L.D.O-19/2019.

**AN ACT TO PROVIDE FOR THE REGULATION OF PROCESSING OF PERSONAL DATA; TO IDENTIFY AND STREGNTHEN THE RIGHTS OF DATA SUBJECTS; TO PROVIDE FOR THE DESIGNATION OF THE DATA PROTECTION AUTHORITY;TO REGULATE THE DISSEMINATION OF UNSOLICITED MESSAGES USING PERSONAL DATA; AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH OR INCIDENTIAL THERETO.**

**Preamble**

**WHEREAS** it has become necessary to facilitate the growth and innovation in digital economy in Sri Lanka whilst safeguarding the rights of the individuals and ensuring the consumer trust:

AND WHEREAS it has become necessary to provide for the regulation of the processing of personal data of individuals in order to safeguard the rights of the individuals and to ensure the consumer trust in information privacy in online transactions and information networks resulting from the growth and innovation of the digital economy:

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

AND WHEREAS it has become the duty of the government of Sri Lanka to provide for a legislative framework to provide for mechanisms including safeguards for the purpose of protection of personal data of individuals whilst respecting domestic written laws and applicable international legal instruments:

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

**Short Title and date of commencement**

**1.** (1) This Act may be cited as the Personal Data Protection Act, No. …. of 2019.

(2) The provisions of this Act other than the provisions of Parts I, II, III, IV, V and VI referred to in subsection (3) and (4), shall commence on the date on which the certificate of the Speaker is endorsed in respect of this Act in terms of Article 79 of the Constitution.

(3) The provisions of Parts I, II, III,IV and VI of this Act, shall come into operation not later than 36 months of such certificate referred to in subsection (2).

(4) The provisions of Part V of this Act shall come into operation not later than 18 months of such certificate referred to in subsection (2).

**Responsibility to ensure effective implementation**

**2.** It shall be the responsibility of the Ministry of the Minister assigned the subject of Data Protection to ensure the effective implementation of the provisions of this Act.

**Application of the Act**

**3.** (1) This Act shall apply to the processing of personal data -

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

(b) by a controller or processor who –

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

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

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

(iv) offers goods or services to data subjects in Sri Lanka; or

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

(2) This Act shall not apply to -

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

(b) any data, which has been irreversibly anonymized in such a manner that causes the individual to be unidentifiable.

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

**4.** (1) It shall be lawful for a public authority to carry out the processing of personal data in accordance with its governing legal framework in so far as such frame work is not inconsistent with the provisions of this Act.

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

## PART I

## PERSONAL DATA PROCESSING OBLIGATIONS

**Obligation to process personal data in a lawful manner**

**5**. (1) Every controller shall process personal data in compliance with the obligations set out in subsection (2).

(2) The processing of personal data shall be lawful if a controller is in compliance with –

(a) any condition specified in Schedule I hereto;

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

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

(d) any condition specified in Schedule IV hereto in the case of processing personal data for criminal investigations.

**Obligation to define a purpose for processing**

**6**. Every controller shall, ensure that personal data is processed for a -

(a) specified;

(b) explicit; and

(c) legitimate,

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

Provided however, a controller may process personal data only for archiving purposes in the public interest, and for scientific, historical, research or statistical purposes under this Act.

**Obligation to confine processing to the defined purpose**

**7.** Every controller shall ensure that processing of personal data is –

(a) adequate;

(b) relevant;

(c) proportionate; and

(d) not excessive,

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

**Obligation to ensure accuracy**

**8.** Every controller shall ensure that processing of personal data shall be –

(a) accurate; and

(b) kept up to date,

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

**Obligation to limit the period of retention**

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

Provided however, a controller may store personal data only for archiving purposes in the public interest or for scientific, historical, research or statistical purposes under this Act, subject to the implementation of appropriate technical and organizational measures as may be prescribed under this Act.

