DREW & NAPIER

Data Protection and Cyber Regulation
- Module Introduction
- Unit 1: Data Protection

David N. Alfred
Director & Co-Head, Data Protection, Privacy & Cybersecurity Practice, Drew & Napier
Co-Head, Drew Data Protection & Cybersecurity Academy

Module Introduction

Topics Covered

- This module comprises the following 4 units (approximate weightage as indicated below):
  - Data Protection 1/3
  - Cybersecurity 1/3
  - Regulation of AI and Data Processing) 1/3
  - Prevention on Online Threats and Falsehoods)
- In **Unit 1: Data Protection**, we shall be covering the following topics relating to the protection of personal data under the Personal Data Protection Act 2012 (PDPA):
  - Purpose and Scope of the PDPA (what is personal data, who it applies to, etc.)
  - Obligations of organisations (including legal bases for processing personal data)
  - Rights of individuals
  - Enforcement of the PDPA

Topics Covered

- In **Unit 2: Cybersecurity**, we shall be covering the following topics relating to regulation of cybersecurity under the PDPA and the Cybersecurity Act 2018 (CYSA):
  - Scope of the Protection Obligation under the PDPA
  - Notification of data breaches under the PDPA
  - Offences relating to the misuse of personal data under the PDPA
  - Protection of critical information infrastructure under the CYSA
  - Prevention of cybersecurity incidents under the CYSA
- In **Unit 3: Regulation of AI and Data Processing**, we shall be covering the following topics :
  - Application of the PDPA to data processing and data governance
  - PDPC's Model AI Governance Framework
  - Data ethics and future regulatory models / issues

Topics Covered

- Finally, in **Unit 4: Prevention of Online Threats and Falsehoods**, we shall be covering topics relating to how threatening and false messages and information are regulated under the Protection from Harassment Act (POHA) and (to a lesser extent) the Protection from Online Falsehoods and Manipulation Act (POFMA) and the recent Online Safety (Miscellaneous Amendments) Act 2023 (Online Safety Act).
- Topics covered will include:
  - Scope and objectives of POHA
  - Offences under POHA and application to the online environment
  - Remedies under POHA
  - Comparison with POFMA and Online Safety Act

Approach

- These slides give an overview of the topics covered
- This module covers a number of Acts and Regulations. The provisions relating to the topics covered in this module are essential knowledge.
- Cases and other reading materials in the reading list will give you a good understanding of the topics
- Optional readings are entirely optional and will not be tested. They are included to give some useful background context.

Unit 1: Data Protection

Topics Covered

1. Introduction and Overview
2. Purpose and Scope of the PDPA
3. Obligations of Organisations
4. Rights of Individuals
5. Enforcement of the PDPA
6. Specific Topics

Readings for this Unit

1. Personal Data Protection Act 2012 (*PDPA*)
2. Personal Data Protection Regulations 2021 (*PDPR*)
3. Personal Data (Notification of Data Breaches) Regulations 2021 (*DBNR*)
4. Personal Data Protection Commission (PDPC), Advisory Guidelines on Key Concepts in the PDPA (*Key Concepts Guidelines*)
5. PDPC, Advisory Guidelines on the PDPA for Selected Topics (*Selected Topics Guidelines*)
6. PDPC, Advisory Guidelines on Enforcement of Data Protection Provisions (*Enforcement Guidelines*)
7. Reed, Michael v Bellingham, Alex (Attorney-General, intervener) [2022] SGCA 60

1| Introduction and Overview

Introduction

- The PDPA, Singapore's first general data protection law, was enacted in 2012 and came into force in stages up to July 2014
  - Personal Data Protection Commission (PDPC) was established in 2013
  - PDPA's Do Not Call and Data Protection Provisions came into force in 2014
- PDPA was significantly amended in 2020 to introduce new obligations in line with modern data protection laws in other jurisdictions
  - New provisions on data protection obligations and rights of individuals
  - New criminal offences relating to misuse of personal data
  - Enhanced enforcement powers for PDPC/Commissioner

