DATA PROTECTION LAWS OF THE WORLD

Sri Lanka

DLA PIPER

SRI LANKA

Last modified 3 January 2024

LAW

Sri Lanka until recently did not have legislation pertaining to protection of data and privacy, although different sector specific laws such as the Computer Crimes Act No. 24 of 2007, the Banking Act No. 30 of 1988, the Electronic Transactions Act No. 19 of 2006, the Right to Information Act No. 12 of 2016 and the Telecommunications Act No. 25 of 1991 recognize the need for privacy and confidentiality. Identifying this lacuna, the Personal Data Protection Bill was first published as a draft bill in 2019. It was subject to several rounds of revisions, and subsequently was passed by the Parliament of Sri Lanka on 19 March, 2022 as the Personal Data Act No. 9 of 2022 (“PDPA”).

Although certified by the Speaker of Parliament, except for Part V of the PDPA which deals with provisions relating to the regulator under the law, i.e. the Data Protection Authority, the PDPA is yet to become operative as it provides for different time periods within which certain parts of the law would come into force, allowing controllers and processors a much-needed grace period. The majority of the law will come into operation within 18 to 36 months from the 19 March, 2022, while the part governing the sending of marketing messages using personal data would become operative within 24 to 48 months from the 19 March, 2022. With regard to Part V, it should be noted that an order has been issued by the Minister of Technology which provides that the said Part V of the PDPA has been brought into operation on 17 July, 2023. Accordingly, the Data Protection Authority is now in the process of being established, upon the completion of which the other parts of the PDPA are expected to follow suit.

The PDPA is primarily inspired by the European Union's General Data Protection Regulation (“GDPR”) and, therefore, shares many similarities with the GDPR.

The PDPA applies both territorially to the processing of personal data where such processing takes place wholly or partly within Sri Lanka, or by a person or entity within Sri Lanka; and extraterritorially, in so far as a person or entity outside Sri Lanka provides goods or services to individuals within Sri Lanka or monitors the behaviour of individuals within Sri Lanka.

Whilst the PDPA is the primary law that governs the protection of personal data in Sri Lanka, the following regulations / directions, which have been promulgated under the relevant sector specific laws, contain detailed provisions on data protection which are as follows:

i. The Financial Consumer Protection Regulations No. 1 of 2023 (the “FCPR”), published on the 9 August, 2023, promulgated under the Monetary Law Act, No.58 of 1949 (now replaced by the Central Bank of Sri Lanka Act, No. 16 of 2023), provides obligations substantially similar to the PDPA in relation to the protection of personal information of financial consumers. The FCPR is applicable to licensed commercial banks, licensed specialised banks, licensed finance companies, specialized leasing companies, authorized primary dealers, authorized money brokers, licensed microfinance companies, participants of the payment and settlement systems or any other financial institutions approved by the Central Bank of Sri Lanka. The FCPR provides protection not only to personally identifiable information but also extends to all information pertaining to financial consumers, which includes corporate entities and other legal bodies. The FCPR also provides for grace periods before the same becomes operational, with a majority of the regulations becoming operational

upon the expiration of 6 months from the date of its publication. Additionally, the requirements of the FCPR pertaining to the security of personal information are buttressed by the Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks, directions No. 16 of 2021, dated 9 December 2021, promulgated under the Banking Act No. 30 of 1988 (as amended). The applicability of this framework however is limited to licensed commercial banks and licensed specialized banks in Sri Lanka and its concentration lies on the information security requirements of such organizations.

ii. The Special Direction No. 91 published by the Consumer Affairs Authority on the 17 May, 2023, under the Consumer Affairs Authority Act No. 09 of 2003 (as amended), sets out provisions governing e-commerce entities and platform operators for the purpose of protecting consumers. These directions, although not in extensive detail, enumerate the principles set out in PDPA, aiming to the protect the personal data of consumers. It should be noted that unlike the PDPA, these directions are operational as at date.