**Obligation to maintain Integrity and Confidentiality**

**10**. (1) Every controller shall ensure integrity and confidentiality of personal data that is being processed, by using technical and organizational measures as may be prescribed including encryption, pseudonymisation, annonymisation or access controls so as to prevent the –

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

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

**Obligation to process personal data in a transparent manner**

**11**. A controller shall, take reasonable measures to provide data subjects -

(a) information referred to in Schedule V; and

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

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

**Accountability in the processing of personal data**

**12**. (1) Every controller shall ensure compliance with the obligations referred to in sections 5, 6, 7, 8, 9, 10 and 11 with regard to the processing of personal data under its control.

(2) For the purposes of giving effect to subsection (1), it shall be the duty of every controller to implement internal controls and procedures, (hereinafter referred to as the "data protection management programme") that-

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

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

(c) provides for appropriate safeguards based on data protection impact assessments specified in section 23;

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

(e) establishes internal oversight mechanisms;

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

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

(h) facilitates exercise of rights of data subject under sections 13, 14, 15, 16 and 19.

## PART II

## RIGHTS OF DATA SUBJECTS

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

**13.** (1) Every data subject shall be entitled to withdraw his consent at any time if such processing is based on the grounds specified in item (a) of Schedule I or item (a) of Schedule II of this Act:

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

(2) Every data subject shall have the right to request the 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 item (e) or (f) of Schedule I or item of (f) of Schedule II unless such grounds outweighs the rights and freedoms of the data subject guaranteed under any written law.

(3) It shall be the duty of the controller to comply with a request made by a data subject under subsection (1) and (2).

**Right of access to personal data**

**14**.(1) Every data subject shall have the right to obtain a confirmation in writing from the controller within three weeks from the date of request, referred to in section 13 as to whether personal data relating to such data subject is being processed by the controller and in the event of any such processing, the data subject shall have the right to access to such personal data and the information set out in Schedule V.

(2) Upon a written request made by the data subject under subsection (1), the controller shall provide the data subject such confirmation and information required to be provided under Schedule V.

**Right to rectification or completion**

**15.**(1) Every data subject shall be entitled to request the controller to rectify or complete the personal data which is either inaccurate or incomplete, and upon a written request to rectify or to complete the personal data of the data subject, the controller shall rectify or complete it without delay:

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

Provided further, where a controller is required to maintain personal data for the evidential purposes under any written law , the controller shall refrain from further processing such personal data without rectification.

(2) A controller may, refuse to comply with a request to rectify or complete the personal data made under subsection (1), in the absence of any legitimate proof provided by the data subject relating to a request for rectification or completion.

**Right to erasure**

**16.**(1) Every data subject shall have a right to make a written request to the controller to have his personal data erased, within twenty one working days from the date of such request, under following circumstances:-

(a) the processing of personal data is carried out in contravention of the obligation to process personal data lawfully referred to in section 5;

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

(c) the personal data is no longer necessary for the purposes for which such personal data was collected or otherwise processed; or

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

Provided however, the controller shall be required to retain personal data, without further processing or erasing in the event such personal data is required -

(a) for the evidentiary purposes under any written law;

(b) for the purpose of retention under any written law; or

(c) for a criminal investigation or judicial proceedings.

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

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

(a) such request has been granted;

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

(c) the controller has refrained from further processing such personal data under subsection (5) and reasons thereof,

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

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

(a) national security;
(b) public order;
(c) any inquiry, investigation or procedure conducted underany written law;
(d) the prevention, detection, investigation or prosecution of criminal offences;
(e)the rights and freedoms of other persons guaranteed under any written law;

(f) the technical and operational feasibility of the controller to act on such request ; or

(g) the inability of the controller to establish the identity of the data subject.

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

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

(5) Where the controller rectifies, completes, erases or refrains from further processing of personal data under sections 15 or 16 the controller shall, inform the data subject, within a period of twenty one working days, the details of personal data which has been subject to rectification, completion, erasure and has been refrained from further processing.

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

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

(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 paragraph (a) and (b).

(7) 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 under this Act .

(8) Where a fee is charged under subsection (7), the controller shall inform data subject the details of charges or levies and reasons for imposing same.

