# ITRC Forum 2022

24 January 2022

## Data Protection in the Cloud

Vincent Ng

Acting Head of Compliance

Office of the Privacy Commissioner for Personal Data

# Growing Trend

- A growing trend for corporations to fully embrace cloud services in place of on-premises servers
- A no-cloud policy will be as rare as a no-internet policy

# Growing Trend

"***Cloud Computing*** *is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

*The National Institute of Standards and Technology (NIST) of the United States*

# Cloud in Privacy Policy

## HOW WE COLLECT AND STORE YOUR DATA

We may store your data locally or overseas, including in the cloud. We apply our global data standards and policies wherever your data is stored.

We're responsible for keeping your data safe in compliance with Hong Kong law.

# Cloud Service Provider (CSP)

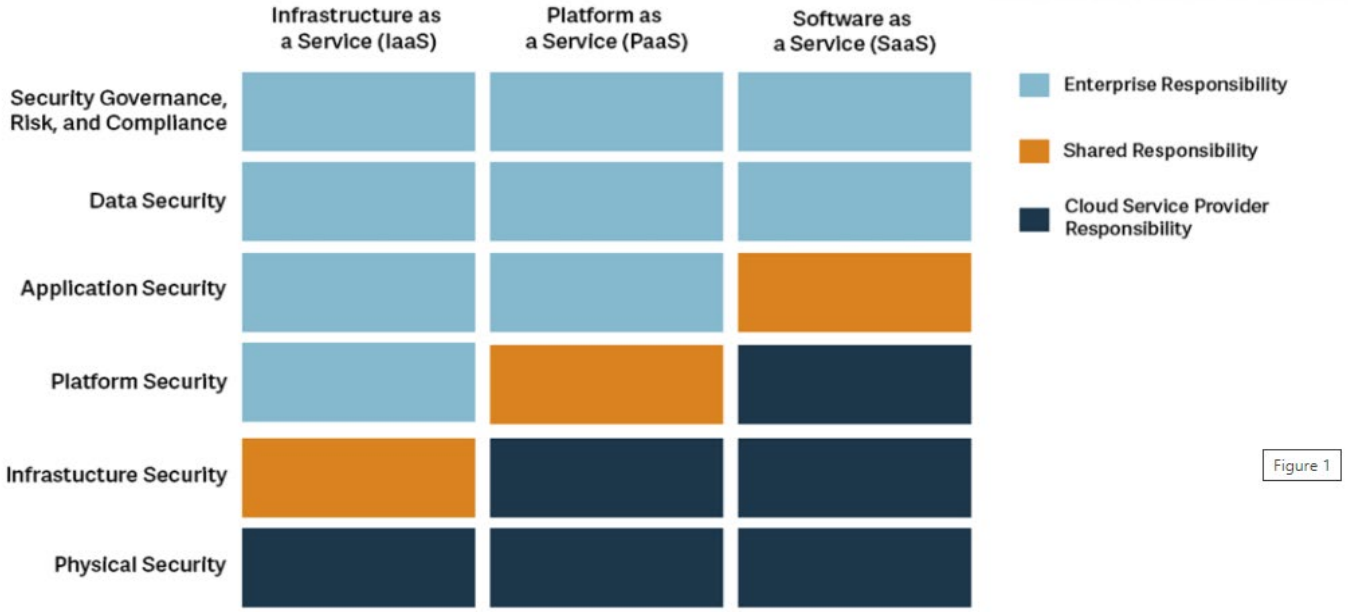



Fig. 1 Responsibility depending on type of cloud service from The Official (ISC)² Guide to the CCSP CBK, 2nd Edition.

Source: https://www.isc2.org/Articles/Responsibility-and-Accountability-in-the-Cloud

