Jurisdiction	*Sri Lanka*
Date	*24th October 2022*
Law Firm	*Varners*
Name and Position of the person in charge	*Krishanth Rajasooriyar* *Attorney-at-Law*
Contact Information	*rajasooriyar@varners.lk*

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the **private sector** at the present or in the near future?

The Personal Data Protection Act, No. 9 of 2022

The Personal Data Protection Act, No. 9 of 2022, ("PDPA") provides for the regulation of processing of personal data, the identification and strengthening of the rights of data subjects in relation to the protection of personal data, and the establishment of the Data Protection Authority.

General Protection under Existing Laws

Before the enactment of the PDPA, the legal framework consisted of (i) the general principles of delictual (civil) liability available under the Roman-Dutch law, and (ii) of various subject wise statutes containing specific provisions on data protection and privacy, applicable only in so far as those specific statutes are concerned. The existing framework will continue in effect notwithstanding the passing of the PDPA.

It should be noted that the Roman-Dutch law does not specifically recognise a right to privacy nor does it directly recognise any right to the protection of personal information. However, the right to have personality protected from several injuries or affronts that are very similar to the modern right to privacy are recognised.

The principles of delictual liability under the Roman-Dutch law protect an individual's dignity and reputation, his or her physical integrity, and form the basis for the protection of personality rights in Sri Lanka. These principles recognise a person's "right to be let alone" or the "right to seclusion of oneself or one's property from the public". However, the affected person must be able to establish the intention of another to injure, cause some impairment to the affected person,

his dignity or reputation, and that the act itself was wrongful.

In addition, a person may be held liable under the principles of Roman-Dutch law relating to delict for any loss, damage or costs sustained by another person as a consequence of any breach by the first mentioned person of a duty of care, skill and diligence. A person may also be liable if he or she fails to take reasonable care in the handling of confidential information. The affected person has to prove that actual patrimonial loss (monetary loss) was suffered by himself as a result of the other person breaching his duty of care in a manner, which was wrongful.

Computer Crimes Act, No. 24 of 2007

The Computer Crimes Act provides that any person who intentionally secures for himself or for any other person access to any information held in any computer, knowing that he has no lawful authority to secure such access or with the intention of committing an offence under the Act or any other law for the time being in force, shall be guilty of an offence.

While the said Act does provide for several related offences relating to information, it should be noted that the primary focus of the Act is not personal data protection.

ii. Does your country have a general law concerning protection of personal information in the **public sector** at the present or in the near future?

The PDPA applies equally to the protection of personal data in the private sector as well as in the public sector. It makes no distinction between its applications other than for certain enhanced provisions relating to the processing of data by public authorities in Sri Lanka.

See above for treatment of personal data under the existing legal framework. The existing framework does not draw any distinction between private or public data.

iii. Does your country have laws concerning protection of personal information **which apply in individual (specific) sectors** at the present or in the near future? (If yes, please describe outline.)

In addition to the PDPA, there are various subject wise statutes (i.e., banking, telecommunication, etc.,) containing specific provisions on data protection and privacy, applicable only in so far as those specific statutes are concerned.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal

information.

i. Please fill in the blanks below about <u>all</u> the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law ：*Personal Data Protection Act, No. 9 of 2022 (not yet operational)*

① The definition of "Personal Information"	*"Personal data" is defined by the PDPA as any information that can identify a data subject directly or indirectly, by reference to (a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of such individual or natural person.* *The person to whom the personal data relates is known as the "data subject" and includes an identified or identifiable natural person, alive or deceased.*
② The scope in which the law applies	*The PDPA applies to the processing of personal data in Sri Lanka, either wholly or partly. It also covers controllers or processors of personal data, who:* • *are domiciled or ordinarily resident in Sri Lanka;* • *are incorporated or established in Sri Lanka;* • *offer goods or services to persons in Sri Lanka; or* • *monitor or profile the behaviour of data subjects in Sri Lanka.* *Any personal data processed purely for personal, domestic, or household purposes by an individual are excluded from the scope of the PDPA. Therefore, a contact list stored in a person's phone is outside the scope if used 'purely' for personal, domestic, or household purposes.*
③ The territorial scope	*The territorial scope of the PDPA applies to the processing of personal data in any of the following circumstances:* *(a) taking place wholly or partly within Sri Lanka;* *(b) carried out by a data controller or processor domiciled or ordinarily resident in Sri Lanka;* *(c) carried out by a data controller or processor incorporated or established in Sri Lanka;* *(d) carried out by a data controller or processor offering goods or services to data subjects in Sri Lanka, inclusive of offerings with specific*