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

**18.**(1) Where a request of the data subject has been refused under section 17(2) or where the controller has refrained from further processing under section 15 or 16, the data subject may, appeal against such decision in the form, manner and the period of time as may be prescribed to the Authority for a determination whether the –

(a) refusal by the controller was lawful;

(b) decision to refrain from further processing of personal data by controller is lawful;

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

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

(4) 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.

**Automated individual decision making**

**19**. (1) Every data subject shall have a right to request a controller to review a decision of a controller based solely on automated processing, which affects the rights and freedoms of the data subject guaranteed under any written law, unless the decision of the controller based on automated processing is -

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

(b) authorized in the manner determinedby the Authority;

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

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

and the controller shall specify such measures as required to safeguard the rights and freedoms of the data subject:

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

(2) The Authority shall determine such criteria applicable to the conditions referred to in paragraph (b) of subsection (1), as may be set out in rules made under this Act.

## PART III

## CONTROLLERS AND PROCESSORS

**Additional obligationsof the controller**

**20**. (1) In addition to the obligations imposed under Part I, the controller shall, appoint Data Protection Officers as required by this Act, having competency and capacity to implement strategies and mechanisms to respond to inquiries and incidents related to processing of personal data.

(2) Where processing is to be carried out by a processor on behalf of a controller, the controller shall -

(a) use only processors providing sufficient guarantees to implement appropriate technical and organizational measures to give effect to the provisions of this Act and ensure the protection of rights of the data subjects as guaranteed under this Act; and

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

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

**Obligations of Processors**

**21**. (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 in compliance with the data protection obligations imposed under Part I;

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

(c) assist the controller in ensuring compliance with its obligations under the Part I of this Act;

(d) assist the controller by providing appropriate technical and organizational measures, for the fulfilment of the obligations of the controller to respond to requests made under Part II of this Act;

(e) upon the written instructions of the controller, erase or return all the personal data to the controller after the end of the provision of services relating to processing, and erase existing copies unless retention of such record is required by or under any written law;

(f) facilitate audits, including inspections upon the request of the controller.

(2) Where a processor contravenes the provisions of paragraph (a) of subsection (1) or determines the process and means of processing by itself, such processor shall be deemed to be controller for the purpose of this Act.

(3) Where a processor engages another processor (hereinafter referred to as the "sub processor") for carrying out specific processing activities -

(a) the provisions of this section shall apply to and in relation to such sub processor; and

(b) where a sub processor fails to fulfil its obligations under paragraph (a), the processor shall be liable to the controller for the perform or carry out the obligations of such sub processor.

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

**Personal Data breach notifications**

**22**. (1) In the event of a personal data breach, a controller shall, in such manner, form and within a period of time as may be prescribed under this Act, inform the Authority regarding such personal data breach.

(2) The Authority shall provide for -

(a) the instances where Authority shall be informed of such data breach;
(b) the instances where the affected data subject shall be informed; and
(c) the manner and content of such notification,

by way of rules made under this Act.

**personal data protection impact assessments**

**23**. (1) Where processing is likely to result in a high risk to the rights and freedoms of data subjects as guaranteed under any written law, a controller shall, prior to such processing, carry out an personal data protection impact assessment in the form and manner as may be prescribed, to ascertain the impact of the envisaged processing on the obligations imposed on the controller under Part I of this Act and the rights of data subjects guaranteed under Part II of this Act by taking into account the nature, scope, context and purposes of the processing or any other criteria as may be prescribed.

(2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a personal data protection impact assessment under subsection (1).

(3) A personal data protection impact assessment referred to in subsection (1) shall be carried out whenever -

(a) a systematic and extensive evaluation of personal data including profiling;

(b) processing of special categories of personal data or personal data relating to criminal convictions and offences, is carried out on a large scale;

(c) a systematic monitoring of a publicly accessible areas or telecommunication networks on a large scale; or

(d) any other processing activity as may be prescribed taking into consideration the scope and associated risks of that processing.

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

(5) The controller shall provide the Authority, the personal data protection impact assessment provided for in this section and, on request, provide any other information, for the purpose of making an assessment on 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 by the Authority.

