

Glimpse of Sri Lanka's Personal Data Protection Act No. 9 of 2022

Introduction

The Personal Data Protection Act (PDPA) No. 9 of 2022 represents a landmark development in Sri Lanka's legal framework, establishing the country's first comprehensive data protection regime. Published by the Media Law Forum Sri Lanka with support from the Centre for Law and Democracy, this guide offers an accessible interpretation of the Act's key provisions for legal professionals, compliance officers, policymakers, and other stakeholders navigating this new legislative landscape.

Background and Significance

The PDPA marks Sri Lanka's formal recognition of data protection as a fundamental right in an increasingly digital society. Drawing inspiration from international best practices, particularly the European Union's General Data Protection Regulation (GDPR), the Act establishes comprehensive protections for individuals' personal data while creating a framework that enables innovation and growth in the digital economy. The legislation strikes a crucial balance between individual privacy rights and legitimate data use.

Key Concepts and Definitions

- Personal Data

The Act defines personal data as any information relating to an identified or identifiable natural person. This includes direct identifiers such as names, identification numbers, and physical characteristics, as well as indirect identifiers that could be used to identify an individual, such as:

- Contact information (address, email, phone numbers)
- Location data
- Online identifiers
- Metadata
- Browsing behavior

- Special Categories of Data

The PDPA establishes enhanced protections for sensitive personal data, including:

1. Health data: Information related to a person's physical or mental health
2. Biometric data: Fingerprints, facial recognition data, iris data

3. Genetic data: Information about a person's genetic characteristics

These special categories require additional safeguards, and organizations processing such data must implement heightened security measures to protect it from unauthorized access or misuse.

General Principles of Data Processing

The PDPA establishes six fundamental principles that must be followed when processing personal data,

- 1. Purpose Limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in ways incompatible with those purposes.
- 2. Data Minimization:** Only data necessary for the specified purpose should be collected and processed.
- 3. Accuracy:** Personal data must be accurate and kept up to date, with reasonable steps taken to rectify or erase inaccurate data.
- 4. Storage Limitation:** Data should be retained only for as long as necessary to fulfill the stated purpose.
- 5. Integrity and Confidentiality:** Appropriate security measures must be implemented to protect personal data from unauthorized access, accidental loss, or damage.
- 6. Transparency:** Processing must be conducted in a transparent manner, with clear information provided to data subjects about how their data is being used.

Rights of Data Subjects

The PDPA grants individuals (data subjects) several rights regarding their personal data:

- 1. Right of Access:** Data subjects can request confirmation of whether their personal data is being processed and access to that data, including information about the purposes of processing, categories of data, recipients, retention periods, and their rights.
- 2. Right to Withdrawal of Consent:** When processing is based on consent, data subjects have the right to withdraw their consent at any time, though this does not affect the lawfulness of processing before withdrawal.
- 3. Right to Object:** Data subjects can object to processing in certain circumstances, particularly when processing is based on legitimate interests, public interest, or direct marketing.
- 4. Right to Rectification:** Data subjects can request correction of inaccurate personal data or completion of incomplete data.

5. Right to Erasure: Also known as the "right to be forgotten," this allows data subjects to request the deletion of their personal data under specific circumstances, such as when the data is no longer necessary for the original purpose or when consent is withdrawn.

Data Controllers and Processors

The PDPA distinguishes between data controllers and processors, establishing different responsibilities for each:

- **Data Controller**

The entity that determines the purposes and means of processing personal data. Controllers must:

- Ensure lawful, fair, and transparent processing
- Implement appropriate security measures
- Inform data subjects about their rights
- Ensure data is not kept longer than necessary

- **Data Processor**

The entity that processes personal data on behalf of the controller. Processors must:

- Process data only as instructed by the controller
- Implement appropriate technical and organizational security measures
- Assist the controller in meeting its obligations

- **Data Protection Officer (DPO)**

Organizations must appoint a Data Protection Officer when they:

- Monitor behavior regularly
- Are a government body dealing with personal data
- Process special categories of data on a large scale

DPOs are responsible for advising on compliance, monitoring adherence to the PDPA, cooperating with the Data Protection Authority, and acting as a point of contact for data subjects.

Cross-Border Transfer of Personal Data

The PDPA regulates the transfer of personal data outside Sri Lanka to ensure continued protection. Such transfers are permitted only when:

1. The receiving country has an adequate level of protection as determined by an adequacy decision issued by the Authority
2. The controller or processor has implemented appropriate safeguards
3. The data subject has explicitly consented to the transfer
4. The transfer is necessary for specific reasons, such as:
 - Performance of a contract with the data subject
 - Important reasons of public interest
 - Protection of vital interests
 - Establishment, exercise, or defense of legal claims

Penalties for Non-compliance

The PDPA establishes a robust enforcement framework with significant penalties:

1. For first instances of non-compliance: Up to 10 million rupees
2. For second and subsequent instances: Up to 20 million rupees
3. For continuous non-compliance: Additional penalty of up to 500,000 rupees per day

When determining penalties, the Authority considers several factors:

- Nature, gravity, and duration of the infringement
- Number of data subjects affected and level of damage
- Intentional or negligent character of the infringement
- Actions taken to mitigate damage
- Previous infringements
- Degree of cooperation with the Authority
- Categories of personal data affected

Exemptions and Derogations

The PDPA includes exemptions for:

1. National security
2. Prevention, detection, and prosecution of criminal offenses
3. Judicial independence and judicial proceedings
4. Enforcement of civil law claims
5. Processing for journalistic, academic, artistic, or literary purposes

Conclusion

Sri Lanka's Personal Data Protection Act represents a significant step forward in safeguarding individual privacy while enabling responsible data use. By establishing clear rights for individuals and obligations for organizations, the PDPA creates a framework that promotes trust in the digital economy. As Sri Lanka joins the global community of nations with comprehensive data protection legislation, this guide serves as an essential resource for understanding and implementing the Act's requirements.

Organizations operating in Sri Lanka must now take concrete steps to ensure compliance, including reviewing data processing activities, implementing appropriate security measures, establishing mechanisms for responding to data subject requests, and fostering a culture of privacy respect and responsible data stewardship across society.