Lanka** of March 25, 2022

PRINTED AT THE DEPARTMENT OF GOVERNMENT PRINTING, SRI LANKA
TO BE PURCHASED AT THE GOVERNMENT PUBLICATIONS BUREAU, COLOMBO 5

Price : Rs. 75.00 **Postage : Rs. 45.00**

This Act can be downloaded from www.documents.gov.lk

Personal Data Protection Act, No. 9 of 2022

[Certified on 19th of March, 2022]

L.D.—O. 19/2019.

AN ACT TO PROVIDE FOR THE REGULATION OF PROCESSING OF PERSONAL DATA; TO IDENTIFY AND STRENGTHEN THE RIGHTS OF DATA SUBJECTS IN RELATION TO THE PROTECTION OF PERSONAL DATA; TO PROVIDE FOR THE ESTABLISHMENT OF THE DATA PROTECTION AUTHORITY; AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH OR INCIDENTAL THERETO

Preamble

WHEREAS it has become necessary to facilitate the growth and innovation in the digital economy in Sri Lanka whilst ensuring the protection of personal data rights of the data subjects:

AND WHEREAS it has become necessary to improve interoperability among personal data protection frameworks as well as to strengthen cross-border co-operation among personal data protection enforcement authorities:

AND WHEREAS it has become necessary for the government of Sri Lanka to provide for a legal framework to provide for mechanisms for the protection of personal data of data subjects ensuring consumer trust and safeguarding privacy whilst respecting domestic written laws and applicable international legal instruments:

NOW THEREFORE BE it enacted by the Parliament of the Democratic Socialist Republic of Sri Lanka as follows: -

Short Title and date of operation

1. (1) This Act may be cited as the Personal Data Protection Act, No. 9 of 2022.

(2) The provisions of this section, shall come into operation on the date on which the certificate of the Speaker is endorsed in respect of this Act in terms of Article 79 of the Constitution.

(3) All other provisions of this Act except the provisions of Part IV and Part V, shall come into operation on such date as the Minister may, appoint by Order published in the *Gazette*, which shall be a date not earlier than eighteen months and not later than thirty six months from the date of the certificate of the Speaker referred to in subsection (2).

(4) The date of operation of the provisions of Part IV of this Act, shall be a date not earlier than twenty-four months and not later than forty-eight months from the date of certificate referred to in subsection (2).

(5) The date of operation of the provisions of Part V of this Act shall be a date appointed by the Minister by Order published in the *Gazette* which shall be a date not later than the date appointed by the Minister under subsection (3).

Application of this Act

2. (1) This Act shall apply to the processing of personal data—

(*a*) where the processing of personal data takes place wholly or partly within Sri Lanka; or

(*b*) where the processing of personal data is carried out by a controller or processor who–

(i) is domiciled or ordinarily resident in Sri Lanka;

(ii) is incorporated or established under any written law of Sri Lanka;

(iii) offers goods or services to data subjects in Sri Lanka including the offering of goods or services with specific targeting of data subjects in Sri Lanka; or

(iv) specifically monitors the behaviour of data subjects in Sri Lanka including profiling with the intention of making decisions in relation to the behavior of such data subjects in so far as such behaviour takes place in Sri Lanka.

(2) For the purposes of paragraphs (iii) and (iv) of subsection (1) respectively, the Authority may, determine by way of rules made under this Act–

(*a*) the circumstances in which the specific targeting of the data subjects may occur; or

(*b*) the circumstances in which the specific monitoring of the data subjects may occur.

(3) This Act shall not apply to–

(*a*) any personal data processed purely for personal, domestic or household purposes by an individual; and

(*b*) any data other than personal data.

The provisions of this Act to prevail in case of any inconsistency

3. (1) 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 authority is governed by any other written law, it shall be lawful for 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.

(2) 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.

PART I

PROCESSING OF PERSONAL DATA

Compliance with the data protection obligations

4. Every controller shall process personal data in compliance with the obligations specified under this Act.

Obligation to process personal data in a lawful manner

5. The processing of personal data shall be lawful if a controller is in compliance with—

(*a*) any condition specified in Schedule I hereto;

(*b*) any condition specified in Schedule II hereto in the case of processing special categories of personal data;

(*c*) all the conditions specified in Schedule III hereto in the case of processing personal data based on the consent of the data subject under item (*a*) of Schedule I or under item (*a*) of Schedule II hereto; or

(*d*) all the conditions specified in Schedule IV hereto in the case of processing personal data in respect of criminal investigations.

Obligation to define a purpose for personal data processing

6. (1) Every controller shall, ensure that personal data is processed for a—

(*a*) specified;

(*b*) explicit; and

(*c*) legitimate,

purposes and such personal data shall not be further processed in a manner which is incompatible with such purposes.

(2) Subject to the provisions of section 10 of this Act, further processing of such personal data by a controller for archiving purposes in the public interest, scientific research, historical research or statistical purposes shall not be considered to be incompatible with the initial purposes referred to in paragraphs (a), (*b*) and (*c*) of subsection (1).

Obligation to confine personal data processing to the defined purpose

7. Every controller shall ensure that personal data that is processed shall be—

(*a*) adequate;

(*b*) relevant; and

(c) proportionate,

to the extent as is necessary in relation to the purpose for which such data shall be collected or processed.

Obligation to ensure accuracy

8. Every controller shall ensure that personal data that is processed shall be—

(*a*) accurate; and

(*b*) kept up to date,

with every reasonable step being taken to erase or rectify any inaccurate or outdated personal data, without undue delay.

Obligation to limit the period of retention

9. Every controller shall ensure that personal data that is being processed shall be kept in a form which permits identification of data subjects only for such period as may be necessary or required for the purposes for which such personal data is processed:

Provided however, subject to the provisions of section 10 of this Act, a controller may store personal data for longer periods in so far as the personal data shall be processed further for archiving purposes in the public interest, scientific research, historical research or statistical purposes.

Obligation to maintain Integrity and confidentiality

10. Every controller shall ensure integrity and confidentiality of personal data that is being processed, by using appropriate technical and organizational measures

including encryption, pseudonymisation, anonymisation or access controls or such other measures as may be prescribed so as to prevent the –

(*a*) unauthorized or unlawful processing of personal data; or

(*b*) loss, destruction or damage of personal data.

Obligation to process personal data in a transparent manner

11. A controller shall, provide data subjects—

(*a*) the information referred to in Schedule V; and

(*b*) the information regarding any decision taken pursuant to a request made under PART II of this Act,

in writing or by electronic means and in a concise, transparent, intelligible and easily accessible form.

Accountability in the processing of personal data

12. (1) It shall be the duty of every controller to implement internal controls and procedures, (hereinafter referred to as the "Data Protection Management Programme") that—

(*a*) establishes and maintains duly catalogued records to demonstrate the manner in which the implementation of the data protection obligations referred to in sections 5, 6, 7, 8, 9, 10 and 11 are carried out by the controller;

(*b*) is designed on the basis of structure, scale, volume and sensitivity of processing activities of the controller;

(*c*) provides for appropriate safeguards based on data protection impact assessments specified in section 24;

(*d*) is integrated into the governance structure of the controller;

(*e*) establishes internal oversight mechanisms;

(*f*) has a mechanism to receive complaints, conduct of inquiries and to identify personal data breaches;

(*g*) is updated based on periodic monitoring and assessments; and

(*h*) facilitates the exercise of rights of data subjects under sections 13, 14, 15, 16 and 18,

for the purpose of complying with the obligations referred to in sections 5, 6, 7, 8, 9, 10 and 11.

(2) The Authority shall from time to time issue such guidelines in respect of the Data Protection Management Programme.

PART II

RIGHTS OF DATA SUBJECTS

Right of access to personal data

13. (1) Every data subject shall have the right to access to personal data of such data subject and to be provided with a confirmation as to whether such personal data has been processed and such information referred to in Schedule V, upon a written request made by such data subject to the controller.

(2) The controller shall, upon receipt of a written request made by the data subject under subsection (1), provide the data subject with such information required to be provided under Schedule V, subject to section 17.

Right of withdrawal of the consent and the right to object to processing

14. (1) Every data subject shall have the right to withdraw his consent at any time upon a written request made by such data subject if such processing is based on the grounds specified in item (*a*) of Schedule I or item (*a*) of Schedule II of this Act:

Provided that, the withdrawal of such consent shall not affect the lawfulness of any processing taken place prior to such withdrawal.

(2) Every data subject shall have the right to request a controller in writing, to refrain from further processing of personal data relating to such data subject, if such processing is based on the grounds specified in items (*e*) or (*f*) of Schedule I or item (*f*) of Schedule II.

