**THE GAZETTE OF THE DEMOCRATIC SOCIALIST REPUBLIC OF**   
**SRI LANKA**

**Part II of November 19, 2021**

**SUPPLEMENT**

*(Issued on 25.11.2021)*



**PERSONAL DATA PROTECTION**

**A**

**BILL**

**to provide for the Regulation of Processing of Personal Data; to identify and stregnthen the Rights of Data Subjects in relation to the protection of Personal Data; to provide for the designation of the Data Protection Authority; and to provide for matters connected therewith or incidental thereto**

*Ordered to be published by His Excellency the President and Minister of Technology*

PRINTEDATTHEDEPARTMENTOFGOVERNMENTPRINTING, SRILANKA   
 TOBEPURCHASEDATTHEGOVERNMENTPUBLICATIONSBUREAU, COLOMBO5   
**Price : Rs. 85.00**  **Postage : Rs. 45.00**

*This Gazette Supplement can be downloaded from* www.documents.gov.lk 

|  |  |
| --- | --- |
| *Personal Data Protection* | 1 |

L.D.O—19/2019.

AN ACTTOPROVIDEFORTHEREGULATIONOFPROCESSINGOF PERSONAL DATA; TOINDENTIFYANDSTREGNTHENTHERIGHTSOF DATASUBJECTS INRELATIONTOTHEPROTECTIONOF PERSONAL DATA; TOPROVIDE FORTHEDESIGNATIONOFTHE DATA PROTECTION AUTHORITY; AND

TOPROVIDEFORMATTERSCONNECTEDTHEREWITHORINCIDENTAL

THERETO

WHEREAS it has become necessary to facilitate the growth Preamble

and innovation in the digital economy in Sri Lanka whilst protecting the personal data rights of the data subjects:

AND WHEREAS it has become necessary to improve 5 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 10 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

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | Democratic Socialist Republic of Sri Lanka as follows: - | | Short Title |
| **1.** | (1) This Act may be cited as the Personal Data |
| and date of |
| Protection Act, No. …. of 2021. | |
| operation |

(2) The provisions of this section, shall come into operation on the date on which the certificate of the Speaker 20 is endorsed in respect of this Act in terms of Article 79 of the Constitution.

2 *Personal Data Protection*

(3) All other provisions of this Act, shall come into operation on such date as the Minister may, determine by Order published in the *Gazette*:

Provided however, the date of operation of the provisions 5 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).

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **2.** | (1) This Act shall apply to the processing of personal | Application |
| data— | where the processing of personal data takes place | of this Act |
| (*a*) |

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 15 Sri Lanka;

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

(iii) is subject to any written law of Sri Lanka;

(iv) offers goods or services to data subjects in 20 Sri Lanka including the offering of goods or services with specific targeting of data subjects in Sri Lanka; or

(v) specifically monitors the behaviour of data subjects in Sri Lanka including profiling with 25 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.

*Personal Data Protection*  3

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

|  |  |  |
| --- | --- | --- |
| 5 | (*a*) | the circumstances in which the specific targeting |
| (*b*) | of the data subjects may occur; or |
| 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 private,

|  |  |
| --- | --- |
| 10 | domestic or household purposes by an individual; and |

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

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **3.** | (1) The provisions of this Act shall have effect | The |
| notwithstanding anything to the contrary in any other written | | provisions of |
| law, relating to the protection of personal data of data | | this Act to |
| prevail in |
| subjects: | |
| case of any |
| Provided however, where a public authority is governed | | inconsistency |

by any other written law, it shall be lawful for such authority to carry out processing of personal data in accordance with

|  |  |
| --- | --- |
| 20 | 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.

25 PART I

PROCESSINGOF PERSONAL DATA

|  |  |  |
| --- | --- | --- |
| **4.** | Every controller shall process personal data in | Compliance with the data protection |
| compliance with the obligations specified under this Act. | |

obligations

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | 4 | *Personal Data Protection* | Obligation to |
| **5.** The processing of personal data shall be lawful if a | |
| controller is in compliance with— | | process |
| personal date |
| (*a*) | any condition specified in Schedule I hereto; | in a lawful |
| manner |
| (*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

|  |  |
| --- | --- |
| 10 | 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.