**Prior consultation**

**24.**(1) Where a personal data protection impact assessment under section 23 indicates that the processing would result in high risks despite any measure taken by the controller to mitigate such risks, the controller shall consult the Authority prior to commencing the processing.

(2) Upon such consultation under subsection (1), if the Authority determines, that the intended processing referred to in subsection (1) contravenes the provisions of this Act, in particular where the controller has insufficiently identified or mitigated the risk, the Authority shall, within such period as may be prescribed, provide written advice to the controller under this Act.

(3) Where the controller consults the Authority under subsection (1), the controller shall provide additional information as may be requested by the Authority.

(4) Notwithstanding anything to the contrary in any other written law, whenever the controller engages in processing of personal data referred to in section 23(3) and where such processing is carried out by a controller in the public interest, including processing in relation to national security, public order and public health, the controller shall consult the Authority.

**Cross-border data flow**

**25.**(1) Where a public authority process personal data as a controller, such personal data shall be processed only in Sri Lanka and shall not be processed outside the territory of Sri Lanka, unless the Authority, in consultation with the controller and the relevant regulatory or supervisory body classifies the categories of personal data which is permitted to processed at a location outside Sri Lanka.

(2) A controller shall not be subject to any specific authorization from the Authority, other than the controllers referred to in subsection (1), if the Minister prescribe a third country, a territory or one or more specified sectors

within that third country, that ensures an adequate level of protection in accordance with the provisions of this Act.

(3) Subject to subsections (1) and (2), a controller may process personal data at a location outside Sri Lanka only if such controller, ensures compliance with the obligations imposed under Part I, Part II and Sections 20, 21, 22, 23 and 24 of Part III of this Act.

(4) For the purpose of ensuring compliance under subsection (3), the controller, shall -

(a) enter into a legally binding and enforceable instrument with the recipient located outside Sri Lanka; or

(b) adopt or enter into such other instrument that may be determined by the Authority.

## PART IV

## USE OF PERSONAL DATA TO DISSEMINATE UNSOLICITED MESSAGES

**Use of personal data on direct marketing**

**26**.(1) Subject to section 35, no controller shall disseminate unsolicited messages to any identified or identifiable data subject.

(2) (a) Without prejudice to subsection (1) and subject to section 13, a controller may use, telecommunication services, electronic or any other similar means for the purposes of disseminating messages only if a data subject has given consent to receive such messages (hereinafter referred to as "solicited messages").

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

(3) When obtaining consent under subsection (2), the controller shall, at the time of collecting contact information and each time a message is sent, provide to the data subject details on how to opt-out of receiving solicited messages.

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

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

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

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

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

using either electronic or telecommunication services or any other similar means, including through the use of automated calling and communication systems with or without human intervention.

## PART V

## DATA PROTECTION AUTHORITY

**Designation of the Authority**

**27**. (1) The Minister shall, by order published in the *Gazette*, designate a Public Corporation, Statutory Body or any other institution controlled by the government or established by or under any written law, 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 subsection (1) take into consideration the capacity, competency and expertise of such Public Corporation, Statutory Body or the institution, for the purpose of determining the ability of such Public Corporation, Statutory Body or the institution, in discharging the obligations under this Act.

(3) The Authority shall be responsible for all matters relating to personal data protection in Sri Lanka and for the implementation of the provisions of this Act.

(4) The operation of the provisions of this section shall be subject to subsection (4) of section 1 of this Act.

**Powers of the Authority**

**28**. The Authority shall have the following powers for the purpose of performing its duties and discharging of its functions under this Act :-

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

(b) to hold inquiries and require any person to appear before it;

(c) to examine such person under oath or affirmation and require such person where necessary to produce any information related to the processing functions of a controller or processor;

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

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

(f) to hear and determine any appeals made to it by the data subjects or any aggrieved person;

(g) to direct a controller or any relevant data protection officer to reimburse fees charged from a data subject for not providing the required information in a timely manner ;

(h) to receive complaints, hold inquiries, and to make determinations or orders;

(i) to enter into the premises of any controller or processor and inspect or seize records and carry out audits for imminent risks;

