Hong Kong Airlines Business Leader Forum
Novotel Citygate Hotel
8 August 2017

Privacy Protection as a Key to Business Success

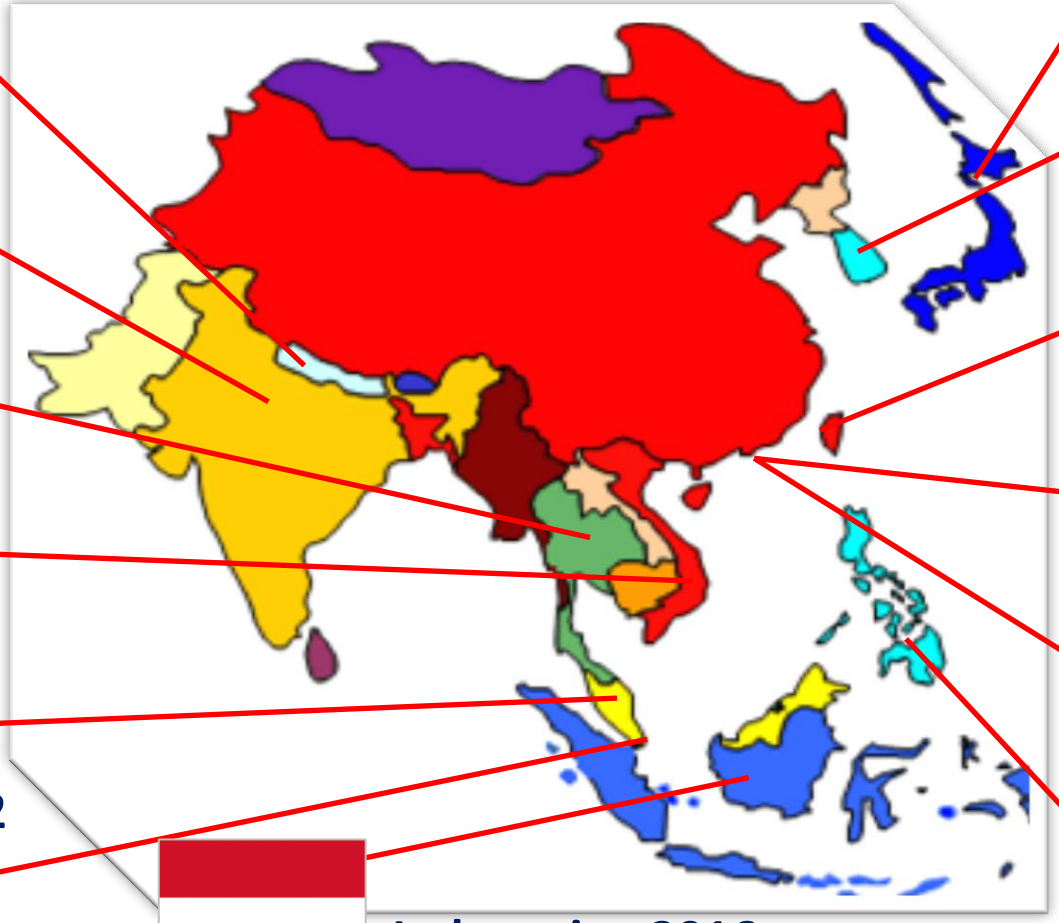
Stephen Kai-yi Wong, Barrister
Privacy Commissioner for Personal Data,
Hong Kong

Presentation Outline

- Overview of Hong Kong's Personal Data (Privacy) Ordinance
- Recent developments of the Ordinance and its enforcement
- Accountability principle in data protection and Privacy Management Programme
- Recent developments in the mainland of China (Cybersecurity Law)
- Major Impact of the EU General Data Protection Regulation (GDPR) 2018
- The Belt and Road Initiative: Hong Kong as a bridge in cross-border data transfers between Hong Kong, Mainland of China and EU