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **6.** | (1) Every controller shall, ensure that personal data | Obligation to |
| 20 | is processed for a— | | define a |
| purpose for |
| (*a*) | specified; | personal data |
| processing |
| (*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, 25 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).

|  |  |  |  |
| --- | --- | --- | --- |
| *Personal Data Protection* | | 5 | Obligation to confine  personal data processing to the defined |
| **7.** | Every controller shall ensure that personal data that | |
| is processed shall be— | | |
| (*a*) | adequate; | |

purpose

|  |  |  |
| --- | --- | --- |
| 5 | (*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.

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **8.** | Every controller shall ensure that personal data that | Obligation to |
| is processed shall be— | | ensure |
| accuracy |
| (*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.

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **9.** | Every controller shall ensure that personal data that | Obligation to |
| is being processed shall be kept in a form which permits | | limit the |
| period of |
| identification of data subjects only for such period as may | |
| retention |
| be necessary or required for the purposes for which such | |

personal data is processed:

20 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.

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | **10.** | Every controller shall ensure integrity and | Obligation to |
| confidentiality of personal data that is being processed, by | | maintain |
| Integrity and |
| using appropriate technical and organizational measures | |
| Confidentiality |

6 *Personal Data Protection*

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

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | (*a*) | unauthorized or unlawful processing of personal | Obligation to |
| (*b*) | data; or |
| loss, destruction or damage of personal data. |
| **11.** | A controller shall, provide data subjects— |

process

|  |  |  |
| --- | --- | --- |
| 10 | (*a*) the information referred to in Schedule V; and | personal data |
| in a |
| (*b*) the information regarding any decision taken | transparent |
| manner |
| 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 15 | **12.** | (1) It shall be the duty of every controller to | | Accountability |
| implement internal controls and procedures, (hereinafter | | | in the |
| referred to as the “Data Protection Management Programme”) | | | processing of |
| personal data |
| that— | | |
| (*a*) | | establishes and maintains duly catalogued records |

to demonstrate the manner in which the

|  |  |
| --- | --- |
| 20 | 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

|  |  |  |
| --- | --- | --- |
| 25 | (*c*) | controller; |
| provides for appropriate safeguards based on data |

protection impact assessments specified in   
section 24;

|  |  |  |
| --- | --- | --- |
| 30 | (*d*) | is integrated into the governance structure of the |
| controller; |

*Personal Data Protection*  7

(*e*) establishes internal oversight mechanisms;

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

|  |  |  |
| --- | --- | --- |
| 5 | (*g*) | is updated based on periodic monitoring and |
| (*h*) | assessments; and |
| facilitates 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.

|  |  |
| --- | --- |
| 10 | (2) The Authority shall from time to time issue such guidelines in respect of the Data Protection Management |

Programme.

PART II

RIGHTSOF DATA SUBJECTS

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **13.** | (1) Every data subject shall have the right to access | Right of |
| to personal data of such data subject and to be provided | | access to |
| personal data |
| 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 20 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.

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | **14.** | (1) Every data subject shall have the right to | Right of |
| withdraw his consent at any time upon a written request | | withdrawal |
| of the |
| made by such data subject if such processing is based on the | |
| consent and |
| grounds specified in item (*a*) of Schedule I or item (*a*) of | |
| the right to |
| Schedule II of this Act: | | object to |
| processing |

8 *Personal Data Protection*

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

|  |  |
| --- | --- |
| 5 | (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.

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **15.** | Every data subject shall have the right to request a | Right to |
| controller in writing to rectify or complete the personal data | | rectification |
| relating to such data subject which is either inaccurate or | | or |
| completion |
| 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 15 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:

20 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.

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | **16.** | Every data subject shall have the right to make a | Right to |
| written request to the controller to have his personal data | | erasure |

erased, under the following circumstances where:–

(*a*) the processing of personal data is carried out in   
 contravention of the obligations referred to in

|  |  |  |
| --- | --- | --- |
| 30 | (*b*) | sections 5,6,7,8,9,10 and 11; |
| 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;

*Personal Data Protection*  9

(*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.

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | **17.** | (1) Where a controller receives a written request | Grant or |
| from a data subject under sections 13, 14, 15 or 16, such | | refusal of |
| rectification, |
| controller shall inform the data subject in writing, within | |
| completion, |
| twenty-one working days from the date of such request, | |
| erasure or |
| 10 |
| whether– | | refrain from |
| further |
| (*a*) | such request has been granted; | processing |
| (*b*) | such request has been refused under subsection (2) |

and the reasons thereof unless such disclosure is   
prohibited by any written law; or

|  |  |  |
| --- | --- | --- |
| 15 | (*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*).