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

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

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

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

(n) to establish provident funds or pension schemes as may be determined by the Authority for the benefit of its staff and consultants;

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

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

(q) to establish standards in relation to data protection (data storage, data processing, obtaining consent etc.);

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

Provided however, the Authority shall obtain prior written approval of the Department of External Resources of the Ministry of the Minister to whom the subject of

Finance is assigned, in respect of all foreign grants, gifts or donations;

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

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

**Duties and Functions of the Authority**

**29**. For the purpose of carrying out its objects, the Authority may exercise, perform and discharge all or any of the following duties and functions :-

(a) direct controllers to comply with the section 11 in accordance with the conditions set out in Schedule V hereto;

(b) monitor the performance and ensure the due compliance by controllers or processors, of the obligations imposed on such controllers or processors under this Act;

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

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

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

(f) exercise its powers to monitor or examine all data processing operations, either of its own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with the provisions ofthis Act;

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

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

(i) advise the Government on all matters relating to data protection;

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

(k) 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;

(l) 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;

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

(n) undertake research on developments of new technologies impacting on processing of personal data; and

(o) perform such other acts not inconsistence with the provisions of this Act or any other written law, as are necessary for the promotion of the objects of this Act.

**Directives made by the Authority**

**30.**(1) Without prejudice to section 32 of this Act, where the Authority is of the opinion any controller or processor –

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

(b) has contravened or failed to comply with, or is likely to contravene or 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 a directive to that controller or processor requiring such controller or processor, 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 directive issued under this section shall be served on such controller or processor to whom it is directed and shall be in force from the date of service thereof.

(3) Every directive issued under this section shall be binding on the controller or processor to whom it is directed.

(4) Where a controller or processor fails to comply with an directive issued under subsection (1), the Authority may, upon application to the Magistrate Courts and upon satisfying the Court that a controller or processor has failed without reasonable excuse to comply in whole or in part with the directive 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 directive.

**Designation of the Data Protection Officer**

**31**.(1) Unless exempted from the provisions of this Act or any written law, every controller shall designate or appoint a Data Protection Officer, (hereinafter referred to as a "DPO"), to ensure compliance with the provisions of this Act, where –

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

(b) the processing is carried out by a private sector entity, in accordance with directives issued by the Authority, based on the nature or magnitude of the processing activity;

(c) the core activities of the controller or processor consist of processing -

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

(ii) on a large scale, special categories of personal data;

(iii) considered by the Authority to be determined as high risk processing activity, based on the nature of processing and its impact on data subjects.

(2) A DPO shall be a senior staff member of the controller who has relevant academic or professional qualifications which may include academic background, knowledge and technical skills in matters relating to data protection and may fulfill other duties and functions which has assigned to him:

Provided that, any such duties and functions do not result in a conflict of interest.

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

(4) A controller or processor shall publish the contact details of the DPO and communicate them to the Authority.

(5) The responsibility of a DPO shall be to –

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

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

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

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

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

(6) A private entity aggrieved by the directive of the Authority made under paragraph (b) of subsection (1), may prefer an appeal to the Secretary to the Ministry of the Minister, within thirty working days from the date of such directive is received by the private entity.

(7) The Secretary to whom an appeal is preferred under subsection (6) shall within 14 working days thereafter conduct an inquiry, providing an

opportunity for the private sector entity and the Authority to be heard, and thereafter make a decision taking into consideration the reasons adduced by the Authority and shall either –

(a) allow the appeal and direct the Authority to revoke its directive; or

(b) disallow the appeal for reasons assigned.

(8) The Authority shall give effect to the decision of the Secretary made under subsection (7).

## PART VI
## PENALTIES

**Imposition of penalties**

**32**.(1) Any controller or processor required to conform to the obligations under Parts I, II, III and IV of this Act or rules or regulations made under this Act, who fails to so conform, may in the first instance be provided a warning in writing by the Authority, and given specified period of time to conform to such requirements or show cause as to why such requirements are not fulfilled with.