DEFINITIONS

Many definitions in the PDPA are similar to that of the GDPR. In particular:

“**Personal data**” is defined to mean any information by which a data subject may be identified, either directly or indirectly by referring to an identifier or one or more factors specific to that individual. Thus, a name of a person is not a necessity for data to constitute personal data, but any factor such as an identification number, financial data, location data or an online identifier or factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual that allows for the tracing of him / her, would constitute personal data under the PDPA.

The PDPA further identifies a category of personal data as “special categories of personal data” with a view of protecting more sensitive personal data which are at a higher risk of adversely affecting an individual in the event such data is exploited. Special categories of personal data are defined to include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data and biometric data, data concerning health or a natural person’s sex life or sexual orientation, personal data in relation to offences, criminal proceedings and convictions or personal data relating to a child.

The term ‘processing’ has been rendered an extremely wide meaning within the PDPA to include (but not be 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.

The PDPA places extensive obligations on controllers of personal data. A ‘controller’ is defined to include any natural or legal person / entity which determines the purposes and means of processing personal data. When two or more controllers jointly determine the ways and means of processing personal data, the PDPA identifies them as joint controllers.

A ‘processor’ on the other hand is any natural or legal person / entity which processes personal data on behalf of the controller.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Authority of Sri Lanka ("**Authority**") is recognized as the regulator of personal data governed by the PDPA. The law provides for comprehensive objects and powers of the Authority as the regulator, which include making rules, issuing guidelines, receiving complaints, conducting inquiries, examining persons under oath, issuing directives and imposing fines in the event of non-compliance with the law.

REGISTRATION

At present, the PDPA does not require registration. Nevertheless, upon the PDPA becoming operative, rules requiring registration may be introduced as the PDPA empowers the Authority to make regulations specifying the categories and criteria of licenses to be issued under the PDPA.

Although not a registration requirement, the PDPA requires controllers and processors to publish the contact details of their data protection officers and ensure that it is communicated to the Authority.

DATA PROTECTION OFFICERS

The PDPA requires controllers and processors which are not public authorities to appoint a Data Protection Officer (“ **DPO**”) where their core activities consist of:

a. processing operations that require regular and systematic monitoring of data subjects on a prescribed scale or magnitude;
b. processing special categories of personal data on a prescribed scale or magnitude; or
c. processing which results in a risk of harm to the rights of the data subjects protected under the PDPA.

The PDPA permits a group of entities to appoint a single DPO provided, however, such DPO is easily accessible by all of the group entities.

Such DPO is required to be a competent individual possessing academic and professional qualifications in matters relating to data protection.

The specific responsibilities of the DPO as per the PDPA includes:

- advising controllers or processers on data processing requirements;
- ensuring on behalf of the controller or processor that the requirements of the PDPA are met;
- enabling capacity building of staff engaging in data processing operations;
- advice on personal data protection impact assessments; and
- co-operation and compliance with all directives and instructions issued by the Authority.

COLLECTION & PROCESSING

Similar to the GDPR, the PDPA enshrines certain principles governing the collection and processing of personal data. Each controller must ensure that personal data is processed in compliance with such principles, which are as follows.

- process lawfully;
- process for specified, explicit and legitimate purposes and not further process in a manner that is incompatible with those purposes;
- process personal data which is adequate, relevant and limited to the purpose;
- ensure that personal data is accurate and where necessary kept up to date;
- keep personal data in a form which permits identification of data subjects for no longer than is necessary, for the purpose(s) for which the data are processed;
- process in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures;
- process in a transparent manner, providing information on such processing to data subjects; and
- ensure accountability in processing by the implementation of internal controls and procedures that are able to demonstrate compliance with the PDPA, identified as the “Data Protection Management Programme”.

Legal Basis

In order to ensure that processing is ‘lawful’ whenever personal data is processed, such processing should be based on the most appropriate legal basis out of the following grounds provided under the PDPA:

- consent of the data subject (consent should be freely given, specific, informed and unambiguous indication in writing or by affirmative action and capable of being withdrawn at any time);
- necessary for the performance of a contract with the data subject in order to take steps at the request of a data subject to enter into a contract with such data subject;
- necessary for compliance with a legal obligation to which the controller / processor is subject to under Sri Lanka law;
- necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person;
- necessary for the performance of a task carried out in the public interest or in the exercise of powers, functions or duties imposed under Sri Lanka law; or

- necessary for the purposes of legitimate interests of the controller or a third party (subject to an assessment where the interests of the controller should be balanced against the rights of the data subjects and accordingly, must not override the interests of the data subject, especially when the data subject is a child).