An Overview of
The Personal Data (Privacy) Ordinance

The Personal Data Protection Landscape in Asia



Nepal - 2007

India - 2011

Thailand - 1997

Vietnam - 2010

Malaysia - 2010

Singapore - 2012

Indonesia - 2016

Japan - 2003

S. Korea - 2011

Taiwan - 2010

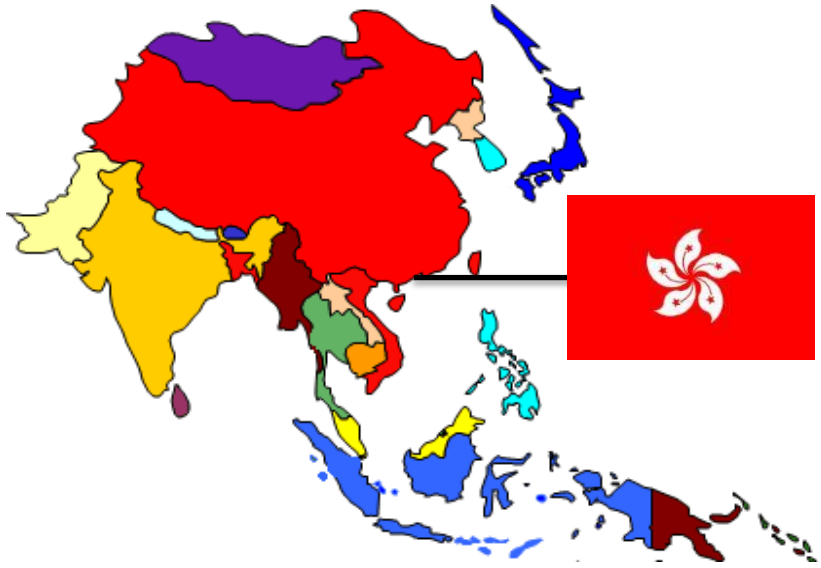
Hong Kong - 1995

Macau - 2005

Philippines - 2012

Personal Data (Privacy) Ordinance

- 1st comprehensive data protection law in Asia
- referenced to 1980 OECD Privacy Guidelines and 1995 EU Data Protection Directive
- single and comprehensive legislation
- covers the public (government) and private sectors



Personal Data (Privacy) Ordinance

- enacted in 1995
- core provisions came into effect on 20 December 1996
- Personal Data (Privacy) (Amendment) Ordinance 2012 effective from 1 October 2012 except for "direct marketing" and "legal assistance" provisions which took effect on 1 April 2013

What is "Personal Data"?

"**Personal data**" (個人資料) means any **data** -

(a) relating directly or indirectly to a living individual;

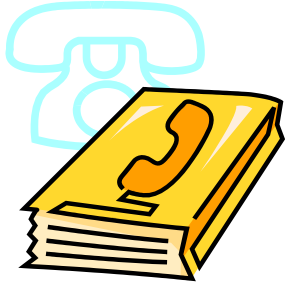
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

"**Data**" (資料) means *any representation of information (including an expression of opinion) in any document*.

Examples of Personal Data in Everyday Life

- a person's name, telephone number, address, sex, age, occupation, salary, nationality, photo, identity card number, medical record, etc.



Who is the “Data Subject”?

- data subject is a living individual who is the subject of the personal data concerned

- under the Ordinance, a person who passed away is not a data subject

Who is the "Data User"?

- **data user** is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data

- even if personal data processing work is outsourced to a contractor, the data user shall be liable for any wrongful act of the contractor

The Six Data Protection Principles (DPPs)

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性儲存及保留 Accuracy & Retention

資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達致原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

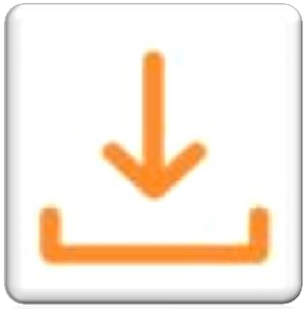
資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

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

Principle 1 – Purpose & Manner of Collection

- must be related to the data user's (i.e. organisation's) functions or activities
- data collected should be adequate but not excessive
- the means of collection must be lawful and fair
- notify data subjects of collection purposes and to whom data will be transferred