(2) Notwithstanding the provisions of subsection (1), where the Authority has reasons to decide that a controller or processor has failed to comply with the provisions of this Act, shall be liable to a penalty as may be prescribed, taking into consideration the nature and extent of relevant non-compliance, its impact on data subjects in accordance with section 33 :

Provided however, such penalty shall not exceed a sum of rupees tenmillion 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.

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

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

(5) The imposition of a penalty under this section shall not preclude a supervisory authority or a regulatory authority from taking any other regulatory measures including, but not limited to, the suspension of such institution 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 Institution.

(6) 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 non-compliance under subsection (1) was a Director, and other officer responsible with management and control of that body corporate ;

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

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

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

**Matters to consider when imposing Penalty**

**33.(1)** In making a determination to impose an administrative penalty, including the amount as provided in subsection (2) of section 32, the Authority shall give due regard to the following:-

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

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

(c) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to subsections (2) and (3) of section 20 ;

(d) the effectiveness of the data protection management programme required of the controller under section 12;

(e) previous contraventions of the provisions of this Act by the controller or processor;

(f) the degree of cooperation with the Authority, in order to remedy the contravention and mitigate the possible adverse effects of such contravention;

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

(h) 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;

(i) the measures referred to in subsection (1) of section 32 have previously been ordered against the controller or processor concerned with regard to the same subject matter, and compliance with those measures;

(j) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

(2) A person who is aggrieved by the imposition of an administrative penalty under section 32 , may appeal against such decision to the Court of Appeal within twenty one working days, from the date of such imposition of such administrative fine was communicated to such person.

## PART VII

## MISCELLANEOUS

**Financial year and Audit of Accounts**

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

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

**Exceptions**

**35.** (1) Exceptions, restrictions or derogations to the provisions of this Act shall not be allowed except where such an exception**,** restriction or derogation is provided for by lawrespects 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, economic and financial interests of Republic of Sri Lanka;

(b) the impartiality and independence of the judiciary;

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

(d) the execution of criminal penalties;

(e) other essential objectives of the interest of the general public; and

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

**Power to borrow**

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

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

**Investment of money of the Authority**

**37**.The Authority may invest its money in such manner as the Authority may determine or use any immovable 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.

**Protection of officers of the Authority from suit or prosecution**

**38**.(1) No liability, whether civil or criminal, shall attach to any officer of the Authorityor to any officer authorized by such officer, for anything which in good faith is done in the performance or exercise of any function or power imposed or assigned to the Authority under this Act.

(2) Any expense incurred by the Authority in any suit or 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 such person as is referred to in subsection (2), 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 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.

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

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

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

**40**.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.

**Directions of Cabinet of Ministers**

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

**Rules**

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

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

(b) the procedure to be observed at the summoning and holding of meetings, Annual General Meeting and extra ordinary meetings of the Authority;

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

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

(e) the form and manner by which appeals may be made to the Authority under the provisions of this Act;

(f) all matters in respect of which, rules are required or authorized to be made under this Act.

(2) The Authority shall make rules under subsection (1), within 24 months from the date of operation of this Act.

(3) No rule made under this section shall have effect until it is approved by the Minister and approved rules and notification of such approval are published in the *Gazette*.

**Regulations**

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

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

(a) additional conditions under Schedules I, II, III and IV;

(b) identify third countries that ensure adequate level of protection under subsection (2) of section 25;

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

(d) conditions for providing appropriate safeguard for the rights and freedoms of data subject.

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

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

(5) Any regulation made by the Minister with concurrence of the Authority may at any time, be amended, added to, varied or rescinded.

**Official Secrecy**

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

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

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

**Removal of difficulties**

**45**.(1) If any difficulty arises in giving effect to the provisions of this Act or the rules, regulations, or Orders made under this Act, the Minister may by Order published in the *Gazette,* make such provision not inconsistent with the provisions of this Act, or any other written law, as appears to the Minister to be necessary or expedient for removing the difficulty for a period of one year from the date of coming into operation of that Order.

(2) Every Order made under this section shall, as soon as practicable after it is made, be laid before Parliament.

