FRAMEWORK FOR THE PROPOSED PERSONAL DATA PROTECTION BILL
Contents

Preamble .................................................................................................................................................. 3
PART I .................................................................................................................................................... 3
1. Application........................................................................................................................................... 3
PART II – Data Protection Principles.................................................................................................... 4
2. Lawfulness in Processing ..................................................................................................................... 4
3. Purpose Limitation ............................................................................................................................... 5
4. Data minimisation ............................................................................................................................... 5
5. Accuracy ............................................................................................................................................... 5
6. Storage Limitation ............................................................................................................................... 5
7. Integrity and Confidentiality ............................................................................................................... 5
PART III - Rights of data Subjects ......................................................................................................... 6
9. Right to withdraw consent .................................................................................................................. 6
10. Right of access by the data subject .................................................................................................... 6
11. Data subject’s rights to rectification .................................................................................................. 6
12. Right to erasure ................................................................................................................................... 7
13. Exercise of rights under sections 9, 10, 11 and 12 ......................................................................... 7
14. Automated individual decision-making ............................................................................................ 9
15. Exercise of rights through the authority .......................................................................................... 9
Part IV – Controllers and processors ................................................................................................... 10
16. Registration of Controllers and Processors ...................................................................................... 10
17. Application for Registration ............................................................................................................. 10
18. Exemption from Registration and Registration Fees ..................................................................... 11
19. Duration of the registration certificate .............................................................................................. 11
20. Register of controllers ...................................................................................................................... 11
21. Cancellation or variation of the certificate ......................................................................................... 11
22. Designation of the Data Protection Officer ....................................................................................... 11
23. Duties and Obligations of the Controller ......................................................................................... 12
24. Duties and Obligations of Processor .................................................................................................. 13
25. Data Breach Notifications ............................................................................................................... 14
26. Data Protection Impact Assessments ............................................................................................... 14
27. Prior consultation .............................................................................................................................. 15
Part V - Exceptions ............................................................................................................................... 16
PREAMBLE

WHEREAS the Constitution guarantees the right of access to information in Article 14A thereof together with the exemption of right to privacy, and there exists a need for the protection of personal information, whilst ensuring rights of natural persons with regards to processing of such information and to reconcile data protection with business and societal needs and commercial interests:

AND WHEREAS it has become necessary to improve consumer confidence and ensure the growth of a digital democracy and innovation and promote both effective protection of personal data and its use in Sri Lanka whilst respecting domestic laws and regulations, applicable international standards governing data protection, and strengthening information security:

AND WHEREAS it is the duty of the Government to regulate processing of personal data and to ensure the consumer trust and confidence in the privacy and security of online transactions and information networks and to reap the benefits of a digitalized society and actively participate in an information-driven global economy as management of personal information is critical in enabling in Sri Lanka:

AND WHEREAS Sri Lanka has growing interest in promoting and protecting the fundamental values of data protection, individual liberties and the global use of information, it is become necessary to improve interoperability among privacy frameworks as well as strengthen cross-border co-operation among enforcement authorities and provide clear guidance and direction to government and businesses entities located or operational in Sri Lanka on generic data protection issues and their impact as well as the manner in which legitimate business practice and government functions are to be conducted:

PART I

1. APPLICATION

1. This Act applies to processing of personal data
   a) when the processing takes place wholly or partly within Sri Lanka, or
   b) by a controller or processor:
      i) who is domiciled or ordinarily resident in Sri Lanka
      ii) who is incorporated or established under the laws of Sri Lanka
      iii) who is subject to Sri Lankan law
      iv) who specifically or systematically offers goods or services to data subjects in Sri Lanka or
      v) who monitors the behaviour of data subjects in Sri Lanka including profiling in so far as such behaviour takes place in Sri Lanka.

2. This Act does not apply to processing of personal data:
i. If processing is done for purely personal or household purposes. For the purpose of this section household shall mean such person’s own household.

ii. If the data is anonymized

3. The provisions of this Act shall come into operation no later than three (3) years (or 2 years), from the date on which the certificate of the Speaker is endorsed in respect of this Act in terms of Article 79 of the Constitution.

Alternative to (3)

(i) The provisions of this Section, Part I, Part II (Principles of Processing) except section 8, Part VII, section 22 (designation of data protection officer), section 48 (Rules and Regulation) shall come into operation on the date on which the certificate is endorsed in respect of this Act in terms of Article 79 of the Constitution.

(ii) All Rules under section 49(4) shall be issued by the Authority within 24 months from the date referred to in sub-section 1.

(iii) All other provisions shall come into operation 24 months from the date referred to in subsection 1.

4. Notwithstanding the provisions of this Act, it shall be lawful for any government department, provincial council or any other regulatory body, established by written law, to stipulate the framework or conditions for processing personal data in accordance with its governing legal framework¹, in so far as such framework or conditions do not contravene the rights, principles and safeguards stipulated pursuant to the provisions of this Act. The duties, obligations, as well as regulatory requirements established under the provisions of this Act, shall be in addition to the duties, obligations and regulatory requirements under any other written law.

PART II – DATA PROTECTION PRINCIPLES

2. LAWFULNESS IN PROCESSING

Personal data shall be processed lawfully, fairly and in a transparent manner. The processing of personal data is lawful only in the following circumstances—

1) at least one of the conditions in Schedule 1 is met,

2) in the case of processing special categories of data, at least one of the conditions in Schedule 2 is also met in addition to the conditions in Schedule 1.

¹Example: Registration of Persons Act, Births and Deaths Act, Elections Ordinance and related laws, Banking Act, Telecommunications Act etc.
3) Where processing is based on consent, where the conditions prescribed in Schedule 3 are satisfied.

