

iapp



CIPP/A Body of Knowledge

Version 2.0.0

Effective date: 14 July 2025

Asian Privacy Certification



Outline of the Body of Knowledge for the Certified Information Privacy Professional/Asia (CIPP/A)

I. Privacy Fundamentals

A. Modern Privacy Principles

- a. The Organisation of Economic Cooperation and Development (OECD) ‘Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data.’ (1980)
- b. The Asia Pacific Economic Cooperation (APEC) privacy principles
- c. Fair Information Practices (FIPs)
- d. Universal Declaration of Human Rights (1948)

B. Adequacy and the Rest of the World

- a. Europe and the General Data Protection Regulation (GDPR)
- b. Deemed adequate: New Zealand, Canada, Israel, Argentina, Uruguay
- c. United States and the EU-U.S. Privacy Shield
- d. Deemed not adequate: Australia, Mexico, Korea, Taiwan

C. Elements of personal information

- a. Personal data (EU) (HK) (SG)
- b. Personally identifiable information (U.S.)
- c. Sensitive personal data information (IND)



- d. Pseudonymisation, de-identification and anonymisation

II. Singapore Privacy Laws and Practices

A. Legislative history and origins

- a. Singapore government and legal system
 - i. Political structure
- b. Social attitudes toward privacy and data protection
- c. Surveillance and identification
- d. Constitutional protections
- e. Common law protections
- f. Sector-specific protections

B. Personal Data Protection Act 2012 (PDPA)

- a. Application and scope
 - i. PDPA predecessor: National Internet Advisory Committee (NIAC) 2002 Report, *Report on a Model Data Protection Code for the Private Sector*.
 - ii. Extraterritorial reach
 - iii. PDPA definitions
 - a. Personal data
 - b. 'Business contact information'
 - c. 'Data intermediary'
 - d. Publicly available
 - e. Survivorship
 - iv. *Do Not Call Registry*
 - a. 'Specified message'
 - v. PDPA in an employment setting
 - vi. Exemptions
 - a. Public-sector
 - b. Response to emergency
 - c. National interest
 - d. Investigations in legal proceedings
 - e. Evaluative purposes
 - f. Journalism and media
- b. Key concepts and practices
 - i. Data protection officer
 - ii. Staff training
 - iii. Consent and exceptions to consent
 - iv. Use
 - v. Disclosure



- vi. Safeguarding/Security
- vii. Accountability and openness
- viii. Access and correction
- ix. Retention and deletion
- x. Transfer out (e.g. APEC, CBPR and PRP)
- xi. Data breach notification obligation

C. Enforcement

- a. Monetary Authority of Singapore
 - i. Regulations and guidances
 - ii. ‘Notices on Prevention of Money Laundering and Countering the Financing of Terrorism’
 - iii. Individual’s access and rights
 - iv. Protection of customer data
 - v. Outsourcing
- b. *Personal Data Protection Commission (PDPC)*
- c. Decision in appealed commissioner rulings, complaints
 - i. Complaint-based vs. audit-based
- d. Commissioner guidance and published positions
- e. Managing consent opt-out mechanisms: their use and limitations, consent to new purposes and documentation
- f. Penalties and sanctions
- g. Policy development and implementation
 - i. Freedom of information legislation
 - ii. Data transfers: doctrine of privity of contract for third-parties

III. Hong Kong Privacy Laws and Practices

A. Legislative history and origins

- a. Hong Kong government and legal system
- b. Social attitudes toward privacy and data protection
- c. Surveillance and identification
- d. Constitutional protections
- e. Common law protections

B. Personal Data (Privacy) Ordinance (PDPO):

- a. Application and scope
 - i. Meaning under PDPO
 - a. Personal data
 - b. Publicly available data
 - c. Sensitive personal data



- d. 'Prescribed consent'
 - e. Rights of data subject
 - ii. Personal Data (Privacy) (Amendment) Ordinance 2012
 - a. 'The New Guidance on Direct Marketing'
 - iii. Major Exemptions
 - a. Staff planning and Employment related (including Personal References)
 - b. Relevant process (Evaluation)
 - c. Crime, etc.
 - d. Legal proceedings, etc.
 - e. Legal professional Privilege and Self-incrimination
 - f. Health and Emergency
 - g. Statistics and Research
 - h. Journalism and news media
- b. Key concepts and practices
 - i. Six Data Protection Principles (DPPs) and the Internet Data Guidance
 - 1. DPP1: Data Collections
 - 2. DPP2: Accuracy and retention
 - 3. DPP3: Data Use
 - 4. DPP4: Data security
 - 5. DPP5: Openness
 - 6. DPP6: Data access and correction
 - ii. Due diligence exemption and exercise
 - iii. Guidance on Personal Data Erasure and Anonymisation
 - iv. Guidance on employment matters
 - v. Data Transfer/Export, Ordinance Section 33
 - a. Data processors
 - b. Model contracts