20 (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–

|  |  |  |
| --- | --- | --- |
| 25 | (*a*) | the national security; |
| (*b*) | public order; |
| (*c*) | any inquiry, investigation or procedure conducted |

under any written law;

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

|  |  |  |
| --- | --- | --- |
| 10 | (*e*) | *Personal Data Protection* |
| 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

|  |  |  |
| --- | --- | --- |
| 5 | (*g*) | controller to act on such request; |
| subject to the provisions of subsection (4), the |

inability of the controller to establish the identity   
of the data subject; or

|  |  |  |
| --- | --- | --- |
| 10 | (*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 15 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 20 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

|  |  |  |
| --- | --- | --- |
| 25 | (*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

*Personal Data Protection*  11

(*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.

|  |  |
| --- | --- |
| 5 | (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 data subject the details of such fees

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | and reasons for imposing same. | | Automated |
| **18.** | (1) Subject to section 19, every data subject shall |
| 15 | have the right to request a controller to review a decision of | | individual |
| decision |
| such controller based solely on automated processing, which | |
| making |
| 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–

|  |  |  |
| --- | --- | --- |
| 20 | (*a*) | authorized by any written law, which a controller is |
| (*b*) | subject to; |
| authorized in a manner determined by the |

Authority;

|  |  |  |
| --- | --- | --- |
| 25 | (*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 30 of the data subject:

12 *Personal Data Protection*

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

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | **19.** | (1) Where a controller– | Right of |
| appeal of the |
| (*a*) has not refrained from further processing of |
| data subjects |
| to the |
| personal data under section 14; or |
| Authority |
| (*b*) has refused to rectify or complete personal | and the |
| process of |
| data under section 15; or | determination |
| of such |
| (*c*) has refused to erase personal data under | appeal |

section 16; or

|  |  |
| --- | --- |
| 10 | (*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),

15 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 to refrain from 20 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;

25 (*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;

*Personal Data Protection*  13

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

(3) After concluding the necessary investigations, the 5 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 10 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.

15 (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

|  |  |  |  |
| --- | --- | --- | --- |
| 20 | CONTROLLERSAND PROCESSORS | | Designation |
| **20.** | (1) Every controller and processor shall designate |
| 25 | or appoint a Data Protection Officer, to ensure compliance | | of the Data |
| Protection |
| with the provisions of this Act, in the following | |
| Officer |
| 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

|  |  |  |
| --- | --- | --- |
| 14 | (*b*) | *Personal Data Protection* |
| 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, 5 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 10 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 15 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 20 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 25 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.

|  |  |
| --- | --- |
| 30 | (4) A controller or processor shall publish the contact details of the Data Protection Officer and communicate them |

to the Authority.

*Personal Data Protection*  15

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

(*a*) advise the controller or processor and their   
 employees on data processing requirements

|  |  |  |
| --- | --- | --- |
| 5 | (*b*) | provided under this Act or any other written law; |
| 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;

|  |  |  |
| --- | --- | --- |
| 10 | (*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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 15 | **21.** | (1) Where processing is to be carried out by a | | Additional |
| processor on behalf of a controller, the controller shall– | | | obligations |
| of the |
| (*a*) | | use only processors who ensure the provision of |
| controllers |

appropriate technical and organizational measures   
to give effect to the provisions of this Act and ensure

|  |  |  |
| --- | --- | --- |
| 20 | (*b*) | the protection of rights of the data subjects under |
| this Act; and |
| ensure that such processor is bound by a contract or |

provisions of any written law which sets out the

|  |  |
| --- | --- |
| 25 | 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

|  |  |
| --- | --- |
| 30 | referred to as “joint controllers” who shall be jointly responsible for discharging the obligations stipulated under |

this Act.

|  |  |  |
| --- | --- | --- |
| 16 | *Personal Data Protection* | 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 and in 5 compliance with the data protection obligations imposed under Part I of this Act;

(*b*) ensure that its personnel are bound by contractual   
 obligations on confidentiality and secrecy;

|  |  |  |
| --- | --- | --- |
| 10 | (*c*) | assist the controller in ensuring compliance with |
| (*d*) | its obligations imposed under Part I of this Act; |
| assist the controller by providing appropriate |

technical and organizational measures, for the   
fulfilment of the obligations of the controller under   
Part II of this Act;

|  |  |  |
| --- | --- | --- |
| 15 | (*e*) | 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 provision of services relating to processing;   
and

|  |  |  |
| --- | --- | --- |
| 20 | (*f*) | facilitate the controller to carry out compliance |
| audits, including inspections upon the request of |

the controller.