Special Categories of Personal Data

In addition to the aforesaid lawful grounds, if processing special categories of personal data, a controller is required to satisfy one of the following additional conditions, on the objective basis of being most appropriate:

- consent of the data subject, which in the case of a child will mean the consent of the parent or legal guardian;
- 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 in so far as it is provided for in Sri Lanka Law, providing for appropriate safeguards for rights of the data subject;
- processing is necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person who is incapable of giving consent;
- relates to personal data which is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for any purpose as provided for under any written law in Sri Lanka or public interest;
- processing is necessary for medical purposes and where such data is processed by a health professional licensed under or authorized by any written law in Sri Lanka; or
- processing is necessary for archiving purposes in the public interest, scientific, historical research or statistical purposes in accordance with law.

Criminal Investigations

The PDPA provides for the processing of personal data in relation to criminal investigations, only where such processing is carried out in accordance with written laws in Sri Lanka, whilst providing for appropriate safeguards for the rights and freedoms of data subjects, which may be prescribed in the future upon the PDPA becoming operative.

Transparency of Data Processing

Transparency is an important principle enshrined in the PDPA and, as stated above, it aims to ensure that data subjects are aware of how their personal data is processed and understand their rights pertaining to such data.

Accordingly, the PDPA requires controllers to provide detailed information to data subjects in a concise, transparent, intelligible and easily accessible form. Therefore, providing the following information to data subjects at the point of collection of their personal data is imperative, which can be fulfilled by the provision of a privacy notice:

- identity and contact details of the controller;
- contact details of the data protection officer (where there is a DPO);
- intended purpose for collecting personal data and the legal basis for the processing;
- legitimate interest pursued by the controller (where applicable);
- categories of personal data collected;
- right of data subjects to withdraw consent for processing and method of withdrawing such consent (if processing is based on consent);
- recipients and third parties with whom personal data will be shared;
- details of cross border data transfer;
- period of data retention;
- rights of data subjects with regard to their personal data and how such rights may be exercised;
- right to file a complaint with the Data Protection Authority (“**Authority**”);
- whether the provision of personal data is a statutory or contractual requirement and the consequences of failing to provide such personal data;
- the existence of automated individual decision-making including profiling and the consequences for the data subject.

In addition, when a controller intends to process personal data for a new purpose, a data subject must be informed of such further processing, providing them with the information set out above.

If in any event personal data is collected via means other than direct collection from the data subject, the above information should be provided to the data subject within one month or at the time of the first communication to that data subject or when the personal data is first disclosed to another recipient, whichever event occurs first.

Rights of Data Subjects

The PDPA provides a series of rights for data subjects, largely similar to that of the GDPR. A controller must respond to any written request made by a data subject pertaining to his rights within 21 working days of receiving the request.

Right to access personal data: data subjects have the right to access their personal data, be provided with confirmation as to whether such personal data has been processed and be provided a copy of such personal data by submitting a written request.

Right to withdraw consent: if processing is based on consent, the data subject has the right to withdraw such consent at any time and the right to request a controller to refrain from further processing of the data subject’s personal data, provided the processing was based on the data subject’s consent.

Right to object to processing: data subjects have the right to object to further processing beyond the original purpose for which it was collected where such processing is based on the grounds of legitimate interests or public interest.

Right to rectification or completion: data subjects have the right to request a controller to rectify or complete any personal data that is inaccurate or incomplete.

Right to request a review of automated decisions: a data subject has the right to request for a review of a decision made by a controller based solely on automated processing which is likely to create “an irreversible and continuous impact on the rights and freedoms of the data subject” under Sri Lankan law, unless such automated processing is:

- authorized by Sri Lanka law;
- authorized in a manner determined by the Authority;
- based on the data subject’s consent; or
- necessary for entering into a performance of a contract between the data subject and the controller.

