ORRADATA

Singapore's Personal Data Protection Act (PDPA)

Simplified Explanation

A concise overview of principles, rights, and compliance requirements

www.orradata.com

Summary:

The Singapore Personal Data Protection Act (PDPA) is a comprehensive data protection framework enacted in 2012 that governs the collection, use, and disclosure of personal data by private organizations. Grounded in a standard of reasonableness, the Act aims to balance the right of individuals to protect their personal information with the need for organizations to use such data for legitimate business purposes. It mandates compliance with several key obligations—including obtaining informed consent, notifying individuals of data usage purposes, ensuring data accuracy and security, and limiting data retention—while also establishing a "Do Not Call" (DNC) Registry to regulate telemarketing. Enforced by the Personal Data Protection Commission (PDPC), the PDPA is designed to foster consumer trust and strengthen Singapore's position as a secure global hub for data flows and innovation.

1. Purpose, Scope & Definitions

- The **PDPA** creates a baseline standard for how private sector organisations handle **personal data** in Singapore
- It **does not apply** to:
  - Public agencies
  - Individuals acting in a personal/domestic capacity
  - Employee activities within their employment
  - Business contact information (e.g. business emails/names)
- **Personal data** covers any information that identifies an individual (e.g. name, NRIC, email, IP address, location data)

2. Do Not Call Registry

- Establishes national **Do Not Call (DNC) Registers**—for voice calls, texts, and fax messages.
- Organisations must respect these registers and avoid unsolicited marketing if a number is registered

3. Data Protection Obligations (the Ten Obligations)

Under the PDPA, organisations must comply with ten key obligations:

1. **Consent Obligation**
   Collect, use, or disclose personal data only with the individual's consent, after clearly informing them of the purposes and implications
2. **Purpose Limitation Obligation**
   Use data only for purposes a reasonable person would consider appropriate and that the individual has been notified about

3. **Notification Obligation**
   Inform individuals before collecting, using, or disclosing their personal data, including the purpose involved
4. **Access and Correction Obligation**
   Individuals can request access to their data (including past 1 year of use/disclosure) and corrections; organisations must respond promptly and forward corrected data to third parties who've received it
5. **Accuracy Obligation**
   Make reasonable efforts to ensure personal data is accurate and complete, especially when it may be shared with others or used in decisions
6. **Protection Obligation**
   Implement reasonable security arrangements to protect data against unauthorized access, modification, or disclosure
7. **Retention Limitation Obligation**
   Retain personal data only as long as necessary for legal or business purposes, and properly dispose of it afterwards
8. **Transfer Limitation Obligation**
   Do not transfer personal data overseas unless comparable protection is ensured, or an exemption applies; PDPC-recognized frameworks such as APEC CBPR can serve as safeguards
9. **Accountability Obligation**
   Organisations must develop policies, appoint a **Data Protection Officer (DPO)**, manage complaints, and ensure internal compliance—demonstrating accountability at all levels
10. **Data Breach Notification Obligation** *(added by 2020 amendments)*
    Organisations must notify the **PDPC** and affected individuals if a breach involves at least 500 individuals or could cause significant harm—within **three calendar days** after assessment

4. Exceptions & Additional Legal Bases

- Beyond **explicit consent**, personal data may be processed under:
  - **Deemed consent** (e.g. implied via opt-out),
  - **Legitimate interests** of the organisation (balanced against individual rights),
  - **Public or individual interest**, and
  - **Contractual necessity** in some cases

5. Additional Rules: NRIC Identifiers

- From **September 1, 2019**, collection or retention of full **NRIC numbers** (and similar national identifiers) is prohibited except where legally required or necessary for high-fidelity identity verification (e.g. banks, healthcare)

6. Enforcement & Penalties

- The **Personal Data Protection Commission (PDPC)** enforces the Act, investigates breaches, and issues fines or notices.
- Example enforcement actions:
  - **SingHealth breach** resulted in record fines (~S$1M),
  - Companies fined S$4,000–S$60,000 for mismanaging data breaches or failing to implement reasonable security arrangements
- Penalties can reach up to **S$1 million** for serious violations (e.g. unauthorized NRIC collection)

7. What PDPA matters

For Individuals (Data Subjects)

- **Privacy rights:** PDPA ensures that people in Singapore have a legal basis to know, control, and restrict how their personal data is collected, used, and shared.
- **Protection against misuse:** It reduces risks such as identity theft, unauthorized marketing, or data leaks.
- **Transparency:** Individuals must be informed about why their data is collected and how it will be used, creating clearer consent processes.

For Organizations

- **Legal compliance:** Businesses operating in Singapore must follow PDPA rules, or face financial penalties and reputational damage.
- **Trust and reputation:** Compliance shows customers and partners that the company respects privacy, which can be a competitive advantage.
- **Operational clarity:** PDPA sets structured obligations (like breach notification and security standards) that guide how companies manage data systematically.

For Singapore's Economy and Society

- **International alignment:** PDPA brings Singapore in line with global data protection standards (e.g., GDPR), supporting cross-border trade and digital services.
- **Cybersecurity improvement:** The Act forces companies to adopt stronger security measures, reducing the risk of large-scale breaches.
- **Digital economy growth:** By building public trust in data handling, PDPA supports Singapore's ambition to be a leading digital and financial hub.

Quick Overview Table

Obligation / Area	Summary Requirement
Consent & Notification	Inform individuals and get consent before handling personal data
Purpose Limitation	Use data only for stated, reasonable purposes
Access & Correction	Allow access and correction upon request
Accuracy	Ensure data is kept accurate and complete
Protection	Use appropriate security measures to safeguard data
Retention Limitation	Delete data when no longer needed
Transfer Limitation	Safeguard data before transferring overseas
Accountability & DPO	Policies, DPO, complaint process, oversight
Data Breach Notification	Notify PDPC and individuals of serious breaches
NRIC Data Rules	Strict limits on collection and retention of national IDs

Disclaimer:
This document is provided for general informational purposes only. It offers a simplified overview of Singapore's PDPA and does not constitute legal advice. Organizations and individuals should consult official regulatory texts or seek professional legal counsel for advice regarding their particular obligations under the PDPA.