දත්ත ආරක්ෂණ අධිකාරිය
தரவுப் பாதுகாப்பு அதிகாரசபை
Data Protection Authority

1 First Floor, Block 5, BMICH, Bauddhaloka Mawatha, Colombo 07, Sri Lanka.
Tel: +94 (0)112697241, Email: info@dpa.gov.lk, Web: www.dpa.gov.lk

My No: DPA/Legal/01/01 Date: 13th September 2024

Personal Data Protection Circular: No. 01/2024

Secretaries to Ministries
Chairpersons of all Commissions
Chief Secretaries of Provinces
Heads of Departments
District Secretaries
Chairpersons of Public Corporations and Statutory Institutions,
Heads of Government Companies and
Chairpersons of State Banks

Application of the Personal Data Protection Act No. 9 of 2022 in the Public Sector and Introduction to the Data Protection Authority

1. Background

1.1. The Personal Data Protection Act No. 9 of 2022 ("PDPA")[1], enacted on 19th March 2022, provides for mechanisms to ensure the protection of the personal data of data subjects engaged in transactions and communications while ensuring regulatory compliance with the provisions of this Act, to facilitate growth and innovation in the digital economy as stated in its preamble.

1.2. The Act regulates the processing of "personal data", i.e. any information that can directly or indirectly identify a natural person, known as a 'data subject'. This Act includes safeguarding the informational privacy of "data subjects" from any adverse impact that may arise when providing services by both public authorities and private sector institutions. Personal data of both citizens and non-citizens are protected equally under the PDPA (The rights of "data subjects" are provided in Part II of the Act).

1.3. "Public authority" means, a Ministry, any Department or Provincial Council, local authority, statutory body or any institution established by any written law, or a Ministry, any Department or other authority or institution established or created by a Provincial Council. The entities who process personal data of data subjects and regulated by the PDPA are "controllers" & "processors", and several specific legal obligations are imposed on "Controllers" under several Parts of the Act who are entities that primarily decide on the means and purposes of processing personal data. On the other hand, "processors" are contracted by a Controller to perform certain personal data processing functions on a controller's behalf.

[1] Available at: http://documents.gov.lk/files/act/2022/3/09-2022_E.pdf

1.4. The PDPA applies 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 also applies extraterritorially if a person or entity outside Sri Lanka specifically provides goods or services to "data subjects" within Sri Lanka or monitors their behaviour within Sri Lanka.

1.5. According to the PDPA's Section 3(1), the PDPA shall have effect notwithstanding anything to the contrary in any other written law, relating to the protection of personal data of data subjects. However, it outlines that where a public authority is governed by any other written law, it shall be lawful for such authority to carry out processing of personal data in accordance with the provisions of such written law, in so far as the protection of personal data of data subjects is consistent with this Act.

2. Enforcement of the Act in Phases

2.1. Through an Order issued by the Minister of Technology by virtue of the powers vested in him by the PDPA and the Constitution of the Democratic Socialist Republic of Sri Lanka (Ref. Extraordinary Gazette No 2341/59 dated 21st July 2023), 17th July 2023, was appointed as the date on which the provisions of Part V (Data Protection Authority) of the Act shall come into operation, especially to appoint the Chairman and the Board of Directors of the 'Data Protection Authority' in August 2023.

2.2. Moreover, the Extraordinary Gazette No. 2366/08 dated 8th January 2024, the following dates have been notified by the Minister of Technology for the operationalization of the PDPA:

(a) 1st December 2023 as the date on which the provisions of Parts VI (Director General and Staff of the Authority), VIII (Fund of the Authority), IX (Miscellaneous) and X (Interpretation) of the aforesaid Act shall come into operation; and

(b) 18th March 2025 as the date on which the provisions of Part I (Processing of Personal Data), II (Rights of Data Subjects), III (Controllers and Processors) and VII (Penalties) of the aforesaid Act shall come into operation.

2.3. Therefore, the PDPA will be fully operational and enforced, commencing 18th March 2025. Citizens who believe that their personal data is being collected, stored, and processed to the detriment of their privacy can complain to the Data Protection Authority (DPA) after 18th March 2025.

2.4. Also, the date on which Part IV of this Act on "Using Personal Data for Dissemination of Unsolicited Messages" will be declared to come into force from a particular date after 18th March 2025.

3. Data Protection Authority (DPA)

3.1. This Act enables the creation of an independent national regulatory mechanism necessary to effectively manage a future data-driven digital society that relies on the processing of personal data. According to the provisions of this Act, the President appointed the Chairman and the Board of Directors of the Authority in August 2023 to formally establish the Data Protection Authority. As of the Section 31 of the PDPA, the objects of the Authority are as follows:

(a) to regulate the processing of personal data in accordance with the provisions of this Act;
(b) to safeguard the privacy of the data subjects from any adverse impact arising from the digitalization of the procedures and services in the public and private sector;
(c) to provide for mechanisms to ensure the protection of personal data of data subjects engaged in digital transactions and communications;
(d) to ensure the regulatory compliance with the provisions of this Act to facilitate for the growth and innovation in digital economy.

