The Hong Kong Council of Social Service | 10 March 2021

Webinar on the Protection of Personal Data Privacy for NGOs

Mr Ivan CHAN
Head of Communications and Education

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

01

Introduction to the PD(P)O

02

Personal Information Collection Statement (PICS)

03

Privacy Policy Statement (PPS)

04

Privacy Management Programme

05

Data Ethics

06

QA session

1. Introduction to the PD(P)O

The Six Data Protection Principles (6 DPPs)

- forms the base of the PD(P)O
- data users must comply with the 6 DPPs in the collection, holding, accuracy, retention period, security, privacy policy and access to and correction of personal data

Principle 1 – Purpose and manner of collection

- shall be collected for purposes related to the functions or activities of the data user
- the means of collection must be lawful and fair
- the data collected should be adequate but not excessive

Principle 1 – Purpose and manner of collection

Inform the data subject of the following immediately or in advance:

a) the purposes of data collection;

b) the classes of persons to whom the data may be transferred;

c) whether it is obligatory or voluntary for the data subject to supply the data;

d) where it is obligatory for the data subject to supply the data, the consequences for him if he fails to supply the data; and

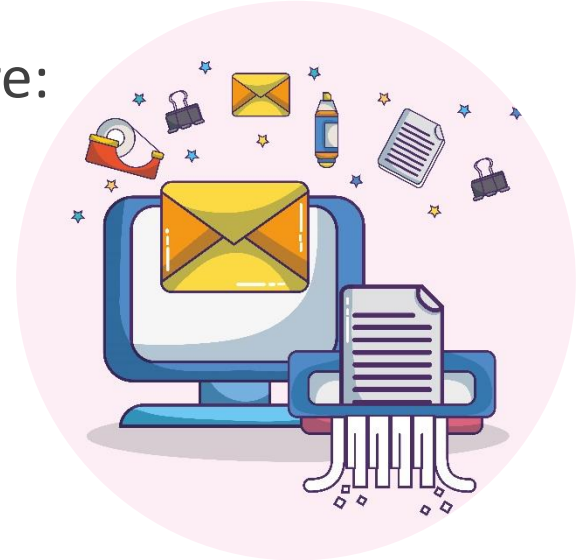
e) the name or job title and address to which access and correction requests of personal data may be made.

Personal Information Collection Statement

Principle 2 – Accuracy and duration of retention

Data users shall take practicable steps to ensure:

- the accuracy of personal data held by them
- personal data is not kept longer than is necessary for the fulfillment of the purpose



Data Retention

- erase personal data held by the data user where the data is no longer required for the purpose
- if a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data

Principle 3 – Use of personal data

- personal data shall not, without the prescribed consent of the data subject, be used for a new purpose

New purpose:

- *any purpose other than the purposes for which they were collected or directly related purposes*

- allow a "relevant person" to give prescribed consent for the data subject under specified conditions

Principle 4 – Security of personal data

- all practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing, erasure, loss and use

- security in the storage, processing and transmission of data

- if a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

Principle 5 – Information to be generally available

Transparency

Data users have to provide: -

(a) policies and practices in relation to personal data;

(b) the kind of personal data held;

(c) the main purposes for which personal data are used

Principle 6 – Access to personal data

Rights of data subjects

A data subject shall be entitled to：

i. request access to his/her personal data；data user may charge a fee for complying with the data access request

ii. request correction of his/her personal data

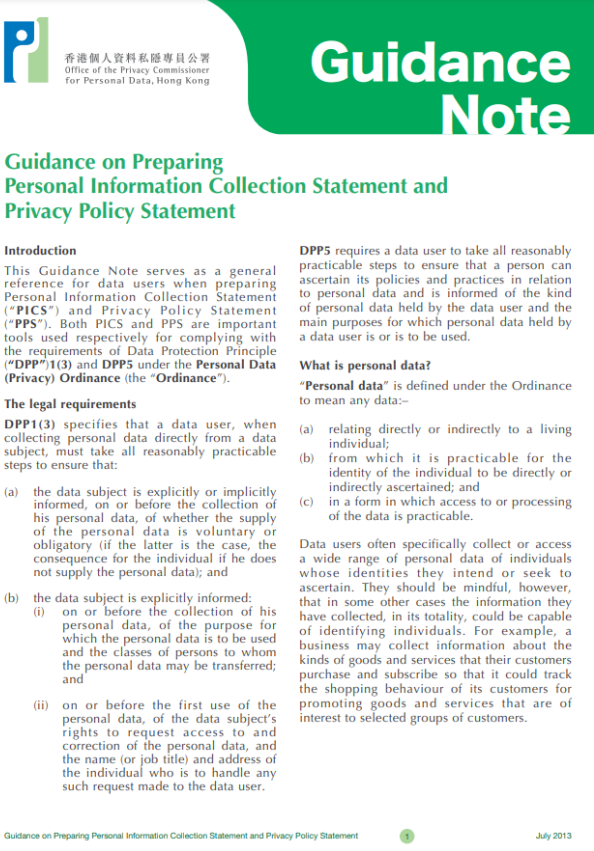
❖ If the data user holds the relevant personal data, it should supply a copy of the requested data within 40 calendar days after receiving the DAR

2. Personal Information Collection Statement (PICS)

What is a Personal Information Collection Statement (PICS)?

- a statement given in compliance with the requirements of the DPP1(3)
- should be given to a data subject on or before collecting personal data directly from that data subjects
- to notify individuals of certain matters when collecting such information from them - a statement of a certain limited content given in relation to specific collections of recorded information from individuals about themselves

❖ **Advice:** to provide written PICS



香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Guidance Note

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement

Introduction

This Guidance Note serves as a general reference for data users when preparing Personal Information Collection Statement ("**PICS**") and Privacy Policy Statement ("**PPS**"). Both PICS and PPS are important tools used respectively for complying with the requirements of Data Protection Principle ("**DPP**")**1(3)** and **DPP5** under the **Personal Data (Privacy) Ordinance** (the "**Ordinance**").

The legal requirements

DPP1(3) specifies that a data user, when collecting personal data directly from a data subject, must take all reasonably practicable steps to ensure that:

(a) the data subject is explicitly or implicitly informed, on or before the collection of his personal data, of whether the supply of the personal data is voluntary or obligatory (if the latter is the case, the consequence for the individual if he does not supply the personal data); and

(b) the data subject is explicitly informed:
(i) on or before the collection of his personal data, of the purpose for which the personal data is to be used and the classes of persons to whom the personal data may be transferred; and

(ii) on or before the first use of the personal data, of the data subject's rights to request access to and correction of the personal data, and the name (or job title) and address of the individual who is to handle any such request made to the data user.

DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can ascertain its policies and practices in relation to personal data and is informed of the kind of personal data held by the data user and the main purposes for which personal data held by a data user is or is to be used.

What is personal data?

"**Personal data**" is defined under the Ordinance to mean any data:–

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable.

Data users often specifically collect or access a wide range of personal data of individuals whose identities they intend or seek to ascertain. They should be mindful, however, that in some other cases the information they have collected, in its totality, could be capable of identifying individuals. For example, a business may collect information about the kinds of goods and services that their customers purchase and subscribe so that it could track the shopping behaviour of its customers for promoting goods and services that are of interest to selected groups of customers.

Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement 1 July 2013

What goes into a PICS?

1. Statement of purpose;
2. Statement as to whether it is obligatory or voluntary for the individual to supply his personal data;
3. Statement of possible transferees;
4. Statement of rights of access and correction;
5. Notice of contact person for requesting access or correction

1. Statement of Purpose

- a statement of the purposes for which personal data will be used following collection

Advice:

❖ *should not be too vague and too wide in scope*

For Job Application

Personal Information Collection Statement (Sample)

Company ABC
Personal Information Collection Statement

The personal data collected in this job application form will be used by us to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

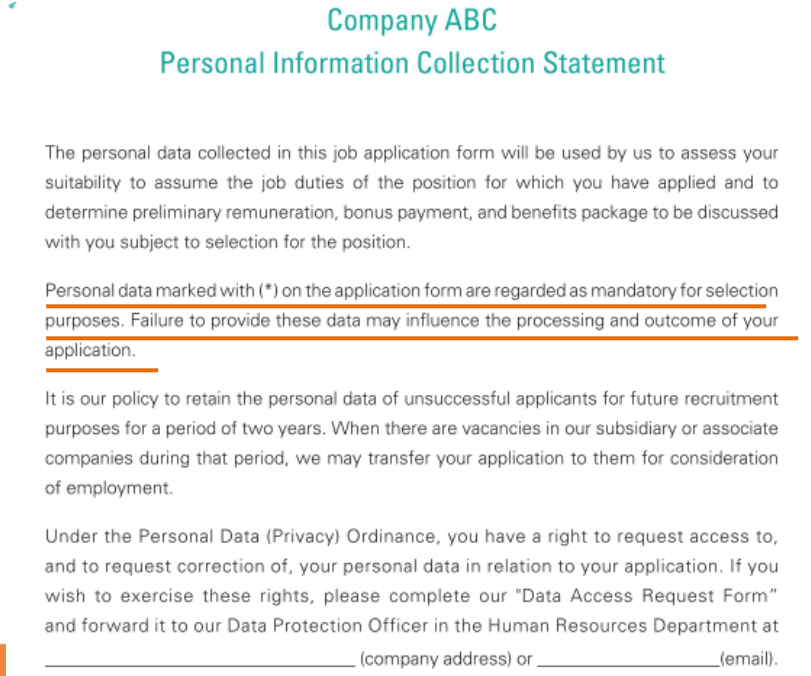
Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Data Access Request Form" and forward it to our Data Protection Officer in the Human Resources Department at _____ (company address) or _____(email).