4) Where the personal data relates to criminal investigations and related matters, where the conditions in Schedule 4 are satisfied.

3. PURPOSE LIMITATION

Personal data shall be collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the said purposes. However, further processing of personal data strictly for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

4. DATA MINIMISATION

Processing shall be adequate, relevant, necessary, proportionate to the purposes for which the personal data is processed.

5. ACCURACY

Controller shall ensure that personal data that is processed is accurate and, where necessary, kept up to date with every reasonable step being taken to ensure that any inaccurate personal data are rectified or erased without delay;

6. STORAGE LIMITATION

Personal data may be kept in a form which permits identification of data subjects for such period as may be necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures provided under this Act in order to safeguard the rights of the data subject prescribed under this Act or any other written law.

7. INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
8. Processing done in contravention of the provisions in this Part shall be an offence under this Act.

**PART III - RIGHTS OF DATA SUBJECTS**

9. **RIGHT TO WITHDRAW CONSENT**

Data subject shall have the right to withdraw his or her consent at any time where processing is done pursuant to section 2(1) and 2(3). The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Any request for withdrawal shall be in writing. For the Data Subject it shall be as easy to withdraw as to give consent.

10. **RIGHT OF ACCESS BY THE DATA SUBJECT**

1) Data subject shall be entitled to obtain from the controller—
   a. confirmation as to whether or not personal data concerning him or her is being processed by that controller or any processor of that controller, and
   b. access to such personal data and the information set out in section 10(2).

2) Information referred to under Section 10(1)(b) above includes information relating to:
   a. the purposes of and legal basis for the processing;
   b. the categories of personal data concerned;
   c. the recipients or categories of recipients to whom the personal data has been disclosed
   d. the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;
   e. the existence of the data subject’s rights to request from the controller—
      i. rectification of personal data, and
      ii. erasure of personal data or the restriction of its processing;
   f. where applicable, the existence of the data subject's right to lodge a complaint with the Data Protection Officer and the contact details of the DPO;
   g. nature and form of personal data undergoing processing and of any available information as to its origin.

11. **DATA SUBJECT'S RIGHTS TO RECTIFICATION**

1) The controller must, if so requested by a data subject, rectify without undue delay, and in any event within the prescribed time period, any inaccurate personal data that is processed relating to the data subject.

2) Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
3) However, this section does not impose any obligation on the controller to process additional personal data that is not required for the purpose of processing, merely to comply with a request made under section 10(1).

4) Where the controller would be required to rectify personal data under this section but the personal data must be maintained for the purposes of evidence, the controller must, restrict the processing of such personal data instead of rectifying the personal data concerned.

5) Nothing in this section 11 prevent a controller from seeking legitimate proof from the data subject who seeks rectification under this section. A controller may object to comply with a request to rectify in the absence of any legitimate proof supporting such rectification.

12. **RIGHT TO ERASURE**

1) The controller must erase personal data without undue delay, in any event within the prescribed time, upon the written request of a data subject to whom such personal data relate, provided that:
   a. the processing of the personal data can no longer be processed on a lawful ground and the controller has not legitimize or cannot legitimize the said processing which includes withdrawal of the data subject’s consent upon which processing is based according to point (a) of Schedule 1 or point (a) of Schedule 2.
   b. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
   c. the personal data have been unlawfully processed or
   d. the personal data have to be erased to comply with a legal obligation stipulated by any law to which the controller is subject to.

2) Where the controller would be required to erase personal data under subsection 12(1) but the personal data must be maintained for the purposes of evidence or retention is mandated by any law or where such personal data is subject to a civil or criminal investigation, the controller must instead of erasing the personal data restrict its processing.

13. **EXERCISE OF RIGHTS UNDER SECTIONS 9, 10, 11 AND 12**

1) Where a data subject makes a written request in the prescribed form under section 9, 10, 11 or 12, the controller must inform the data subject in writing—
   a. whether such request has been granted, or
   b. if it has been refused—
      i. of the reasons for the refusal,
      ii. of the data subject’s right to lodge a complaint with the Authority.
2) Where a data subject makes a request under subsection 9, 10, 11 or 12, the controller must comply with the respective request without undue delay and in any event within the prescribed time period.

3) The controller may restrict, wholly or partly, the rights conferred by section 9, 10, 11 or 12 to the extent that and for so long as the restriction is, having regard to the rights and legitimate interests of the data subject, a necessary and proportionate measure to—
   a. avoid obstructing an official or legal inquiry, investigation or procedure;
   b. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
   c. protect public security;
   d. protect national security;
   e. protect the rights and freedoms of others

4) Where the rights of a data subject under section 9, 10, 11 or 12 is restricted, wholly or partly, the controller must inform the data subject in writing without undue delay and in any event within the prescribed time period —
   a. that the rights of the data subject under the appropriate section 9, 10, 11 or 12 have been restricted,
   b. of the reasons for the restriction unless providing the reasons may prejudice the purpose of restriction and
   c. of the data subject's right to lodge a complaint with the Authority

5) The controller must—
   a. record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject,
   b. if requested to do so by the Authority, submit such record to the Authority.

6) Where the controller rectifies, erases or restricts the processing of personal data pursuant section 9, 10, 11 or 12 -
   a. the controller must notify the recipients unless this proves impossible or involves disproportionate effort, and
   b. the recipients must similarly rectify, erase or restrict the processing of the personal data so far as they retain responsibility for it.