C. Enforcement

- a. *The Office of the Privacy Commissioner for Personal Data*
- b. Commissioner rules
- c. Commissioner guidance and published positions
 - i. *Octopus Rewards Ltd.*
- d. Decisions in appealed commissioner rulings, complaints
- e. *Personal Data (Privacy) Advisory Committee*
- f. Managing consent opt-out mechanisms: their use and limitations, consent to new purposes and documentation
- g. Enforcement notice
- h. Policy development and implementation



- i. Law reform proposals for third-party benefit exception
- i. Privacy incidents: trends in commissioner expectations

IV. India Privacy Law and Practices

A. Legislative history and origins

- a. Indian government and legal system
 - i. Political structure
- b. Social attitudes toward privacy and data protection
- c. Surveillance and identification
 - i. Credit Information Companies (Regulation) Act 2005
- d. Constitutional protections
 - i. Article 21
 - ii. The Right to Information Act 2005
 - iii. The Protection of Human Rights Act 1993
- e. Common law protections (e.g. 2017 Supreme Court judgment on the Right to privacy - Puttaswamy judgment)
- f. Information Technology Act 2000 (IT Act) and Information Technology Amendment Act 2008 (ITAA)

B. Digital Personal Data Protection Act 2023 (DPDPA)

- a. Application and scope: replaces section 43A from the Information Technology Act 2000
 - i. Right to access information about personal data
 - ii. Right to correction and erasure of personal data
 - iii. Right of grievance redressal
 - iv. Right to nominate other individuals to act on their behalf
 - v. Right to withdraw consent
 - vi. Children's data
 - vii. Exemptions
 - a. Processing of publicly available personal data
 - b. Processing of personal data for research/statistical purpose (i.e., training AI)
 - c. Research, archiving and statistical purposes
 - d. Judicial, investigation, mergers & acquisitions purposes
 - e. Non-digital data
- b. DPDPA Rules
 - i. Privacy notices and consent: Rules 3-4
 - ii. Exemptions for state agencies to process personal data: Rule 5
 - iii. Security safeguards and notification procedures for data breaches: Rules 6-7



- iv. Retention period and erasure of personal data: Rule 8
- v. Contact info for Data Protection Officer: Rule 9
- vi. Parent/guardian consent, consent exemptions for children: Rules 10-11
- vii. Annual data protection impact assessments, audits: Rule 12
- viii. Right to access, correct, delete personal data: Rule 13
- ix. Regulating cross-border transfer of personal data: Rule 14
- x. Exemptions for research purposes: Rule 15
- xi. Data Protection Board setup, Board appeal process: Rules 16-21
- xii. Allows government to request information from Data Fiduciaries for purposes in the Seventh Schedule: Rule 22
- xiii. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

C. Enforcement

- a. The Ministry of Communication and Information Technology
- b. The Department of Electronics and Information (DeitY)
- c. The Telecom Regulatory Authority of India (TRAI) and Do Not Call Registry
 - i. Banning Free Basics and Net Neutrality
- d. Data Protection Board
- e. Commissioner rulings, appeals and complaints
- f. Penalties and sanctions
 - i. DPDPA Chapter VIII
- g. Commissioner guidance and published positions
- h. Grievance officers
- i. Managing consent opt-out mechanisms: their use and limitations, consent to new purposes and documentation
- j. Policy development and implementation
 - i. Data transfers: doctrine of privity of contract for third-parties
- k. Public-sector exemption

V. Common themes among principle frameworks

- A. Comparing protections and principles
 - i. Sensitive data protections
 - ii. Children's data protections
 - iii. Natural persons vs. legal persons
 - iv. Data breach notification
 - v. Public Registers
 - vi. Surveillance



- a. National identity systems
 - i. SingPass
 - ii. HKID
 - iii. India's UIDAI
 - b. Legislation
 - a. Hong Kong: *PCPD Code of Practice on Identity Card Number and Other Personal Identifiers*, 1997
 - vii. Data processing and export
 - viii. Intermediaries
 - ix. Extraterritorial operations
- B. Rights of the data subject
 - i. 'Domestic' use
 - ii. Breadth of exemption
 - a. Hong Kong
 - i. Chinese central government organisations
 - ii. Media
 - b. Singapore
 - i. Public-sector
 - ii. Public authorities
 - iii. Publicly available information
 - iv. 'Public agency'
 - v. Business contracted by Singapore government
 - c. India
 - i. Public sector
 - ii. Public authorities
 - iii. Publicly available information
 - iv. Section 17(3): Specific businesses especially exempted by government, such as 'startups'