DATA PROTECTION LEGISLATION IN SRI LANKA

Nisali Pieris

The Personal Data Protection Act No. 9 of 2022 ("PDPA") was passed in Parliament and was certified by the Speaker on the 19th of March 2022. It is the principal legislation dealing with the protection of personal data of individuals. The PDPA synchronises Sri Lanka's law on privacy with global legislation, such as the EU's General Data Protection Regulation and the APEC Privacy Framework.

Applicability of the PDPA

The PDPA shall apply to the processing of personal data in the following circumstances;

a. Where the processing of personal data takes place wholly or partly within Sri Lanka;

b. Where the processing is carried out by a controller or processor who;
   - is domiciled or resident in Sri Lanka;
   - is incorporated or established under a Sri Lankan law;
   - offers goods or services to persons in Sri Lanka; or
   - specifically monitors the behavior of persons in Sri Lanka.

The PDPA does not apply to personal data processed only for personal, domestic or household purposes by an individual and data that is not personal data.

"Personal data" has been defined in the PDPA as any information that can identify a person directly or indirectly by reference to an identifier or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person.

"Processing" has been broadly defined in the PDPA to mean any operation performed on personal data. The PDPA goes on to specify examples such as collection, storage and erasure.

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

A "processor" has been defined as a natural or legal person, public authority or other entity established by or under any written law, which processes personal data on behalf of the controller.

Parts I, II, III, VI, VII, VIII, IX and X will come into operation on a date to be appointed by the Minister, which shall be a date between 18 – 36 months of the PDPA being certified by the Speaker. Part V of the PDPA which institutes the Data Protection Authority, the statutory body set up to regulate data privacy, came into operation on 17th July 2023. Part IV of the PDPA, governing the use of personal data to disseminate solicited messages, shall come into operation on a date between 24 – 48 months of the PDPA being certified by the Speaker.

Grounds for processing personal data

Personal data can be processed under the following circumstances;

a. a person has given consent to the processing of his personal data;
b. processing is necessary for the performance of a contract to which the person is a party;
c. processing is necessary to comply with a legal obligation of the data controller or processor;
d. processing is necessary to respond to an emergency that threatens the life, health or safety of a person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of powers, functions or duties conferred, imposed or assigned on the controller or processor by or under a written law; or
f. processing is necessary for the purpose of legitimate interests pursued by the controller except where such interests are overridden by the interests of the person which requires the protection of personal data.

Obligations of a controller and/or processor

Personal data should be processed for the limited, proportionate and specified purpose for which it is collected. A controller has an obligation to ensure that personal data that is collected is accurate and upto date. Controllers are required to ensure the confidentiality of personal data by using appropriate technical and organizational measures to prevent the unauthorised access to data or the loss, destruction or damage of personal data. Controllers are also required to provide data subjects the specified information referred to in Schedule V of the PDPA. Controllers have a duty to implement internal controls and procedures assessing the mechanisms employed to safeguard data protection and to ensure that the rights given to persons under the PDPA are safeguarded.

Data processors and controllers are required to designate or appoint a Data Protection Officer to ensure compliance with the PDPA.

Where processing is done on behalf of a controller the processor is required to ensure the following;

- ensure that processing is carried out only on the written instructions of the controller;
- ensure that contractual obligations are instituted to protect confidentiality and secrecy;
- facilitate the controller to carry out compliance audits; and
- erase copies of personal data on receiving written instructions by the controller.

The PDPA sets out compliance requirements that controllers must follow if a data breach occurs, which includes notifying the Data Protection Authority.

Rights of persons

Every person has the right to access his personal data. Consent given for processing of personal data may be withdrawn. A person may ask the controller to complete or rectify incomplete or inaccurate data or to erase the personal data where the controller has acted in contravention to the PDPA or where the person wishes to withdraw consent.

Cross border data flow

Where a public authority processes personal data, such data must only be processed in Sri Lanka unless the Data Protection Authority permits the data to be processed outside Sri Lanka. This is subject to the Minister issuing an 'adequacy decision' whereby he prescribes a list of countries where data may be processed. A controller or processor other than a public authority may process personal data in a third country if an adequacy decision has been issued or in a country which is not subject to an adequacy decision only where such controller or processor ensures that the obligations imposed under the PDPA may be satisfied. The PDPA sets out specific circumstances where such data processing can be done in the absence of an adequacy decision or appropriate safeguards as described above.

Data Protection Authority

The PDPA sets up the Data Protection Authority, to act as the data protection regulator. The regulator is responsible for ensuring regulatory compliance with the PDPA. To this end, the regulator has the power to require controllers and processors to conduct inquiries, receive complaints, impose penalties, and make rules and guidelines under the PDPA. A right of appeal from a decision of the Data Protection Authority to the Court of Appeal has been granted, which may affirm or revise the decisions of the Data Protection Authority.

Sri Lanka was the first country in South Asia to enact data protection legislation. Its effectiveness and its interaction with other laws, especially the Right to Information Act remain to be seen.