2. Statement as to whether it is obligatory or voluntary for the individual to supply his personal data

- inform the individual whether it is obligatory or voluntary for him/her to supply personal data
- inform him/her of the consequences of failure to supply his personal data



Company ABC

Personal Information Collection Statement

The personal data collected in this job application form will be used by us to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Data Access Request Form" and forward it to our Data Protection Officer in the Human Resources Department at _____ (company address) or _____(email).

3. Statement of possible transferees

- declare the classes of persons to whom personal data collected from the data subjects may be transferred or disclosed

Advice:

❖ *avoid using broad and general terms*

For Job Application

Personal Information Collection Statement (Sample)

Company ABC
Personal Information Collection Statement

The personal data collected in this job application form will be used by us to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Data Access Request Form" and forward it to our Data Protection Officer in the Human Resources Department at _____ (company address) or _____(email).

3. Statement of possible transferees

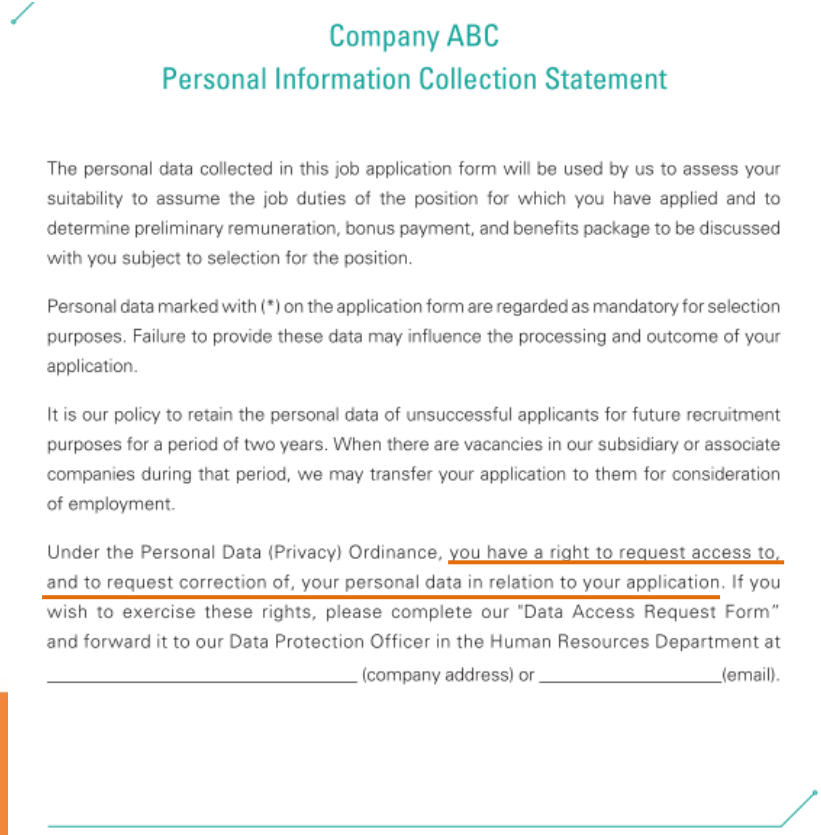
Examples of ill-defined data transferees:

Example 1:
...any other persons under a duty of confidentiality to our company…

Example 2:
…any company within our Group, our respective subsidiaries and any company in which the same has an interest…

4. Statement of rights of access and correction

- to inform the data subject that he/she has the right to request access to and correction of his/her personal data that is held by the data user



Company ABC

Personal Information Collection Statement

The personal data collected in this job application form will be used by us to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

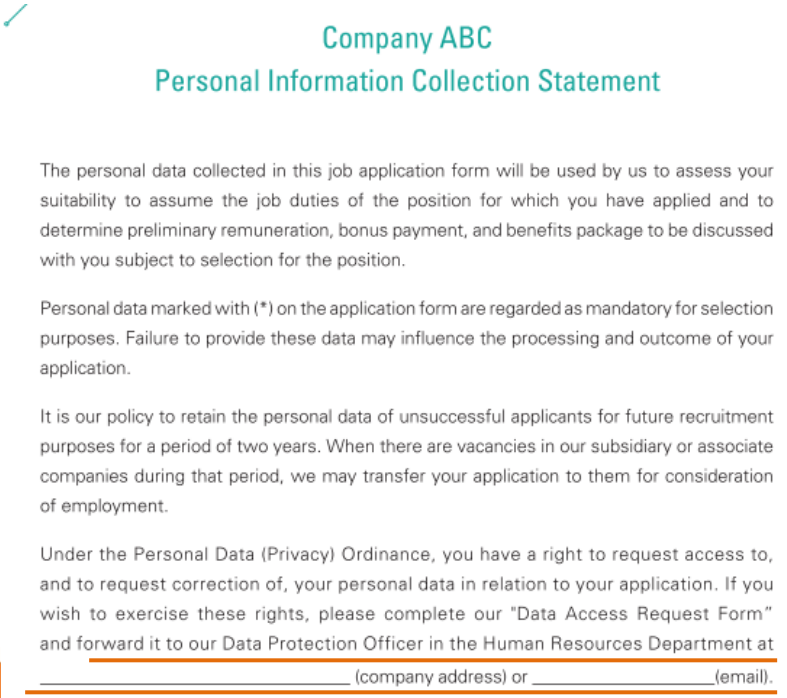
Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Data Access Request Form" and forward it to our Data Protection Officer in the Human Resources Department at _____ (company address) or _____(email).

5. Notice of contact person for requesting access or correction

- to provide the name (or job title) and contact details of the individual who is responsible for handling any data access and data correction requests



Company ABC

Personal Information Collection Statement

The personal data collected in this job application form will be used by us to assess your suitability to assume the job duties of the position for which you have applied and to determine preliminary remuneration, bonus payment, and benefits package to be discussed with you subject to selection for the position.

Personal data marked with (*) on the application form are regarded as mandatory for selection purposes. Failure to provide these data may influence the processing and outcome of your application.

It is our policy to retain the personal data of unsuccessful applicants for future recruitment purposes for a period of two years. When there are vacancies in our subsidiary or associate companies during that period, we may transfer your application to them for consideration of employment.

Under the Personal Data (Privacy) Ordinance, you have a right to request access to, and to request correction of, your personal data in relation to your application. If you wish to exercise these rights, please complete our "Data Access Request Form" and forward it to our Data Protection Officer in the Human Resources Department at _____ (company address) or _____(email).

Preparation of Personal Information Collection Statement

Practical Tips

Design the layout of PICS (including font size, spacing and use of appropriate highlights) in an easily readable manner

Present PICS in a conspicuous manner, e.g. in a stand-alone notice or section

Use reader friendly language, e.g. simple words

Provide further assistance to customers such as help desk or enquiry service

Link to Privacy Policy Statement

3. Privacy Policy Statement (PPS)

What is a PPS?

- a statement given in compliance with the requirements of the DPP5
- should be made available to anyone at ALL TIMES, in an easily accessible manner
- wider scope which may includes data retention policy, data security measures, data breach handling and use of special tools
- includes Statement of policy and Statement of practices

What goes into a PPS?

Statement of policy

- To Express a data user's overall commitment in protecting the privacy interests of the individuals who provide information about themselves to the data user

Example:
"We are committed to protecting the privacy, confidentiality and security of the personal information we hold by complying with the requirements of the PD(P)O with respect to the management of personal information. We are equally committed to ensuring that all our employees and agents uphold these obligations."

What goes into a PPS?

Statement of practices

- To include the kind of personal data held by the data user and the purposes for which it uses the data

Example 1:
"We will not provide your personal data to third parties for direct marketing or other unrelated purposes without your consent."

Example 2:
"Your personal details, job particulars, salary and benefits, appraisal and disciplinary records collected and held by us will be used for the purpose of human resource management."

Recommended good practices – content of PPS

- Not advised to collect personal data from minors (particularly those who are incapable of making an informed decision) without prior consent from a person with parental responsibility for the individual
- Give information about retention of personal data
- Explain how to use, process, handle and transfer sensitive personal data
- Disclosure or sharing of personal data should be stated
- State protection measures to ensure the security and confidentiality of the personal data collected

Recommended good practices – content of PPS

State clearly what personal data will be transferred to such third parties and how such third-parties will ensure protection of the personal data collected

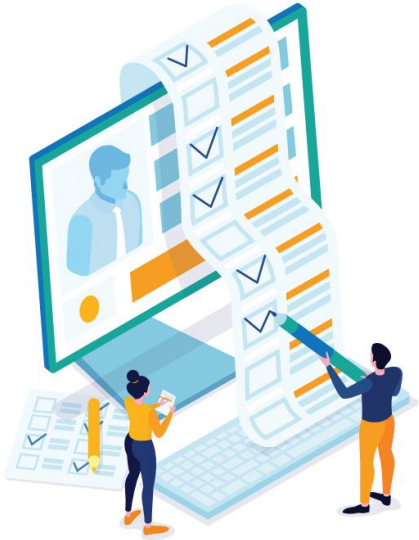
Make it known through a PPS if no personal data is collected

State the policy on handling data subject's requests to access and to correct their personal data