Principle 2 – Accuracy & duration of retention

- data users shall take all practicable steps to ensure the accuracy of personal data held by them, and destroy data after the purpose of use is satisfied (i.e. reasonable time)

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" means any purpose other than the purposes for which they were collected or directly related purposes

Principle 4 – Security of personal data

- data users shall take all practicable steps, to safeguard personal data against unauthorised or accidental access, processing, erasure, loss or use

Principle 5 – Information to be generally available (Transparency)

- data users shall **provide**:

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

  (b) the **kinds of personal data held**;

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

Principle 6 – Access to personal data

- data subject is entitled to request access to and correction of his personal data
- data user may charge a non-excessive fee
- data user shall respond within 40 days

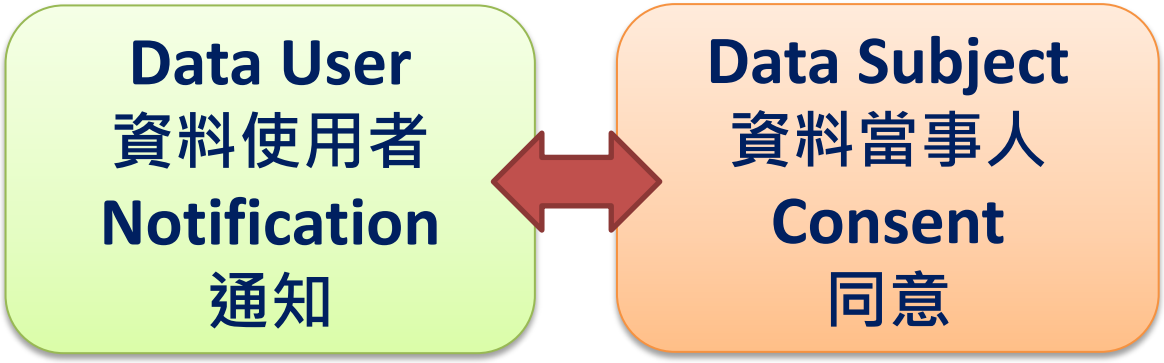
Direct Marketing

New Direct Marketing Regime

- **2012 Ordinance review exercise**
- **new direct marketing regime came into force on 1 April 2013**
- **direct marketing activities under the Ordinance include such activities made to specific persons by mail, fax, email and phone**

Direct Marketing Requirements

Intends to use or provide personal data to others for direct marketing



Provides personal data

Provide "prescribed information" and response channel for data subjects to elect whether to give consent Notification must be easily understandable	Consent should be given explicitly and voluntarily "Consent" includes an indication of "no objection"

Direct Marketing Requirements

- data user must comply with the data subject's opt-out request without charge [section 35G]

- criminal sanctions if data user fails to comply with requirements of notification, consent and opt-out requests

Direct Marketing Conviction Cases

Date	Case	Penalty
Sept 2015 (1st conviction after the 2012 amendment)	• A telecommunication company ignored customer's opt-out requests. • The company appealed against its conviction at the High Court, and the appeal was dismissed in Jan 2017.	Fined $30,000
Sept 2015	• A storage service provider failed to take specified actions and obtain the data subject's consent before direct marketing.	Fined $10,000
Nov 2015	• A healthcare services company ignored customer's opt-out requests.	Fined $10,000