Overview

- The following subsidiary legislation expand on the obligations of organisations or procedurals aspects of the PDPA:
  - Personal Data Protection (Appeal) Regulations 2021
  - Personal Data Protection (Composition of Offences) Regulations 2021
  - Personal Data Protection (Do Not Call Registry) Regulations 2013
  - Personal Data Protection (Enforcement) Regulations 2021
  - *Personal Data Protection (Notification of Data Breaches) Regulations 2021
  - *Personal Data Protection Regulations 2021
  - Rules of Court 2021, Order 57

  (*only these are covered in this unit)

Overview

- PDPC has issued several advisory guidelines (under PDPA section 49) and may other publications and materials to assist organisations in complying with the PDPA
- The following are covered in this unit (full names in the Reading List):
  - Key Concepts Guidelines
  - Selected Topics Guidelines
  - Enforcement Guidelines

Checkpoint 1 | Review Questions

- What is the legal effect of advisory guidelines issued by PDPC under the PDPA?

2| Purpose and Scope of the PDPA

Purpose: PDPA Section 3

- Govern collection, use and disclosure of personal data by organisations
- Recognises
  - Right of individuals to protect their personal data
  - Needs of organisations
- Does not confer proprietary rights over personal data (usual laws apply)
- Key terms:
  - Personal data, individuals (target subject-matter)
  - Organisations (entities required to comply)
  - Collection, use, disclosure / data processing (target activities)

Substantive Scope: PDPA Section 2(1)

- **Personal Data**
  - Data about an identifiable individual
  - Includes factual information and opinions
  - Does not depend on truth of the data
  - Note exclusions, e.g. for business contact information
- **Individual**
  - Natural person, living or deceased
- **Organisation**
  - Includes (non-exhaustive) any individual, company, association or body of persons regardless of where formed, recognised, resident or having an office / place of business
  - Excludes individuals acting in a personal or domestic capacity or as an employee
  - Excludes public agencies (covered under a separate framework / law)

Substantive Scope: PDPA Section 2(1)

- **Data intermediaries (DIs)**
  - Sometimes known as data processors in other jurisdictions' laws
  - Organisations that processes personal data on behalf of another organisation
  - Fewer obligations under the PDPA: only sections 24, 25, 26C(3)(a) and 26E and Part 6B
- **Data controllers (DCs)**
  - Not a defined term in the PDPA
  - Refers to the organisation on whose behalf a DI is processing personal data
  - Controls the purposes and sometimes the manner of processing
  - Responsible for personal data processed on its behalf by the DI
- **Collection, use and disclosure**
  - Not defined in the PDPA
  - Overlaps with the defined term "processing"

Interaction with other laws: PDPA Section 4(6)

- Nothing in the Data Protection Provisions affects any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law
- But, performance of a contractual obligation is not an excuse for contravening the PDPA
- In the event of any inconsistency between the Data Protection Provisions and provisions of another written law, the provisions of the other written law will prevail

Checkpoint 2 | Review Questions

- What are the key elements of the scope of the PDPA?
- How do we determine if data is personal data?
- What provisions / obligations apply to personal data of deceased individuals?
- What kinds of organisations does the PDPA apply to? List some examples.
- What is “written law” in section 4(6) of the PDPA?