3.2. Section 33 of the PDPA outlies Duties and functions of the Authority in detail.

3.3. The DPA expects to formulate the policy framework and the Rules and Regulations to enforce the Act, using a consultative approach, during the 3rd and 4th quarters of 2024 and create awareness of these policies, rules, and regulations during the 4th quarter of 2024 and 1st quarter of 2025. Pending a series of standard Rules, Regulations, and Guidelines to be issued by the DPA exercising the powers of the Act, special attention of Heads of all public institutions is drawn on the following implications irrespective of the volumes and nature of personal data processed by them.

4. Implications of PDPA on Public Authorities

4.1. As many public institutions serve as controllers of personal data of both internal and external data, appropriate technical and organizational measures should be in place to give effect to the provisions of PDPA. (e.g., identify personal data breaches, and provide encryption or other information security measures).

4.2. Therefore, all public institutions acting in the capacity of a 'controller' must ensure that personal data will be collected and processed in accordance with the processing obligations under Part I of the PDPA. They must comply with obligations concerning lawfulness (Sec. 5), purpose specification (Sec. 6), purpose limitation (Sec. 7), maintaining accuracy (Sec. 8), retention limitation (Sec. 9), integrity & confidentiality obligations (Sec. 10) and transparency (Sec. 11).

(a) All public institutions will need to ensure accountability for compliance with the above obligations through an effective "Data Protection Management Program" under Section 12. This will include facilitating the exercise of the rights of data subjects under Part II of the PDPA.
(b) Additional obligations under Part III, such as appointing a suitable "data protection officer" must be complied with by each institution (Sec. 20), and where required carry out data protection impact assessments for certain personal data processing activities under section 24 of the PDPA.
(c) A contracted third party who process personal data on behalf of a controller is terms as a "processor" under the PDPA, and should assist the controller to ensure compliance with this Act

4.3. Your special attention is also drawn to the provisions of the PDPA concerning cross-border data flow as described in its Section 26. It concerns with the movement of personal data out of the territory of Sri Lanka for the purpose of processing personal data in a third

country, with the assistance of cloud service providers (CSPs). Please make sure that the CSPs comply with the applicable data protection laws and regulations as well as the government policies associated with the utilization of cloud services for data management, including of personal data. Please also note that some of the institutions which serve as government owned business undertakings may not fall into the category of a 'public authority'.

4.4. The DPA has realized the importance of proactive engagement of all institutions and fields as much as possible, to ensure due compliance with the provisions of the PDPA. Accordingly, in so far as permitted by the PDPA, the DPA expects to maintain a regular dialogue about other practical situations with the representatives of main sectors/fields related to the collection and processing of personal data such as finance and banking, insurance, health, telecommunications, civil registration and tourism and relevant Advisory Committees shall be formed to enhance readiness to implement the rules and regulations issued under the provisions of the Act.

4.5. Moreover, awareness and advanced certificate programmes will be commenced soon for government officials by the Sri Lanka Institute of Development Administration (SLIDA) and volunteers from the private sector. An awareness program series commencing from mid-October 2024 to further elaborate the above-mentioned legal provisions as well as the associated managerial aspects prescribed in the PDPA, and subsequent regulatory frameworks announced by this Authority will be organized for key officers of each organization covering heads of departments, legal officers, officers in charge of information and communication technology infrastructure and human resource management.

4.6. Please inform all institutions under your purview to issue relevant directives/instructions in order to initiate activities to comply with the provisions of the PDPA. An illustration of what such activities may include is provided in **Annexure-1** to this circular for your ease of reference.

4.7. All key information and related legal instruments will be published in the official website of the Data Protection Authority (URL: www.dpa.gov.lk). The DPA may also be contacted via its email address: info@dpa.gov.lk.

(Sgd./-)
Arjuna Herath
Chairman
Data Protection Authority

Copy

1. Secretary to the President - *for your info. and necessary action please*
2. Secretary to the Prime Minister - ,,
3. Secretary to the Cabinet of Ministers - ,,
4. Secretary General of Parliament - ,,

Annexure 1 – Complying with the Personal Data Protection Act (PDPA):

The Initial Steps

(1) Awareness:
Take steps to ensure all staff are aware of the provisions and the corresponding compliance requirements under the PDPA.

(2) Governance Structure:
Set up an internal governance structure by appointing a Data Protection Officer (DPO), privacy champions and/or internal steering committee to oversee the PDPA compliance.

(3) Personal Data Audit:
Document what personal data you hold, where it came from and who you share it with, and why you have it, and the processes involved.

(4) Gap Assessment:
Ascertain the gaps between your current processing activities and what is required under the PDPA. Formulate remediation plan to address the gaps.

(5) Policy Implementation:
Formulate and implement appropriate data protection policies for the institution (ex: responding to data subjects rights, data retention, privacy notices, consent management, training etc.) to meet the compliance requirements.

(6) Training and Capacity Building:
Ensure the staff understands and complies with the compliance requirements stemming from the PDPA and develop the necessary technical skills on an ongoing basis.

Initial steps to ensure PDPA compliance