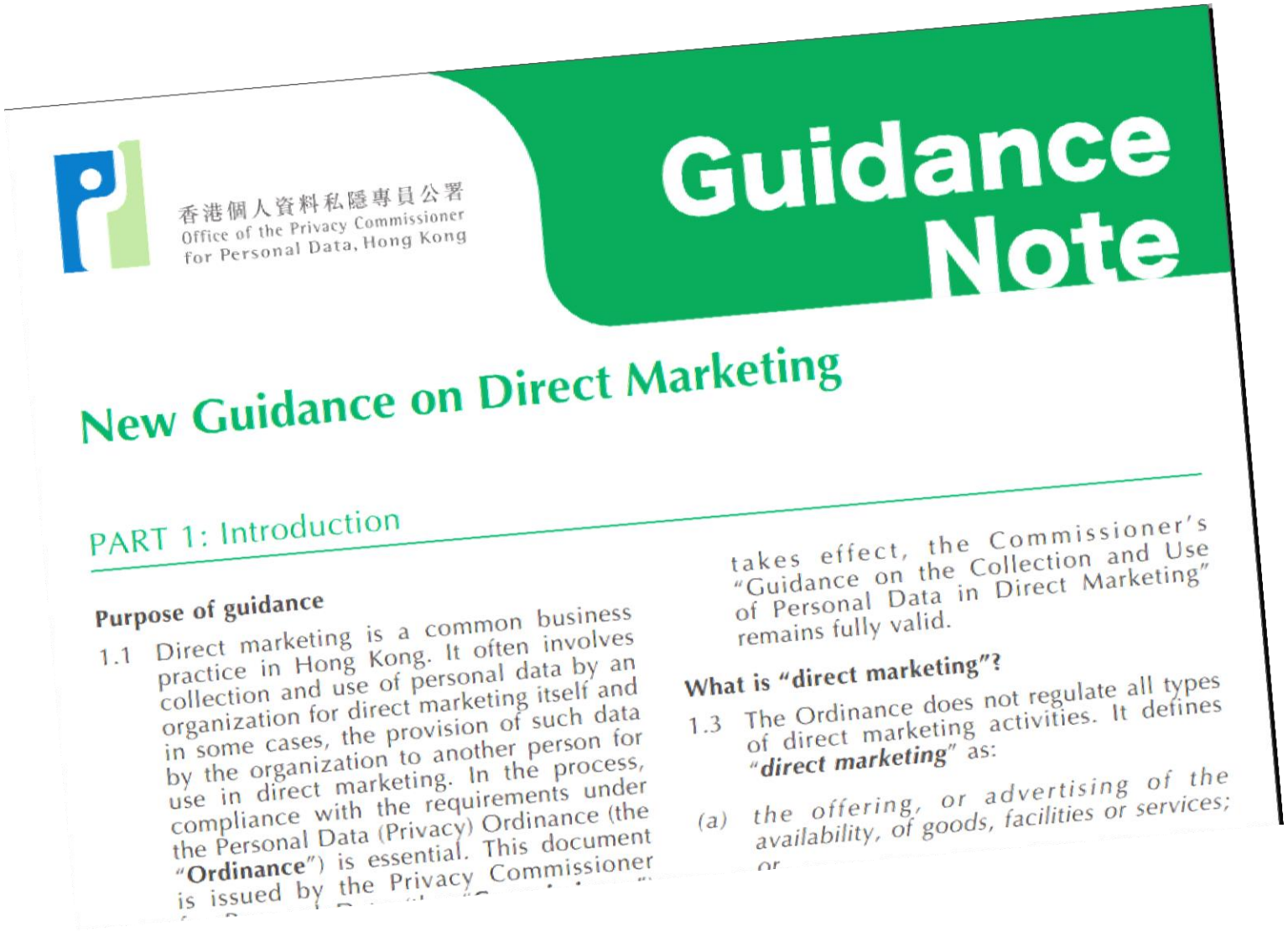
Direct Marketing Conviction Cases

Date	Case	Penalty
Dec 2015	• An individual provided personal data to a third party for direct marketing without taking specified actions and obtaining the data subject's consent. • The individual appealed against the conviction at the High Court, and the appeal was dismissed in June 2017.	Fined $5,000
Apr 2016	• An insurance agent used personal data in direct marketing without taking specified actions and obtaining the data subject's consent. • The agent also failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time.	Community Service Order of 80 hours for each charge
May 2016	• A telemarketing company used a customer's personal data in direct marketing without taking specified actions and obtaining his consent. • The company also ignored opt-out requests.	Fined $8,000 for each charge