	targeting of data subjects in Sri Lanka; or *(e) carried out by a data controller or processor that specifically monitors the behavior of data subjects in Sri Lanka, including profiling with the intention of making decisions;*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*http://www.documents.gov.lk/files/act/2022/3/09-2022_E.pdf*
⑤ The **effective** date *	*The PDPA will come into operation on such date as the Minister may appoint by order published in the Government Gazette. The said date shall be a date not earlier than 18 months and not later than 36 months from the date of certification by the Speaker of Parliament of Sri Lanka (i.e., 19th March 2022)*

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：*Banking Act, No. 30 of 1988, as amended*

① The definition of "Personal Information"	*N/A*
② The scope in which the law applies	*The Act provides for the regulation of banking business in Sri Lanka, the licencing of persons carrying on the banking business, the acceptance of deposits and investing such money by persons, and provides for the control of matters relating to such banking business.*
③ The territorial scope	*Within Sri Lanka*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*The law has been amended several times, and there is no single consolidated version containing all such amendments.*
⑤ The **effective** date*	*Circa 1988, last amended 30 November 2006*

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：*Direction No. 02 of 2012 (Outsourcing of Business Operations of a Licensed Commercial Bank and Licensed Specialised Bank) issued under the Banking Act, No. 30 of 1988*

① The definition of "Personal Information"	*N/A*
② The scope in which the law applies	*Outsourcing of Business Operations of Licensed Commercial Banks and Licensed Specialised Banks.*

③ The territorial scope	*Within Sri Lanka*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*N/A*
⑤ The **effective** date*	*21 December 2012*

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：*Computer Crimes Act, No. 24 of 2007*

① The definition of "Personal Information"	*It does not define "personal information", but "information" is defined as including data, text, images, sound, codes, computer programmes, databases or microfilm.*
② The scope in which the law applies	*The Act applies in respect of the identification of computer crime and to provide the procedure for the investigation and prevention of such crimes.*
③ The territorial scope	*The territorial scope of the Computer Crimes Act applies in any of the following circumstances:* *(a) a person committing an offence under the Act while being present in Sri Lanka or outside Sri Lanka;* *(b) the computer, computer system, or information affected by the act constitutes an offence under the Act was at the relevant time in Sri Lanka or outside Sri Lanka;* *(c) the facility or service, including any computer storage, or data or information processing service, used in the commission of an offence under the Act was at the relevant time situated in Sri Lanka or outside Sri Lanka; or* *(d) the loss or damage is caused within or outside Sri Lanka by the commission of an offence under the Act to the state or to a person resident in Sri Lanka or outside Sri Lanka.*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*http://www.documents.gov.lk/files/act/2007/7/24-2007_E.pdf*
⑤ The **effective** date*	*Circa 2007*

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：*Intellectual Property Act, No. 36 of 2003*

① The definition of "Personal Information"	*N/A*
② The scope in which the law applies	*The Act codifies the law relating to intellectual property and provides for an efficient procedure for the registration, control and administration of intellectual property.*
③ The territorial scope	*Within Sri Lanka*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*The law has been amended several times, and there is no single consolidated version containing all such amendments.*
⑤ The **effective** date*	*Circa 2003, and last amended 16 March 2022*

* If the law has been amended, please fill in the effective date of the amended law.

ii. If there are any special instructions about the laws, please describe them.

N/A

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Sections 4 and 5 of the PDPA require personal data to be acquired in a lawful manner with the consent of the data subject where required, and provide that personal data must be processed only in compliances with the obligations specified under the PDPA.

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

Section 7 of the PDPA requires personal data being processed to be adequate, relevant, and proportionate in relation to the purpose for which such data is collected or processed, and Section 8 of the PDPA requires personal data to be accurate and kept up-to-date.