7) Any right conferred on an individual in this Act may be exercised –
   a. where the data subject is a minor, by a person who has parental authority over the minor or has been appointed as his guardian;
   b. where the data subject is physically or mentally unfit, by a person who has been appointed as his guardian or legal administrator by a Court; or
   c. in any other case, by a person duly authorised in writing by the data subject to make a request under this Part.

8) Where a request from a data subject under section 9, 10, 11 or 12 is manifestly unfounded or excessive, the controller may—
   a. charge a reasonable fee for dealing with the request, or
   b. refuse to act on the request.
Explanation:

An example of a request that may be excessive is one that merely repeats the substance of previous requests.

9) Where a controller refuse a request pursuant to section 13(8), it shall be the responsibility of the controller to establish that the request has been manifestly unfounded or excessive.

10) Where the controller has reasonable doubts about the identity of an individual making a request under section the controller may—
   a. request the provision of additional information to enable the controller to confirm the identity, and
   b. delay dealing with the request until the identity is confirmed.

11) The Authority may by rules prescribe limits on the fees that a controller may charge in accordance with subsection 13(8)(a).

14. AUTOMATED INDIVIDUAL DECISION-MAKING

1) A controller shall not take a significant decision based solely on automated processing unless that decision is required or authorised by law provided such law lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests or is based on the data subject's explicit consent. A decision is a “significant decision” for the purpose of this section if, in relation to a data subject it produces an adverse legal effect concerning the data subject, or significantly affects the exercise of any legal rights of the data subject.

2) The Authority shall impose such criteria and conditions applicable in the exercise of a data subject's rights under this section by way of rules issued hereunder.

15. EXERCISE OF RIGHTS THROUGH THE AUTHORITY

1) Where a controller has refused to comply with a request according to section 13(1)(b), the data subject may make an appeal to the Authority in the prescribed form and within such prescribed time, requesting the Authority to determine —
   a. if the restriction imposed by the controller was lawful;
   b. if the charges claimed by the controller is lawful or
   c. that the refusal of the data subject's request was lawful.

2) The Authority shall take such appropriate measures in the exercise of his investigative powers under section 37 and investigate on such claim made by data subject.

3) After concluding the necessary investigations pursuant to the preceding sub-section, the Authority must inform the data subject without undue delay in any event within such prescribed time that:
   a. the restriction imposed by the controller was lawful
   b. the charges levied by the controller is lawful
   c. the controller's refusal of the data subject's request was lawful or
d. Where the Authority is not satisfied that the restrictions or refusal by the controller is lawful, the Authority may also inform the data subject of any further steps that the Authority is considering taking against the controller under the provisions of this Act

4) If the data subject is not satisfied with the decision of the Authority, such data subject may prefer an appeal to the Court of Appeal within such prescribed time.

**PART IV – CONTROLLERS AND PROCESSORS**

**16. REGISTRATION OF CONTROLLERS AND PROCESSORS**

1) Subject to exemptions provided under this Act, no person shall act as a controller unless registered with the Authority in accordance with the provisions of this Section and by paying such annual fee as prescribed.

2) Controllers that are Public Authorities who are deemed controllers shall be excluded from the payment of the registration fee under section 16(1).

**17. APPLICATION FOR REGISTRATION**

1) Every person who intends to act as a controller shall apply to the Authority in the prescribed form within such time period as prescribed.

2) An application under subsection (1) shall provide the following particulars –
   a. A description of the personal data to be processed by the applicant, and of the category of data subjects, to which the personal data relates;
   b. a statement as to whether the applicant is likely to hold any special categories of personal data;
   c. a description of the purpose for which the personal data is to be processed;
   d. a description of any recipient to whom the applicant intends or may intend to disclose the personal data;
   e. the name, or a description of, any country to which the applicant intends or may wish, directly or indirectly, to transfer the personal data;
   f. statement as to a representative for the purposes of this Act and details of such representative;
   g. a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data; and
   h. any other details as may be prescribed by the Authority.

3) A controller who knowingly supplies any false or misleading detail under subsection 17(2) commits an offence under this Act.

4) The Authority shall issue a certificate of registration to an applicant who satisfies the prescribed criteria to be registered as a controller.

5) Where there is a change in any particular outlined under subsection (2), the controller shall notify the Authority of such change in prescribed period. On receipt of such notification the Authority shall amend the respective entry in such Register maintained by the Authority.
6) A controller who fails to comply with the provisions of subsection (1) and (5) commits an offence under this Act.

18. **EXEMPTION FROM REGISTRATION AND REGISTRATION FEES**

The Minister shall by regulation with the concurrence of the Authority, prescribe processing activities that may be exempted from the payment of registration fee under this Act and specify tiers of fees payable by a controller having taken into account the nature and extent of the processing activity.

19. **DURATION OF THE REGISTRATION CERTIFICATE.**

A registration certificate issued under section 17(4) shall be valid for a period of one year and the holder shall apply for the renewal within a prescribed period.

20. **REGISTER OF CONTROLLERS.**

1) The Authority shall keep and maintain a Register of the registered controllers in such form and manner as maybe prescribed.

2) The Authority may, at the request of a controller, remove any entry in the Register upon being satisfied that such controller is no longer required to be a registered controller under this Act.

3) The Register shall be a public document and available for inspection by any person.

4) A person may request the Authority for a certified copy of any entry in the Register.

21. **CANCELLATION OR VARIATION OF THE CERTIFICATE**

1) The Authority may, upon issuance of a notice to show cause, cancel or vary terms and conditions of the certificate of registration where—
   a. any information given to by the applicant is false or misleading; or
   b. the holder of the registration certificate, without lawful excuse fails to comply with any —
      i. requirement of this Act; or
      ii. any term or condition specified in the registration certificate they may be specified.

