iapp

CIPP/A
BODY OF KNOWLEDGE

VERSION 1.0.2

EFFECTIVE DATE: 09/01/2021

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. DDP3: 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)

B. Information Technology Act 2000 (IT Act)
    a. Application and scope
        i. *Information Technology Act 2000*
            a. Section 43
            b. Section 66A and its removal
        ii. *Information Technology (Amendment) Act 2008 (ITAA)*
            a. Section 43A
            b. Definitions
                i. Personal data
                ii. Sensitive personal data
                iii. Body corporate
                iv. Rights of data subjects
        iii. Exemptions
            a. Religious and social, charitable organisations
            b. Non-commercial organisations
            c. Non-automated data
    b. Section 43A and the 2011 Rules: Rules 3-8
        i. Privacy policies required: Rule 3
        ii. Data protection principles: Rule 4
            a. Consent and purpose limitation
            b. Lawful purpose and minimal collection
            c. Notice and purpose limitation
            d. Retention
            e. Use
            f. Subject access and correction
            g. Option to refuse or withdraw consent
            h. Security
            i. Complaint handling

iii. Disclosure imitations and exceptions: Rule 5
iv. Data processing: Rule 6
v. Data export restriction: Rule 7
vi. Reasonable security: Rule 8
vii. 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. Commissioner rulings, appeals and complaints
e. Penalties and sanctions
    i. IT Act Sections 43(b) and (g)
    ii. IT Act Sections 72 and 72A
f. Commissioner guidance and published positions
g. Grievance officers
h. Managing consent opt-out mechanisms: their use and limitations, consent to new purposes and documentation
i. Policy development and implementation
    i. Data transfers: doctrine of privity of contract for third-parties
j. 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
        j. 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. Limited application for 'sensitive data'
ii. Limited application to 'providers' not data subjects
iii. Freedom of speech
iv. Lack of openness