Right to rectification or completion

15. Every data subject shall have the right to request a controller in writing to rectify or complete the personal data relating to such data subject which is either inaccurate or incomplete, and the controller shall, upon such a written request made by the data subject, rectify or complete the personal data without undue delay subject to the provisions of section 17:

Provided however, the provisions of this section shall not impose any obligation on a controller to collect and process any additional personal data that is not required for the purpose of processing:

Provided further, where a controller is required to maintain personal data for the evidentiary purposes under any written law or on an order of a competent court, the controller shall refrain from further processing such personal data without rectifying.

Right to erasure

16. Every data subject shall have the right to make a written request to the controller to have his personal data erased, under the following circumstances where–

(*a*) the processing of personal data is carried out in contravention of the obligations referred to in sections 5,6,7,8,9,10 and 11;

(*b*) the data subject withdraws his consent upon which the processing is based, in accordance with item (*a*) of Schedule I or item (*a*) of Schedule II;

(*c*) the requirement to erase personal data is required by any written law or on an order of a competent court to which the data subject or controller is subject to.

Grant or refusal of rectification, completion, erasure or refrain from further processing

17. (1) Where a controller receives a written request from a data subject under sections 13, 14, 15 or 16, such controller shall inform the data subject in writing, within twenty-one working days from the date of such request, whether–

(*a*) such request has been granted;

(*b*) such request has been refused under subsection (2) and the reasons thereof unless such disclosure is prohibited by any written law; or

(*c*) the controller has refrained from further processing such personal data under sections 14(2) or 15 and reasons thereof,

and inform the availability of the right of appeal to the data subject in respect of the decisions made by the controller under paragraphs (*b*) or (*c*).

(2) The controller may, refuse to act on a request made under sections 13, 14, 15 or 16 of this Act, by a data subject having regard to–

(*a*) the national security;

(*b*) public order;

(*c*) any inquiry conducted, investigation or procedure carried out under any written law;

(*d*) the prevention, detection, investigation or prosecution of criminal offences;

(*e*) the rights and freedoms of other persons under any written law;

(*f*) subject to the provisions of subsection (4), the technical and operational feasibility of the controller to act on such request;

(*g*) subject to the provisions of subsection (4), the inability of the controller to establish the identity of the data subject; or

(*h*) the requirement to process personal data under any written law.

(3) A controller shall, record the reasons for any refusal under subsection (2) and submit such records to the Authority upon a written request from the Authority.

(4) Where a controller is unable to establish the identity of a data subject making a request under sections 13, 14, 15 or 16, such controller may, request the data subject to provide additional information to enable the controller to carry out such requests.

(5) Any right conferred on a data subject under this Part may be exercised–

(*a*) where the data subject is a minor, by parents or a person who has the parental authority over the minor or who has been appointed as his legal guardian; or

(*b*) where the data subject is physically or mentally unfit, by a person who has been appointed as his guardian or administrator by a Court; or

(*c*) by a person duly authorized in writing by the data subject to make a request under this Part except in the cases referred to in paragraphs (*a*) and (*b*); or

(*d*) an heir to exercise a deceased data subject's rights within a period of ten years from the date of demise of such data subject,

in the manner prescribed by regulations.

(6) A request made by a data subject under sections 13, 14, 15 or 16 may be accompanied by such fees, as may be prescribed by regulations made under this Act.

(7) Where a fee is charged under subsection (6), the controller shall inform the data subject the details of such fees and reasons for imposing same.

Automated individual decision making

18. (1) Subject to section 19, every data subject shall have the right to request a controller to review a decision of such controller based solely on automated processing, which has created or which is likely to create an irreversible and continuous impact on the rights and freedoms of the data subject under any written law.

(2) The provisions of subsection (1) shall not apply where a decision of a controller, based on automated processing is–

(*a*) authorized by any written law, which a controller is subject to;

(*b*) authorized in a manner determined by the Authority;

(*c*) based on the consent of the data subject; or

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

and the controller shall comply with such measures and applicable criteria as may be specified by the Authority by rules made in that behalf to safeguard the rights and freedoms of the data subject:

Provided however, the requirement under paragraph (*d*) shall not apply to special categories of personal data.

Right of appeal of the data subjects to the Authority and the process of determination of such appeal

19. (1) Where a controller–

(*a*) has not refrained from further processing of personal data under section 14; or

(*b*) has refused to rectify or complete personal data under section 15; or

(*c*) has refused to erase personal data under section 16; or

(*d*) has refused the request of the data subject under section 17(2); or

(*e*) has refused the request to review a decision based solely on automated processing under section 18(1),

the data subject may, appeal against such decision in the form, manner and within such period of time as may be prescribed.

(2) The Authority may determine whether the –

(*a*) decision of the controller not to refrain from further processing of personal data under section 14 was lawful;

(*b*) decision of the controller to refuse to rectify or complete personal data under section 15 was lawful;

(*c*) decision of the controller to refuse the erasure of personal data under section 16 was lawful;

(*d*) refusal under section 17(2) by the controller was lawful;

(*e*) refusal to review a decision based solely on automated processing under section 18(1) was lawful.

(3) After concluding the necessary investigations, the Authority shall determine, within such period as may be prescribed, whether the appeal is allowed or disallowed and the Authority shall inform the data subject and the controller the determination with reasons thereof.

(4) Where the Authority allows the appeal under subsection (2), the controller shall take steps to give effect to the decision of the Authority, within such period as may be determined by the Authority, and the controller shall inform the data subject and the Authority, the steps taken to give effect to its decision.

(5) Any data subject or controller aggrieved by the decision of the Authority, may prefer an appeal to the Court of Appeal not later than thirty days from the date of such decision.

PART III

CONTROLLERS AND PROCESSORS

Designation or appointment of the Data Protection Officer

20. (1) Every controller and processor shall designate or appoint a Data Protection Officer, to ensure compliance with the provisions of this Act, in the following circumstances:–

(*a*) where the processing is carried out by a ministry, government department or public corporation, except for judiciary acting in their judicial capacity; or

(*b*) where the core activities of processing carried out by the controller or processor consist of the following:–

(i) operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a scale and magnitude as may be prescribed; or

(ii) processing of special categories of personal data on a scale and magnitude as may be prescribed; or

(iii) processing which results in a risk of harm affecting the rights of the data subjects protected under this Act based on the nature of processing and its impact on data subjects.

(2) A Data Protection Officer shall possess relevant academic and professional qualifications as may be prescribed which may include academic background, knowledge and technical skills in matters relating to data protection having competency and capacity to implement strategies and mechanisms to respond to inquiries and incidents related to processing of personal data.

(3) Where the controller is a group of entities, such controller may appoint a single Data Protection Officer who is easily accessible by each entity. Where a controller or a processor is a Public Authority, a single Data Protection Officer may be designated for several such public authorities, taking into account their organizational structures.

(4) A controller or processor shall publish the contact details of the Data Protection Officer and communicate such details to the Authority.

(5) The responsibility of the Data Protection Officer shall be to–

(*a*) advise the controller or processor and their employees on data processing requirements provided under this Act or any other written law;

(*b*) ensure on behalf of the controller or processor that the provisions of this Act are complied with;

(*c*) facilitate capacity building of staff involved in data processing operations;

(*d*) provide advice on personal data protection impact assessments; and

(*e*) co-operate and comply with all directives and instructions issued by the Authority on matters relating to data protection.

Additional obligations of a controller

21. (1) Where processing is to be carried out by a processor on behalf of a controller, the controller shall–

(*a*) use only processors who ensure the provision of appropriate technical and organizational measures to give effect to the provisions of this Act and ensure the protection of rights of the data subjects under this Act; and

(*b*) ensure that such processor is bound by a contract or provisions of any written law which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of the data subjects and the obligations of the controller.

(2) Where two or more controllers jointly determine the purposes and means of processing, such controllers shall be referred to as "joint controllers" who shall be jointly responsible for discharging the obligations stipulated under this Act.

Additional obligations of the processors

22. (1) Where a processor is engaged in processing activities on behalf of the controller, the processor shall–

(*a*) ensure that processing activities are carried out only on the written instructions of the controller;

(*b*) ensure that its personnel are bound by contractual obligations on confidentiality and secrecy by the implementation of appropriate technical and organizational measures;

(*c*) facilitate the controller to carry out compliance audits, including inspections upon the written request of the controller, taking into account the nature of processing and the information available to the processor; and

(*d*) upon the written instructions of the controller, erase existing copies of personal data or return all personal data to the controller after the completion of the provisions of services relating to processing.

