AURORA
LAW

Singapore
Data Protection 101

A Practical Introduction to the
Personal Data Protection Act (PDPA)

www.aurora-law.io
hello@aurora-law.io
February 2026

Introduction

If your business operates in Singapore or handles the personal data of individuals in Singapore, you will need to comply with the Personal Data Protection Act 2012 (PDPA). The PDPA is Singapore's principal data protection legislation and establishes a comprehensive framework governing how organisations collect, use, disclose, and care for personal data.

This guide provides a concise, non-exhaustive overview of the PDPA's key requirements to help businesses understand their core data protection obligations. It is not intended as a substitute for legal advice tailored to your specific circumstances.

What is the PDPA?

The PDPA was enacted in 2012 and has been progressively updated, most significantly through the Personal Data Protection (Amendment) Act 2020, with key amendments taking effect from 1 February 2021. The PDPA is administered and enforced by the Personal Data Protection Commission (PDPC), a statutory body established under the Act.

The PDPA aims to balance two objectives: protecting individuals' personal data from misuse, and enabling organisations to collect and use personal data for legitimate and reasonable purposes. This pragmatic approach is a hallmark of Singapore's regulatory philosophy.

Who Does the PDPA Apply To?

The PDPA applies to all private-sector organisations in Singapore, regardless of size. This includes companies, partnerships, sole proprietors, associations, and any body of persons, whether incorporated or not. Notably, the PDPA has extraterritorial reach – it can apply to organisations outside Singapore if they collect, use, or disclose personal data of individuals in Singapore.

*The PDPA does **not** apply to: public agencies (which are subject to separate rules), individuals acting in a personal or domestic capacity, employees acting in the course of their employment, or business contact information (such as business email addresses and job titles).*

Key Definitions

Personal Data	Any data, whether true or not, about an individual who can be identified from that data, or from that data and other information the organisation has or is likely to have access to.
Organisation	Any individual, company, association, or body of persons, whether incorporated or not, that collects, uses, or discloses personal data.

Data Intermediary	An organisation that processes personal data on behalf of another organisation (similar to a "data processor" under the EU's GDPR). Data intermediaries have limited obligations under the PDPA.
PDPC	The Personal Data Protection Commission – the statutory authority responsible for administering and enforcing the PDPA.
DPO	Data Protection Officer – every organisation must appoint at least one DPO whose business contact information must be publicly accessible from Singapore.

The Core Data Protection Obligations

The PDPA sets out 11 key obligations that organisations must comply with when handling personal data. These obligations form the backbone of Singapore's data protection regime.

1. Consent	Obtain the individual's consent before collecting, using, or disclosing personal data. The PDPA also recognises "deemed consent" in certain situations (e.g., contractual necessity or where the individual has been notified and has not opted out).
2. Purpose Limitation	Collect, use, or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances, and that the individual has been informed of.
3. Notification	Inform individuals of the purposes for which their personal data is being collected, used, or disclosed.
4. Access	Upon request, provide individuals with access to their personal data held by the organisation and information about how that data has been used or disclosed within the past year.
5. Correction	Correct errors or omissions in an individual's personal data upon request, and send the corrected data to other organisations that received the data within the past year.
6. Accuracy	Make reasonable efforts to ensure that personal data collected is accurate and complete, especially if it is likely to be used to make a decision affecting the individual or disclosed to another organisation.
7. Protection	Implement reasonable security arrangements (technical and organisational) to protect personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks.
8. Retention Limitation	Cease to retain personal data (or anonymise it) when it is no longer needed for any business or legal purpose.
9. Transfer Limitation	Ensure that personal data transferred outside Singapore receives a comparable standard of protection. This can be achieved through

	contractual arrangements, binding corporate rules, or reliance on recognised certifications.
10. Accountability	Implement policies and practices to meet PDPA obligations, communicate them to staff, and designate a Data Protection Officer (DPO).
11. Data Breach Notification	Notify the PDPC and affected individuals when a data breach is assessed as notifiable (see below for details).

Data Breach Notification

Since 1 February 2021, the PDPA imposes a mandatory data breach notification obligation. A "data breach" is defined broadly and includes any unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data, as well as the loss of any storage medium or device containing personal data where unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely.