## PART IX

## INTERPRETATION

**Interpretation**

**46**. In this Act, unless the context otherwise requires -

"annonymize" means permanent 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 behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"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 an affirmative action signifying a data subject's agreement to the processing of his personal data;

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

“cross-border flows of personal data” means movement of personal data out of the territory of Sri Lanka;

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

“Data Protection Authority” means thedesignated regulatory body under the provisions of this Act;

“Data Protection Officer (DPO)” means the person designated under section 31;

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

“ 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;

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

“financial data” means any alpha-numeric identifier or other personal data which can identify an account opened by a data subject, or card or payment instrument issued by a financial institution to a data subject or any personal data regarding the relationship between a financial institution and a data subject 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 Digital Infrastructure and Information Technology under Article 43 or 44 of the Constitution and Ministry shall be construed accordingly;

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

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

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

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

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

"prescribed " means prescribed by regulations;

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

"processor" means a natural or legal person, public Authority or other body which processes personal data on behalf of the controller; for the avoidance of doubt, a processor shall be a separate entity or person from the controller and not a person subject to any hierarchical control of the Controller and excludes processing that is done internally such as one department processing for

another, or an employee processing data on behalf of their 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.*

“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, behavior, habits, location or movements;

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

"public authority" means a Ministry, a Government Department, Provincial Council, local authority, any government institution, public corporation, statutory body or any institution established by any written law, and includes a company registered under the Companies Act, No. 7

of 2007 inwhich the government or a public corporation or a local authority 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 under any written law which regulates, authorizes or supervises the controller";

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

"special categories of personal data" means the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, financial data, 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, and personal data relating to a child;

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

Sinhala text to prevail in case of inconsistency

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

(Section 5(2) (b))

SCHEDULE I

CONDITIONS FOR LAWFUL PROCESSING

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

(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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject to under this Act;

(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 any written law; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject which require protection of personal data, in particular where the data subject is a child.

(Section 5(2) (b))

SCHEDULE II

ADDITIONAL CONDITIONS FOR PROCESSING SPECIAL CATEGORIES PERSONAL OF 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.

(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 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 writtenlaw providing for appropriate safeguards for rights of the data subject;

(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;

(d) processing relates to personal data which is 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 or 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 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;

(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 such data is processed by a health professional licensed under or authorized by any writtenlaw 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 otherwritten law and provide for suitable and specific measures to safeguard the rights and freedoms of the data subject.

(Section 5(2) (c))

SCHEDULE III

CONDITIONS FOR CONSENT OF THE DATA SUBJECT

(a) the controller shall be able to demonstrate that the data subject has consented to processing of his personal data;

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

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

(c) when assessing whether consent is freely given, 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.

(Section 5 (2) (d))

SCHEDULE IV

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 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 or provisions under any other written law;

(c) conditions for providing appropriate safeguards for the rights and freedoms of data subjects under this schedule.

(Section 11 and 14)

SCHEDULE V

CONDITIONS FOR COLLECTION OF PERSONAL DATA

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

(a) the identity and contact details of the controller and where applicable of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the intended purposes for which the personal data is processed and the legal basis for the processing;
(d) the legitimate interest pursued by the controller or by a third party where processing is based on item (f) of Schedule 1;
(e) the categories of personal data being collected;

(f) where processing is intended to be based on consent pursuant to item (a) of Schedule I and item (a) of Schedule II, the existence of the right of the data subject to withdraw his consent, and the procedure for such withdrawal, without affecting the lawfulness of processing based on consent before its withdrawal;
(g) recipients or third parties with whom such personal data may be shared, if applicable;

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

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

(j) the existence of and procedure for the exercise of rights of the data subject 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; or

(m) the existence of automated decision-making, including profiling, referred to in section 19 and, at least in those cases, reasonably meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

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

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

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

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

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

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

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

6. items 1 to 4 of this schedule shall not apply where –

(a) the controllers proves that the data subject has already been provided the information;

(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, historical, research or statistical purposes, subject to the conditions and safeguards provided in this Act or in so far as the obligation referred to in item 1 of this Schedule is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the rights and freedoms of data subject guaranteed under any written law, including making the information publicly available;

(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 guaranteed under 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.

03/10/2019