(2) Where a processor fails to comply with the provisions of paragraph (*a*) of subsection (1) or determines the purposes and means of processing by itself, such processor shall, for the purposes of this Act be deemed to be a controller, in respect of such processing.

(3) Where a processor engages another processor (hereinafter referred to as the "sub processor") for carrying out specific processing activities, the provisions of this section shall apply to and in relation to such sub processor.

(4) Where a sub processor fails to fulfil its obligations under subsection (3), the processor shall be liable to the controller for the performance or carrying out of the obligations of such sub processor.

(5) For the purposes of this section "personnel" means any employee, consultant, agent, affiliate or any person who is contracted by the processor to process personal data.

Personal Data breach notifications

23. (1) In the event of a personal data breach, a controller shall notify the Authority, regarding such personal data breach in such form, manner and within such period of time as may be determined by rules made under this Act.

(2) The Authority shall provide for–

(*a*) the circumstances where the Authority shall be notified of such data breach;

(*b*) the circumstances where the affected data subject shall be notified; and

(*c*) the form, and manner of making such notification, and information which shall be provided in such notification relating to the data breach,

by way of rules made under this Act.

Personal data protection impact assessments

24. (1) Where a Controller intends to carry out any processing which involves–

(*a*) a systematic and extensive evaluation of personal data or special categories of personal data including profiling;

(*b*) a systematic monitoring of publicly accessible areas or telecommunication networks; or

(*c*) a processing activity as may be determined by way of rules taking into consideration the scope and associated risks of that processing,

such controller shall, prior to such processing, carry out a personal data protection impact assessment in a form and manner as may be prescribed, to ascertain the impact of the intended processing on the obligations imposed on the controller under Part I of this Act and the rights of data subjects under Part II of this Act.

(2) The personal data protection impact assessment shall contain such information and particulars including any measures and safeguards taken by the controller to mitigate any risk of harm caused to the data subject by the processing referred to in subsection (1).

(3) The controller shall seek the assistance of the Data Protection Officer, where designated, when carrying out a personal data protection impact assessment under subsection (1).

(4) The controller shall conduct a fresh personal data protection impact assessment in accordance with this section whenever there is any change in the methodology, technology or process adopted in the processing for which a personal data protection impact assessment has already been carried out.

(5) The controller shall submit to the Authority, the personal data protection impact assessment required under this section and, on written request made by the Authority, provide any other information, for the purpose of making an assessment on the compliance of the processing and in respect of any risks of harm associated with the protection of personal data of the data subject and of the related safeguards recommended by the Authority.

Measures to mitigate risks of harm and the requirement for prior consultation

25. (1) Where a personal data protection impact assessment carried out under section 24 indicates that the processing is likely to result in a risk of harm to the rights of the data subjects guaranteed under this Act or any written law, a controller shall take such measures to mitigate such risk of harm, prior to any processing of personal data.

(2) Where a Controller, despite having taken measures under subsection (1), is not able to mitigate such risks of harm to the data subject, such controller may consult the Authority prior to such processing.

(3) Upon such consultation, the Authority may issue written instructions to the controller requiring him to take additional measures to mitigate any risk of harm to the data subject or to cease such processing.

(4) Where the controller consults the Authority under subsection (2), the controller shall provide additional information as may be requested by the Authority.

(5) Where the controller fails to comply with the instructions of the Authority without any reasonable cause, such controller shall contravene the provisions of this Act.

(6) For the avoidance of doubt it is declared that when processing of personal data referred to in items (*b*), (*f*), (*g*) and (*h*) of Schedule II, such processing shall be considered to have provided such measures and appropriate safeguards to protect the rights of the data subjects required under Schedule II.

(7) Notwithstanding anything to the contrary in any other written law, whenever the controller engages in processing of personal data referred to in section 24(1) and where such processing is carried out by a controller in relation to national security, public order and public health, the controller shall consult the Authority.

Cross-border data flow

26. (1) Where a public authority process personal data as a controller or processor, such personal data shall be processed only in Sri Lanka and shall not be processed in a third country, unless the Authority in consultation with, that controller or processor as the case may be and the relevant regulatory or statutory body, classifies the categories of

personal data which may be permitted to be processed in a third country, prescribed by the Minister pursuant to an adequacy decision made under subsection (2).

(2) (*a*) For the purpose of making an "adequacy decision", the Minister shall, in consultation with the Authority take into consideration the relevant written law and enforcement mechanisms relating to the protection of personal data in a third country and the application of the provisions of Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of this Act, and such other prescribed criteria relating to the processing of personal data, in a third country for the purpose of cross border data flow.

(*b*) Any adequacy decision made by the Minister under this subsection shall–

(i) be subject to periodic monitoring of the developments in a third country that may affect such decisions and the Minister may review such decision at least every two years; and

(ii) remain in force until amended or revoked by the Minister in consultation with the authority.

(3) A controller or processor other than a public authority may process personal data–

(*a*) in a third country prescribed pursuant to an adequacy decision; or

(*b*) in a country, not being a third country prescribed pursuant to an adequacy decision, only where such controller or processor as the case may be, ensures compliance with the respective obligations imposed under Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of this Act.

(4) For the purpose of ensuring compliance under paragraph (*b*) of subsection (3), a controller or processor

shall adopt such instruments as may be specified by the Authority to ensure binding and enforceable commitments of the recipient in the third country to ensure appropriate safeguards to the rights of the data subjects and remedies protected by this Act.

(5) In the absence of any adequacy decision pursuant to subsection (2) or appropriate safeguards pursuant to subsecion (4), a controller or processor other than a public authority may process personal data outside Sri Lanka if–

(*a*) the data subject has explicitly consented to the proposed processing of personal data outside Sri Lanka, after having been informed of the possible risks of such processing for the data subject due to the absence of an adequacy decision and appropriate safeguards; or

(*b*) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of any pre contractual measures taken by the controller at the request of the data subject; or

(*c*) the transfer is necessary for the establishment, exercise or defence of legal claims relating to the data subject; or

(*d*) the transfer is necessary for reasons of public interest as defined in item (g) of Schedule I of this Act; or

(*e*) the transfer is necessary to respond to an emergency that threatens the life, health, or safety of the data subject or another person and where the data subject or his legal guardian is physically or legally incapable of giving consent; or

(*f*) such processing is permitted under any other conditions as may be prescribed under this Act.

PART IV

USE OF PERSONAL DATA TO DISSEMINATE SOLICITED MESSAGES

Solicited messages to data subjects by controllers

27. (1) Subject to section 14, a controller may use postal services, telecommunication services, electronic means or any other similar means for the purposes of disseminating messages only if a data subject has given consent to receive such messages (hereinafter referred to as "solicited messages").

(2) For the purpose of subsection (1), consent shall be obtained by a controller in accordance with the conditions of Schedule III of this Act.

(3) When obtaining a consent under subsection (1), the controller shall, at the time of collecting contact information and each time where a message is sent, provide to the data subject details on how to opt-out of receiving solicited messages free of charge.

(4) A controller using postal, electronic, telecommunication or any other similar means to disseminate any solicited message, shall inform the data subjects, to whom such messages are intended, of the nature of the message and the identity of the controller or third party on behalf of whom the message is disseminated by the controller.

(5) The Authority may, in consultation with the relevant regulatory or statutory body, determine by way of rules made under this Act, any code or prefix that controllers shall adopt in order to identify different categories of solicited messages.

(6) For the purpose of this section, a "message" includes any written, electronic, oral, pictorial, or video message, that is intended to promote–

(*a*) goods or services of a controller or any third party; or

(*b*) any person, entity or organisation including the controller,

using postal, electronic or telecommunication services or any other similar methods, including the use of automated calling and communication systems with or without human intervention, other than any internet based advertisements to which a data subject has consented to obtain a service, free of charge from the controller.

PART V

DATA PROTECTION AUTHORITY

Establishment of the data Protection Authority

28. (1) There shall be established an authority which shall be called the Data Protection Authority of Sri Lanka (in this Act referred to as the "Authority") for the purposes of this Act.

(2) The Authority shall, by the name assigned to it by subsection (1), be a body corporate and shall have perpetual succession and a common seal and may sue and be sued in such name.

Constitution of the Board of Directors

29. (1) The administration, management and control of the affairs of the Authority shall be vested in a Board of Directors (in this Act referred to as the "Board").

(2) The Board shall, for the purpose of administering the affairs of the Authority, exercise, perform and discharge the powers, duties and functions conferred on, assigned to or imposed on, the Authority by this Act.