3| Obligations of Organisations

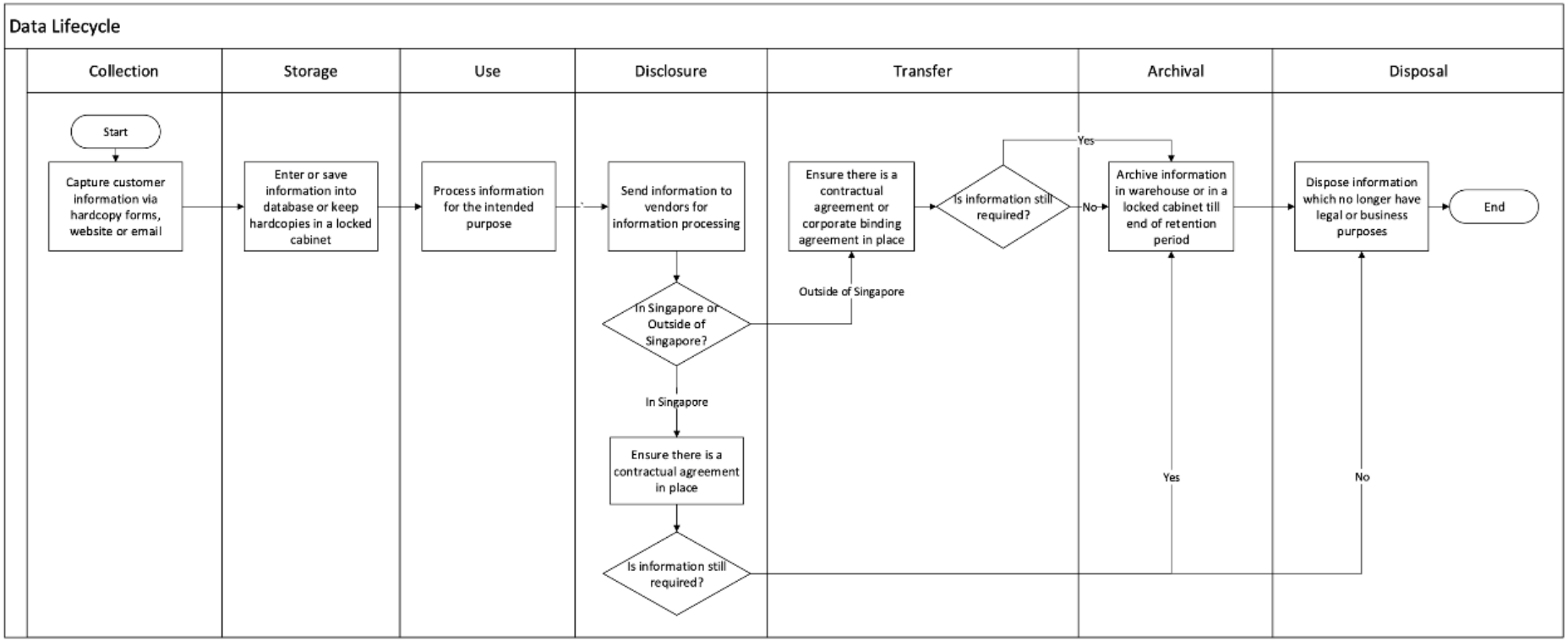
Obligations of Organisations: Overview

- When are organisations permitted to collection, use and disclose personal data?
  - Purpose Limitation Obligation
  - Consent Obligation / Legal Bases for Processing
  - Notification Obligation
- What must organisations do while processing personal data?
  - Data Minimisation (part of Purpose Limitation)
  - Accuracy Obligation
  - Protection Obligation
  - Data Breach Notification Obligation
  - Retention Limitation Obligation