Right to erasure: the data subject may, under a limited set of circumstances, request the controller to erase their personal data. This includes when a controller is in contravention of its obligations and when the erasure is mandated by a written law of Sri Lanka or order of a competent court.

A controller is permitted to refuse to a request of a data subject based on the above rights only in limited instances, having regard to the following:

- national security;
- public order;
- any inquiry, investigation or procedure carried out under Sri Lanka law;
- the prevention, investigation and prosecution of criminal offences;
- the execution of criminal penalties;
- the protection of the rights and fundamental freedoms of persons under Sri Lanka law;
- where the controller is unable to establish the identity of a data subject;
- the requirement to process personal data under any other law in Sri Lanka.

TRANSFER

The PDPA allows for cross-border data flow and the processing of data in a third country outside Sri Lanka, subject to the parameters set out in the PDPA.

In case of a public authority acting as a controller or a processor, such transfer should only be made to a third country prescribed

pursuant to an adequacy decision. The Minister in charge of the subject matter has the power to make an adequacy decision in consultation with the Authority, and factors such as the relevant written laws and the enforcement mechanisms available in such third country will be considered in making such an adequacy decision.

A controller or processer that is not a public authority may also process personal data in a third country subject to an adequacy decision. If no adequacy decision has been made, personal data may be transferred to such third country only where the controller or processor effecting such transfer is able to ensure compliance with the obligations imposed under Part I, II and sections 20 to 25 of the PDPA by the imposition of appropriate safeguards. The transferor effecting such transfer is required to adopt an instrument that may be specified by the Authority in order to ensure compliance with the provisions of the PDPA by the transferee.

It is noteworthy that no such adequacy decisions have been made yet, considering the fact that the majority of the law is yet to become operative.

In the absence of an adequacy decision or appropriate safeguards, the PDPA provides the following limited instances where personal data could still be transferred to a third country (provided that the transferor in such instance is not a public authority):

- the data subject has explicitly consented, upon having been informed of the risks of such processing;
- the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of any pre-contractual measures taken by the controller at the request of the data subject;
- the transfer is necessary for the establishment, exercise or defence of legal claims relating to the data subject;
- the transfer is necessary for reasons of public interest;
- the transfer is necessary to respond to an emergency that threatens the life, health, or safety of the data subject or another person and where the data subject is incapable of giving consent; or
- any other condition that may be prescribed under the PDPA in the future.

SECURITY

The PDPA does not prescribe the specific technical measures or standards that ought to be implemented but requires the adoption of appropriate technical and organizational measures to ensure security that is commensurate to the risk of the processing activity.

Nonetheless, it provides insight into such technical and organizational measures by setting out that such measures include encryption, pseudonymization, anonymization or access controls.

Moreover, the PDPA also requires processors of personal data to have in place such technical and organizational measures, and ensure that their personnel data are bound by contractual obligations of confidentiality and secrecy.

BREACH NOTIFICATION

A ‘personal data breach’ is broadly defined in the PDPA to mean “*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* ”. The PDPA imposes a general obligation on a controller to notify the Authority in the event of a personal data breach.

The manner, form and the time period within which such notification should be made is to be prescribed by way of rules made under the PDPA, which are likely to be published upon the Authority being established. Accordingly, the threshold for a notifiable breach, the timeframe within which such notification has to be made, and the circumstances where the Authority and the data subjects should be notified, are yet to be specified under the PDPA.

Additionally, the Data Protection Management programme, which is required to be implemented by every controller, must also include a mechanism to detect breaches of personal data.

ENFORCEMENT

Enforcement of the PDPA is carried out by the Data Protection Authority of Sri Lanka (“**Authority**”). As an initial

step, the PDPA provides that data subjects aggrieved by the decisions of controllers have the right appeal to the Authority. The Authority is empowered to conduct investigations, and to allow or disallow such appeals at its discretion. In the event an appeal is allowed, the controller in question is required to give effect to the decision of the Authority, and inform the action taken in line with such decision, to both the relevant data subject and the Authority.

