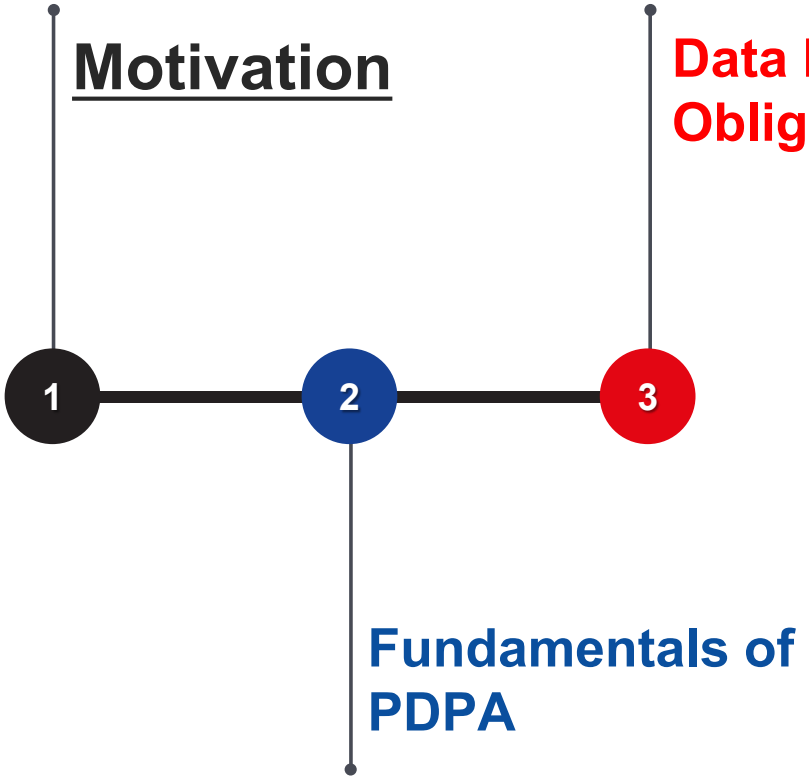
NANYANG
THE INNOVATIVE POLYTECHNIC

Data Privacy and Protection

Topic 4

PDPA
The Personal Data Protection Act

Contents

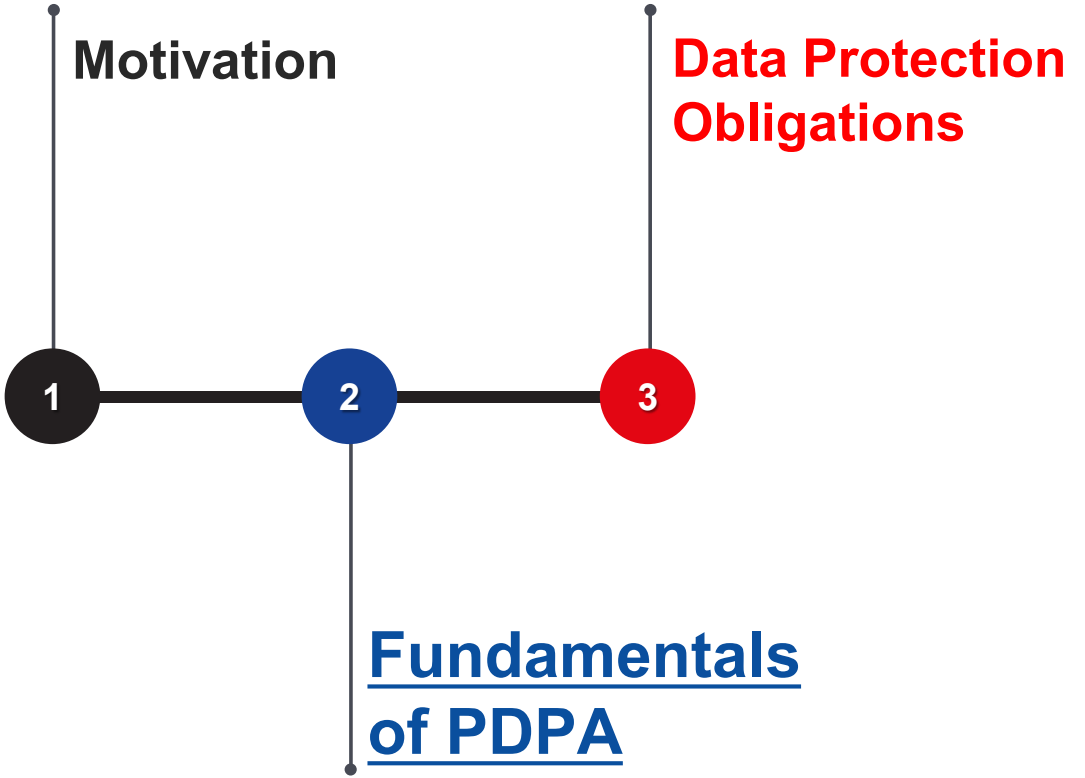

Motivation
Data Protection Obligations
1
2
3
Fundamentals of PDPA

PDPA – Protecting Personal Data

… everyone has a part to play – both the individual and organisations

https://youtu.be/jNTjFsEOeR4

Contents


Motivation
Data Protection Obligations
1
2
3
Fundamentals of PDPA

Fundamentals of Personal Data Protection Act

What – PDPA …

- Is Singapore's **data privacy regulation**
- Governs the **collection, use, disclosure and care** of personal data
- **Regulates telemarketing** practices through the Do Not Call registry

Why – PDPA …

- Is designed to **encourage business innovation**, while also **guaranteeing that personal data protection**
- Aims to strengthen Singapore's position as a **trusted hub for businesses**

Fundamentals of Personal Data Protection Act

Who – PDPA …

- Recognizes the **right of individuals** to protect their personal data
- Recognizes the **need for organisations** to collect, use or disclose personal data for legitimate and reasonable purposes
- **Does not apply to the public sector**, which has separate rules under the government

Where – PDPA …

- Has extraterritorial effect.
- It is applicable to organizations collecting, using or disclosing personal data in Singapore, regardless of the organization's physical presence or where it was incorporated

Fundamentals of Personal Data Protection Act

Cost – Failure to comply PDPA obligation

- For organizations with an annual turnover in Singapore exceeding SGD 10 million, the **maximum** financial penalty is 10% of their annual turnover in Singapore.
- For all other organizations, including those with an annual turnover of SGD 100,000, the **maximum** financial penalty is SGD 1 million.
- Additional cost:
  - **Reputation damage**

Breach of the Protection Obligation by SAP Asia

21 Sep 2021

A financial penalty of $13,500 was imposed on SAP Asia for failing to put in place reasonable security arrangements to protect personal data of its former employees. This resulted in an unauthorised disclosure of the personal data to unintended recipients.

Breach of the Protection Obligation by Ninja Logistics

04 Nov 2019

Directions, including a financial penalty of $90,000, were imposed on Ninja Logistics for failing to put in place reasonable security arrangements to protect customers' data in relation to the Tracking Function Page on the Ninja Logistics website. This resulted in customers' data on the website to be accessible by the public.