(3) The Board shall consist of not less than five members and not more than seven members appointed by the President from among persons who have reached eminence and proven

professional expertise in the fields of engineering, medicine, banking and finance, telecommunications, Law and persons who have experience in different sectors such as public utilities, business process outsourcing (BPO), logistics, Insurance, banking and financial sectors, of whom at least two members shall have prior experience in the public sector entities.

(4) The persons appointed to the Board shall also have experience and knowledge in regulatory matters, privacy and data protection, information security, data science, data analytics, economics, finance, information technology or related fields.

(5) The provisions of Schedule VI to this Act, shall have effect in relation to the disqualifications and grounds for removal, resignation, leave or absence, and term of office of members of the Board and meetings, and seal of the Authority.

Chairperson of the Board

30. (1) The President shall appoint one of the members who has demonstrated effective leadership qualities in public or private sector entities to be the Chairperson of the Board.

(2) The Chairperson may resign from his office by letter addressed to the President and such resignation shall be effective from the date on which it is accepted by the President.

(3) The President may, for reasons assigned therefor remove the Chairperson from the office of the Chairperson.

(4) Subject to the provisions of subsections (2) and (3), the term of office of the Chairperson shall be the period of his membership of the Board.

(5) Where the Chairperson is temporarily unable to exercice, perform and discharge the powers, duties and functions of his office due to ill health, other infirmity, absence from Sri Lanka or any other cause, the President may oppoint any other member to act as the Chairperson in addition to his normal duties as a member.

Objects of the Authority

31. The objects of the Authority shall be–

(*a*) to regulate the processing of personal data in accordance with the provisions of this Act;

(*b*) to safeguard the privacy of the data subjects from any adverse impact arising from the digitalization of the procedures and services in the public and private sector;

(*c*) to provide for mechanisms to ensure the protection of personal data of data subjects engaged in digital transactions and communications;

(*d*) to ensure the regulatory compliance with the provisions of this Act to facilitate for the growth and innovation in digital economy.

Powers of the Authority

32. The Authority may exercise the following powers, for the purpose of performing duties and discharging functions under this Act:–

(*a*) to carry out whether directly or through any officer, agent, entity or institutions authorized in that behalf by the Authority, all such matters as may be necessary for the implementation of the provisions of this Act;

(*b*) to take all such steps to ensure that controllers and processors carry out their duties and obligations in accordance with the provisions of this Act and inspect any information held by a controller or a processor in order to ensure the performance of his duties and obligations;

(*c*) to direct a controller or a processor to take steps to comply with the provisions of this Act, including the requirement to publish terms and conditions subject to which and the manner in which processing activities are carried out;

(*d*) to direct a controller or any relevant data protection officer to reimburse fees charged from a data subject for failure to provide the required information in a timely manner;

(*e*) to conduct inquiries, receive complaints, require any person to appear before it, make directives and impose fines in accordance with the provisions of this Act;

(*f*) to examine a person under oath or affirmation and require such person where necessary to produce any information relating to the processing of functions of a controller or processor in the manner prescribed, for the purpose of discharging the functions of this Act;

(*g*) to enter into the premises of any controller or processor and inspect or seize records and carry out investigations where the Authority has reasonable grounds to believe that processing poses an imminent risk to the rights of the data subjects;

(*h*) to carry out periodical evaluations into the manner in which and procedures used for any processing activities carried out by a controller or processor, including the data protection management programme;

(*i*) to appoint advisory committees consisting of members whose qualifications, experience and powers and duties shall be as prescibed;

(*j*) to recognize certification and certifying bodies in relation to personal data protection;

(*k*) to enter into agreements with or engage in any activity, either alone or in conjunction with other apex government or regulatory institutions or international agencies or organizations, responsible for data protection outside Sri Lanka for the purposes of this Act;

(*l*) to acquire, take and hold any property movable or immovable which may become vested in it or by virtue of any purchase, grants, gifts or otherwise and to sell, mortgage, lease, grant, convey, device, assign, exchange or dispose of, any such movable or immovable property;

(*m*) to employ such officers and staff including consultants and advisors subject to such terms and conditions of employment to serve as experts as the Authority may consider appropriate for the Authority to discharge its functions;

(*n*) with the concurrence of the Minister assigned the subject of Finance, to pay such remuneration and other benefits and to establish provident funds or pension schemes as may be determined by the Authority for the benefit of its staff and officers, consultants or advisors with whom a contract of employment or service is entered into by the Authority as the case may be;

(*o*) to invest its funds in such manner as the Authority may deem necessary;

(*p*) to open, operate and close bank accounts;

(*q*) to establish standards in relation to data protection and data storage, data processing, obtaining consent and such other matters as may be necessary for the proper implementation of the provisions of this Act;

(*r*) to receive grants, gifts or donations whether from local or foreign sources:

Provided however, the Authority shall obtain prior written approval of the Department of External Resources of the Ministry of the Minister to whom the subject of Finance is assigned, in respect of all foreign grants, gifts or donations;

(*s*) to make rules and issue guidelines and directives in respect of the matters for which rules, guidelines and directives are required to be made or issued under this Act; and

(*t*) to do any other acts as may be necessary or conducive to the attainment of the objects of the Authority under this Act.

Duties and functions of the Authority

33. For the purpose of carrying out its objects, the Authority shall, perform and discharge all or any of the following duties and functions:–

(*a*) direct controllers to comply with the provisions of sections 11 and 13 in accordance with the information set out in Schedule V hereto;

(*b*) monitor and examine all data processing operations to ensure the due compliance by controllers or processors, of the obligations imposed on such controllers or processors under this Act, either of its own motion or at the request of a data subject;

(*c*) issue directives to any specific controller or processor regarding any processing activity performed by such controller or processor;

(*d*) facilitate or undertake training, based on international best practices, for controllers and processors to ensure the effective implementation of the provisions of this Act;

(*e*) issue directives to ensure effective implementation of data protection management programmes by the controllers;

(*f*) promote transparency and self-regulation among controllers and processors;

(*g*) ensure domestic compliance of data protection obligations under international conventions;

(*h*) recommend to the Government on all matters relating to data protection;

(*i*) represent the Government internationally on matters relating to data protection with the approval of the Minister;

(*j*) promote studies and educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities;

(*k*) manage technical co-operation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or inter-governmental organisations, on its own behalf or on behalf of the government;

(*l*) carry out functions conferred on the Authority under any other written law;

(*m*) undertake research into the use and impact of new technologies on processing of personal data;

(*n*) make rules governing the sharing of personal data between controllers which are public authorities, in accordance with the provisions of this Act, where such data can be shared between the controllers via a secure interoperability platform, including setting in place criteria mandating the sharing of personal data between controllers thereby restricting the duplication of collection and storage of data already available with another controller;

(*o*) appoint advisory committees to formulate sectoral guidelines, rules and to identify criteria and define categories of processing by controllers or processors requiring a licence for the purpose of regulating identity management and related services provided to data subjects under any written law;

(*p*) make rules in relation to the use of special categories of personal data, the use of personal data for the dissemination of solicited messages, in complience with section 27, the use of personal data for profiling of individuals, the use of personal data for automated decision making; and

(*q*) perform such other acts not inconsistent with the provisions of this Act or any other written law, as are necessary for the promotion of the objects of the Authority under this Act.

Authority may issue licences

34. (1) The Authority may, issue licences to controllers or processors requiring a licence based on the recommendations of the advisory committee, for the purpose of regulating identity management and related services provided to data subjects under any written law.

(2) The recommendations of the advisory committee shall identify criteria and define categories of processing by controllers or processors requiring a licence.

(3) The categories, criteria, terms and conditions, form and duration, procedure for application, renewal, suspension, cancellation, relating to such licences, appeal against the refusal, suspension or cancallation of licence and fees to be charged may be prescribed.

(4) The Authority may, review and monitor the compliance of such controllers or processors with applicable terms and conditions of such licences.

Directives made by the Authority

35. (1) Where on receipt of a complaint or otherwise, the Authority has reason to believe, that any controller or processor–

(*a*) is engaged in, or is about to engage in any processing activity in contravention of this Act; or

(*b*) has contravened or failed to comply with or is likely to contravene or, fails to comply with the provisions of this Act or any rule under paragraph (*d*), (*e*) or (*f*) of section 52, any regulation, guideline or Order made under this Act or under any other written law relating to the processing of personal data,

the Authority may, conduct an inquiry in accordance with the procedure as may be prescribed.

(2) The Authority may, after giving an opportunity to the controller or processor to be heard at any inquiry under subsection (1), issue a directive to the controller or processor requiring such controller or processor within such time as may be prescribed–

(*a*) to cease and refrain from engaging in, the act, omission or course of conduct related to processing; or

(*b*) to perform such acts as in the opinion of the Authority are necessary to rectify the situation; or

(c) to make a payment of such sum of money as compensation as determined by the Authority to an aggrieved person who has suffered harm, loss or damage as a result of any contravention by a controller or processor under subsection (1).