(2) Where a processor fails to comply with the provisions of paragraph (*a*) of subsection (1) or determines the purposes 25 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

|  |  |
| --- | --- |
| 30 | out specific processing activities, the provisions of this section shall apply to and in relation to such sub processor. |

*Personal Data Protection*  17

(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 (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.

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **23.** | (1) In the event of a personal data breach, a controller | Personal Data |
| shall notify the Authority, regarding such personal data | | breach |
| breach in such manner, form and within such period of time | | notifications |

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;

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

(*c*) the form, and manner of making such notification, and the information which shall be provided in such notification relating to 20 the data breach,

by way of rules made under this Act.

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | **24.** | (1) Where a Controller intends to carry out any | Personal data |
| processing which involves– | | protection |
| impact |
| (*a*) | a systematic and extensive evaluation of personal | assessments |
| data or special categories of data including | |

profiling;

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

|  |  |  |
| --- | --- | --- |
| 18 | (*c*) | *Personal Data Protection* |
| 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 5 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.

10 (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).

|  |  |
| --- | --- |
| 15 | (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 20 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.

25 (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 30 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | *Personal Data Protection* | | 19 | Measures to |
| **25.** | (1) Where a personal data protection impact | |
| assessment carried out under section 24 indicates that the | | | mitigate risks |
| of harm and |
| processing is likely to result in a risk of harm to the rights of | | |
| the |
| the data subjects guaranteed under this Act or any written | | |
| requirement |
| law, a controller shall take such measures to mitigate such | | | for prior |
| consultation |
| 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 10 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.

15 (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, 20 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 25 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

|  |  |
| --- | --- |
| 30 | processing is carried out by a controller in relation to national security, public order and public health, the controller shall |

consult the Authority.

|  |  |  |
| --- | --- | --- |
| 20 | *Personal Data Protection* | 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, 5 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).

10 (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

|  |  |
| --- | --- |
| 15 | 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.

|  |  |  |
| --- | --- | --- |
| 20 | (*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

|  |  |  |
| --- | --- | --- |
| 25 | (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–

|  |  |  |
| --- | --- | --- |
| 30 | (*a*) | in a third country prescribed pursuant to an |
| (*b*) | adequacy decision; or |
| in a country, not being a third country prescribed |

pursuant to an adequacy decision, only where such

*Personal Data Protection*  21

controller or processor ensures compliance with the   
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

|  |  |
| --- | --- |
| 5 | 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 10 protected by this Act.

PART IV

USEOF PERSONAL DATATO DISSEMINATE UNSOLICITED   
MESSAGES

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **27.** | (1) Subject to section 14, a controller may use postal | Use of |
| services, telecommunication services, electronic means or | | personal data |
| on direct |
| any other similar means for the purposes of disseminating | |
| marketing |
| messages only if a data subject has given consent to receive | |

such messages (hereinafter referred to as “solicited messages”).

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

(3) When obtaining consent under subsection (1), the controller shall, at the time of collecting contact information 25 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

|  |  |
| --- | --- |
| 30 | 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.

22 *Personal Data Protection*

(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.

5 (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

|  |  |  |
| --- | --- | --- |
| 10 | (*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 15 intervention.

PART V

DATA PROTECTION AUTHORITY

|  |  |  |  |
| --- | --- | --- | --- |
| 20 | **28.** | (1) The Minister may, by Order published in the | Designation |
| *Gazette*, designate a public corporation, statutory body or | | of the |
| Authority |
| any other institution established by or under any written | |

law and controlled by the government as the “Data Protection Authority of Sri Lanka” (in this Act referred to as the “Authority”), for the purposes of this Act.