22. **DESIGNATION OF THE DATA PROTECTION OFFICER**

1) Every controller and processor shall designate or appoint a data protection officer in order to comply with the provisions of this Act and where -
   a. the processing is carried out by a public authority except for courts acting in their judicial capacity unless otherwise prescribed;
b. the core activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
c. the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data;
d. or such other criteria the Authority may prescribe.

2) A data protection officer must be an employee of the respective controller or processor and shall fulfil other tasks and duties stipulated under this Act.

3) A holding company may appoint a single data protection officer for all its subsidiaries.

4) Where a controller or a processor is a public authority, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures.

5) A person shall be designated or appointed as a data protection officer, if that person has relevant academic and professional qualifications capable of performing the obligations under this Act which includes relevant academic background, knowledge and technical skills in matters relating to information technology, privacy, data protection, data science and law.

7) A controller or processor shall make publicly available the contact details of the data protection officer and communicate them to the Authority.

8) The responsibility of a 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 data controller or processor that this Act is complied with;
c. facilitate capacity building of staff involved in data processing operations;
d. provide advice on data protection impact assessment; and
e. Cooperate with the Authority and any other authority on matters relating to data protection.

23. DUTIES AND OBLIGATIONS OF THE CONTROLLER

1) The controller shall comply with the provisions of this Act when processing personal data and adhere to the principles of processing enumerated in Part II of the Act (principles of processing).

2) Controller shall implement appropriate technical and organisational measures such as encryption, pseudonymisation, anonymisation, data minimisation techniques, privacy-by-design techniques, adopt privacy enhancing technologies as applicable, to ensure and to be able to demonstrate that processing is done in accordance with the provisions of this Act.

3) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.
4) Conduct privacy impact assessments when required by this Act and in accordance with the provisions of this Act.
5) Implement internal oversight mechanisms and integrate such mechanism into its governance structure;
6) Appoint DPO as required by this Act and implement strategies and mechanism to respond to inquiries and incidents related to processing;
7) Where processing is to be carried out by a processor on behalf of a controller:
   a. the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Act and ensure the protection of the rights of the data subject as guaranteed by this Act.
   b. Any processing by a processor on behalf of a controller shall be governed by a contract or any other written law that is binding on the processor that 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 data subjects and the obligations and rights of the controller.
8) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers who shall be jointly responsible in discharging the obligations stipulated above.

24. DUTIES AND OBLIGATIONS OF PROCESSOR

1) Processes the personal data only on documented instructions from the controller.
2) Ensures that its personnel are bound by contractual obligations on confidentiality and secrecy (personnel means any employee, consultant, agent, affiliate or any person who is contracted by the processor to process personal data).
3) Assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in this Act.
4) Assists the controller in ensuring compliance with the obligations under this Act.
5) At the written instructions of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless retention of such record is required by any written law.
6) Allow for and contribute to audits, including inspections upon controller’s request.
7) If a processor infringes this Act by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing and shall be required to comply with the provisions under section 23.
8) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
9) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller:
a. The same data protection obligations as set out in this section shall be imposed on that other processor, hereinafter “sub-processor”.
b. The processor shall remain liable to the controller for the performance
c. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

25. DATA BREACH NOTIFICATIONS

1) In the case of a personal data breach, the controller shall without undue delay and in any event within the prescribed time and in such manner and form as prescribed by the Authority inform the Authority of becoming aware of a personal data breach. The Authority shall issue rules prescribing the following:
   a. The instances where DPA should be informed of such data breach and
   b. Instances where the affected data subject should be informed
   c. Manner and content of such notification

26. DATA PROTECTION IMPACT ASSESSMENTS

1) Wherever and whenever a type of processing is likely to result in a high risk to the rights of data subject prescribed by this Act, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data as stipulated in this Act by taking into account the nature, scope, context and purposes of the processing or any other prescribed criteria and in such manner and form that may be prescribed.

2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3) A data protection impact assessment referred to in section 26(1) shall be mandatory whenever:
   a) a systematic and extensive evaluation of personal data including profiling;
   b) processing on a large scale of special categories data, or of personal data relating to criminal convictions and offences
   c) a systematic monitoring of a publicly accessible areas or telecommunication networks on a large scale or
   d) any other prescribed processing activity

4) The assessment shall contain at least:
   a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
   b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   c) an assessment of the risks to the rights of data subjects referred to in this Act; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act taking into account the rights and legitimate interests of data subjects and other persons concerned; and
e) any other criteria that the Authority may prescribe by rules.

5) Controller shall conduct a fresh data protection impact assessment in accordance with this section whenever there is any significant change in the methodology, technology or process used in the processing activity to which a data protection impact assessment has already been done.

6) Upon the request of the Authority, the controller shall provide the Authority with the data protection impact assessment provided for in this section and, on request, with any other information, so as to allow the Authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7) The Authority shall by Rules published in the Gazette provide guidelines regarding the form and manner in conducting a data protection impact assessment under this section.

27. PRIOR CONSULTATION

1) The controller shall consult the Authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk despite any measure taken by the controller to mitigate the risk.

2) Where the Authority is consulted under section 27(1) above, and the Authority is of the opinion that the intended processing referred to in paragraph above would infringe this Act, in particular where the controller has insufficiently identified or mitigated the risk, the Authority shall, within such prescribed time, provide written advice to the controller and may use any of its powers referred to in this Act.

3) When consulting the Authority pursuant to to this section 27(2), the controller shall provide the Authority with such information that may be prescribed.