(3) Every directive issued to such controller or processor under this section shall be in writing and be communicated to such controller or processor to whom it is directed by registered post, electronic communication or other similar means determined by the Authority, and such directive shall be binding on such controller or processor, who shall comply with such directive from the date of such communication.

PART VI

DIRECTOR-GENERAL AND THE STAFF OF THE AUTHORITY

Appointment of the Director-General

36. (1) The Board shall appoint a Director-General of the Authority who have achieved eminence and the proven professional expertise in providing leadership to public sector or private sector.

(2) The Director-General shall be the chief executive officer of the Authority and the conditions of employment including remuneration of the Director-General shall be determined by the Board by way of rules.

(3) The Board shall not appoint any person as the Director-General of the Authority, if such person-

(*a*) has been previously found guilty of serious misconduct by a court or tribunal or has been subject to a disciplinary action by a regulatory body;

(*b*) has been previously dismissed from office; or

(*c*) has committed a breach of the provisions of this Act, or regulations, rules or directives made thereunder.

(4) The Director-General shall, subject to the general direction and control of the Board, be charged with the direction of the affairs and transactions of the Authority, the exercise, performance and discharge of its powers, duties and functions, and the administration and control of the officers and employees of the Authority.

(5) The Board may remove the Director-General appointed under subsection (1), from office having regard to any one of the following reasons:–

(*a*) the likelihood of any confict of interests in carrying out his duties or functions for the Authority;

(*b*) that person becomes of unsound mind or incapable of carrying out his duties or functions;

(*c*) that person is guilty of serious misconduct in relation to his duties or functions; or

(*d*) that person is involved in any activity which may interfere with his independence in discharging his duties or functions or not complied with the general directions of the Board:

Provided that, the Board shall grant an opportunity to the Director-General of being heard prior to such removal.

Staff of the Authority

37. (1) Nothwithstanding anything to the contrary in any other written law, the Authority may create cadre positions and employ officers and employees as it considers necessary for the efficient discharge of its functions and may fix their salaries and wages or other remuneration, benefits and pensions of such officers and employees for the purposes of carrying out its duties and functions under the provisions of this Act.

(2) The Authority shall promote and sponsor the training of technical personnel on the subjects of information security, data science, data analytics, information technology, finance, law and other related subjects and for this purpose, the Authority shall be authorised to defray the costs of study, in Sri Lanka or abroad of the officers and employees of the Authority who are of proven merit as determined by the Authority.

(3) The Authority shall prepare a code of conduct which shall be applicable to the officers and employees of the Authority.

(4) The Authority may revise such code of conduct by modifying, rescinding or amending from time to time.

(5) The Authority shall not appoint any person to the staff of the Authority where such person–

(*a*) has been previously found guilty of serious misconduct by a court or tribunal or has been subject to a disciplinary action by a regulatory body;

(*b*) has been previously dismissed from office; or

(*c*) has committed a breach of the provisions of this Act or regulations, rules or directives made thereunder.

(6) At the request of the Authority any officer in the public service may, with the consent of the officer and the Public Service Commission established by the Constitution be temporarily appointed to the Authority for such period as may be determined by the Authority or with like consent, be permanently appointed to such staff.

(7) Where any officer in the public service is temporarily appointed to the staff of the Authority, the provisions of subsection (2) of section 14 of the National Transport Commission Act, No. 37 of 1991, shall *mutatis mutandis*, apply to and in relation to such officer.

(8) Where any officer in the public service is permanently appointed to the staff of the Authority, the provisions of subsection (3) of section 14 of the National Transport Commission Act, No. 37 of 1991, shall *mutatis mutandis*, apply to and in relation to such officer.

(9) Where the Authority employs any person who has agreed to serve the Government for a specified period, any period of service to the Authority by that person shall be regarded as service to the Government for the purpose of discharging the obligations of such agreement.

(10) The Authority may with the consent of such officer or employee propose secondment of its officers or employees to other state institutions or regulatory authorities in Sri Lanka or abroad for a period determined by the Board on an assignment agreed upon between such institution and the Authority. The period of secondment shall be deemed to be considered as service to the Authority.

PART VII

PENALTIES

Imposition of penalties

38. (1) Where a controller or processor fails to comply with a directive issued under the provisions of section 35, the Authority shall after taking into consideration the impact on data subjects, the nature and extent of relevant non-compliances and the matters referred to in section 39 of this Act, by notice require such controller or processor to pay a penalty, which shall not exceed a sum of rupees ten million for each non-compliance.

(2) Where a controller or processor has been subjected to a penalty on a previous occasion, subsequently fails to conform to a directive on any further occasion such person shall in addition to the penalty which may be imposed on him under subsection (1) be liable to the payment of an additional penalty consisting of twice the amount imposed as a penalty on the second and for each subsequent non-compliance.

(3) The Authority shall be responsible for the collection of a penalty imposed under this section and the money so collected shall be credited to the Consolidated Fund after deducting such sum of money collected as compensation if any payable to the aggrieved person affected by reason of the non-compliance of the provisions of paragraph (*c*) of subsection (2) of section 35.

(4) If a controller or processor becomes liable to a penalty in terms of subsection (1) or (2) fails to pay such penalty, within such period as may be specified in such notice, the Authority may make an exparte application to the Magistrate Court of Colombo for an order requiring the payment of the penalty recovered in a like manner as a fine imposed by such court notwithstanding such sum may exceed the amount of fine which that court may, in the exercise of its ordinary jurisdiction impose.

(5) The imposition of a penalty under this section shall not preclude a relevant regulatory or statutory body from taking any other regulatory measures including, but not limited to, the suspension of such controller or processor from carrying on of a business or profession or the cancellation of a licence or authority granted for the carrying on of a business or profession, as may be permitted in terms of any applicable written law or rules for the regulation or supervision of such controller or processor.

(6) Where a penalty is imposed under this section on a body of persons, then–

(*a*) if that body of persons is a body corporate, every person who at the time of non-compliance under subsection (1) was a director, and other officer responsible with management and control of that body corporate;

(*b*) if that body of persons is a firm, every partner of that firm; or

(*c*) if that body is not a body corporate, every person who at the time of non-compliance of requirements under subsection (1) was the officer responsible with management and control of that body,

shall be liable to pay such penalty, unless he proves that he had no knowledge of the failure to comply with the requirement under subsection (1) or that he exercised all due care and diligence to ensure the compliance therewith.

(7) A controller or processor who is aggrieved by the imposition of an administrative penalty under this section, may appeal against such decision to the Court of Appeal within twenty-one working days, from the date of the notice of the imposition of such administrative penalty was communicated to such person.

(8) Until rules are made under Article 136 of the Constitution pertaining to appeals under this section, the

rules made under that Article pertaining to an application by way of revision to the Court of Appeal, shall apply in respect of every appeal made under subsection (7) of this section.

(9) Any controller or processor who prefer an appeal to the Court of Appeal under subsection (7), shall, deposit in cash as a security such sum of money equal to the penalty imposed under subsections (1) or (2) before the registrar of the Court of Appeal.

(10) Where an appeal is preferred under subsection (7), the burden of proof shall be on the controller or the processor as the case may be, to prove that he has acted in compliance with the provisions of this Act.

Matters to consider when imposing a Penalty

39. In making a determination to impose an administrative penalty, including the amount as provided in subsection (1) of section 38, the Authority shall have regard to the following matters:–

(*a*) the nature, gravity and duration of the contravention taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(*b*) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(*c*) the effectiveness of the data protection management programme required from the controller under section 12;

(*d*) the degree of co-operation with the Authority, in order to remedy the contravention and mitigate the possible adverse effects of such contravention;

(*e*) the categories of personal data affected by any contravention;

(*f*) the manner in which a contravention became known to the Authority, in particular whether, and if so to what extent, the controller or processor notified the contravention to the Authority;

(*g*) the previous non - compliances by such controller or processor under this Act;

(*h*) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, arising out of or in relation to the contravention of this Act by a controller or processor as the case may be.

Exemptions, restrictions or derogations

40. Any exemption, restriction or derogation to the provisions of this Act shall not be allowed except where such an exemption, restriction or derogation is provided for in any law and respects the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society for–

(*a*) the protection of national security, defense, public safety, public health, economic and financial systems stability of the Republic of Sri Lanka;

(*b*) the impartiality and independence of the judiciary;

(*c*) the prevention, investigation and prosecution of criminal offences;

(*d*) the execution of criminal penalties; and

(*e*) the protection of the rights and fundamental freedoms of persons, particularly the freedom of expression and the right to information.