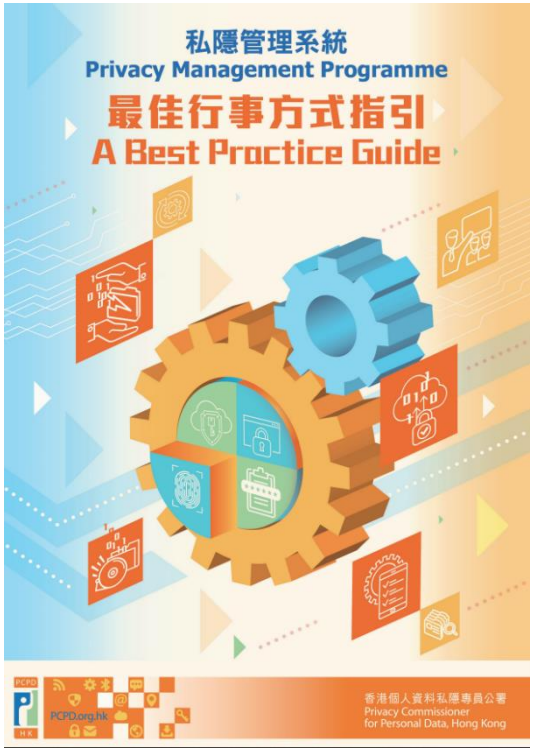
Provide contact details for enquiries

Recommended good practices – format of PPS

- User-friendly language and presentation
- Layered presentation

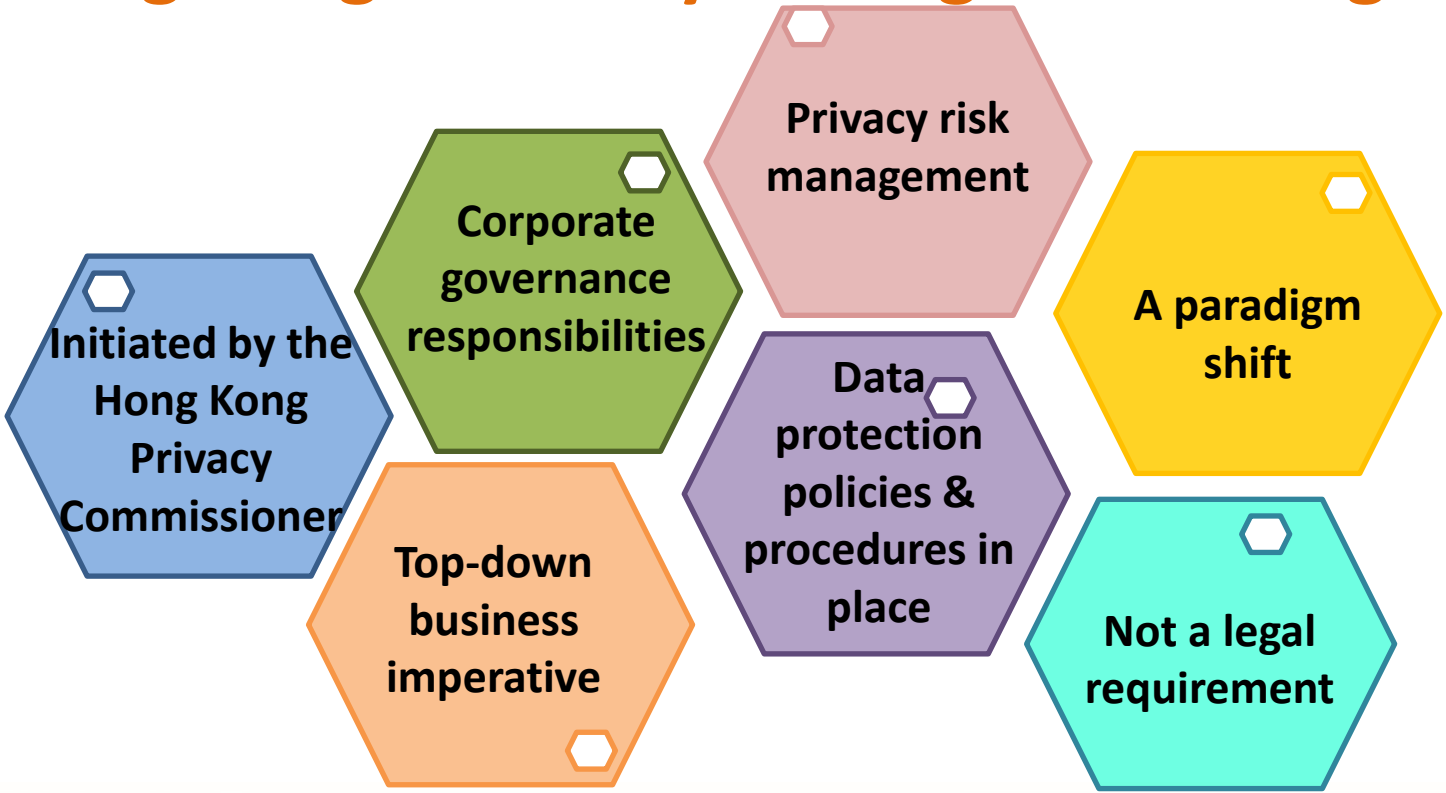


4. Privacy Management Programme



www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf

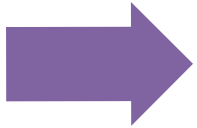
Hong Kong – Privacy Management Programme



Paradigm Shift

Compliance Approach

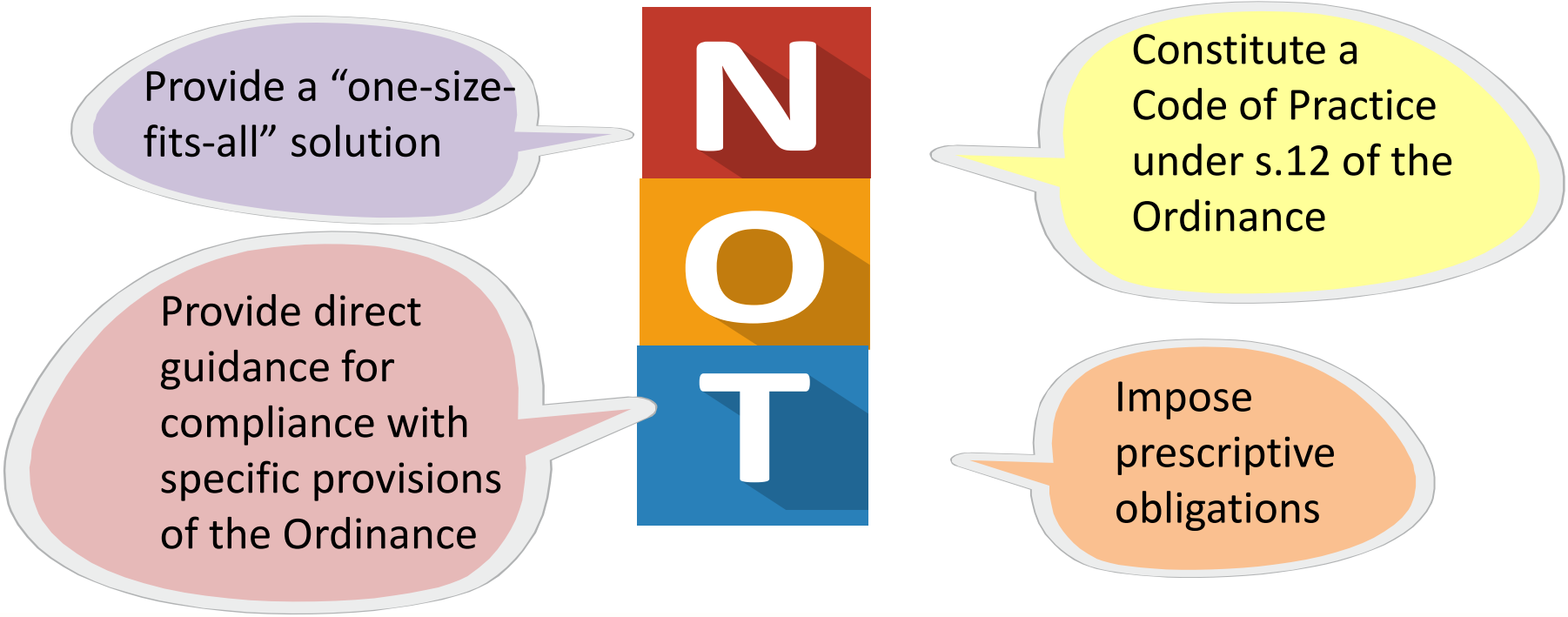
- Passive
- Passive
- Remedial
- Problem-based
- Handled by compliance team
- Minimum legal requirement
- Bottom-up



Accountability Approach

- Active
- Proactive
- Preventive
- Based on customer expectation
- Directed by top-management
- Reputation building
- Top-down

The Best Practice Guide does not…



Benefits of implementing a PMP

You understand how privacy and data protection fit in to your overall business strategy

There is a clear understanding of what data is held, where is it and who has access to it

You know how well you are protecting the data, and where you are not

The risks introduced to the data by third parties are well understood and managed

The data is being used for the purpose that you have committed to, and nothing more

Minimise the risks of data breaches

Major Components of a PMP

1. Organisational Commitment:

1.1 Buy-in from the Top

- Top management should:
  - endorse the PMP
  - appoint Data Protection Officer(s) ("**DPO**")
  - allocate sufficient budget and manpower for implementation
  - actively engage in the review and assessment process

1. Organisational Commitment:

1.2 Data Protection Officer/Office

Role

- Establish and implement programme controls
- Coordinate with other appropriate persons responsible for related disciplines and functions within the organisation
- Be responsible for the ongoing assessment and revision of programme controls
- Represent the organisation in the event of an enquiry, an inspection or an investigation by the Commissioner
- Advocate personal data protection within the organisation itself