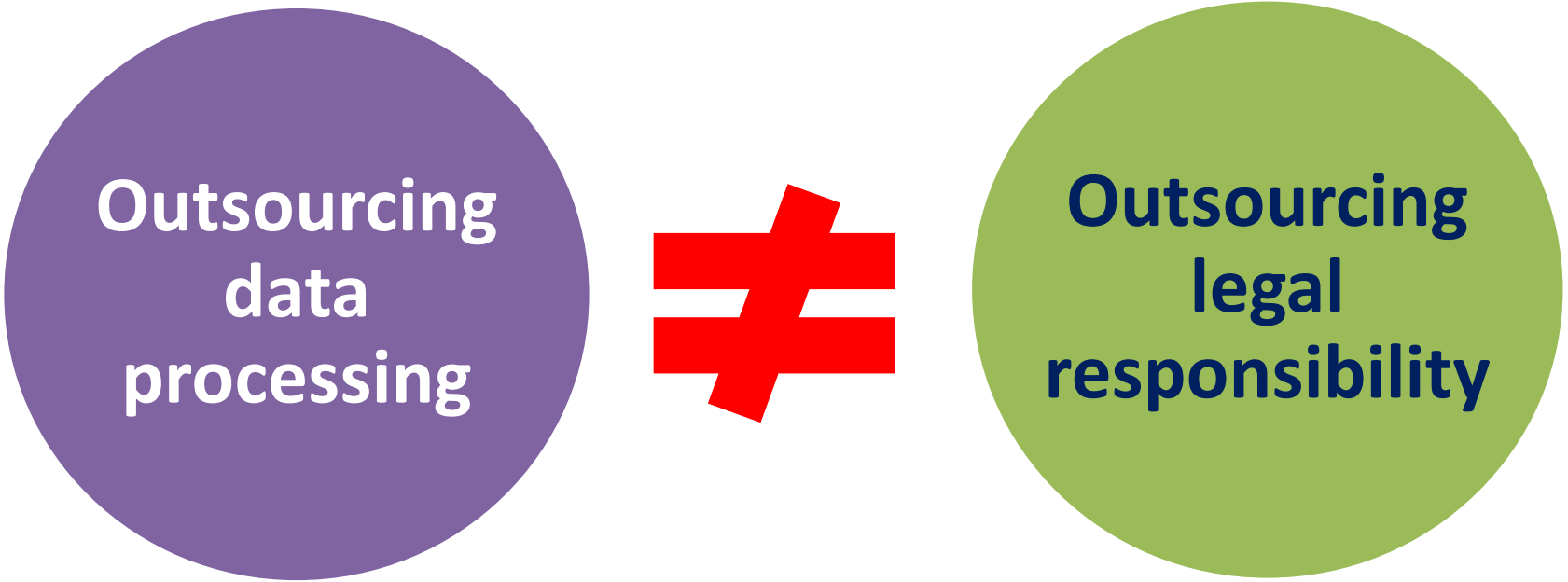
# Responsibility

Data User > Data Processor

Data Controller > Data Processor

個人信息處理者 > 受託人

# Responsibility



# Practical Tips (1)

A corporation should carefully evaluate the standard services and contract terms provided by the Cloud Service Provider to see if they meet the requirements of the PDPO and commonly accepted data security standards, and ask for ‘customised’ contract terms if necessary

# Practical Tips (2)

A corporation should require the Cloud Service Provider to notify it of data breaches so that speedy remedial action may be taken

# Practical Tips (3)

A corporation should obtain formal, contractual assurance from the Cloud Service Provider that the same level of protection and compliance controls are equally applicable to their sub-contractors

# Practical Tips (4)

A corporation should scrutinise the audit reports on data security and privacy compliance of the Cloud Service Provider, if it is not possible to audit the operation of the Cloud Service Provider

Information security management systems requirements (ISO/IEC 27001:2013)