Breach of the Protection Obligation by SingHealth and IHiS

15 Jan 2019

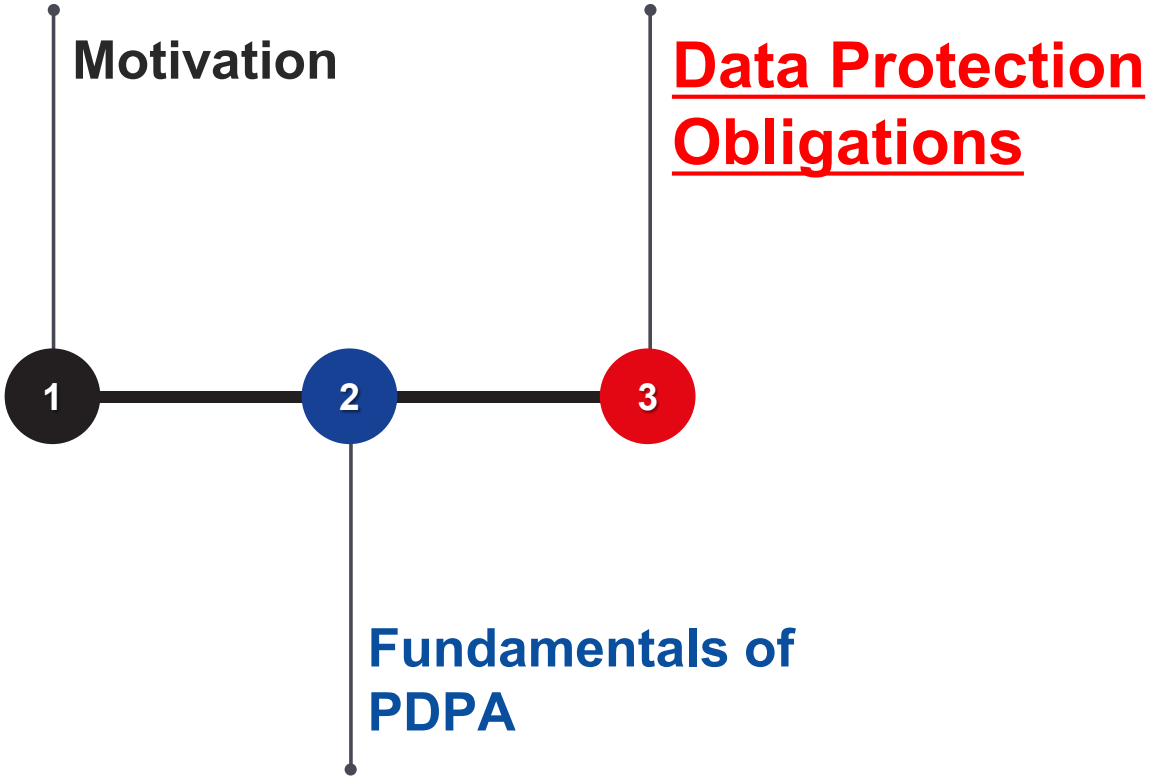
A financial penalty of $250,000 and $750,000 was imposed on SingHealth and IHiS respectively for the failure to make reasonable security arrangements to protect personal data of individuals.

Breach of the Protection Obligation by Horizon Fast Ferry

02 Aug 2019

A financial penalty of $54,000 was imposed on Horizon Fast Ferry for failing to appoint a data protection officer, develop and implement data protection policies and practices, and put in place reasonable security arrangements to protect the personal data collected from its customers.