1. Organisational Commitment:

1.2 Data Protection Officer/Office

- Be a senior staff member
- May or may not be a full-time job
- May be supported by dedicated staff (Data Protection Office)
- (for larger organisations) Ideal to have a data protection coordinator in each major department to assist the DPO in the implementation of the PMP
- Large organisation VS. small organisation

1. Organisational Commitment:

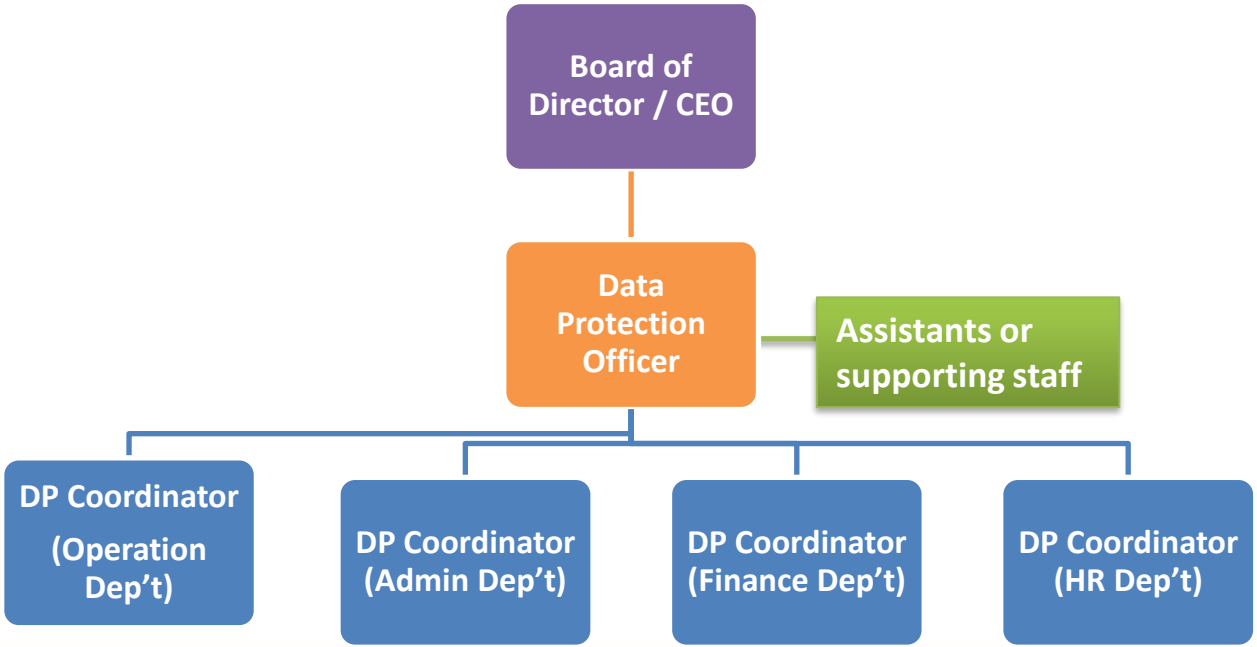
1.3 Reporting

- Clear line of reporting effectively reaches top management

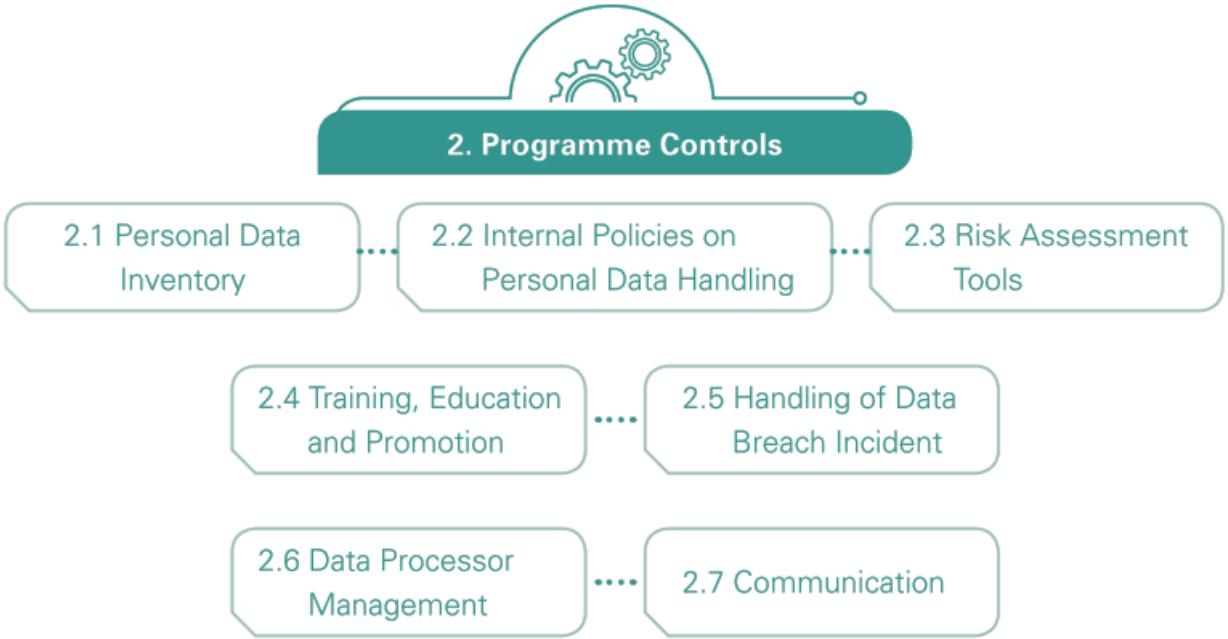
  (e.g.: Board of Directors)
- Assurance programme must be in place so that the day-to-day effectiveness and compliance issues can be reported
- Effectiveness and compliance of the PMP is communicated to top management regularly

1. Organisational Commitment:

1.3 Reporting



Major Components of a PMP



2. Programme Controls:

2.1 Personal Data Inventory

An organisation should

- be clear about:
  - what kinds of personal data it holds
  - where the personal data is stored
  - why the personal data is collected
  - what are the limitations on the use of the personal data (e.g.: direct marketing)
  - what is the retention period
- and properly document the above

2. Programme Controls:

2.2 Policies

- Develop and document internal policies that address obligations under the PD(P)O:
  - Policy for handling of customers' personal data
  - Human resources management policy (include employee monitoring)
  - Policy for outsourcing
  - IT and data security policy
  - CCTV policy
  - Policy for handling data access request from law enforcements, etc.
- Training or briefing to relevant employees
- Update and re-circulate the policies regularly

2. Programme Controls:

2.3 Risk Assessment Tools

- Periodic Risk Assessment
- Privacy Impact Assessment (“PIA”)

2. Programme Controls:

2.4 Training and Education

- Tailored to specific needs of relevant employees (i.e. those handling personal data)
- Be given to new employees in its induction programme and periodically thereafter
- Cover organisation's policies and procedures
- Be delivered in an appropriate and effective manner
- Circulate essential information to relevant employees as soon as practical if an urgent need arises
- Monitor and keep records for attendance

2. Programme Controls:

2.5 Breach Handling

- Breach handling and notification procedure in place

- Set out procedures and designate officer(s) to manage data breaches

2. Programme Controls:

2.6 Data Processor Management

- Data processor is a person who:
  (a) processes personal data on behalf of another person; and
  (b) does not process the data for any of the person's own purposes
- Must adopt contractual or any other means to prevent:
  - personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP2(3))
  - unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2))
- A data users is liable to the act and practice of its data processor (S.65(2))

2. Programme Controls:

2.7 Communication

Communication should be:

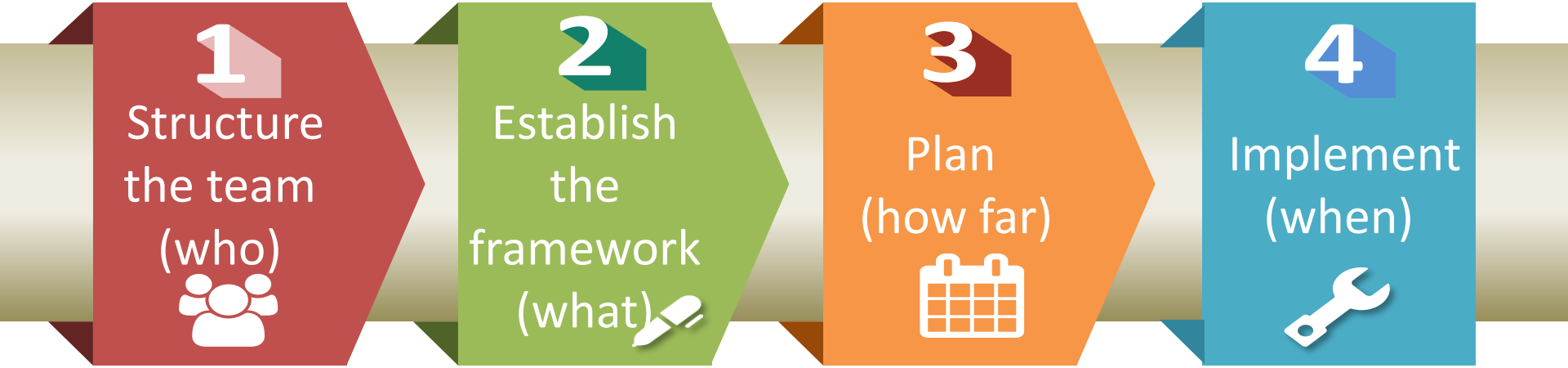
- readily available to clients, employees and other stakeholders
- clear, comprehensive, concise and easily understandable
- not simply reiteration of the PD(P)O