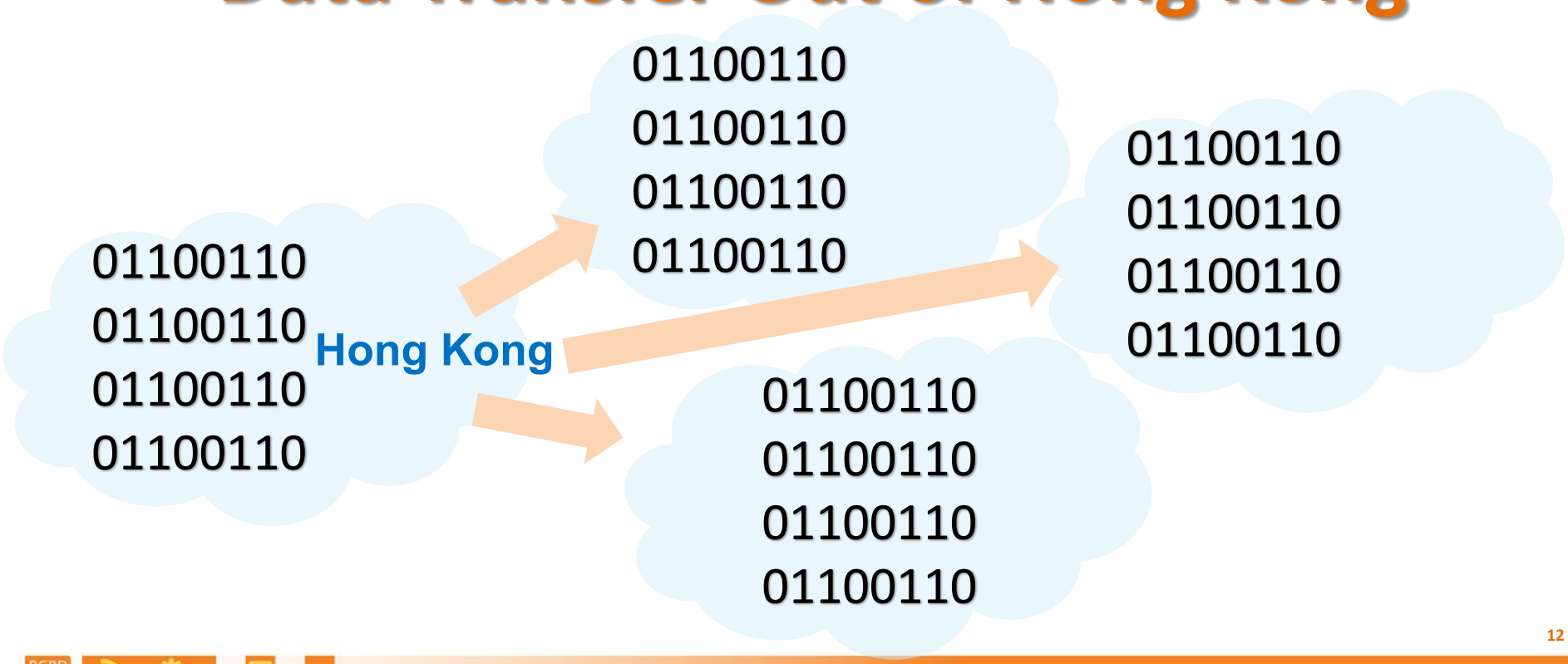
Code of practice for information security controls for cloud services (ISO/IEC 27017:2015)

Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2019)

# Practical Tips (5)

A corporation should implement encryption for personal data in transit to and from cloud and in cloud storage

# Data Transfer Out of Hong Kong

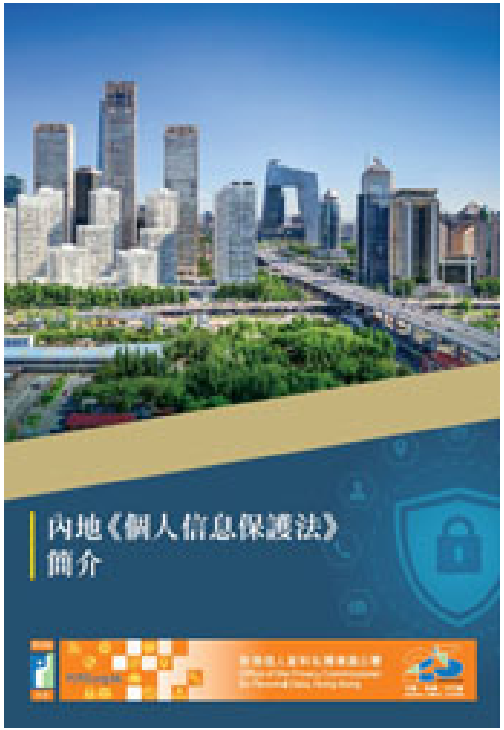


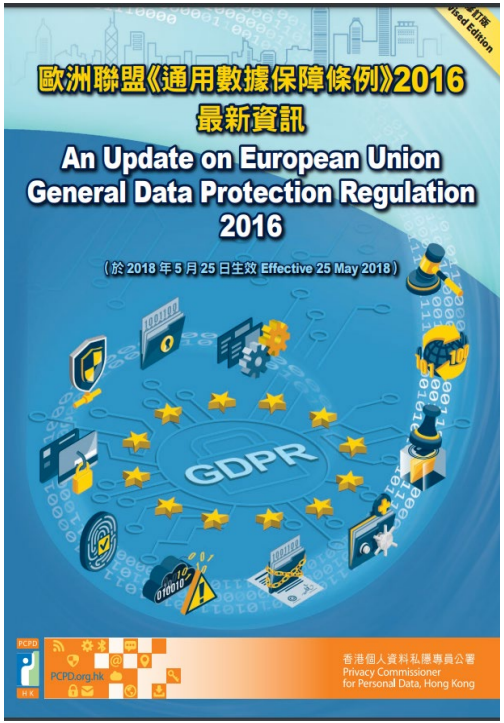
# Data Transfer Out of Hong Kong

A corporation using cloud services should always seek disclosure from the Cloud Service Provider the locations / jurisdictions where the data will be stored, so that this information may be made known to the corporation's customers being the data subjects