When Must You Notify?

An organisation must notify the PDPC if the data breach:

- results in, or is likely to result in, **significant harm** to any affected individual (e.g., the breach involves financial data, health records, identification numbers, or authentication credentials); or
- is of a **significant scale** – as a general rule, this means 500 or more individuals are affected.

Notification Timelines

Notify	Timeline
PDPC	As soon as practicable, but no later than 3 calendar days after the organisation has assessed the breach as notifiable.
Affected Individuals	As soon as practicable, at the same time as or after notifying the PDPC.
Data Intermediary → Organisation	Without undue delay, once the data intermediary has credible grounds to believe a breach has occurred.

> ⚠ **Important: The 3-Day Clock**
>
> The 3 calendar day deadline runs from the time the organisation has completed its assessment and determined the breach is notifiable – not from when the breach was first discovered. However, the PDPC expects organisations to conduct this assessment expeditiously.

The Data Protection Officer (DPO)

Every organisation subject to the PDPA must designate at least one individual as its Data Protection Officer (DPO). The DPO's role includes:

- Ensuring the organisation's compliance with the PDPA.
- Developing and implementing data protection policies and practices.
- Handling complaints and inquiries related to personal data.
- Communicating the organisation's data protection policies to staff and the public.
- Serving as the point of contact for the PDPC.

The business contact information of at least one DPO must be made publicly available and readily accessible from Singapore. This is typically done by publishing it on the organisation's website or in its privacy policy.

> **Practical Tip**
> The DPO does not need to be a dedicated full-time role. In smaller organisations, the DPO function is often performed by an existing employee (such as the compliance officer or a senior manager) alongside other responsibilities. What matters is that a specific person is accountable and contactable.

Consent Under the PDPA

Consent is a cornerstone of the PDPA. Organisations must obtain an individual's consent before collecting, using, or disclosing their personal data. However, the PDPA provides several nuanced mechanisms beyond simple express consent:

Types of Consent

- **Express Consent –** The individual actively and clearly agrees (e.g., by signing a form, ticking a box, or giving verbal agreement).
- **Deemed Consent –** Consent is inferred from the individual's conduct (e.g., voluntarily providing personal data for a purpose which is objectively obvious and reasonably appropriate from the surrounding circumstances).
- **Deemed Consent by Notification –** Introduced in 2021. Organisations may rely on deemed consent if they notify the individual of the organisation's intention to collect, use or disclose the personal data, the intended purpose for such personal data, give a reasonable period to opt out, and the individual does not opt out.
- **Deemed Consent by Contractual Necessity –** Where the collection, use, or disclosure is reasonably necessary for the performance of a contract between the organisation and the individual.

Exceptions to Consent

The PDPA also provides for situations where consent is not required, including:

- **Legitimate Interests –** Organisations may collect, use, or disclose personal data without consent where the benefit to the public or organisation clearly outweighs any adverse effect on the individual (subject to a risk assessment and other safeguards).
- **Business Improvement –** Use of personal data to improve goods, services, or business operations, subject to certain conditions.
- **Research –** Use for research purposes where, among others, there is a clear public benefit to using the personal data for the research purpose and the results will not identify specific individuals.
- **Legal and Vital Interests –** Where necessary for legal proceedings, emergencies threatening life or health, or required by law.

Cross-Border Data Transfers

The PDPA's Transfer Limitation Obligation requires that organisations transferring personal data outside Singapore ensure the recipient provides a standard of protection that is comparable to what the PDPA requires. This can be achieved through several mechanisms:

- **Contractual arrangements –** Binding obligations on the recipient to protect the data to a standard comparable to the PDPA.
- **Binding Corporate Rules –** Intra-group arrangements that apply across all entities in a corporate group.
- **Certifications –** Reliance on recognised certifications such as those under the Asia Pacific Economic Cooperation ("**APEC**") Cross-Border Privacy Rules ("**CBPR**") System or APEC Privacy Recognition for Processors System.
- **Comparable laws –** Transfer to a jurisdiction with data protection laws that are comparable to the PDPA.

Singapore actively promotes cross-border data flow interoperability and participates in initiatives such as the ASEAN Model Contractual Clauses and the Global CBPR Forum.