4) Notwithstanding anything to the contrary in any other law, the Authority shall be consulted whenever any person or controller engages in processing activity referred to in section 26(3) when such processing amounts to a task carried out by the controller or such person in the public interest, including processing in relation to national security, public safety and public health.
PART V - EXCEPTIONS

28. No exception, restriction or derogation to any of the provisions set out in this Act shall be allowed by the Authority except when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

1) the protection of national security, defence, public safety, economic and financial wellbeing of Sri Lanka, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest.

2) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression and right to information.

PART VI – CROSS-BORDER FLOW OF PERSONAL DATA

29. Any processing of personal data by a controller which is a government Ministry, Department or statutory body shall be processed only in Sri Lanka and shall not be processed outside the territory of Sri Lanka unless the Authority in concurrence with such controller and relevant regulatory body classify categories of personal data that should be localised.

30. A controller or processor shall not be subject to any specific authorisation from the Authority if the Minister by Regulation prescribes a third country, a territory or one or more specified sectors within that third country, or the international organisation, where processing takes place, ensures an adequate level of protection in accordance with the provisions of this Act.

31. However, where such decision under Section 30 has not been made, a controller or processor may process data at a location outside Sri Lanka only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

32. The appropriate safeguards referred to in section 31 may be provided for, without requiring any specific authorisation from DPA by way of:

1) a legally binding and enforceable instrument between joint-controllers or controller and processors which includes enforceable and effective data subject rights, or

2) adopting any other instrument that may be prescribed by the Authority.
33. DPA shall prescribe by rules the grounds on which processing may be lawful when carried out at a location other than Sri Lanka by any processor or controller and the instances where prior authorisation of the Authority is required to process data outside Sri Lanka.

PART VII – DATA PROTECTION AUTHORITY

34. ESTABLISHMENT OF THE DATA PROTECTION AUTHORITY

1) There shall be established an authority which shall be called the Data Protection Authority of Sri Lanka (hereinafter referred to as “the Authority” / “DPA”) for the purposes of this Act.

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

3) The Authority shall be the Apex body for all matters relating to Data Protection matters in Sri Lanka and shall be responsible for the implementation of the provisions of this Act.

35. CONSTITUTION OF THE AUTHORITY

1) The management and administration of the affairs of the Authority shall be vested in a Board of Directors (hereinafter referred to as the “Board” which shall consist of the following:
   a. ex-officio members, namely –
      i. the Secretary to the Ministry of the Minister to whom the subject of Public Administration is assigned;
      ii. the Secretary to the Ministry of the Minister to whom the implementation of this Act is assigned;
      iii. the Secretary to the Treasury or a Deputy Secretary to the Treasury nominated by the Secretary;
      iv. A Deputy Governor nominated by the Monetary Board of the Central Bank of Sri Lanka;
      v. A Director nominated by the Telecommunication Regulatory Commission of Sri Lanka;
      vi. Director General of Health;
   b. Three appointed members to be selected through an public application process, from amongst persons who have experience and have demonstrated professional excellence in the fields of Public or Private sector Management, Law, Finance, Science and Technology and Data Sciences, and who have applied personally or through an industry body or a recognised institution and selected through an interview by the ex-officio members and thereafter appointed by the Minister, on the recommendation of the ex-officio members.
2) The Board shall select one of the appointed members to be the Chairman of the Authority, with approval of the Minister in charge of the subject.

3) Where the Chairman is temporarily unable to perform his duties of his office due to ill health, absence from Sri Lanka or for any other reason, the Chairman may nominate a member to act on his behalf. If Chairman does not make such a nomination or is unable to do so, the members may elect another member as the acting Chairman in addition to his normal duties as a member.

4) The Minister shall, prior to appointing a person as a member of the Authority, satisfy himself that such person has no financial or other conflict of interest in the affairs of the Authority, as is likely to affect adversely, the discharging of his functions as a member of the authority.

5) The Minister shall also satisfy himself, from time to time, that no member of the Authority has since being appointed acquired any such interest referred to in subsection (4).

6) A member of the Authority who is in any way, directly or indirectly interested in any contract made or proposed to be made by the Authority, shall disclose the nature of his interest at a meeting of the authority and such disclosure shall be recorded in the minutes of the Authority and the member shall not participate in any deliberation or decision of the Authority with regard to that contract.

7) Disqualification criteria:
   An appointed member under sub-section 1(b) can be removed by the Minister on the recommendation of the Board where:
   a. such member has become permanently incapable of performing his or her duties owing to any physical disability or unsoundness of mind;
   b. such member is unfit to perform his or her duties on the basis of moral turpitude; or
   c. such member is convicted of an offence by a competent court of law.

8) Holding of meetings:
   a. The Board shall meet at least once in every month or as often as may be necessary.
   b. The quorum for any meeting of the Board shall be five members which includes remote participation.
   c. Where a vote is equally split, the Chairman shall have a casting vote.

36. EMPLOYEES OF THE AUTHORITY

1) The Authority shall appoint-
   a. Director-General who shall be the Chief Executive Officer of the Authority;
   b. such officers and other employees as it considers necessary appointed in accordance with the scheme of recruitment and selection criteria approved by the Authority.

2) The Director-General shall be responsible for the general supervision, direction and management of the affairs of the Authority and exercise disciplinary control over the officers and employees of the Authority.
3) The Director-General and other officers and employees appointed under subsection (1), shall be subject to such terms and conditions of service as shall be determined by the Authority and be paid such remuneration as determined by the Authority in consultation with the Minister assigned the subject of Finance.