Obligations of Organisations: Overview

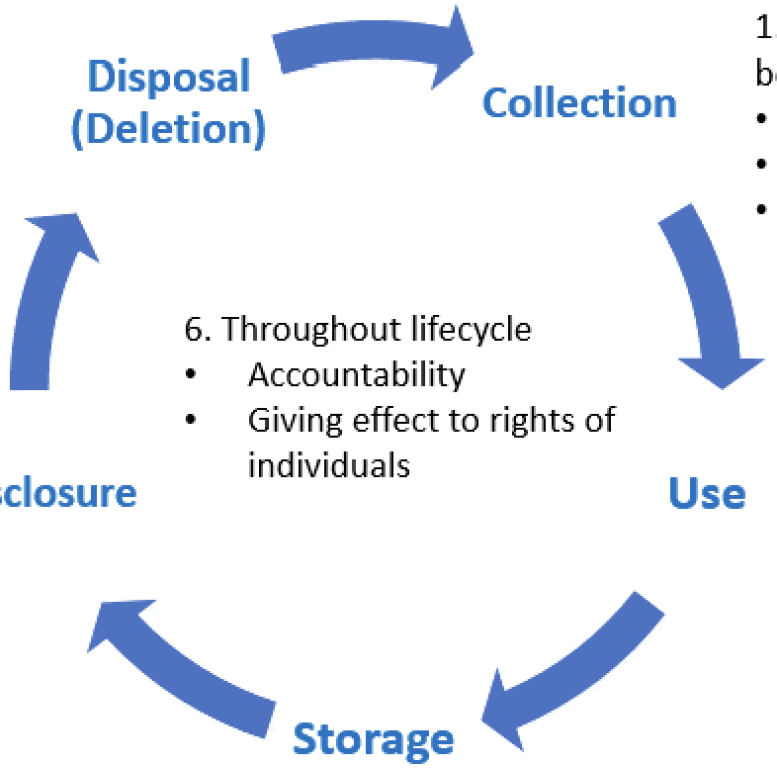
- What must organisations do if they disclose or transfer personal data to another organisation (DC or DI)?
  - Obligations relating to disclosure to DIs
  - Transfer Limitation Obligation
- What governance measures must organisations put in place?
  - Accountability Obligation

Obligations of Organisations: The Data Lifecycle



- Source: : PDPC, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Data-Flow-Illustration-PDF-v2.pdf (last accessed 5 July 2023)

Data Protection Obligations and the Data Lifecycle



1. When can personal data be collected?
- Purpose Limitation
- Notification
- Consent / Other Legal Bases

2. How should personal data be processed?
- Data Minimisation (Purpose Limitation)
- Accuracy

3. Security requirements
- Protection
- Data Breach Notification
- Offences against misuse of personal data

4. How should disclosed personal data be protected?
- Requirements for outsourcing (use of data intermediaries)
- Transfer Limitation

5. How should personal data be disposed of?
- Retention Limitation

6. Throughout lifecycle
- Accountability
- Giving effect to rights of individuals

Obligations of Organisations: Some Points to Note

- **Purpose Limitation**
  - Keywords: reasonable, appropriate, lawful, legitimate, relevant
- **Consent**
  - One of several legal bases under which organisations may collect, use and disclose personal data
  - Legal bases for processing under the PDPA include:
    - Legal obligations / authority under written law
    - Consent and general deemed consent
    - Deemed consent by contractual necessity
    - Vital interests of individuals
    - Public matters
    - Legitimate interests of organisations
    - Business assess transactions
    - Business improvement purposes and research

Obligations of Organisations: Some Points to Note

- **Data Minimisation and Accuracy**
  - Data minimisation is part of Purpose Limitation
  - Lay the groundwork for good data analysis and decision-making
  - Ensures relevant, accurate and complete data is used by organisations
- **Disclosure to DIs**
  - Pursuant to contract
  - What clauses / obligations must be included?
  - What optional clauses / obligations may be included (depending on the scope of services)?
  - Hint: Consider each of the Data Protection Provisions
- **Transfer Limitation**
  - Permitted modes are set out in PDPR Part 3

Obligations of Organisations: Some Points to Note

- **Accountability**
  - Two key elements:
    - Responsibility for personal data (see PDPA section 11(2))
    - Being able to demonstrate how the organisation has discharge its responsibility
  - May include:
    - Measures specified in the PDPA (e.g. appoint a DPO, develop data protection policies and practices)
    - Measures required to comply with the Data Protection Provisions (e.g. conduct a data inventory)
  - PDPC has given guidance on developing a Data Protection Management Programme (DPMP) and related documents and practices (not covered in this unit)
- **Do Not Call Obligations**
  - Not covered in detail but note the 3 main obligations (sections 43, 44 and 45)
  - Note that telemarketing is also covered by the Data Protection Provisions

Checkpoint 3 | Review Questions

- What is the PDPA's standard of reasonableness?
- What purposes can an organisation collect, use and disclose personal data for (in general)?
- What are the legal bases for processing personal data which are permitted under the PDPA? Where are they found in the PDPA and when do they apply?
- When is notification of purposes required under the PDPA?
- How can organisations ensure accuracy of personal data collected?
- How long can organisations retain documents containing personal data? What are the legal and business purposes mentioned in section 25 of the PDPA?
- What are the obligations of data controllers in relation to their data intermediaries?
- How can an organisation meet its obligations under the PDPA if they wise to transfer personal data out of Singapore?
- What are the Accountability measures organisations must implement?