PART VIII

FUND OF THE AUTHORITY

Fund of the Authority

41. (1) The Authority shall have its own fund (hereinafter referred to as the "Fund").

(2) There shall be paid into the Fund–

(*a*) all such sums of money as may be voted by Parliament for the use of the Authority ; and

(*b*) all such sums of money as may be received by the Authority in the exercise, performance and discharge of its powers, duties and functions under this Act; and

(*c*) all such sums of money as may be paid as fees under the provisions of this Act; and

(*d*) all such sums of money as may be received by the Authority by way of gifts, grants or donations from the Consolidated Fund, the Government, or a foreign Government, State Agencies and from multilateral and bilateral agencies whether within or outside Sri Lanka.

(3) There shall be paid out of the Fund all such sums as are required to defray expenditure incurred by the Authority in the exercise, performance and discharge of its powers, duties and functions under this Act or under any other written law and all such sums as are required to be paid out of the Fund.

(4) Monies belonging to the Fund of the Authority may be invested by the Authority in such manner as may be detemined by the Board.

Financial year and Audit of Accounts

42. (1) The financial year of the Authority shall be the calendar year.

(2) The provisions of Article 154 of the Constitution relating to the audit of the accounts of public corporations shall apply to the audit of the accounts of the Authority.

PART IX

MISCELLANEOUS

Power to borrow

43. The Authority may with the consent of the Minister given in concurrence with the Minister assigned the subject of Finance borrow temporarily by way of overdraft or otherwise, such sums of money as the Authority may require for defraying any expenditure incurred by it in the exercise, performance and discharge of its powers, duties and functions under this Act:

Provided that, the aggregate of the amounts outstanding in respect of any loans raised by the Authority under this section, shall not exceed such sum as may be determined by the Minister in consultation with the Minister assigned the subject of Finance.

Delegation of powers, duties and functions of the Authority

44. (1) The Board may, subject to such conditions as may be specified in writing, delegate to the Director-General or any officer of the Authority, any of its powers, duties and functions under this Act and the Director-General or such officer shall exercise, perform and discharge such power, duty or function subject to any special or general directions issued by the Board.

(2) Notwithstanding any delegation made under subsection (1), the Board may exercise, perform and discharge any such power, duty or function so delegated.

Delegation of powers, duties and functions by the Director-General

45. (1) The Director-General may delegate any of his powers, duties or functions under this Act, to any officer of the Authority.

(2) An officer to whom any power, duty or function is delegated under subsection (1), shall exercise, perform and discharge such power, duty and function subject to such directions as may be given by the Director-General.

(3) The Director-General shall, notwithstanding any delegation made under subsection (1), have the right to exercise, perform and discharge any power, duty or function so delegated.

Expenses to be paid out of the Fund of the Authority

46. (1) All expenses incurred by the Authority in any suit or prosecution brought by or against it before any court, shall be paid out of the Fund of the Authority and only costs paid to or recovered by the Authority in any such suit or prosecution, shall be credited to the Fund of the Authority.

(2) Any expense incurred by a member of the Board, Director-General, or any officer or other employees of the Authority, in any suit or prosecution brought by or against such person before any court in respect of any act which is done or purported to be done by such person under this Act, shall if the court holds that the act was done in good faith, be paid out of the Fund of the Authority, unless such expenses are recovered by him in such suit or prosecution.

Review of the performance of the Authority

47. The Minister shall from time to time review the performance of the Authority and require the Authority to submit such reports relating to its affairs and activities as may be required by the Minister.

Annual Report

48. (1) The Authority shall within six months of the end of each financial year, submit to the Minister an annual

report of the activities carried out by the Authority during that financial year, with such supporting documents as the Minister may require from time to time for the evaluation of the performance of the Authority.

(2) The Minister shall, lay copies of the report and documents submitted under subsection (1) before Parliament within six months from the date of receipt of such report and the documents.

Protection of officers of the Authority from suit or prosecution

49. A liability whether civil or criminal, shall not be attached to any officer of the Authority or to any officer authorized by such officer, for anything which is done in good faith in the performance or exercise of any function or power imposed or conferred on the Authority under this Act.

All officers and employees of the Authority deemed to be public servants for the purposes of Penal Code

50. All officers and employees of the Authority, shall be deemed to be public servants within the meaning and for the purposes of Penal Code (Chapter 19).

Authority deemed to be a scheduled institution for the purposes of Bribery Act

51. The Authority shall be deemed to be a Scheduled institution within the meaning of the Bribery Act, (Chapter 26) and the provisions of that Act shall be construed accordingly.

Rules

52. (1) The Authority shall make rules in respect of–

(*a*) the schemes of recruitments, terms of appointment, employment and dismissal of various officers and employees and their powers, functions including the powers and functions of the Director-General and the payment of remuneration;

(*b*) the procedure to be observed at the summoning and holding of meetings of the Authority;

(*c*) the management of the affairs of the Authority;

(*d*) the form and manner of exercising rights of data subjects under Part II;

(*e*) criteria for refusal of the request of data subjects under section 17.

(*f*) all matters for which, rules are required or authorized to be made under this Act.

(2) The Authority shall make first rules under subsection (1), within twenty-four months from the date of coming into operation of the provisions of Part V of this Act.

(3) The Authority shall, prior to making rules under paragraphs (*d*), (*e*) or (*f*) of subsection (1), hold public consultations for a period of not less than two weeks.

(4) The period of public consultation referred to in subsection (3) may be extended for a further period as may be specified by the Authority.

(5) A rule made under this section shall not have effect until it is approved by the Minister and approved rules and notification of such approval are published in the *Gazette*.

(6) Every rule made under paragraphs (*d*), (*e*) or (*f*) of subsection (1), shall within three months after its publication in the *Gazette* be brought before Parliament for approval and any rule, which is not so approved, shall be deemed to be rescinded with effect from the date of such disapproval, but without prejudice to anything previously done thereunder.

(7) Notification of the date on which any rule made by the Authority is deemed to be rescinded shall be published in the *Gazette*.

Regulations

53. (1) The Minister may make regulations with the concurrence of the Authority in respect of any matter required by this Act to be prescribed or in respect of which regulations are authorized by this Act to be made.

(2) In particular and without prejudice to the generality of the powers conferred by subsection (1), the Minister with the concurrence of the Authority may make regulations in respect of the following matters:–

(*a*) amendment, addition to or variation of the conditions under Schedules I, II, III and IV;

(*b*) identification of the third countries that ensure level of protection referred to in subsection (2) of section 26 taking into consideration, the relevant legislation, enforceability of the data subject's rights and freedoms, international commitments, effective administrative and judicial redress availability for the data subjects whose personal data are being transferred;

(*c*) specifying the fees and charges levied for any service provided under this Act;

(*d*) specifying the categories and criteria of licenses to be issued under this Act;

(*e*) providing for terms and conditions, form and duration, procedure for application, renewal, suspension, cancellation of such licences and appeal against the refusal, suspension or cancellation of licences;

(*f*) charging of fees for the issue of licences;

(*g*) specifying the conditions for providing appropriate safeguard for the rights and freedoms of data subjects relating to protection of personal data;

(*h*) specifying the form and manner by which appeals may be made to the Authority under the provisions of this Act.

(3) Every regulation made under subsection (1), shall be published in the *Gazette* and shall come into operation on the date of such publication or on such later date as may be specified in such regulation.

(4) Every regulation made under subsection (1), shall within three months after its publication in the *Gazette* be brought before Parliament for approval and any regulation, which is not so approved, shall be deemed to be rescinded with effect from the date of such disapproval, but without prejudice to anything previously done thereunder.

(5) Notification of the date on which any regulation made by the Minister is deemed to be rescinded shall be published in the *Gazette*.

Official Secrecy

54. Every person appointed under the authority of this Act shall, before entering upon his duties, sign a declaration pledging himself to observe strict secrecy in respect of any information, which may come to his knowledge in the exercise, performance and discharge of his powers, duties and functions under this Act, shall by such declaration pledge himself not to disclose any such information, except–

(*a*) when required to do so by a Court of law; or

(*b*) in order to comply with any of the provisions of this Act or any other written law.

Removal of difficulties

55. (1) If any difficulty arises in giving effect to the provisions of this Act or the rules, regulations, or Orders made under this Act, the Minister may by Order published in the *Gazette*, make such provision not inconsistent with the provisions of this Act, or any other written law, as appears to the Minister to be necessary or expedient for removing the difficulty:

Provided that, no such Order shall be made after the expiry of a period of five years from the date of coming into operation of this Act.