(2) The Minister shall, in making the Order referred to in 25 subsection (1) take into consideration the–

(*a*) capacity, competency and expertise;

(*b*) the availability of the staff, infrastructure and other   
 resources;

*Personal Data Protection*  23

(*c*) the composition and the governing structure, and   
 any other matter relating to the administration,

of such public corporation, statutory body or the institution, for the purpose of determining the ability of such public

|  |  |
| --- | --- |
| 5 | corporation, statutory body or the other institution as designated to efficiently exercise, perform and discharge |

the powers, duties and functions of the Authority under this Act.

(3) The Minister shall from time to time review the

|  |  |
| --- | --- |
| 10 | 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.

(4) The Authority shall within six months of the end of each financial year, submit to the Minister an annual report 15 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.

(5) The Minister shall, lay copies of the report and 20 documents submitted under subsection (4) before Parliament within six months from the date of receipt of such report and the documents.

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | **29.** | The objects of the Authority shall be– | Objects of |
| the Authority |
| (*a*) | to regulate the processing of personal data in |
| (*b*) | accordance with the provisions of this Act; |
| 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;

|  |  |  |
| --- | --- | --- |
| 30 | (*c*) | to provide for mechanisms to ensure the protection |

of personal data of data subjects engaged in digital   
transactions and communications;

|  |  |  |
| --- | --- | --- |
| 24 | (*d*) | *Personal Data Protection* |
| to ensure the regulatory compliance with the |

provisions of this Act to facilitate for the growth   
and innovation in digital economy.

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | **30.** | The Authority may exercise the following powers, | Powers of the |
| for the purpose of performing duties and discharging | | Authority |

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

10 necessary for the implementation of the provisions of this Act;

(*b*) to examine a person under oath or affirmation and   
 require such person where necessary to produce any   
 information relating to the processing of functions

|  |  |
| --- | --- |
| 15 | of a controller or processor in the manner prescribed, for the purpose of discharging the functions of this |

Act;

(*c*) to take all such steps to ensure that controllers and   
 processors carry out their duties and obligations in

|  |  |
| --- | --- |
| 20 | 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;

|  |  |  |
| --- | --- | --- |
| 25 | (*d*) | 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;

|  |  |  |
| --- | --- | --- |
| 30 | (*e*) | 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;

*Personal Data Protection*  25

(*f)*  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

|  |  |  |
| --- | --- | --- |
| 5 | (*g*) | imminent risk to the rights of the data subjects; |
| to carry out periodical evaluations into the manner |

in which and procedures used for any processing   
activities carried out by a controller or psoes,   
including the data protection management

|  |  |  |
| --- | --- | --- |
| 10 | (*h*) | programme; |
| to recognize certification and certifying bodies in |

relation to personal data protection;

(*i*) to enter into agreements with or engage in any activity, either alone or in conjunction with other 15 apex government or regulatory institutions or international agencies or organizations, responsible for data protection outside Sri Lanka for the purposes of this Act;

|  |  |  |
| --- | --- | --- |
| 20 | (*j*) | 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;

|  |  |  |
| --- | --- | --- |
| 25 | (*k*) | 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;

|  |  |  |
| --- | --- | --- |
| 30 | (*l*) | 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

26 *Personal Data Protection*

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;

|  |  |  |
| --- | --- | --- |
| 5 | (*m*) | to invest its funds in such manner as the Authority |

may deem necessary;

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

(*o*) to establish standards in relation to data protection and data storage, data processing, obtaining consent 10 and such other matters as may be necessary for the proper implementation of the provisions of this Act;

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

Provided however, the Authority shall obtain 15 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;

|  |  |  |
| --- | --- | --- |
| 20 | (*q*) | 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

(*r*) to do any other acts as may be necessary or conducive to the attainment of the objects of the 25 Authority under this Act.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | *Personal Data Protection* | | 27 | Duties and |
| **31.** | For the purpose of carrying out its objects, the | |
| Authority shall, perform and discharge all or any of the | | | functions of |
| following duties and functions:– | | | the Authority |
| (*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 10 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;

|  |  |  |
| --- | --- | --- |
| 15 | (*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;

|  |  |  |
| --- | --- | --- |
| 20 | (*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;

|  |  |  |
| --- | --- | --- |
| 25 | (*g*) | ensure domestic compliance of data protection |
| (*h*) | obligations under international conventions; |
| 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