37. **POWERS OF THE AUTHORITY**

For the purpose of performing its duties and discharging of its functions under this Act, the Authority shall have the power-

1) taking, purchasing or otherwise acquiring, holding, charging or disposing of movable and immovable property;
2) entering into contracts;
3) to carry out all duties and functions set out in section 39 and perform all such matters connected or incidental thereto.
4) doing such other legal acts necessary for the proper performance of the functions of the Authority
5) make orders in accordance with section 38
6) to direct a controller to reimburse fees charged from a citizen due to any information
7) For the purpose of investigating into a complaint received by the Authority, holding an inquiry in relation to an appeal or making an order under section 38:  
   a. require any person to appear before it;
   b. examine such person under oath or affirmation and require such person where necessary to produce any information related to processing
   c. to inspect any information strictly related to the processing in question that is held or controlled by a controller or processor by an officer authorized on that behalf by the Authority. In any event, such officer shall be a senior staff member of the Authority having relevant expertise to conduct such inspection.
   d. make a determination in accordance with the provisions of this act with due consideration of the information available to it
8) to enforce its orders or determinations made under this Act against a controller or processor through prosecution.
9) Data Protection Authority has power and has a duty to prosecute for the offences under this Act
10) Prescribe rules under this Act including but not limited to registration as a controller, registration fees and procedure for conducting data protection impact assessments.
11) Notwithstanding anything to the contrary in any other law, the Authority shall be consulted during the preparation of a proposal for a legislative measure to be adopted by Parliament, or of a regulatory framework based on such a legislative measure, which relates to processing of personal data.
12) To act independently when exercising its powers, duties and functions in accordance with this Act.
13) The Authority may carry out periodical audits in relation to any processing activity carried out by a controller or processor to ensure compliance with this Act.

38. ORDERS TO BE MADE BY THE AUTHORITY

1) Without prejudice to section 52(1), where the Authority is of the opinion any person –
   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 fail to comply with the provisions of this Act, or any rule, regulation, instruction, directive or order given under this Act or any other written law which in the opinion of the Authority relates to processing of personal data,

   make an order to that person requiring such person, within such time as the Authority considers necessary —
   i. to cease and refrain from engaging in the act, omission or course of conduct related to processing; and
   ii. to perform such acts as in the opinion of the Authority are necessary to rectify the situation.

2) Every Order issued under this section shall be served on such person to whom it is ordered and shall be in force from the date of service thereof.

3) Every order issued under this section shall be binding on the person to whom it is directed.

4) Where a controller or processor fails to comply with an order issued under subsection (1), the Authority may, upon application to the High Court of the Western Province, holden in Colombo and upon satisfying the Court that a controller or processor has failed without reasonable excuse to comply in whole or in part with the order issued by it under subsection (1), obtain an order against the controller or processor and any or all of the officers or employees of that controller or processor in such terms as the Court deems necessary to enforce compliance with such obligation.

39. DUTIES AND FUNCTIONS OF THE AUTHORITY

The duties and functions of the Authority shall be, to –

1) to direct a controller to publish it clear explicit terms of processing activities in accordance with schedule 5.

2) monitor the performance and ensure the due compliance by controllers and processors of the duties cast on them under this Act;

3) provide directions to any specific controller regarding any processing activity performed by such controller;
4) issue guidelines based on reasonableness, for determining registration fee to be levied from controllers registered under this Act;
5) facilitate or undertake training activities for controllers on the effective implementation of the provisions of this Act;
6) issue guidelines for the proper data protection management for controllers and processors
7) establish and maintain a Register of controllers;
8) exercise its powers to monitor or examine all data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;
9) promote self-regulation among controllers and processors;
10) ensure country's compliance on data protection obligations under international conventions;
11) to advise the Government on all matters relating to data protection;
12) to represent the Government internationally on matters relating to data protection;
13) to conduct research and studies and promote educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities;
14) to 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;
15) to carry out functions conferred on the Authority under any other written law;
16) undertake research on developments in data processing of personal data;
17) perform such other functions as may be prescribed by any other law or as considered necessary for the promotion of object of this Act.

40. FUNDS OF THE AUTHORITY

1) The Authority shall have its own Fund, into which shall be credited-
   a. all such sums of money as may be voted upon by Parliament for the establishment and administration of the Authority;
   b. revenue generated from registration fees
   c. penalties imposed by the Authority

2) There shall be paid out of the Fund all such sums of money required to defray the expenditure incurred by the Authority in the exercise, discharge and performance of its powers, duties and functions.
The financial year of the Authority shall be the calendar year.

The Authority shall cause proper books of accounts to be maintained of the income and expenditure and all other transactions of the Authority.

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.

The provisions of Part II of the Finance Act, No. 38 of 1971 shall, mutatis mutandis apply to the financial control and accounts of the Authority.

The members and officers and all other employees of the Authority shall be deemed to be public servants within the meaning and for the purposes of the Penal Code (Chapter 19) and every inquiry held by the Authority under this Act shall be deemed to be a judicial proceeding within the meaning of the Code of Criminal Procedure Act, No. 15 of 1979.

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.

Any expenses incurred by any member, officer or employee of the Authority in any suit or prosecution brought by or against such person before any court in respect of any act or omission which is done or purported to be done by such person in good faith for the purpose of carrying out the provisions of this Act shall, if the court holds that such act or omission 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.

The Authority shall within six months of its establishment, formulate and give adequate publicity to the procedural requirements.
47. **DELEGATION OF POWERS OF THE AUTHORITY**

The Authority may, subject to such conditions as the Authority may impose, delegate any power conferred under this Act or any rules or regulations made under this Act to— (a) an employee of the Authority, (b) A regulator or professional body, or any other public body established through an Act of parliament or any other law.