Information to be covered:

- purpose of collection
- potential transferees
- retention period
- data security measures
- data subjects' right to access and correction of data
- contact person for privacy-related issues

Major Components of a PMP

Key Steps


1
Structure the team (who)
2
Establish the framework (what)
3
Plan (how far)
4
Implement (when)

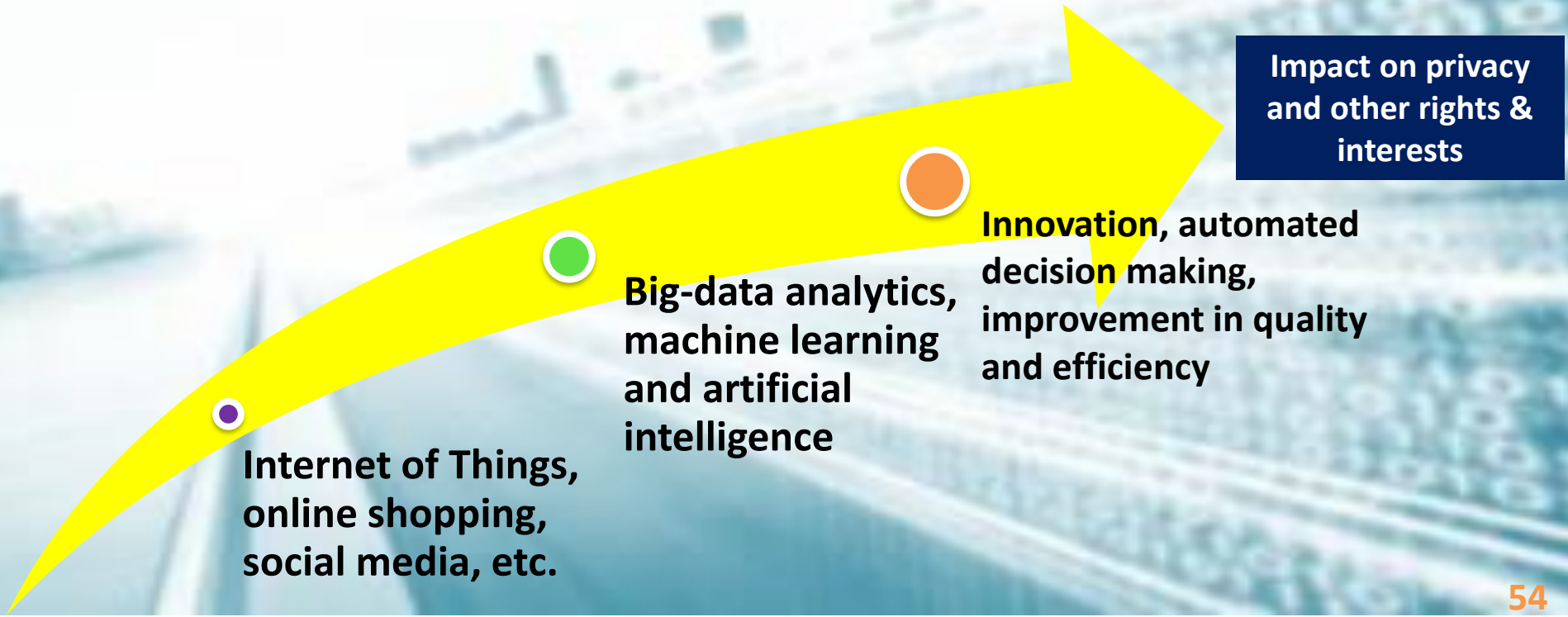
"Trust is the new gold."

Andrea Jelinek,
Chair of European Data Protection Board

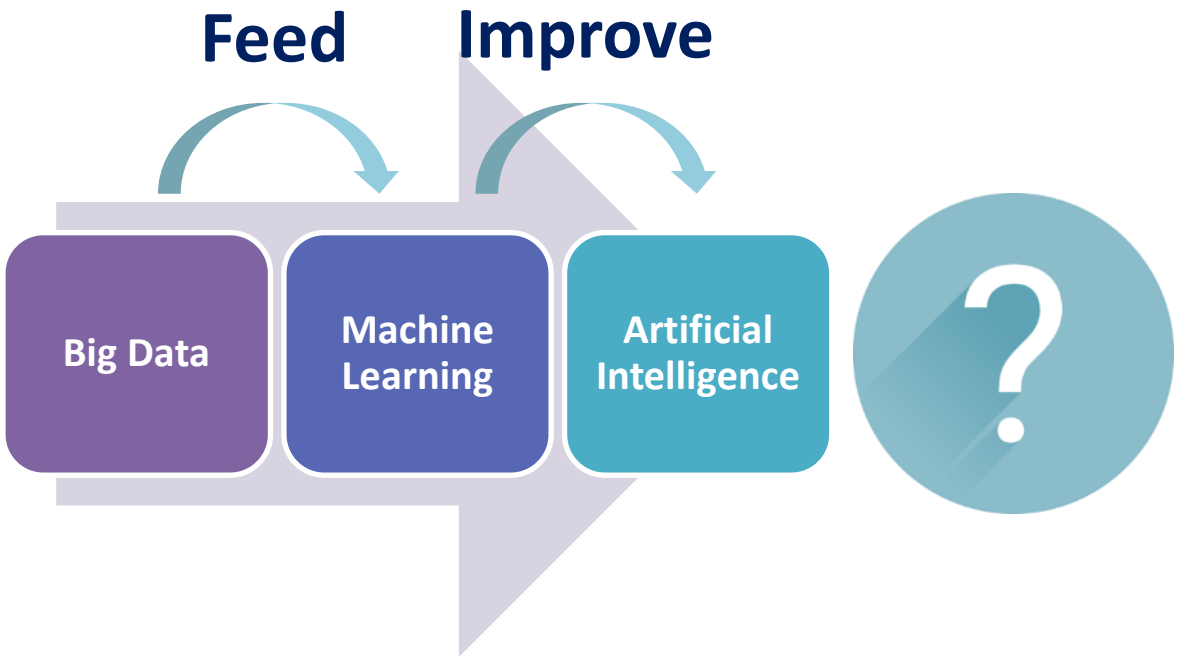
4. Data Ethics

Why Data Ethics?

Data is the lifeblood of the data-driven economy



Risks of AI & Big Data



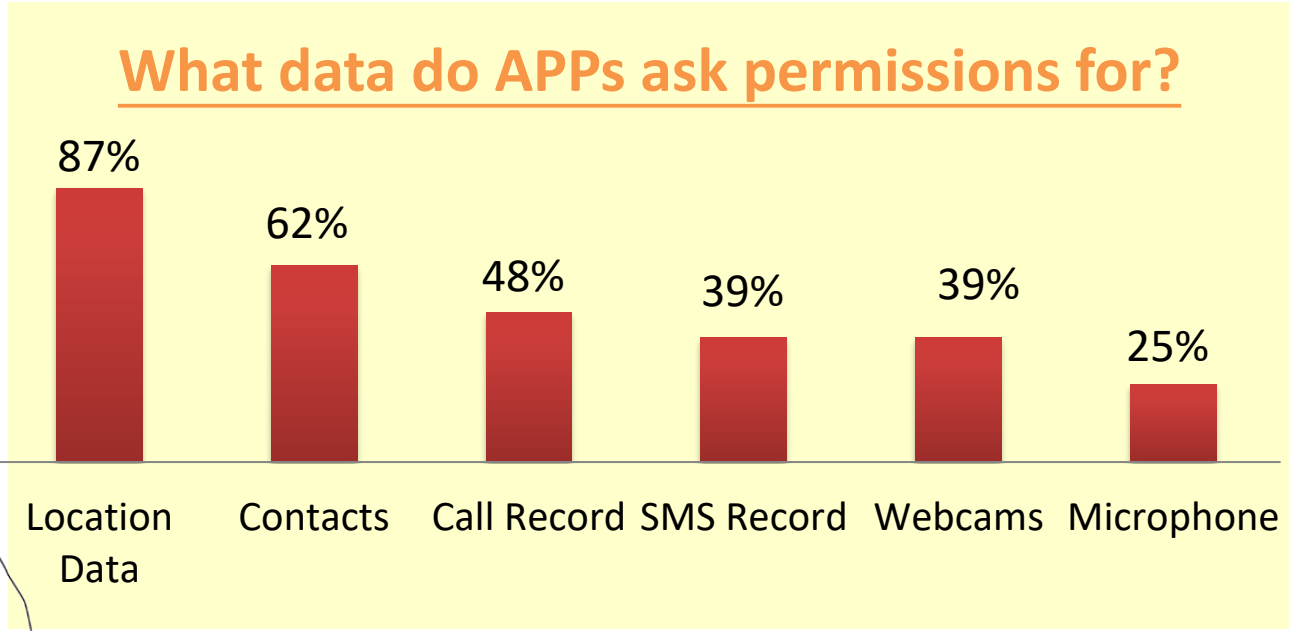
- Excessive collection
- Lack of transparency
- Unpredictable use
- Bias & discrimination resulting from inaccurate predictions
- Re-identification
- Loss of control by individuals
- Manipulation of human behaviour