30 of the Minister;

|  |  |  |
| --- | --- | --- |
| 28 | (*j*) | *Personal Data Protection* |
| promote studies and educational activities relating |

to data protection, including organising and   
conducting seminars, workshops and symposia

|  |  |  |
| --- | --- | --- |
| 5 | (*k*) | relating thereto, and supporting other organisations |
| conducting such activities; |
| 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,

|  |  |  |
| --- | --- | --- |
| 10 | (*l*) | on its own behalf or on behalf of the government; |
| 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;

|  |  |  |
| --- | --- | --- |
| 15 | (*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 20 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;

|  |  |  |
| --- | --- | --- |
| 25 | (*o*) | make rules in relation to the use of special categories |
| of personal data, the use of personal data for the |

dissemination of unsolicited 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

|  |  |  |
| --- | --- | --- |
| 30 | (*p*) | 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | *Personal Data Protection* | | 29 | Directives |
| **32.** | (1) Where on receipt of a complaint or otherwise, | |
| the Authority has reason to believe, that any controller or | | | made by the |
| Authority |
| 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*) and (*f*) of section 43, any regulation, guideline or Order 10 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 15 controller or processor 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–

|  |  |  |
| --- | --- | --- |
| 20 | (*a*) | to cease and refrain from engaging in, the act, |
| omission or course of conduct related to |

processing; and

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

(3) Every directive issued to such controller or processor 25 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 in force from the date of such communication.

30 *Personal Data Protection*

PART VI

PENALTIES

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | **33.** | (1) Where a controller or processor fails to comply | Imposition of |
| with a directive issued under the provisions of section 32, | | penalties |
| 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 34 of this Act, by notice require such controller or processor to pay a penalty, which shall not exceed a sum of rupees ten million 10 for each noncompliance.

(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 15 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 noncompliance.

(3) The Authority shall be responsible for the collection 20 of a penalty imposed under this section and the money so collected shall be credited to the Consolidated Fund.

(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 25 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 30 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

*Personal Data Protection*  31

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

|  |  |
| --- | --- |
| 5 | 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–

|  |  |  |
| --- | --- | --- |
| 10 | (*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;

|  |  |  |
| --- | --- | --- |
| 15 | (*b*) | if that body of persons is a firm, every partner of |
| (*c*) | that firm; or |
| 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,

|  |  |
| --- | --- |
| 20 | 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

|  |  |
| --- | --- |
| 25 | 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.

30 (8) 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.

32 *Personal Data Protection*

(9) 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | **34.** | In making a determination to impose an | | Matters to |
| 10 | administrative penalty, including the amount as provided | | | consider |
| when |
| in subsection (1) of section 33, the Authority shall have | | |
| imposing a |
| regard to the following matters:– | | |
| Penalty |
| (*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;

|  |  |  |
| --- | --- | --- |
| 15 | (*b*) | any action taken by the controller or processor to |
| (*c*) | mitigate the damage suffered by data subjects; |
| the effectiveness of the data protection management |

programme required from the controller under   
section 12;

|  |  |  |
| --- | --- | --- |
| 20 | (*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;

|  |  |  |
| --- | --- | --- |
| 25 | (*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;

*Personal Data Protection*  33

(*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 5 the contravention of this Act by a controller or processor as the case may be.

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **35.** | Exemptions, restrictions or derogations to the | Exemptions, |
| provisions of this Act shall not be allowed except where | | restrictions |
| such an exemption, restriction or derogation is prescribed | | or |
| derogations |
| by regulations and respects the essence of the fundamental | |
| rights and freedoms and constitutes a necessary and | |

proportionate measure in a democratic society for–

(*a*) the protection of national security, defense, public   
 safety, public health, economic and financial

|  |  |  |
| --- | --- | --- |
| 15 | (*b*) | systems stability of Republic of Sri Lanka; |
| the impartiality and independence of the judiciary; |
| (*c*) | the prevention, investigation and prosecution of |

criminal offences;

|  |  |  |
| --- | --- | --- |
| 20 | (*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 VII

MISCELLANEOUS

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | **36.** | (1) The financial year of the Authority shall be the | Financial |
| calendar year. | | year and |
| Audit of |
| (2) The provisions of Article 154 of the Constitution | | Accounts |

relating to the audit of the accounts of public corporations shall apply to the audit of the accounts of the Authority.

34 *Personal Data Protection*

**37.**  The Authority may with the consent of the Minister Power to given in concurrence with the Minister assigned the subject borrow

of Finance borrow temporarily by way of overdraft or otherwise, such sums of money as the Authority may require 5 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 10 section, shall not exceed such sum as may be determined by the Minister in consultation with the Minister assigned the subject of Finance.

