SmartSuite

Framework / Privacy / Global Privacy Regulations

Singapore Personal Data Protection Act 2012 (Amended 2020)

Singapore's Personal Data Protection Act 2012 governs how organizations collect, use and disclose personal data, with breach notification and turnover-based penalties enforced by the PDPC.



What it is

The Personal Data Protection Act 2012 (PDPA, Act 26 of 2012, cited in its 2020 Revised Edition) is Singapore's data protection law: it governs how organizations collect, use and disclose personal data and establishes the Do Not Call Register, and it is administered and enforced by the Personal Data Protection Commission (PDPC). The data protection provisions in Parts 3 to 6A have applied to every private-sector organization handling personal data in Singapore since July 2, 2014, whether or not the organization is formed or located in Singapore.

At a glance

PUBLISHER
Parliament of Singapore (Act 26 of 2012); administered and enforced by the Personal Data Protection Commission (PDPC)

TYPE
Framework

VERSION
Personal Data Protection Act 2012, 2020 Revised Edition, as amended by the Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020) and Act 19 of 2025

EFFECTIVE
July 2, 2014 (data protection provisions); Commission from January 2, 2013; Do Not Call from January 2, 2014; 2020 amendments from February 1, 2021 and penalty cap from October 1, 2022

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
Singapore

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: sso.agc.gov.sg/Act/PDPA2012

Why it matters

- **Named obligations with section numbers** Consent (sections 13 to 17), purpose limitation (18), notification (20), access and correction (21 and 22), accuracy (23), protection (24), retention limitation (25), transfer limitation (26) and accountability (11 and 12) give a compliance program a fixed structure.
- **A fixed breach clock** Part 6A requires an assessment of a suspected breach, which the PDPC's guide expects within 30 calendar days, and notification to the Commission no later than three calendar days after the breach is assessed to be notifiable (section 26D).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Singapore PDPA

PDPA Obligation Library

Load the obligations in Parts 3 to 6A as requirements, each citing its section, with owner, status and linked policy and evidence.

Data Inventory and Purpose Register

Record the personal data held, the purposes notified under section 20, the consent basis or schedule exception relied on and the retention rule under section 25.

Access and Correction Requests

Log section 21 and 22 requests with the data and the past year's uses and disclosures, the Fifth and Sixth Schedule exceptions applied, deadlines and the response sent.

Overseas Transfer Register

Track each transfer outside Singapore with the regulation 12 mechanism relied on, the contractual clauses or certification and the data intermediary involved, in Third Party Risk Management.

Breach Assessment and Notification

Run the Part 6A workflow: discovery date, the 30-day assessment, the significant harm and 500-individual tests, the three-calendar-day notice to the Commission and the notices to individuals.

Accountability Evidence

Keep the data protection officer designation, the section 12 policies and practices, staff communication and the complaints process as evidence for the Commission and for customer assessments.

Common framework mappings

APEC CBPR System | CCPA/CPRA | GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27018 | ISO 27701 | NIST Privacy Framework v1.0

Official resources

Personal Data Protection Act (PDPA)

Defines the legal framework for personal data protection in Singapore by the PDPC.

sso.agc.gov.sg/Act/PDPA2012

Advisory Guidelines on Key Concepts in the PDPA (PDPC)

The PDPC's chapter-by-chapter interpretation of every data protection obligation in the Act, with examples.

pdpc.gov.sg/organisations/regulations-decisions/regulatory-guidance/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act

Guide to Developing a Data Protection Management Programme

Outlines steps for organizations to create a PDPA-compliant data protection program.

pdpc.gov.sg/organisations/resources/guidance-by-topic/guide-to-developing-a-data-protection-management-programme

Guide to Handling Access Requests

Explains how organizations should handle personal data access requests under PDPA.

pdpc.gov.sg/organisations/resources/guidance-by-topic/guide-to-handling-access-requests

Frequently asked questions

Who must comply with the Singapore PDPA?

Every organization that collects, uses or discloses personal data in Singapore, whether or not it is formed, recognized or located there (section 2). Section 4 excludes public agencies, individuals acting in a personal or domestic capacity and employees acting in the course of their employment, and it limits a data intermediary processing under a written contract to the Protection and Retention Limitation Obligations and the breach duties in Part 6A.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the PDPA's data protection obligations?

Parts 3 to 6A set them out: accountability, including a designated data protection officer and written policies (sections 11 and 12); consent and its exceptions (13 to 17); purpose limitation and notification (18 and 20); access and correction (21 and 22); accuracy (23); protection (24); retention limitation (25); transfer limitation (26); and data breach notification (26A to 26E). The Do Not Call provisions are in Part 9.

When must a data breach be reported to the PDPC?

Under Part 6A an organization must assess a suspected breach reasonably and expeditiously, which the PDPC's guide expects within 30 calendar days. If the breach is likely to result in significant harm to affected individuals, or affects 500 or more individuals, the organization must notify the Commission as soon as practicable and no later than three calendar days after that assessment (section 26D), and notify affected individuals at the same time or after unless an exception applies.

What are the maximum penalties under the PDPA?

Since October 1, 2022, section 48J allows the Commission to impose a financial penalty of up to 10 percent of an organization's annual turnover in Singapore where that turnover exceeds S$10 million, and otherwise up to S$1 million, for an intentional or negligent contravention of the data protection provisions. Turnover is taken from the most recent audited accounts (section 48J(5A)). Part 9B also creates criminal offenses for unauthorized disclosure, improper use and unauthorized re-identification of anonymized data.

What did the 2020 Amendment Act change?

The Personal Data Protection (Amendment) Act 2020 was passed on November 2, 2020. From February 1, 2021 it introduced mandatory breach notification (Part 6A), deemed consent by notification (section 15A), the legitimate interests and business improvement exceptions in the First and Second Schedules and the Part 9B offenses; from October 1, 2022 it raised the financial penalty cap in section 48J. Its data portability provisions (Part 6B) had not been brought into operation as of October 15, 2026.

License included / downloadable: Yes The Personal Data Protection Act 2012 is Singapore legislation published free on Singapore Statutes Online by the Attorney-General's Chambers; the PDPC's advisory guidelines and guides are free PDFs on pdpc.gov.sg.

Full framework page and mappings: smartsuite.com/frameworks/singapore-personal-data-protection-act-pdpa