Direct Marketing Conviction Cases

Date	Case	Penalty
Nov 2016	• Two financial intermediaries used personal data in direct marketing without taking specified actions and obtaining data subject's consent, total 11 charges, and all convicted. • Two senior management of the companies were also charged, but were acquitted due to lack of evidence.	Two companies fined $165,000 in total ($15,000 per charge), plus damages to claimants for 25% of profits ($47,800).
Dec 2016	• A watch company used an individual's personal data in direct marketing without taking specified actions and obtaining his consent. • The company also failed to inform the individual of his opt-out right when using his personal data in direct marketing for the first time.	Fined $8,000 for each charge
Jan 2017	• A bank failed to comply with client's opt-out request.	Fined $10,000

Direct Marketing Guidance Note



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

Guidance Note

New Guidance on Direct Marketing

PART 1: Introduction

Purpose of guidance

1.1 Direct marketing is a common business practice in Hong Kong. It often involves collection and use of personal data by an organization for direct marketing itself and in some cases, the provision of such data by the organization to another person for use in direct marketing. In the process, compliance with the requirements under the Personal Data (Privacy) Ordinance (the "**Ordinance**") is essential. This document is issued by the Privacy Commissioner

takes effect, the Commissioner's "Guidance on the Collection and Use of Personal Data in Direct Marketing" remains fully valid.

What is "direct marketing"?

1.3 The Ordinance does not regulate all types of direct marketing activities. It defines "***direct marketing***" as:

(a) *the offering, or advertising of the availability, of goods, facilities or services;*

Source: https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf

Recent Incidents

The "Octopus Incident" (2010)


South China Morning Post EDITION: HONG KONG

HONG KONG NEWS BUSINESS TECH LIFESTYLE COMMENT SPORT PRO

Octopus sold personal data of customers for HK$44m

Phyllis Tsang and Ng Kang-chung

PUBLISHED : Tuesday, 27 July, 2010, 12:00am


CHINADAILY

Thursday, Mar 10, 2016 中国日报

Home China Business Metro Beijing Regional World Opinion

Hong Kong

Octopus chairman to step down in Dec

By Michelle Fei (HK Edition)

Updated: 2010-10-20 06:57


THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

ASIA TECHNOLOGY

Octopus CEO Resigns Over Data Sale

By JEFFREY NG

Updated Aug. 4, 2010 11:43 a.m. ET

VTech Data Breach (2015)

SECTIONS | The New York Times | SUBSCRIBE | LOG IN

Uber Faces Federal Inquiry Over Use of Greyball Tool to Evade Authorities

THE MONEY ISSUE
The Online Marketplace That's a Portal to the Future of Capitalism

STRATEGIES
The Fabulous Apple Cash Machine

Security Breach at Toy Maker VTech Includes Data on Children

By DANIEL VICTOR NOV. 30, 2015

Learning Lodge is an online store for VTech devices where users can download apps, games, e-books, videos and music, all geared toward children. Tyrone Siu/Reuters

South China Morning Post | HK CHINA ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT

115 SHARES | NOW READING Hacking of Hong Kong's VTech may prove worst

Hacking of Hong Kong's VTech may prove worst cybersecurity breach of 2015 in Asia

Attack exposed over 6 million children's profiles at the educational toy maker

PUBLISHED : Thursday, 10 December, 2015, 11:33pm
UPDATED : Thursday, 10 December, 2015, 11:33pm

Yahoo Data Breach (2016)

CNN tech

by Seth Fiegerman @sfiegerman

September 23, 2016: 10:39 AM ET

Yahoo confirms massive data breach

Yahoo (YHOO, Tech30) confirmed on Thursday data "associated with at least 500 million user accounts" have been stolen in what may be one of the largest cybersecurity breaches ever.

LAW360 A LexisNexis® Company

News, cases, companies, firms

Take a F

Yahoo GC Steps Down, CEO Loses Bonus After Data Breaches

By **Allison Grande**

Law360, New York (March 2, 2017, 9:49 PM EST) -- Yahoo's general counsel has resigned and its CEO Marissa Mayer will not be paid her annual bonus for 2016 in the wake of an internal probe that concluded that certain senior executives failed to adequately respond to a trio of data breaches believed to have affected at least 1.5 billion users, the company revealed Wednesday.