**PART VIII – DIRECT MARKETING**

48. **USE OF PERSONAL DATA ON DIRECT MARKETING**

1) Natural or legal persons may use electronic or digital communication or telecommunication services or any other means for the purposes of sending direct marketing communications to end-users who are natural persons that have given their unambiguous consent.

2) Where a natural or legal person obtains contact details from its customer, in the context of the sale of a product or a service, that natural or legal person may use these contact details for direct marketing of its own similar products or services with the consent of such customer.

3) The right to object shall be given at the time of collection and each time a message is sent.

4) Without prejudice to sub-section 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:
   
   a. present the identity of a line on which they can be contacted; or
   
   b. present a specific code/or prefix identifying the fact that the call is a marketing call

5) Natural or legal persons shall ensure that right to object to direct marketing by data subjects is always complied with.

6) Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, from receiving further marketing communications.

7) The Authority shall be empowered to adopt implementing measures in consultation with the relevant regulatory bodies in specifying the code/or prefix to identify marketing calls, pursuant to sub-section 4(b).

8) For the purpose of this section, 'direct marketing communications' means any form of advertising, directly or indirectly, whether written or oral, sent to one or more identified or identifiable end-users via electronic or digital communication or telecommunication services or any other means including the use of
automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.. In addition to the offering of products and services for commercial purposes, this also include messages sent by political parties and other organisations that contact natural persons via electronic or digital communication or telecommunication services or any other means in order to promote their parties or organisation or any member of such party or organisation. The same applies to messages sent by other non-profit organisations to support the purposes of such organisation.

PART IX – GENERAL

49. RULES AND REGULATION

1) The Minister shall upon the recommendation of the Authority, make regulations in respect of all matters required by this Act to be prescribed or in respect of which regulations are necessary to be made in order to give effect to the principles and provisions of this Act including the following matters:
   a. Recognising the rights and the manner of exercising such rights of data subject in relation to automated decision making under section 14, data portability and such other rights having duly considered the extensive and innovative uses of personal data that may potentially increase data protection risks;
   b. Additional conditions under Schedule 1, 2, 3 and 4
   c. Recognising third countries with adequate protection under section 30.

2) 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 the regulation.

3) Every regulation made under subsection (1) shall, forthwith 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 as from the date of such disapproval but without prejudice to anything previously done thereunder. The date on which any regulation is deemed to be so rescinded shall be published in the Gazette.

4) The Authority may make rules concerning any of the following matters:-
   a. Prescribing the form and manner of exercising rights under section 9, 10, 11 and 12
   b. the form and manner in which appeals may be made to the Authority under section 15.
   c. manner and form of applying for registration under section 17
   d. conditions for exemptions for registration under section 18.
   e. data breach notification procedure under section 25
   f. form and manner of conducting data protection impact assessments under section 26(7)
g. Conditions for effective cross border data transfers under section 33
h. the procedure for holding inquiries under section 37(7)

50. No rule made under this subsection (4) shall have effect until it is approved by the Minister and notification of such approval is published in the Gazette.

51. Any regulation or rule made under this Act prior to being published in the Gazette shall be first published by the Authority for public consultation. The prescribed time period for receiving public observations shall not be less than 2 weeks.

52. IMPOSITION OF A PENALTY BY THE AUTHORITY TO ENFORCE COMPLIANCE

1) Where a person required to conform to the provisions prescribed by this Act, who fails to so conform, shall be liable to a penalty as may be prescribed taking into consideration the nature and gravity of relevant non-compliance. Provided however such penalty shall not exceed 2% of global turnover of such controller or processor or a sum of rupees twenty-five million, whichever is higher, in any given case. Where a person who has been subjected to a penalty on a previous occasion, subsequently fails to conform to a requirement on any further occasion such person shall be liable to the payment of an additional penalty in a sum consisting of double the amount imposed as a penalty on the first occasion and for each non-compliance after such first occasion.

2) If a person who becomes liable to a penalty in terms of subsection (1) fails to pay such penalty, the Authority may make an ex-parte application to the High Court of the Western Province holden in Colombo for an Order requiring the payment of the penalty and upon such order being made such amount shall be recoverable in the same manner as a fine imposed by Court.

3) The imposition of a penalty under this section shall not preclude a supervisory authority or a regulatory or self regulatory authority of an Institution from taking any regulatory or disciplinary measures including, but not limited to, the suspension of such controller or processor from the 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.

4) Where a penalty is imposed under this section on a body of persons, then-
   a. if that body of person is a body corporate, every person who at the time of the imposition of the requirements under subsection (1) was a Director, General Manager, Secretary or other similar officer of that body; or
   b. if that body is not a body corporate, every person who at the time of the imposition of such requirements was the President, Manager, Secretary, partner or other similar officer 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 or that he exercised all due diligence to ensure compliance therewith.

53. DEFINITIONS

- ‘anonymize’ means permanant removal of any personal identifiers to render any personal data from being related to a identified or identifiable natural person
- ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- ‘child’ notwithstanding anything to the contrary in any law, a child means a natural person who is below the age of 18
- ‘consent’ means any freely given, specific, informed and unambiguous indication by way of a written declaration or a affirmative action signifying a data subject’s agreement to the processing of his/her personal data;
- ‘data concerning health’ means personal data related to the physical or psychological health of a natural person, which includes any information that indicates his/her health situation or status;
- ‘Data Protection Officer (DPO)’ means the person designated under section 22
- ‘data subject’ means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier including but not limited to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person;
- ‘encryption’ means the act of ciphering or altering data using mathematical algorithm to make such data unintelligible to unauthorised 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 including financial status and credit history;
- ‘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;
- ‘Minister’ means the Minister assigned the subject of Information Technology and Digital Infrastructure
‘personal data breach’ means any act or omission that results in accidental or unlawful destruction, loss, alteration, unauthorised 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 related to the race or ethnicity of a natural person.