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **38.** | The Authority may invest its money in such manner | Investment |
| as the Authority may determine or use any immovable | | of money of |
| the Authority |
| property that is in its possession as collateral for the purpose | |

of satisfying any liabilities incurred by it, in accordance with such directions that may be issued by the Minister assigned the subject of Finance for that purpose.

|  |  |  |  |
| --- | --- | --- | --- |
| 20 | **39.** | (1) A liability, whether civil or criminal, shall not | Protection of |
| be attached to any officer of the Authority or to any officer | | officers of |
| the Authority |
| authorized by such officer, for anything which is done in | |
| from suit or |
| good faith in the performance or exercise of any function or | | prosecution |

power imposed or conferred on the Authority under this Act.

(2) Any expense incurred by the Authority in any suit or 25 prosecution brought by or against the Authority before any court shall be paid out of the Consolidated Fund, and any costs paid to, or recovered by, the Authority in any such suit or prosecution shall be credited to the Consolidated Fund.

(3) Any expense incurred by any person referred to in 30 subsection (1) in any suit or prosecution brought against him before any court in respect of any act which is done or purported to be done by him under this Act or any

*Personal Data Protection*  35

appropriate instrument, or on the direction of the Authority, shall, if the court holds that the act was done in good faith, be paid out of the Consolidated Fund, unless such expense is recovered by him in such suit or prosecution.

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | **40.** | All officers and servants of the Authority, shall be | All officers |
| deemed to be public servants within the meaning and for the | | and servants |
| of the |
| purposes of Penal Code (Chapter 19). | |
| Authority |

deemed to be   
public   
servants for   
the purposes   
of Penal   
Code

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **41.** | The Authority shall be deemed to be a Scheduled | Authority |
| institution within the meaning of the Bribery Act, | | deemed to be |
| as cheduled |
| (Chapter 26) and the provisions of that Act shall be | |
| institution |
| construed accordingly. | |
| for purposes |

of Bribery   
Act

|  |  |  |  |
| --- | --- | --- | --- |
| 15 | **42.** | The Minister may from time to time, convey relevant | Directions of |
| directions taken by the Cabinet of Ministers in connection | | the Cabinet |
| with the exercise, performance and discharge of its powers, | | of Ministers |
| duties and functions under this Act or under any other written | |

law.

|  |  |  |
| --- | --- | --- |
| **43.** | (1) The Authority shall make rules in respect of– | Rules |

(*a*) the appointment, employment and dismissal of various officers and their powers, functions 20 and conduct and the payment of remuneration;

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

|  |  |
| --- | --- |
| 25 | (*c*) the management of the affairs of the Authority; |

36 *Personal Data Protection*

(*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.

5 (*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 commencement of this Act.

10 (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 15 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 20 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 25 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*.

|  |  |  |  |
| --- | --- | --- | --- |
| **44.** | *Personal Data Protection* | 37 | Regulations |
| (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.

5 (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:–

|  |  |  |
| --- | --- | --- |
| 10 | (*a*) | amendment, addition to or variation of the |
| (*b*) | conditions under Schedules I, II, III and IV; |
| 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 15 rights and freedoms, international commitments, effective administrative and judicial redress availability for the data subjects whose personal data are being transferred;

|  |  |  |
| --- | --- | --- |
| 20 | (*c*) | specifying the fees and charges levied for any |
| (*d*) | service provided under this Act; |
| specifying the conditions for providing appropriate |

safeguard for the rights and freedoms of data subjects   
relating to protection of personal data;

|  |  |  |
| --- | --- | --- |
| 25 | (*e*) | 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 30 specified in such regulation.

38 *Personal Data Protection*

(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 5 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*.

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | **45.** | Every person appointed under the authority of this | Official |
| Act shall, before entering upon his duties, sign a declaration | | Secrecy |

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 15 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.

|  |  |  |  |
| --- | --- | --- | --- |
| 20 | **46.** | (1) If any difficulty arises in giving effect to the | Removal of |
| difficulties |
| 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 25 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.