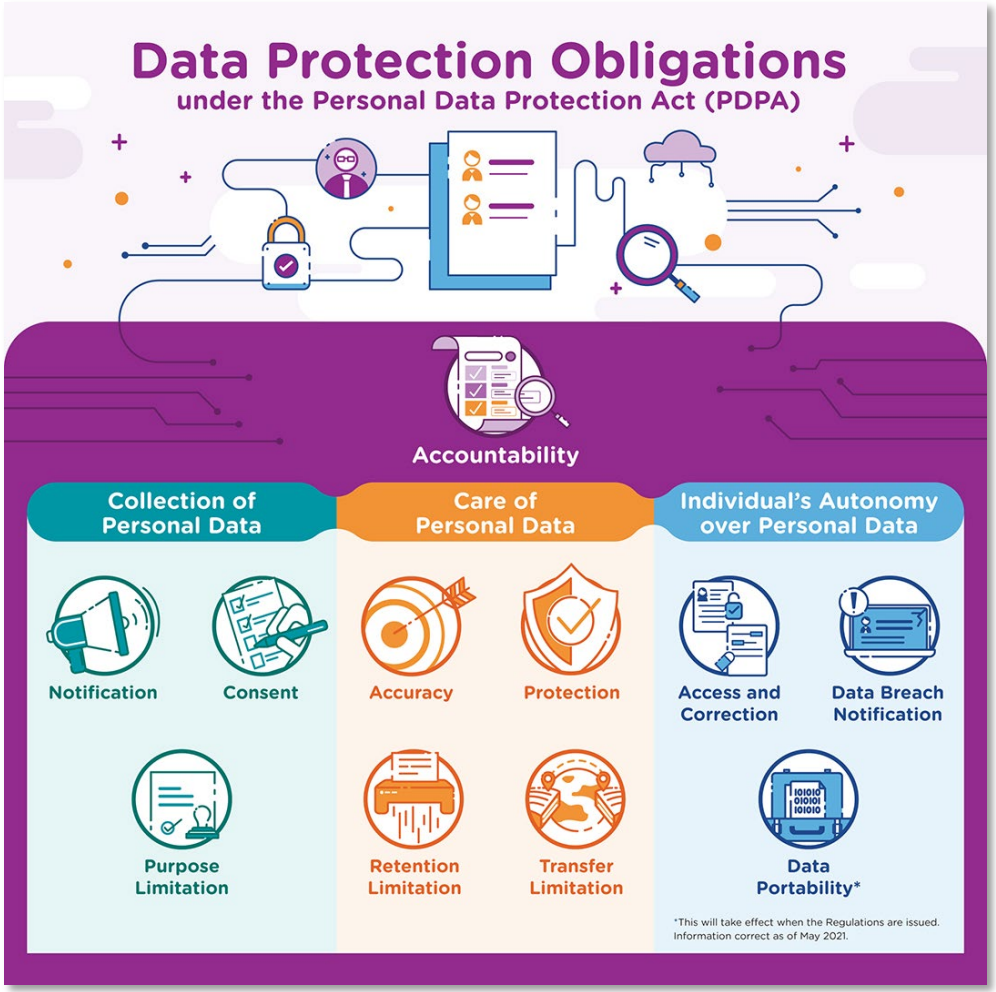
Contents


Motivation
Data Protection Obligations
1
2
3
Fundamentals of PDPA

Data Protection Obligations

- The PDPA outlines 11 obligations

- Organisations are required to comply with these obligations when undertaking activities relating to the collection, use or disclosure of personal data



Accountability

Accountability helps organisations to strengthen trust and enhance competitiveness.

Organisations must take responsibility for the personal data under their possession or control

- Appoint a data protection officer
- Develop data protection policies
- Foster a data protection awareness and culture
- Implement measures to meet PDPA obligations

Notification

Notify individuals of the purposes for which the organisation is intending to collect, use or disclose their personal data

Important considerations for Notification include:

- Content of the notification
- Format of the notification
- When to notify

Consent

Personal data may be collected, used or disclosed only after consent has been given by the individual

Important considerations for obtaining Consent include:

- Consent cannot be accepted, unless the individual has been Notified of the purposes
- Allow the individual to withdraw consent
- Consent can be obtained in writing or verbally

Purpose Limitation

Personal data may be collected, used or disclosed ONLY for the purposes that is reasonable to provide the organisation's product or service

Important considerations for Purpose Limitation include:

- Collect, use and disclose personal data, that are relevant for the purposes
- Ensure the purposes are reasonable for the product or service provided

Accuracy

Organizations should ensure that the personal data collected is accurate and complete

Important considerations for Accuracy include:

- Reliability of the data
- Currency of the data
- Impact of the data

Protection

Organizations should put in place the required security measures to protect personal data to prevent unauthorized access

Important considerations for Protection include:

- Well-trained personnel responsible for ensuring information security
- Robust information security policies and procedures
- Breach response preparedness

Retention Limitation

Organizations should cease retention of personal data or dispose of it in a proper manner

Important considerations for Protection include:

- Review the need to hold personal data on a regular basis
- Render personal data completely irretrievable or inaccessible
- No means to associate the personal data with particular individuals

Transfer Limitation

Ensure that the standard of protection is comparable to the PDPA when transferring personal data to another country.