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Schedule V of the PDPA requires the purposes of collection to be specified at the time of collection, and the data subject to be informed in case of further processing of personal data. However, further processing of personal data for archiving purposes in the public interest, scientific research, historical research, or for statistical purposes shall not be considered to be incompatible with the defined purpose.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (c) Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

Section 6 of the PDPA requires personal data to be processed for a specified, explicit, and legitimate purpose. The term processing has been defined to also include collection and disclosure of personal data.

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Section 10 of the PDPA imposes an obligation on every controller to maintain the integrity and confidentiality of personal data that is being processed so as to prevent the (a) unauthorized or unlawful processing of personal data, or (b) loss, destruction or damage of personal data.

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

Section 11 of the PDPA imposes an obligation to process personal data in a transparent manner, and Schedule V of the PDPA requires the data subject to be made aware of the processing of personal data, and where such data has been obtained by the controller indirectly, the source of such personal data and information relating to the identity and contact details of the controller should also be disclosed.

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Part II of the PDPA pertains to the rights of data subjects and provides for the rights described in items i) to iv) of this question (g).

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.

Section 12 of the PDPA provides for accountability in the processing of personal data by controllers, and requires controllers to implement internal controls and procedures. The said section makes it the duty of controllers to implement internal controls and procedures which provide for appropriate safeguards based on data protection impact assessments.

Section 38 of the PDPA permits the imposition of penalties on a controller or processor by the Data Protection Authority.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

Any exemption, restriction, or derogation from the provisions of the PDPA will only be allowed where it 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, defence, public safety, public health, economic and financial systems stability of Sri Lanka;
(b) the impartiality and independence of the judiciary;
(c) the prevention, investigation and prosecution of criminal offences;
(d) the execution of criminal penalties; and
(e) the protection of the rights and fundamental freedoms of persons, particularly the freedom of expression and the right to information.

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as **comprehensive government access (e.g., limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the**

attorney-client privilege) to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

Data Localisation

The PDPA mandates public authorities to process personal data only in Sri Lanka and not in any third country as a controller or processor.

The processing of personal data by public authorities outside Sri Lanka involves a two-step process;

- *Firstly, the Minister in consultation with the Data Protection Authority is required to prescribe a third country for the purposes of the PDPA. This should be done by the Minister after making an adequacy decision considering the relevant laws and enforcement mechanisms relating to the protection of personal data in such third country, and*
- *Secondly, the Data Protection Authority should classify the categories of personal data that can be processed in a third country prescribed by the Minister pursuant to an adequacy decision.*

A private sector controller or processor may process personal data in a third country prescribed pursuant to an adequacy decision, or in any other country if it can ensure that the personal data will be processed in such other country in conformity with the data protection obligations laid down under the PDPA.

Government Access

The PDPA specifically provides that it shall have effect notwithstanding anything to the contrary in any other written law relating to the protection of personal data of data subjects. It further mandates public authorities to carry on the processing of personal data (as required under any other law) only so far as the protection of personal data is consistent with the provisions of PDPA.

Schedule IV of the PDPA provides for the processing of personal data in respect of criminal investigations. This allows processing to be carried out for the purposes of lawful investigations of offences or related security measures in accordance to the applicable laws, whilst providing appropriate safeguards for the rights and freedoms of data subjects.

As explained in our response to the second part of question III above, exemptions, restrictions, or derogations from the PDPA will only be allowed where it respects the

essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society for purposes listed above.

In addition to the PDPA,

- *attorney-client privilege is strictly recognized in Sri Lanka, and is embodied in law as well as in the rules made by the Supreme Court of Sri Lanka; and*
- *the various subject wise statutes (i.e., banking, telecommunication, etc.,) contain their own mechanisms on data protection and privacy limiting unauthorized access by public authorities. However, it should be noted that provisions tend to be rudimentary in nature.*

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

At this time, there is no data protection authority in Sri Lanka.

The Data Protection Authority will be set up only once the PDPA becomes operational after at least 18 months from the date of its certification (i.e., 19th March 2022).