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

*Personal Data Protection*  39

PART VIII

INTERPRETATION

|  |  |  |
| --- | --- | --- |
| **47.** | In this Act, unless the context otherwise requires– | Interpretation |

“anonymise” in relation to personal data means

|  |  |
| --- | --- |
| 5 | 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 10 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

|  |  |
| --- | --- |
| 15 | allow or confirm the unique identification of that natural person, including facial images, |

dactyloscopy data or iris related data;

“certifying bodies” means, the bodies local or foreign that provide certification services 20 relating to the processing of personal data or qualifications of Data Protection Officers;

“child” means, a natural person who is below the   
 age of 18 years;

“consent” means, any freely given, specific, 25 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,

|  |  |  |  |
| --- | --- | --- | --- |
| 30 | public | authority, | non-governmental |

40 *Personal Data Protection*

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;

|  |  |
| --- | --- |
| 5 | “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;

“dactyloscopy data” means, data relating to 10 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 15 situation or status;

“Data Protection Authority” means, the   
designated regulatory body established under   
section 28 of this Act;

“Data Protection Officer” means, the person designated 20 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 25 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

30 unauthorized users;

*Personal Data Protection*  41

“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 5 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 10 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

|  |  |
| --- | --- |
| 15 | 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 20 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;

|  |  |
| --- | --- |
| 25 | “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,

30 by reference to–

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

42 *Personal Data Protection*

(*b*) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or 5 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 10 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;

15 “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, 20 retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical or arithmetical operations on personal data;

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

for the avoidance of doubt, a processor shall 30 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

*Personal Data Protection*  43

such as one department processing for another,   
or an employee processing data on behalf of   
their employer;

*Illustration:* Hospital A, employs a data 5 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 10 management of patient records are concerned.

The data scientist of the hospital is only an   
employee of the controller and not a   
processor.

|  |  |
| --- | --- |
| 15 | “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,

20 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

|  |  |
| --- | --- |
| 25 | 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;

|  |  |
| --- | --- |
| 30 | “public authority” means, a Ministry, any Department or Provincial Council, local |

authority, public corporation, statutory body or any institution established by any written law, or a Ministry, any Department or other 35 authority or institution established or created

44 *Personal Data Protection*

by a Provincial Council, and includes a   
company registered under the Companies Act,   
No. 7 of 2007 in which the government or a   
public corporation or a local authority

|  |  |
| --- | --- |
| 5 | directly holds fifty *per centum* or more of the shares of that company; |

“relevant regulatory or statutory body” means, the regulatory or statutory body established by or under any written law which regulates, 10 authorizes or supervises the controller and includes a Ministry which carries out the supervisory functions for the purpose of sections 26, 27 and 33 of this Act;

“recipient” means, a natural or legal person to 15 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 20 personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, financial data, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data 25   
 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;

30 “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 35 within the premises of a Sri Lankan mission

*Personal Data Protection*  45

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

|  |  |
| --- | --- |
| 5 | 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 10 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 15 the controller or processor, are authorized to process personal data;

“written” includes a document written manually   
 or electronically.

|  |  |  |  |
| --- | --- | --- | --- |
| 20 | **48.** | In the event of any inconsistency between the | Sinhala text |
| Sinhala and Tamil texts of this Act, the Sinhala text shall | | to prevail in |
| prevail. | | case of |
| inconsistency |

46 *Personal Data Protection*

(Section 5 (*a*))

SCHEDULE I

**CONDITIONSFOR 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 or   
 including any circular, direction or code issued by the   
 government;

(*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.

*Personal Data Protection*  47

(*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 the 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

**CONDITIONSFOR PROCESSING SPECIAL CATEGORIESOF 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 prescribed by 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

|  |  |  |
| --- | --- | --- |
| 48 | (*d*) | *Personal Data Protection* |
| 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 prescribed by   
 any written law 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*))

SCHEDULEIII

**CONDITIONSFORCONSENTOFTHE 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.

*Personal Data Protection*  49

(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; 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*))

SCHEDULEIV

**PROCESSING PERSONAL DATA RELATINGTO 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 as   
 may be prescribed.

(Section 11 and 13)

SCHEDULEV

**COLLECTIONOF 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;

|  |  |  |
| --- | --- | --- |
| 50 | (*c*) | *Personal Data Protection* |
| 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 mentioned 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.

*Personal Data Protection*  51

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.

52 *Personal Data Protection*

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.

|  |  |
| --- | --- |
| *Personal Data Protection* | 53 |

Department of Government Printing