An important consideration for Transfer Limitation:

- In transferring data overseas, the receiving organisation is not subject to Singapore laws
- The Accountability Obligation requires that the transferring organisation ensures that personal data under its care continue to be protected to the same standard as that established in PDPA

Access and Correction

Individuals have the right to request for access to their personal data and for correction of their personal data

Organizations may not accede to an access request where the provision of personal data is expected to:

- threaten the safety or physical or mental health of an individual
- reveal personal data about another individual
- be contrary to the Singapore's national interest

Data Breach Notification

In the event of a data breach, that likely results in significant harm to individuals, or are of significant scale, PDPC and the affected individuals need to be notified

Significance in Breach Notification include:

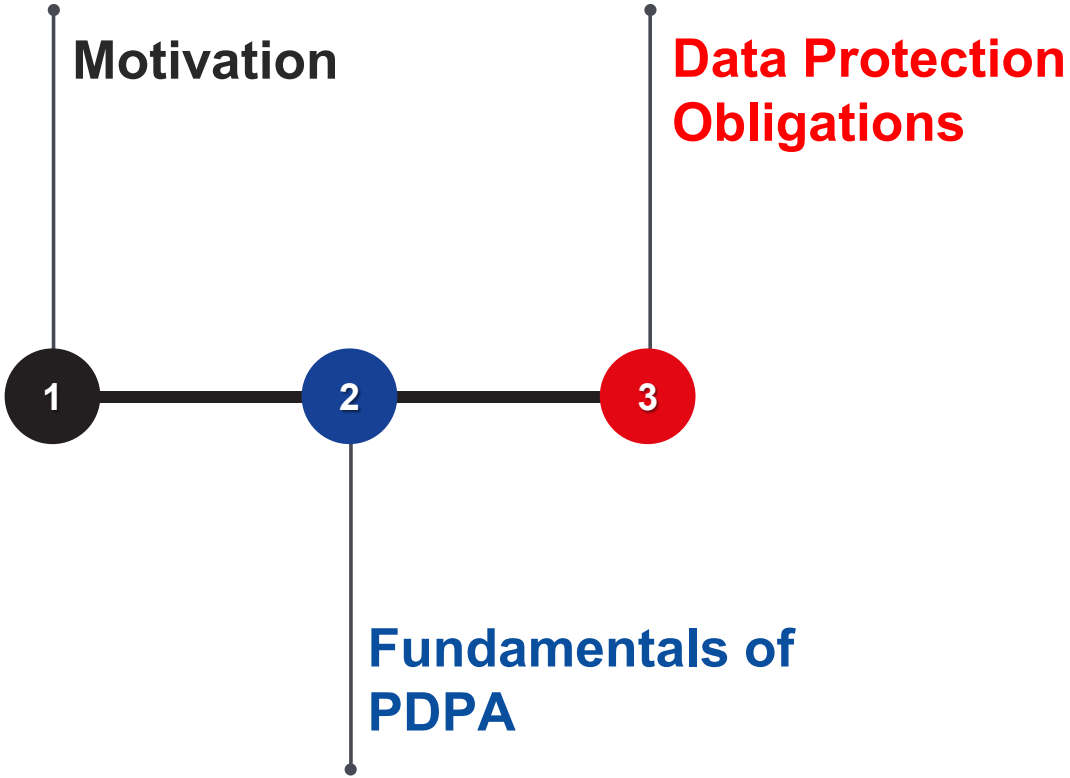
- Name or alias or full national identification number
- Financial/health information, not publicly disclosed
- Identification of vulnerable individuals
- Private key used to authenticate/sign an digital document

Data Portability*

At the request of the individual, organisations are required to transfer the individual's data to another environment

**As at March 2022, this Obligation is under review and will take effect when it is later issued*

Contents


Motivation
Data Protection Obligations
1
2
3
Fundamentals of PDPA