The company's disclosure came as part of its annual report filed with the U.S. Securities and Exchange Commission, which covered a range of topics, including legal and regulatory fallout from three separate data security breaches announced during the past year and the impact of these incidents on its pending sale to Verizon, which last month **slashed $350 million** from its planned $4.83 billion acquisition of the tech company's core business.

The filing also touched on "management changes" that Yahoo's board of directors had elected to take in the wake of these breaches and a subsequent report prepared by an internal committee that found shortcomings in the way executives handled the incidents. Specifically, the company disclosed that its general counsel Ronald S. Bell had resigned on Wednesday, and that "no payments are being made to Mr. Bell in connection with his resignation."

Yahoo's board has also decided not to award CEO Mayer a cash bonus for 2016 "that was otherwise expected to be paid to her," and Mayer has separately offered to forgo any 2017 annual equity award, according to the filing. The filing explained that Mayer had decided to give up her equity award because one of the breaches — the theft of information related to 500 million user accounts in late 2014 — had "occurred during her tenure," an explanation that Mayer confirmed in a Tumblr post Wednesday.

Suspected Data Leakage by an Airline's Mobile App (2016)

HONGKONG AIRLINES 香港航空

Search | Live Chat | Login

Plan & Book | Offers & Promotion | Travel Information | Our Services | CSR | Frequent Flyer

Book Flight

Type: Round Trip / One-way / Stopover/Multi-city

From

To

Departure Date 2017-01-23

Return Date 2017-01-26

Cabin Economy

Adult (Aged 12 or above) 1

Child (2-11 years) 0

Payment Hong Kong Dollar HKD

Search

Book Hotel

Flight Status

Fortune Wings Miles Join Now!

24h Reservation Hotline	Mon-Sun
+852 3916 3666	Hong Kong
+86 950715	Mainland China
+0080 1853033	Taiwan
+61 29009 7988	Australia
+64 9913 4177	New Zealand
+1 855 393 3880	U.S
Flight Status Enquiry	Mon-Sun
+852 3713 1388	0900-2200

Home > Special News

Special News

Hong Kong Airlines Statement Regarding Mobile APP

Last Updated:(Hong Kong)2017-01-03

Hong Kong Airlines (the "Company") is actively investigating a recent case of leakage information from Hong Kong Airlines mobile APP (the "APP"). Immediate remedial actio taken to suspend the non-member customers using Android system from conducting o and booking information enquiry via the APP. The Company has engaged a third party c inquire into this situation, aiming to find a comprehensive solution that will prevent re Company has also reported the case to the Office of the Privacy Commissioner for Perso Kong (PCPD).

Only non-member customers using a few mobile phone brands installed with Android sy 6.0 or above) via the APP are potentially affected in this incident. The problem only exis and does not affect Hong Kong Airlines official website or mobile website. Based on o investigation, 57 customers were affected in this incident.

Hong Kong Airlines attaches great importance to the personal priva sincerely apologies for the inconvenience that may cause to the immediate actions to prevent further leakage and recurrence.

Please refer to the Frequently Asked Questions below for further inf

1. How do I know if I am one of the affected party?

Based on our preliminary investigation, we have identified 57 aff customers using a few mobile phone brands installed with Androi the APP are potentially affected in this incident. We will contact possible. If you are concerned whether you are an affected custome dedicated email address at app.enquiry@hkairlines.com.

2. What data might have been leaked in this incident?

As of now, the known affected data includes passenger name, nan (if applicable), email (if applicable), ticket number, ID or travel do number, online check-in status and QR code of the boarding pass. Please rest assured that the payment details of customers includi strict protection and have NOT been affected.