(2) Every Order made under this section shall, within three months after it is made, be laid before Parliament.

PART X

INTERPRETATION

Interpretation

56. In this Act, unless the context otherwise requires–

"anonymise" in relation to personal data means permanent removal of any personal identifiers from personal data to render any such personal data from being related to a identified or identifiable natural person;

"automated processing" means, processing that does not involve any manual processing;

"biometric data" means, personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, including facial images, dactyloscopic data or iris related data;

"certifying bodies" means, the bodies local or foreign that provide certification services relating to the processing of personal data or qualifications of Data Protection Officers;

"child" means, a natural person who is below the age of sixteen years;

"consent" means, any freely given, specific, informed and unambiguous indication by way of a written declaration or an affirmative action signifying a data subject's agreement to the processing of his personal data;

"controller" means, any natural or legal person, public authority, public corporation, non-governmental organization, agency or any other body or entity which alone or jointly with others determines the purposes and means of the processing of personal data;

"cross-border data flow " means, the movement of personal data out of the territory of Sri Lanka for the purpose of processing personal data in a third country;

"dactyloscopic data" means, data relating to fingerprints;

"data concerning health" means, personal data related to the physical or psychological health of a natural person, which includes any information that indicates his health situation or status;

"Data Protection Authority" means, the Authority established under section 28 of this Act;

"Data Protection Officer" means, the person designated or appointed under section 20 of this Act;

"data subject" means, an identified or identifiable natural person, alive or deceased, to whom the personal data relates;

"identifiable natural person" is a natural person who can be identified, directly or indirectly, by reference to any personal data;

"encryption" means, the act of ciphering or altering data using mathematical algorithm to make such data unintelligible to unauthorized users;

"financial data" means, any alpha-numeric identifier or other personal data which can identify an account opened by a data subject, or card or payment instrument issued by a financial institution to a data subject or any personal data regarding the relationship between a financial institution and a data subject, financial status and credit history relating to such data subjects, including data relating to remuneration;

"genetic data" means, personal data relating to the genetic characteristics of a natural person which gives unique information about the physiology or the health of that natural person which results from an analysis of a biological sample or bodily fluid of that natural person;

"local authority" means, a Municipal Council, Urban Council or a Pradeshiya Sabha and includes any authority created or established by or under any law to exercise, perform and discharge powers, duties and functions corresponding or similar to the powers, duties and functions exercised, performed or discharged by any such Council or Sabha;

"Minister" means, the Minister assigned the subject of data protection under Article 44 or 45 of the Constitution;

"personal data" means, any information that can identify a data subject directly or indirectly, by reference to–

(*a*) an identifier such as a name, an identification number, financial data, location data or an online identifier; or

(*b*) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person.

"personal data breach" means, any act or omission that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"personal data revealing racial or ethnic origin" means, any personal data including photographs that may indicate or be related to the race or ethnicity of a natural person;

"prescribed" means, prescribed by regulations made under this Act;

"processing" means, any operation performed on personal data including but not limited to collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical or arithmetical operations on personal data;

"processor" means, a natural or legal person, public authority or other entity established by or under any written law, which processes personal data on behalf of the controller;

for the avoidance of doubt, a processor shall be a separate entity or person from the controller and not a person subject to any hierarchical control of the controller and excludes processing that is done internally such as one department processing for another, or an employee processing data on behalf of their employer;

Illustration: Hospital A, employs a data scientist as an employee to manage its analysis of patient records. The Hospital has decided to store its patient records on a third-party local cloud platform hosted by Company B. Hospital A is the controller, and the Company B is the processor where management of patient records are concerned. The data scientist of the hospital is only an employee of the controller and not a processor.

"profiling" means, processing of personal data to evaluate, analyse or predict aspects concerning that data subject's performance at work, economic situation, health, personal preferences, interests, credibility, behavior, habits, location or movements;

"pseudonymisation" means, the processing of personal data in such a manner that the personal data cannot be used to identify a data subject without the use of additional information and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to a data subject;

"public authority" means, a Ministry, any Department or Provincial Council, local authority, statutory body or any institution established by any written law, or a Ministry, any Department or other authority or institution established or created by a Provincial Council;

"relevant regulatory or statutory body" means, the regulatory or statutory body established by or under any written law which regulates, authorizes or supervises the controller and includes a Ministry which carries out the supervisory functions for the purpose of sections 26, 27 and 38 of this Act;

"recipient" means, a natural or legal person to whom the personal data is disclosed, or a public Authority or any incorporated or unincorporated body to which the personal data is disclosed;

"special categories of personal data" means, the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, personal data relating to offences, criminal proceedings and convictions, or personal data relating to a child;

"Sri Lanka" means, the territorial limits of Sri Lanka as stipulated by Article 5 of the Constitution and includes the territorial waters or air space of Sri Lanka, any ship or aircraft registered in Sri Lanka, any location within the premises of a Sri Lankan mission or the residence of the Head of such mission, diplomatic agent or any other member of such mission, situated outside Sri Lanka, or within any premises occupied on behalf of, or under the control of, the Government of Sri Lanka or any statutory body established in Sri Lanka and situated outside Sri Lanka;

"third country" means, a country prescribed under section 26 for the purpose of cross-border data flow;

"third party" means, a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who are under the direct authority of the controller or processor, are authorized to process personal data;

"written" includes a document written manually or electronically.

Sinhala text to prevail in case of inconsistency

57. In the event of any inconsistency between the Sinhala and Tamil texts of this Act, the Sinhala text shall prevail.

(Section 5 (*a*))

SCHEDULE I

CONDITIONS FOR LAWFUL PROCESSING

(*a*) the data subject has given consent to the processing of his personal data; or

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

(*c*) processing is necessary for compliance with a legal obligation to which the controller or processor is subject to under any written law; or

(*d*) processing is necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person; or

(*e*) processing is necessary for the performance of a task carried out in the public interest or in the exercise of powers, functions or duties conferred, imposed or assigned on the controller or processor by or under any written law including any circular, direction or code issued by the government; or

(*f*) 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 of the data subject which require protection of personal data, in particular where the data subject is a child.

(*g*) for the purpose of item (*e*) of this Schedule, "public interest" includes-

(i) processing of personal data is necessary for health purposes such as public health and social protection and the management of health care services;

(ii) processing of personal data is necessary for the control of communicable deceases and other serious threats to health;

(iii) processing of personal data is necessary by official authorities for achieving the purposes or objects laid down by law.

(*h*) for the purpose of item (*f*) of this Schedule, "legitimate interest" includes–

(i) processing in situations where the data subject is a client or in the service of a controller;

(ii) whether a data subject reasonably expects at the time and in the context of the collection of the personal data that processing for that purpose may take place;

(iii) processing of personal data is strictly necessary for the purposes of preventing fraud;

(iv) processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security.

(Section 5 (*b*))

SCHEDULE II

CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

(*a*) the data subject has given consent, to the processing of special categories of personal data for one or more purposes specified by the controller at the time of processing, unless any other written law prohibits the processing of such personal data notwithstanding the consent of the data subject concerned. In the case of a child, consent shall mean the consent of the parent or legal guardian of such child; or

(*b*) processing is necessary for the purposes of carrying out the obligations of the controller and exercising of the rights of the data subject, in the field of employment, social security including pension, and for public health purposes ensuring public safety, monitoring and public alert systems relating to impending health or other emergencies, the prevention or control of communicable diseases and other serious threats to public health and the management of public health-care services in so far as it is provided for in any written law providing for appropriate safeguards for rights of the data subject; or

(*c*) processing is necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person where the data subject is physically or legally incapable of giving consent; or

(*d*) processing relates to personal data which is manifestly made public by the data subject; or

(*e*) processing is necessary for the establishment, exercise or defence of legal claims before a court or tribunal or such similar forum, or whenever courts are acting in their judicial capacity; or

(*f*) processing is necessary for, any purpose as provided for in any written law or public interest as determined under item (*g*) of Schedule I, which shall be necessary and proportionate to the aim pursued whilst providing suitable and specific measures to safeguard the rights and freedoms of the data subject; or

(*g*) processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where such data is processed by a health professional licensed under or authorized by any written law prevailing in Sri Lanka; or

(*h*) processing is necessary for archiving purposes in the public interest, scientific research or historical research purposes or statistical purposes in accordance with law which shall be proportionate to the aim pursued, protecting the data protection rights enumerated in this Act or any other written law and provide for suitable and specific measures to safeguard the rights and freedoms of the data subject.