‘personal data’ means any information whether true or not, relating to a data subject.

‘profiling’ means processing personal data to evaluate, analyse or predict aspects concerning that data subject's performance at work, economic situation, health, personal preferences, interests, credibility, behaviour, 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 organisational measures to ensure that the personal data are not attributed to a data subject.

‘public authority’ means:
   a) a Ministry of the Government;
   b) any body or office created or established by or under the Constitution, any written law, other than the Companies Act No. 7 of 2007, except to the extent specified in paragraph (e), or a statute of a Provincial Council;
   c) a Government Department;
   d) a public corporation as defined by the Constitution;
   e) a company incorporated under the Companies Act, No. 7 of 2007, in which the State, or a public corporation or the State and a public corporation together hold twenty-five per centum or more of the shares or otherwise has a controlling interest;
   f) a local authority;
   g) any department or other authority or institution established or created by a Provincial Council;
   h) non-governmental organisations that are substantially funded by the government or any department or other authority established or created by a Provincial Council or by a foreign government or international organisation, rendering a service to the public in so far as the information sought relates to the service that is rendered to the public;
   i) higher educational institutions including private universities and professional institutions which are established, recognised or licensed under any written law or funded, wholly or partly, by the State or a public corporation or any statutory body established or created by a statute of a Provincial Council;

‘recipient’ means a natural or legal person, public authority, or any other body, to which the personal data is disclosed.
• ‘**special categories of data**’ personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, financial data, and 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, personal data relating to a child and any other personal data that the Minister may determine upon the recommendation of the Authority from time to time by Regulation in accordance with the provisions of this Act.

• ‘**controller**’ means any natural or legal person, public authority or other body which, alone or jointly with others, engages in processing and determines the purposes and means of processing.

• ‘**cross-border flows of personal data**’ means movement of personal data out of the territory of Sri Lanka.

• ‘**Data Protection Authority (DPA)**’ means the regulatory body established under the provisions of 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 and/or arithmetical operations on personal data data;

• ‘**processor**’ means a natural or legal person, public authority or other body which processes personal data on behalf of the controller; for the avoidance of doubt, a processor shall be a separate entity/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 manager.

Illustration: A Hospital 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. The Hospital is the controller. And Company B is the processor where management of patient records are concerned. The data scientist of the hospital is only and employee of the controller and not a processor.

• ‘**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.
SCHEDULE 1 CONDITIONS FOR LAWFUL PROCESSING

(a) the data subject has given consent to the processing of his or her personal data.
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject to;
(d) processing is necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller by law;
(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) Any other condition as may be specified by the Authority.
SCHEDULE 2 - ADDITIONAL CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF DATA

(a) the data subject has given consent, to the processing of those personal data for one or more purposes specified by the controller at the time of processing, unless any other law prohibits the processing of those 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.

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security including pension, and for public health purposes such as security, monitoring and alert purposes, 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 prescribed by any law providing for appropriate safeguards for rights of the data subject;

(c) processing is necessary 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;

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

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

(f) processing is necessary for reasons of substantial public interest, as prescribed by law which shall be necessary and proportionate to the aim pursued whilst providing suitable and specific measures to safeguard the rights and the interests of the data subject;

(g) where 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 those data are processed by a health professional licensed under or authorised by any law prevailing in Sri Lanka.

(h) processing is necessary for archiving purposes in the public interest, scientific 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 law and provide for suitable and specific measures to safeguard the rights and the interests of the data subject.
SCHEDULE 3 - CONDITIONS FOR CONSENT

(a) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(b) If the data subject's consent 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. Any part of such a declaration which constitutes an infringement of this Act shall not be binding.

(c) When assessing whether consent is freely given, utmost account shall be taken on 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.

(d) Prior to giving consent, the data subject shall be informed thereof that consent can be withdrawn anytime.

(e) Any other condition as may be specified by the Authority.
SCHEDULE 4 - PROCESSING OF PERSONAL DATA RELATING TO CRIMINAL INVESTIGATIONS AND OFFENCES

(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, 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 or provisions under any written law.

(c) Conditions for providing appropriate safeguards for the rights and freedoms of data subjects under this schedule may be prescribed by the Authority.
SCHEDULE 5 – NOTICE CONDITIONS

The controller shall provide the data subject with the following information, no later than at the time of collection of the personal data or, if the data is not collected from the data subject, as soon as is reasonably practicable—

1. the purposes for which the personal data is to be processed;
2. the categories of personal data being collected;
3. the identity and contact details of the controller and the contact details of the data protection officer, if applicable;
4. the right of the data subject to withdraw such consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;
5. the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds in Schedule 1 or Schedule 2;
6. the source of such collection, if the personal data is not collected from the data subject;
7. the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;
8. information regarding any cross-border transfer of the personal data that the controller intends to carry out, if applicable;
9. the period for which the personal data will be retained in terms of section 6 or where such period is not known, the criteria for determining such period;
10. the existence of and procedure for the exercise of data subject rights mentioned in Part III and any related contact details for the same;
11. the existence of a right to file complaints to the Authority; and
12. any other information as may be prescribed by the Authority.