A corporation should opt for a Cloud Service Provider that would allow it to choose or specify locations / jurisdictions where there is adequate legal protection to personal data

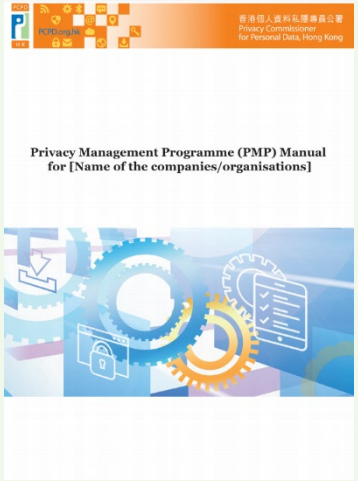
# PCPD Booklets



## Privacy Management Programme: A Best Practice Guide


## General Reference Guide – Privacy Management Programme (PMP) Manual



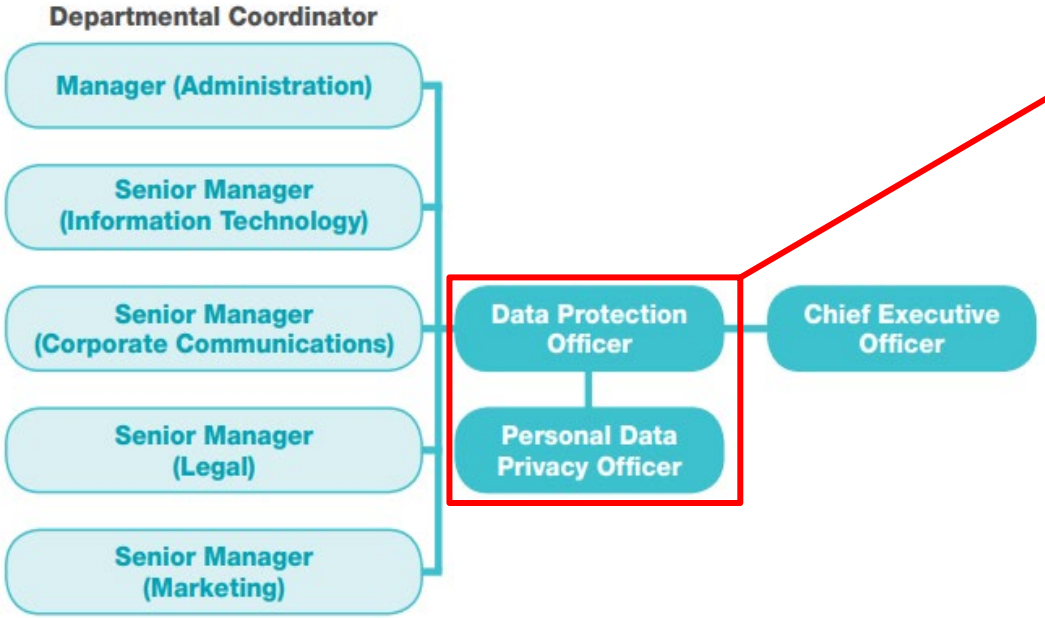
# Privacy Management Programme (PMP)


1.1 Buy-in from the Top

1.2 Appointment of Data Protection Officer/Establishment of Data Protection Office

1.3 Establishment of Reporting Mechanisms

# 1.2 Appointment of Data Protection Officer/Establishment of Data Protection Office




**Duties of a DPO, e.g.-**

- Establish and implement PMP
- Review the effectiveness of PMP
- Report to top management periodically

# Privacy Management Programme (PMP)


2.1 Personal Data Inventory

2.2 Internal Policies on Personal Data Handling

2.3 Risk Assessment Tools

2.4 Training, Education and Promotion

2.5 Handling of Data Breach Incident

2.6 Data Processor Management

2.7 Communication

# Privacy Management Programme (PMP)


3.1 Develop an Oversight and Review Plan

3.2 Assess and Revise Programme Controls

# Thank you!

Telephone： 2827 2827

Website： www.pcpd.org.hk

Email： communications@pcpd.org.hk