The Authority is also empowered to conduct inquiries on a complaint made, or otherwise if the Authority believes that a controller or a processor *inter alia* has contravened, is acting in contravention of or is likely to contravene the PDPA or any other legislation in Sri Lanka relating to processing of personal data.

The Authority has wide powers in conducting inquiries, which includes requiring persons to appear before it, examine persons under oath or affirmation and require the furnishing of information relating to the processing functions of a controller or processor.

Corrective Powers

Upon an inquiry where the controller or processor will be given an opportunity to be heard, the Authority is empowered to issue a binding directive which may include any one or more of the following:

- cease and refrain from the activity in question;
- take certain measured to rectify the situation;
- pay compensation to the person aggrieved.

Administrative Penalties

In the event a controller or processor fails to comply with directives issued by the Authority, the Authority may impose a penalty that will not exceed LKR ten million (10,000,000) for each non-compliance.

In imposing a penalty, the Authority will consider a number of factors, including the following:

- the nature, gravity and duration of the contravention;
- action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the effectiveness of the controller’s data protection management programme;
- the degree of co-operation by the controller with the Authority, in remedying the contravention and mitigating any adverse effects;
- the categories of personal data affected by the contravention;
- whether the controller or processor notified the Authority of the contravention;
- previous contraventions by controller or processor;
- financial benefits gained or losses avoided by the contravention.

Where a controller or processor has been subject to a penalty on a previous occasion and subsequently does not conform to a directive by the Authority, in addition to the penalty, such controller or processor will be liable to pay an additional penalty of twice the amount imposed as the penalty.

If the payment of a penalty is in default, the Authority may make an *ex-parte* application to the Magistrate Court of Colombo for an order requiring the payment, which can be recovered as a fine imposed by such court, even if such fine exceeds the amount such courts in its ordinary jurisdiction would impose.

The PDPA however makes provisions for an appeal to the Court of Appeal to a controller or processor that is aggrieved by the imposition of a penalty, which appeal should be referred within 21 working days from the date the notice of the imposition of such penalty was communicated to such controller or processor.

ELECTRONIC MARKETING

The data protection principles enshrined in the PDPA apply in relation to any electronic marketing activity carried out using personal data.

In addition, if direct marketing messages are to be sent using electronic or any other means, the controller must first obtain consent from the data subject prior to sending such message, which are identified as ‘**solicited messages**’ under the law.

Therefore, unlike the GDPR, legitimate interests cannot be used as the legal basis for processing personal data in sending electronic marketing messages to data subjects.

Consent under the PDPA is required to be freely given, specific, informed and unambiguous indication in writing or by affirmative action. The conditions governing consent under the PDPA set out that:

- the controller should be able to demonstrate that consent was obtained from the data subject;
- if consent is provided in a written form which also concerns other matters, the request for consent should be clearly distinguishable;
- the performance of a contract should not be conditional on a data subject’s consent to processing his personal data that is not necessary for the same; and
- the data subject must be informed, before they give consent, that they may withdraw consent at any time.

Additionally, when sending solicited messages, the controller should:

- provide the data subject information on how they may opt out of receiving such messages, free of charge; and
- inform the data subject of the nature of the message, to whom it is intended, and the identity of the controller or the third party on whose behalf the controller is disseminating the message.

The PDPA also allows the Authority to introduce rules, codes or prefixes that controllers should adopt to identify different categories of solicited messages. However, given that the law is in its transitional stage, such rules have not yet been introduced.

The aforesaid restrictions on marketing would not apply where marketing is aimed at corporate subscribers.

ONLINE PRIVACY

At present there are no requirements specifically applicable to aspects of online privacy such as cookies and location data. However, controllers and processors would be required to adhere to the general obligations set out in the PDPA, and data subjects would still be eligible to the rights and protections afforded to their personal data under the PDPA, when personal data is processed for online purposes.

KEY CONTACTS

FJ&G de Saram
www.fjgdesaram.com/

Shanaka Gunasekara
Partner
T +94 74 390 2018
shanaka.gunasekara@fjgdesaram.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.