(Section 5 (*c*))

SCHEDULE III

CONDITIONS FOR CONSENT OF THE DATA SUBJECT

(*a*) the controller shall demonstrate that the data subject has consented to processing of the personal data relating to such data subject;

(*b*) if the consent of the data subject is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language:

Provided that, such a declaration shall not constitute an infringement of any provisions of this Act.

(*c*) when assessing whether consent is freely given, special consideration shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract; and

(*d*) prior to giving consent, the data subject shall be informed thereof that consent can be withdrawn anytime subject to the provisions of this Act.

(Section 5 (*d*))

SCHEDULE IV

PROCESSING OF PERSONAL DATA RELATING TO CRIMINAL INVESTIGATIONS

(*a*) processing of personal data relating to lawful investigations of offences or related security measures shall be carried out only in accordance with applicable written laws, whilst providing for appropriate safeguards for the rights and freedoms of data subjects;

(*b*) for the avoidance of doubt, processing of personal data may be considered lawful under this Schedule if investigations are carried out pursuant to the provisions of the Code of Criminal Procedure Act, No. 15 of 1979 or provisions under any other written law; and

(*c*) conditions for providing appropriate safeguards for the rights and freedoms of data subjects under this Schedule may be as prescribed.

(Sections 11 and 13)

SCHEDULE V

COLLECTION OF PERSONAL DATA

1. where the personal data relating to a data subject is collected from the data subject, the controller shall provide the data subject with the following information, at the time of collection of such personal data -

(*a*) the identity and contact details of the controller and where applicable of the controller's representative;

(*b*) the contact details of the Data Protection Officer, where applicable;

(*c*) the intended purposes for which the personal data is processed and the legal basis for the processing;

(*d*) the legitimate interest pursued by the controller or by a third party where processing is based on item (f) of Schedule 1;

(*e*) the categories of personal data being collected;

(*f*) where processing is intended to be based on consent pursuant to item (a) of Schedule I and item (a) of Schedule

II, the existence of the right of the data subject to withdraw his consent, and the procedure for such withdrawal, without affecting the lawfulness of processing based on consent before its withdrawal;

(*g*) recipients or third parties with whom such personal data may be shared, if applicable;

(*h*) information regarding any cross-border transfer of the personal data that the controller intends to carry out, if applicable;

(*i*) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;

(*j*) the existence of and procedure for the exercise of rights of the data subject referred to in Part II;

(*k*) the existence of a right to file complaints to the Authority;

(*l*) whether the provision of personal data by the data subject is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and

(*m*) the existence of automated individual decision-making referred to in section 18, including profiling, and, at least in those cases, reasonably meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where the controller intends to further process the personal data for a purpose other than for which it was originally collected, the controller shall provide the data subject detailed information on the further processing in the manner provided in item 1 of this Schedule and the purpose thereof.

3. Items 1 and 2 of this Schedule shall not apply where the data subject already has obtained or made aware of the information.

4. Where the personal data of the data subject has been obtained other than through a direct interaction with the data subject, the controller shall provide the data subject, the source from which the personal data originate, and whether or not it came from publicly accessible source, where applicable in addition to the information required under item 1 of this Schedule.

5. Where the personal data of the data subject has been obtained other than through a direct interaction with the data subject, the controller shall provide the information under items 1 and 4 of this Schedule –

(*a*) within a reasonable period of time after obtaining the personal data, but at least within one month, having regard to the specific circumstances in which the personal data is processed;

(*b*) if the personal data is to be used for communication with the data subject, at least at the time of the first communication to that data subject; or

(*c*) if a disclosure to another recipient is envisaged, at least when the personal data is first disclosed.

6. Items 1 to 4 of this Schedule shall not apply where –

(*a*) the controller has established the fact that the data subject has already been provided with or made aware of the information; or

(*b*) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archival purposes in the public interest in the manner provided for by any written law, scientific research, historical research or statistical research purposes, subject to the conditions and safeguards provided in this Act or in so far as the obligation referred to in item 1 of this Schedule is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the rights and freedoms of data subject protected under any written law, including making the relevant information publicly available; or

(*c*) obtaining or disclosure is expressly laid down by any written law to which the controller is subjected to and which provides appropriate measures to protect the rights and freedoms of data subjects protected under this Act and such written law; or

(*d*) the personal data shall remain confidential, consequent to obligations of professional privilege or is not permitted to be disclosed under any written law, including a statutory obligation of secrecy.

(Section 29 (5))

SCHEDULE VI

Term of office of members

1. Every member of the Board other than the Chairperson shall, unless he vacates office earlier by death, resignation or removal, hold office for a term of three years from the date of his appointment and unless he has been removed from office, be eligible for reappointment:

Provided that, a member appointed in place of a member who had vacated office, by death, resignation or removal, shall hold office for the unexpired term of office of the member whom he succeeds.

Resignation of members of the Board

2. (1) Any member of the Board may at any time resign his office by letter addressed to the President and such resignation shall take effect upon it being accepted by the President.

(2) In the event of vacation of office of any member by reason of death, resignation, removal, the President may appoint another person having regard to the provisions of subsection (3) and (4) of section 29 to hold office for the unexpired period of the term of office of the member whom he succeeds.

(3) If any member other than the Chairperson is temporarily unable to perform the duties of his office for a period exceeding three months due to ill health or absence from Sri Lanka or for any other cause, the President may appoint some other person to act in his place during such period having regard to the provisions of subsection (3) and (4) of section 29.

(4) A member of the Board who, without leave of the first being obtained, absents himself from three consecutive meetings of the Authority shall be deemed to have vacated his office.

Disqulifications and grounds for removal of a member of the Board

3. (1) A person shall be disqulified from being appointed or from continuing as a member of the Board if he–

(*a*) is or becomes a member of Parliament, or a member of any Provincial Council or any local authority;

(*b*) is or becomes of unsound mind or incapable of carrying out his duties;

(*c*) is or has become an undischarged bankrupt;

(*d*) is or has been convicted of an offence which involves moral turpitude;

(*e*) has been previously removed from office.

(2) The President shall remove a member of the Board from continuing as a member if he–

(*a*) is guilty of serious misconduct in relation to his duties;

(*b*) abuses his position so as to render his continuation in office detrimental to the interest of the Authority;

(*c*) is disqualified under paragraph (1) of item 3; or

(*d*) contravenes the provisions of this Act.

Members to disclose any interest

4. A member who is directly or indirectly interested in any decision that is to be taken on any matter by the Board shall disclose the nature of such interest at the meeting of the Board where such decision is being taken, and such disclosure shall be recorded in the minutes of the meetings of the Board and such member shall not take part in any deliberation or decision of the Board with regard to that matter, and shall withdraw from such meeting while such deliberation is in progress or such decision is being made.

Remuneration of members

5. The members of the Board, may be remunerated in such manner in consultation with the Minister assigned the subject of Finance and shall carry out their functions subject to such terms and conditions as may from time to time be determined by the President.

Quorum and the Meetings of the Board

6. (1) The *quorum* for any meeting of the Board shall be three members including the Chairperson.

(2) The Director-General shall summon all meetings of the Board.

(3) A meeting of the Board may be held either–

(*a*) by the number of members who constitute a *quorum* being assembled at the place, date and time appointed for the meeting; or

(*b*) by means of audio-visual communication by which all members participating and constituting a *quorum* can simultaneously see and hear each participating member for the duration of the meeting.

(4) All questions for decision at any meeting of the Board shall be decided by the vote of the majority of members present and voting at such meeting. In the case of an equality of votes, the Chairperson shall, in addition to his vote, have a casting vote.

(5) The Chairperson shall preside at every meeting of the Board. In the absence of the Chairperson from any meeting of the Board, any member elected by the members present shall preside at such meeting of the Board.

(6) The meetings of the Board shall be conducted in conformity with the rules made and procedure established, by it from time to time.

Proceedings, acts or decisions not invalidated by reason of a vacancy

7. No proceeding, act or decision of the Board shall be invalidated by reason only of the existence of a vacancy among its members or of any defect in the appointment of a member thereof.

Seal of the Authority

8. (1) The seal of the Authority shall be in the custody of the Board.

(2) The seal of the Authority may be altered in such manner as may be determined by the Board.

(3) The seal of the Authority shall not be affxed to any instrument or document except in the presence of one member of the Board and the Director-General of the Authority or in the absence of the Director-General, in the presence of any two members of the Board, who shall sign the instrument or document in token of their presence.

(4) The Board shall maintain a register of the instruments and documents to which the seal of the Authority has been affixed.

English Acts of the Parliament can be purchased at the "Prakashana Piyasa", Department of Government Printing, No. 118, Dr. Danister De Silva Mawatha, Colombo 8.