Penalties for Non-Compliance

The PDPC has broad enforcement powers and can investigate complaints, conduct inspections, and issue directions. Penalties for non-compliance can be significant:

Type	Details
Financial Penalties	Up to SGD 1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher.

Directions	The PDPC may direct organisations to stop collecting, using or disclosing personal data, destroy personal data, or take specific remedial actions.
Criminal Offences	Individuals who knowingly or recklessly misuse personal data, or re-identify anonymised data, may face criminal penalties including fines of up to SGD 200,000 and/or imprisonment of up to 3 years.
Private Right of Action	Individuals may bring a civil claim against an organisation for loss or damage directly caused by a contravention of the PDPA's data protection provisions.

> ⚠ **Enforcement in Practice**
>
> The PDPC regularly publishes enforcement decisions on its website. Breaches of the Protection Obligation (failure to implement adequate security measures) are by far the most common basis for enforcement action. The PDPC also considers an organisation's remedial actions and level of cooperation when determining penalties.

The Do Not Call (DNC) Registry

The PDPA also establishes a national Do Not Call (DNC) Registry, which allows Singapore telephone number holders to opt out of receiving unsolicited telemarketing messages (calls, text messages, and faxes). Organisations engaging in telemarketing must:

- Check the DNC Registry before sending marketing messages to Singapore telephone numbers.
- Obtain clear and unambiguous consent if the individual's number is listed on the registry.
- Maintain records of consent for compliance purposes.

These obligations apply even to organisations based outside Singapore that send marketing messages to Singapore telephone numbers.

PDPA and the GDPR: Key Differences

Many businesses operating internationally will be familiar with the EU's General Data Protection Regulation (GDPR). While the PDPA shares some similarities with the GDPR, there are notable differences:

Aspect	PDPA	GDPR
Scope	Private-sector organisations only.	All data controllers and processors, public and private.

Business Contact Info	Excluded from the PDPA.	Generally covered.
Consent Model	Flexible – includes deemed consent and notification-based consent.	Stricter – requires clear affirmative action for consent.
Data Portability	Not in force.	Fully in force (Art. 20).
Breach Notification	3 calendar days after assessment.	72 hours after becoming aware.
Maximum Penalty	SGD 1M or 10% of local turnover.	€20M or 4% of global turnover.

Practical Steps for Compliance

For organisations looking to achieve and maintain PDPA compliance, the following practical steps are recommended:

1. **Appoint a DPO** and make the DPO's business contact information publicly available.
2. **Develop a data protection policy** that explains how personal data is collected, used, disclosed, and protected.
3. **Conduct a data inventory** to understand what personal data the organisation holds, where it is stored, and how it flows through the organisation.
4. **Implement appropriate security measures** – both technical (e.g., encryption, access controls) and organisational (e.g., staff training, clear procedures).
5. **Establish a data breach response plan** with clear escalation procedures and assigned responsibilities.
6. **Review consent practices** and ensure that consent is properly obtained and documented for all data processing activities.
7. **Review third-party and cross-border arrangements** to ensure adequate contractual protections are in place.
8. **Train employees regularly** on data protection policies, recognising phishing attempts, and proper data handling procedures.

Useful Resources

- **PDPC (Personal Data Protection Commission):** www.pdpc.gov.sg
- **PDPA Full Text:** sso.agc.gov.sg
- **PDPC Advisory Guidelines:** pdpc.gov.sg/guidelines-and-consultation
- **Data Breach Management Guide:** pdpc.gov.sg/data-breach-management-guide
- **Do Not Call Registry:** www.dnc.gov.sg
- **PDPC Enforcement Decisions:** pdpc.gov.sg/enforcement-decisions

Disclaimer

This guide is intended for general informational purposes only and does not constitute legal advice. The PDPA and its subsidiary legislation are subject to change, and the PDPC regularly issues new advisory guidelines and enforcement decisions that may affect the interpretation and application of the law. You should seek independent professional advice tailored to your specific circumstances before making any decisions based on the contents of this guide.

Questions? Get in touch.

Aurora Law LLC
1 Scotts Road, #24-10, Shaw Centre, Singapore 228208
hello@aurora-law.io | www.aurora-law.io