Conflicts of Big Data and AI with Privacy Principles

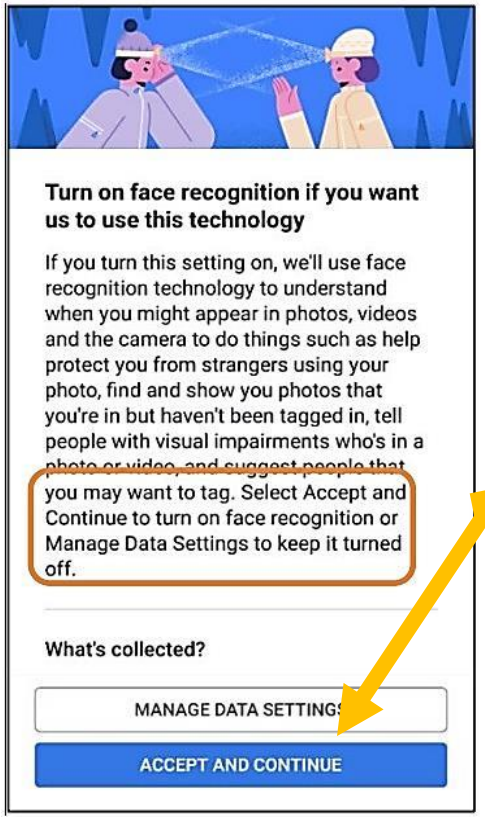
**** May impact fundamental human rights beyond privacy intrusions (e.g. freedom of speech, free election)***

Excessive collection of personal data by Apps

- 67.2% respondents think smartphone APPs collect unnecessary personal information



Source: China Consumers' Association 'Report on Personal Data Leakage from APPs' (August 2018)



Apps used **"dark patterns"** to discourage users from exercising their privacy rights:

- Making the least privacy-friendly settings as the default settings
- Making the alternative privacy settings difficult to navigate
- Using eye-catching buttons for less privacy-friendly options
- Emphasize the positive aspects of less privacy-friendly options, glossing over potential privacy risks
- Falsely claiming that not accepting the default option would affect the functionality

Source: Norwegian Consumer Council – "Deceived by Design" (June 2018)

Doxxing

What is doxxing?

- collecting personal data of the target person(s) or related person(s) (such as family members, relatives and friends)
- commonly by online search engines, social platforms and discussion forums, public registers, anonymous reports, etc., and publish on the Internet, social media or other public platforms (such as public places)

The provision related to doxing in the PD(P)O

- Doxxing acts may constitute contravention of the PD(P)O
  - Section 64 of the PD(P)O provides that a person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent to obtain gain, or causes psychological harm to the data subject

- Contravention of section 64 of PD(P)O bears serious consequences. On conviction, the maximum penalty is a fine of HK$1,000,000 and imprisonment for 5 years

Doxxing acts may be subject to civil liabilities

- Doxxing brings anxiety and psychological distress to the victims which puts heavy pressure, burden and even harm both emotionally and psychologically
- The reputation of the victims is also damaged. Victims can file a civil lawsuit to seek compensation from the doxxers

Doxxing acts may involve other offences

- Breaching injunction order may be charged of contempt of court and subject to **an immediate custodial sentence**

For example:

1. Injunction order (HCA 1957/2019) Doxxing and Harassment against Police Officers, Special Constables and their Families
2. Injunction order (HCA 2007/2019) Promotion, Encouragement and Incitement of the Use or Threat of Violence via Internet-based Platform or Medium
3. Injunction order (HCA 1847/2020) Doxxing and Harassment against Judicial Officers and their Families

→ *Depending on the circumstances of the case, doxxing acts may also involve criminal intimidation related to use of computer or forgery of documents*

Data Ethics & Trust

Data

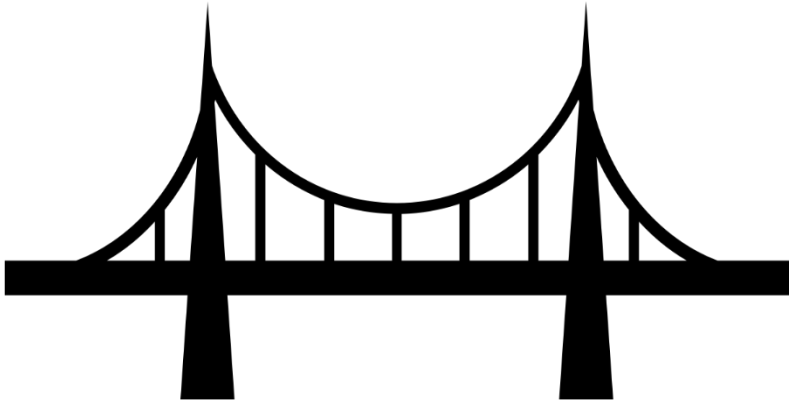
Consumers/ service receivers

Businesses/ organisations

Ethical Obligations

Accountability & ethics as a bridge between law and expectation

Accountability & Data Ethics



Legislation

Technology development

Public expectation

Vast amount of data collected & processed

Ethics, Laws, & Accountability

Extended obligation to ensure compliance with laws

Legal obligations, usually based on communal values

Communal values shared by the public in general, guiding our daily living

Ethics, Laws, & Accountability

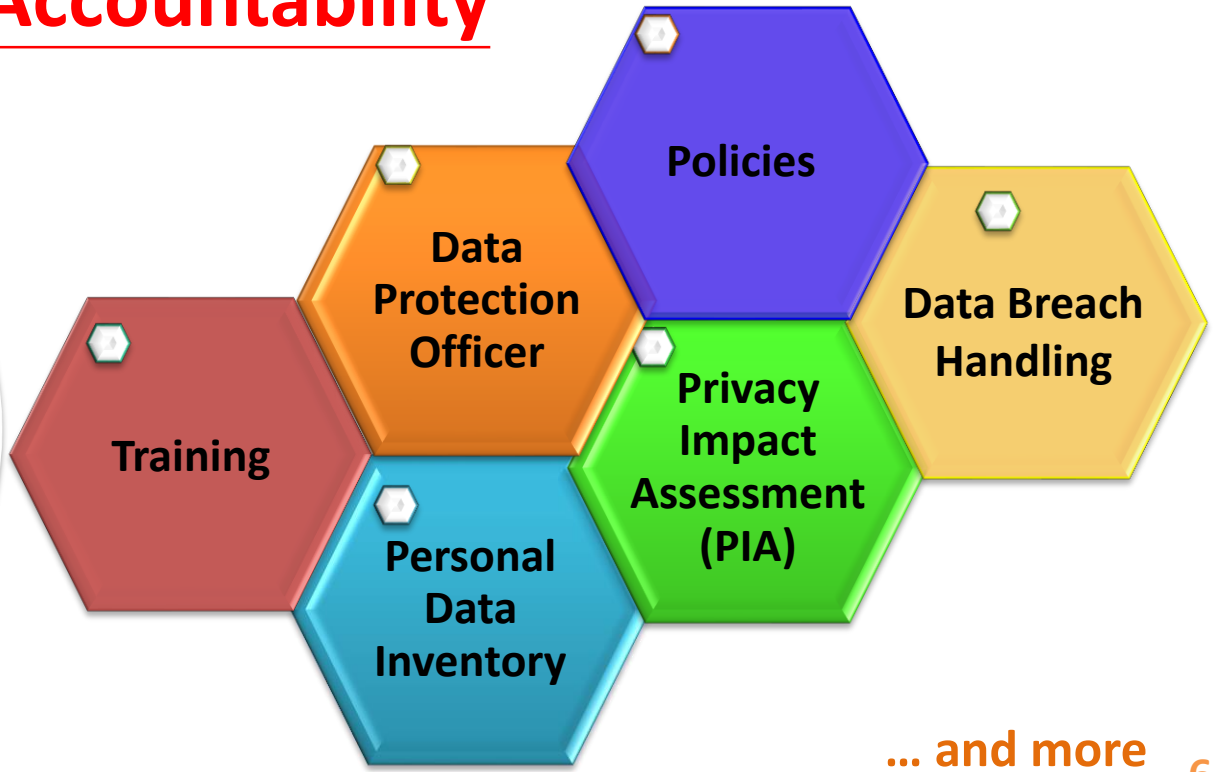
- **Meeting expectations of all stakeholders**
  (i.e. multi-stakeholder approach)
- **Conform with communal values shared by the public in general**
  (i.e. more than legal compliance)

Ethics, Laws, & Accountability

Comply with legal requirements
(e.g. PD(P)O, GDPR, etc.)

Ethics, Laws, & Accountability

Accountability
(Policies and measures to ensure compliance with laws)



… and more

Paradigm Shift

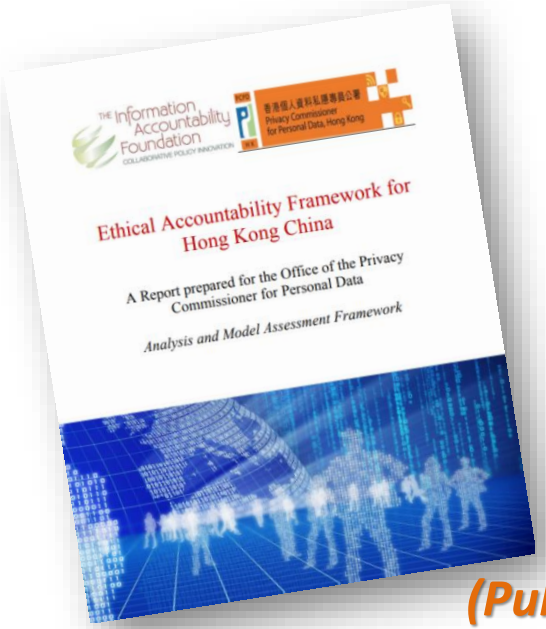
Fiduciary:

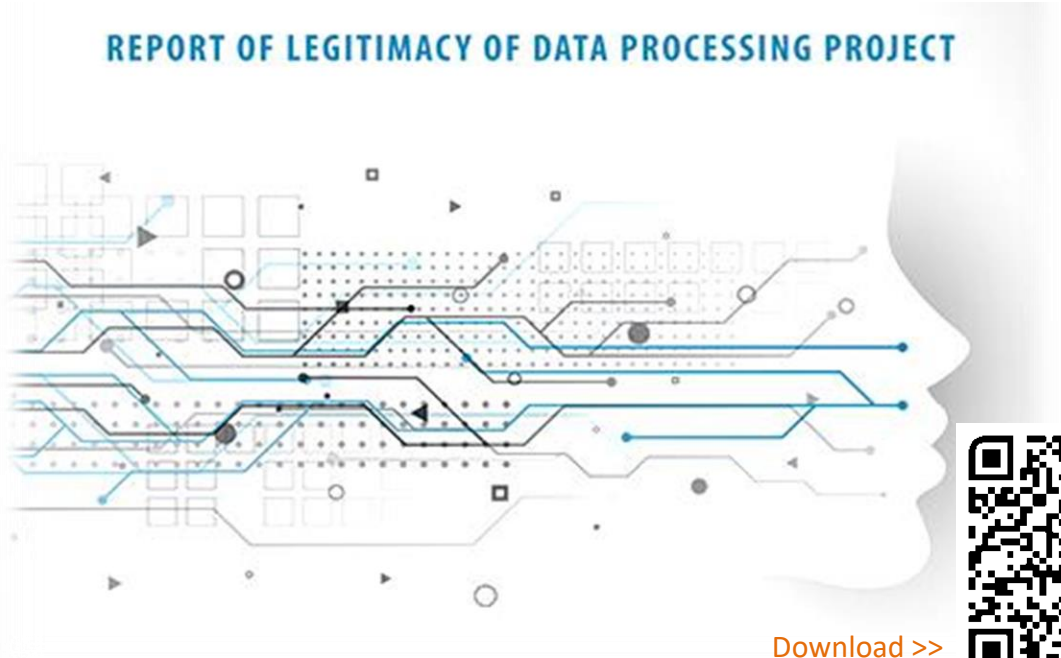
- Acting on behalf of another person
- Acting for the benefit of that other person
- Oweing to that other person the duties of good faith and trust

Ethics

“Ethical Accountability Framework for Hong Kong China”

REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT

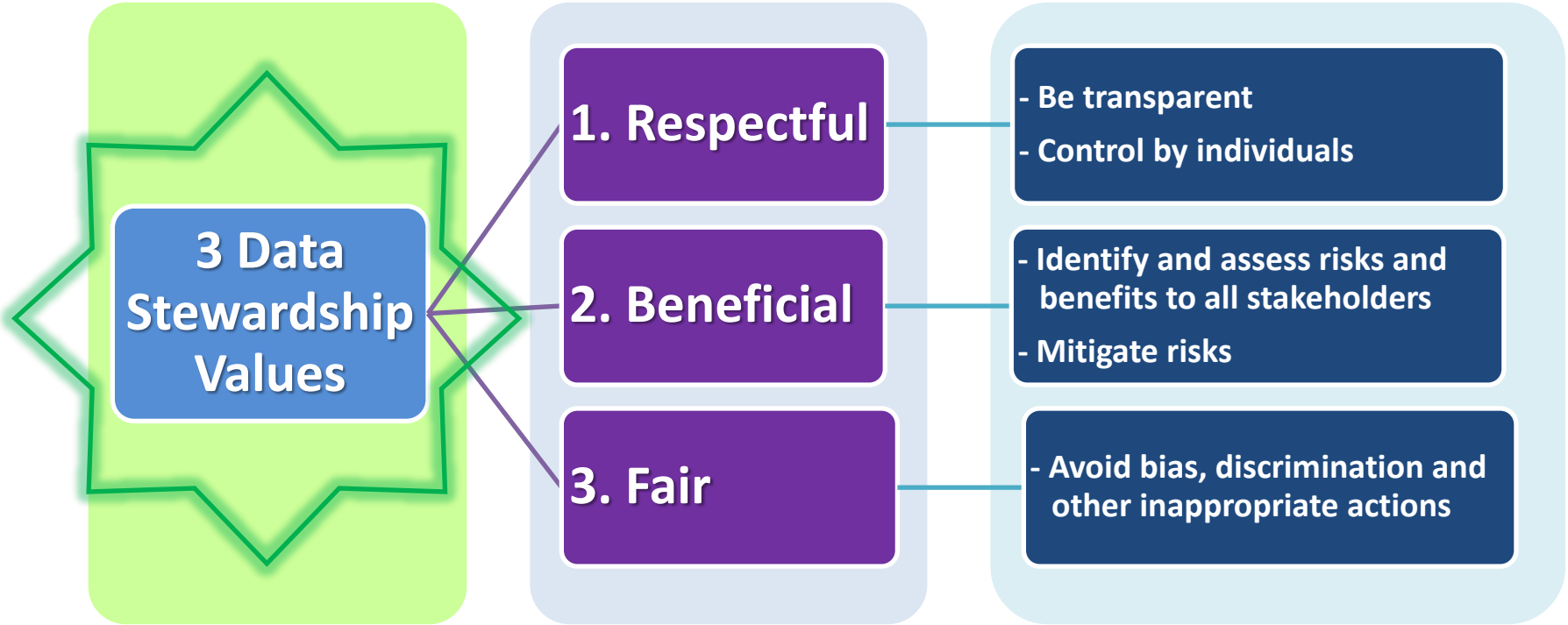




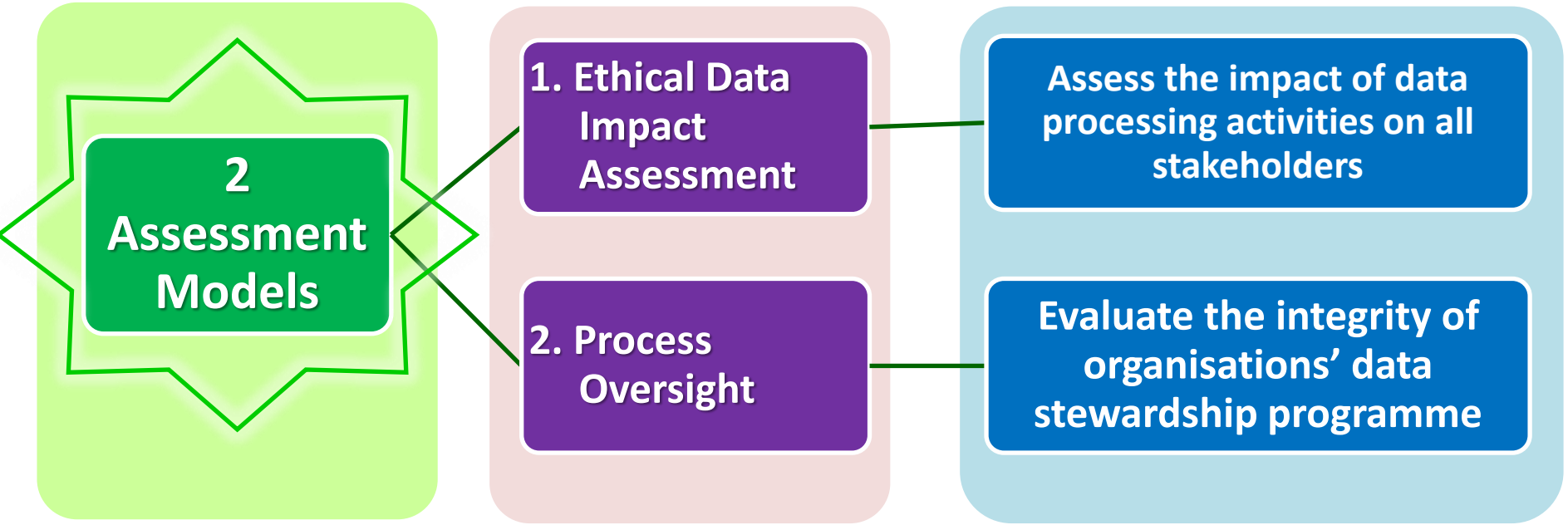
Download >>

(Published on 24 October 2018)

Multi-stakeholders' Approach – Three Core Values



Multi-stakeholders' Approach – Two Assessment Models

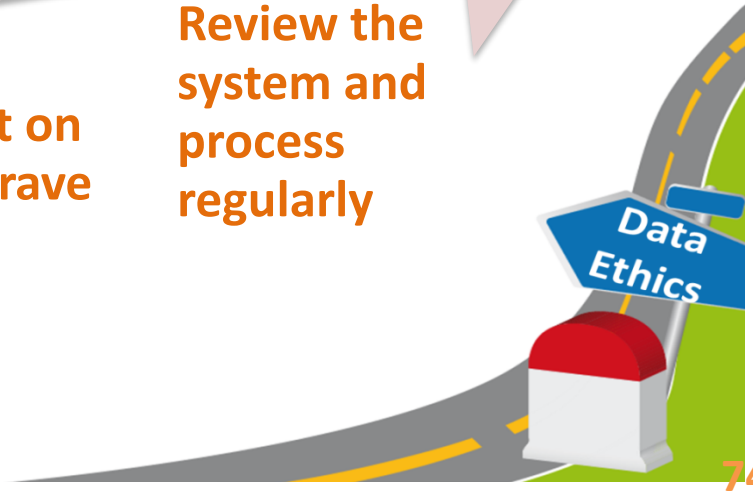


Data Ethics

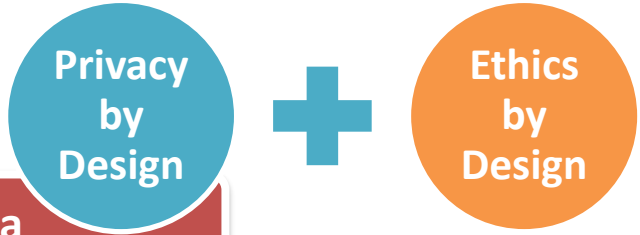
Think, plan and execute with multi-stakeholders' interests