4| Rights of Individuals

Rights of Individuals: Overview

- Organisations must give effect to rights on individuals under the PDPA
- Depends on exercise of the right by the individual concerned
- Main rights:
  - Right to Withdraw Consent
  - Right of Access) PDPC's Access and Correction
  - Right of Correction) Obligation
  - Right to Data Portability - PDPC's Data Portability Obligation
  - Right of private action

Rights of Individuals: Highlights

- **Right to Withdraw Consent**
  - PDPA section 16
  - Organisations must give effect to the withdrawal of consent, although this does not affect the legal consequences which may arise
  - Organisations may continue to collect, use and disclose personal data if doing so without consent is required or authorised under written law
- **Rights of Access and Correction**
  - PDPA sections 21 and 22 and PDPR Part 2
- **Right to Data Portability**
  - Not yet in force (not covered in this unit)
- **Right of Private Action**
  - PDPA section 48O
  - See [2022] SGCA 60 (Note: This case relates to the former PDPA section on right of private action which was repealed and replaced by section 48O)

Checkpoint 4 | Review Questions

- How can an individual withdraw consent for collection, use and/or disclosure of their personal data under the PDPA?
- How can an individual make a request for access to, or correction of, their personal data?
- How should an organisation process a request for access to, or correction of, personal data? When is an organisation permitted (or required) to deny or refuse such a request?
- What is the scope of individuals' private right of action under the PDPA?
- What did the court decide in the Michael Reed v. Alex Bellingham case [2022] SGCA 60?

5| Enforcement of the PDPA

PDPC's Investigative and Enforcement Powers

- PDPC exercises powers of investigation under PDPA section 50 and various powers of enforcement under PDPA Part 9C
- Powers of enforcement include:
  - Power to refer a complaint to mediation or other modes of alternative dispute resolution
  - Power to review an organisations response to a request for access to, or correction or porting of, personal data
  - Power to issue a direction for non-compliance
  - Power to require payment of a financial penalty of up to 10% of the annual turnover of the organisation in Singapore or $1 million, whichever is higher (for breaches of the Data Protection Provisions)
  - Power to accept a voluntary undertaking
- PDPA includes provisions for reconsideration of, and appeal against, PDPC's decision (section 48N and Part 9C)

Checkpoint 5 | Review Questions

- How does PDPC exercise its powers of investigation and enforcement? What is its approach to resolving or addressing a complaint? (Hint: See Enforcement Guidelines)
- When could PDPC terminate an investigation?
- What are the directions / remedies which PDPC may give under the PDPA?
- What is a voluntary undertaking? When could an organisation give one to PDPC?
- How are PDPC's directions enforced (i.e. if an organisation fails or refuses to comply with a direction)?
- When can an organisation or person apply for reconsideration of a PDPC decision or direction? When can they appeal against a PDPC decision or direction?

6| Specific Topics

Specific Topics

- Consider how the PDPA applies to the following (see Selected Topics Guidelines):
  - Analytics and research
  - Anonymisation
  - Online activities
  - Cloud services

Checkpoint 6 | Review Questions

- What are the PDPA provisions which whether/how organisation can conduct any kind of research?
- What is anonymisation? When is data considered to be anonymised? Why do organisations need (or want to anonymise personal data?
- What types of data may be created and/or used during online activities? Which of these constitute personal data? When is consent required for use of cookies?
- What are the obligations of cloud service providers, and the organisations which use them, under the PDPA?

Drew & Napier LLC
10 Collyer Quay, #10-01 Ocean Financial Centre, Singapore 049315
www.drewnapier.com