Get data management on a cradle-to-grave basis in an institutional system and process

Review the system and process regularly



Data Ethics - Implementation



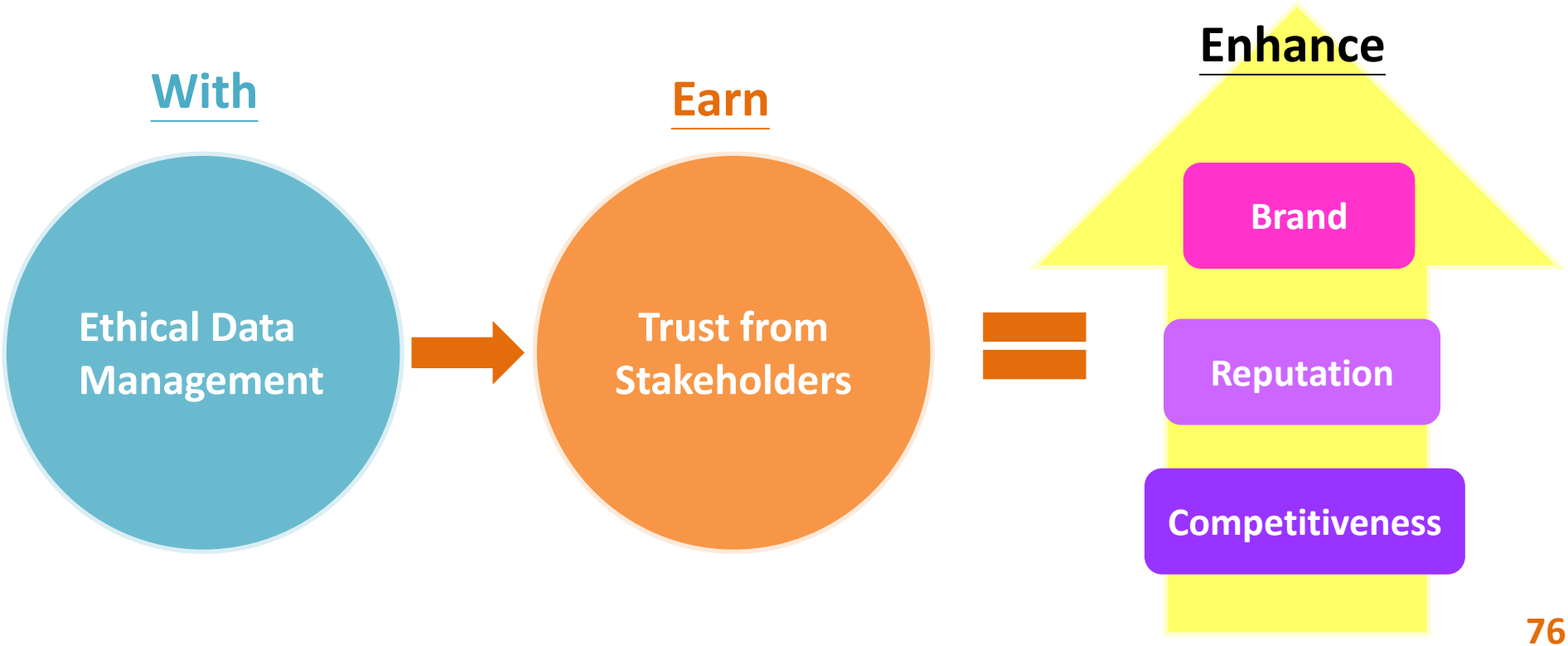
Step 1: Analyse the business objective and purpose of the data processing activity

Step 2: Assess the nature, source, accuracy and governance of the data

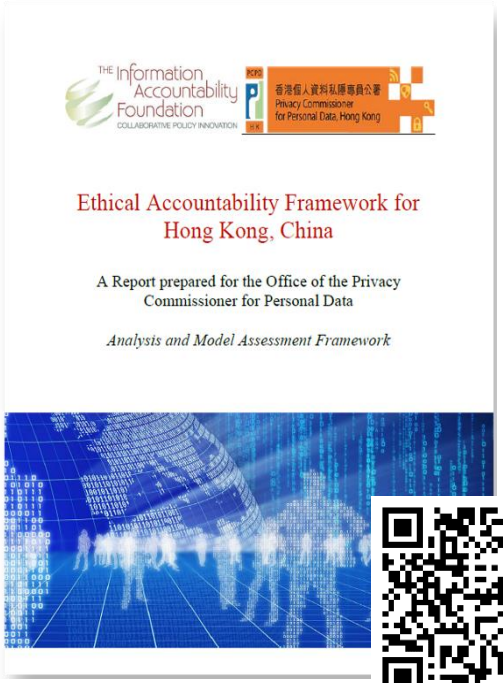
Step 3: Conduct impact assessment, i.e. risks and benefits to the individuals, the society and the organisation itself

Step 4: Balance between expected benefits and the mitigated risks to all stakeholders

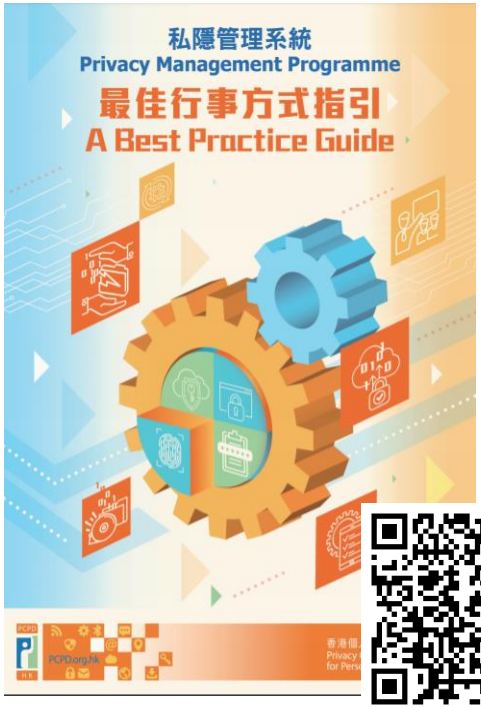
Benefits


With
Earn
Enhance
Ethical Data Management
Trust from Stakeholders
Brand
Reputation
Competitiveness

https://www.pcpd.org.hk//english/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf



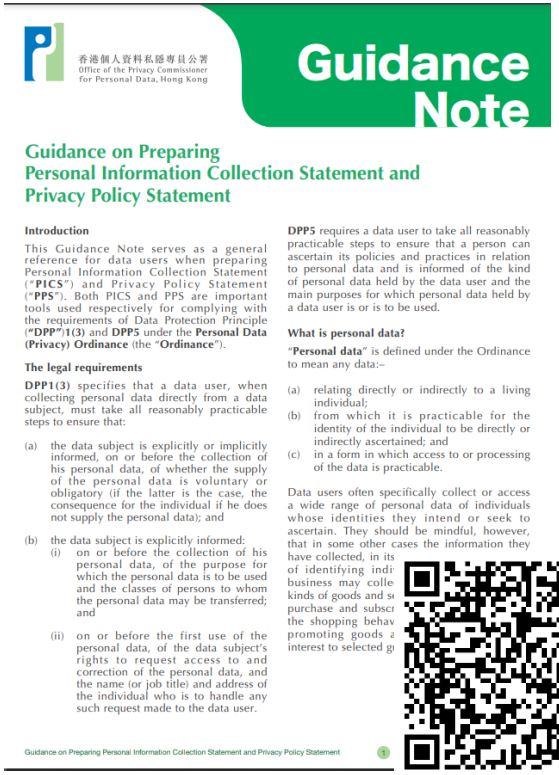
https://www.pcpd.org.hk/misc/files/EthicsReport_combined.pdf



https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf

https://www.pcpd.org.hk/tc_chi/resources_centre/publications/books/files/sme_toolkit.pdf

https://www.pcpd.org.hk/english/resources_centre/publications/files/dataethics_en.pdf



https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

JOIN

Data Protection Officers' Club

(Membership Application)

保障資料主任聯會
DATA PROTECTION OFFICERS' CLUB

By becoming a DPOC member, you will:

- **advance your knowledge and practice of data privacy compliance through experience sharing and training;**
- **enjoy 20% discount on the registration fee for PCPD's Professional Workshops;**
- **receive updates on the latest development in data privacy via regular e-newsletter**

As a DPOC member, your organisation's name will be published on DPOC membership list at PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK$350 per year

Enquiries: dpoc@pcpd.org.hk

https://www.pcpd.org.hk/misc/dpoc/files/AppForm_1920_NewMembers.pdf

Contact Us

- **Hotline** 2827 2827
- **Fax** 2877 7026
- **Website** www.pcpd.org.hk
- **E-mail** communications@pcpd.org.hk
- **Address** 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, HK

Q & A session


ngiyabonga
danke
謝謝
teşekkür ederim
спасибо
dank je
thank you
gracias
tapadh leat
mochchakkeram
hvala
mauruuru
bedankt
dziękuję
go raibh maith agat
obrigado
sagolun
sukriya
kop khun krap
arigatō
takk
dakujem
grazie
terima kasih
мерси
감사합니다
ευχαριστώ
merci