學者：收集大量資料無必要

Registration and Electoral Office's Loss of Laptops (2017)

South China Morning Post | HK CHINA ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT WEEK IN ASIA POST MAG STYLE .TV

612 SHARES

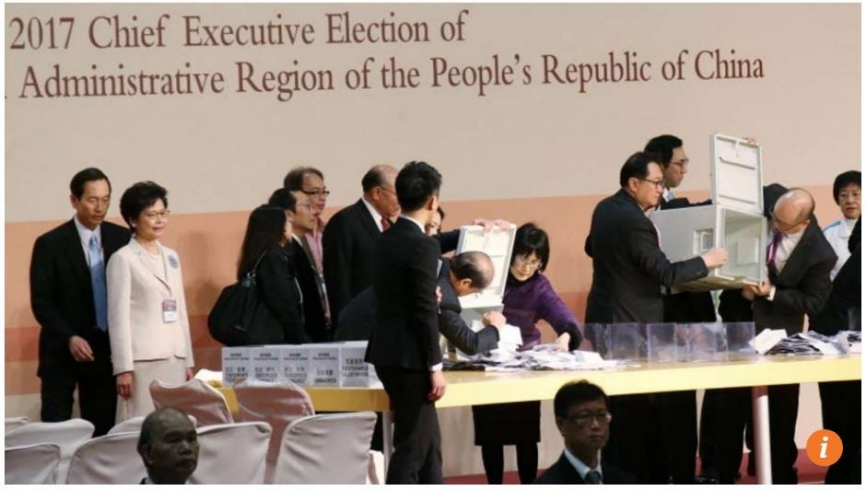
NOW READING Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive e

Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive election

Devices contained ID card numbers, addresses and mobile numbers

PUBLISHED : Tuesday, 28 March, 2017, 12:30am
UPDATED : Tuesday, 28 March, 2017, 1:42am

COMMENTS: 24



In what could be one of Hong Kong's most significant data breaches ever, the personal information of the city's 3.7 million voters was possibly compromised after the Registration and Electoral Office reported two laptop computers went missing at

信報財經新聞

熱門：大灣區 一帶一路 搜尋：黃國英課程 新書推介 炒另類磚頭

搜尋 Tips

ejinsight 港股360 EJFQ8 信報月刊 LJ優雅生活

主頁 即時新聞 今日信報 港股360 滬港通 地產投資

全部 港股直擊 香港財經 地產新聞 中國財經 國際財經 時事脈搏 即市股評 重要通告 港交所

恒生指數 25,380.22 ↑223.88 國企指數 10,453.37 ↑170.72 上證指數 3,090.23 ↑6.72

« 返回前頁

Like 52

列印 預設字型

2017年4月3日 時事脈搏

選舉處失電腦 花500萬發信道歉

選舉事務處遺失兩部載有300多萬選民資料的電腦，總選舉主任黃思文於立法會財委會特別會議上表示，目前已去信向受影響選民道歉，預計要花約500萬元。

財委會副主席田北辰批評，無故花費公帑去道歉，形容「道歉都幾重皮」。

對於多名議員質疑當時有否安排保安看守該兩部電腦，黃思文表示，同事測試完電腦後便將電腦鎖進儲物室，直至27日才返回收回電腦，承認期間沒有保安看守，而現時正檢視做法是否符合標準措施。

他透露，電腦內的選民資料已採取比保安要求更高級別的方式去處理，強調資料經多重加密，理論上難以破解，更提醒市民放心，並非得到電腦就能夠閱讀相關資料。

Call-Blocking App Leaks Personal Data (2017)

FactWire News Agency 中文 ENGLISH

Exclusive | Interview | Follow Up | Security | Technology | Hong Kong | English

Mobile Numbers of Chinese and Local Officials Exposed By Baidu App

May 13, 2017 | Staff Reporter, FactWire

May 13, Hong Kong, (FactWire) - A smartphone application (app) developed by China's Baidu (NASDAQ:BIDU) may have invaded millions of users' mobile contacts, exposing mobile numbers of senior Chinese and Hong Kong officials, an investigation by the FactWire reveals.

香港01 港聞 / 主頁 新聞 新特首內閣 01觀點 01

港聞 >

《傳真社》揭侵私隱後　百度App封搜尋結果　《01》發現仍有漏洞

撰文：陳惠嫻　梁融軒　楊婉婷　發佈日期：2017-05-13 19:47
最後更新日期：2017-05-13 21:08

標籤： 商務及經濟發展局 + 傳真社FactWire + 電話促銷 +

讚好 66 分享

私隱管理系統
Privacy Management Programme

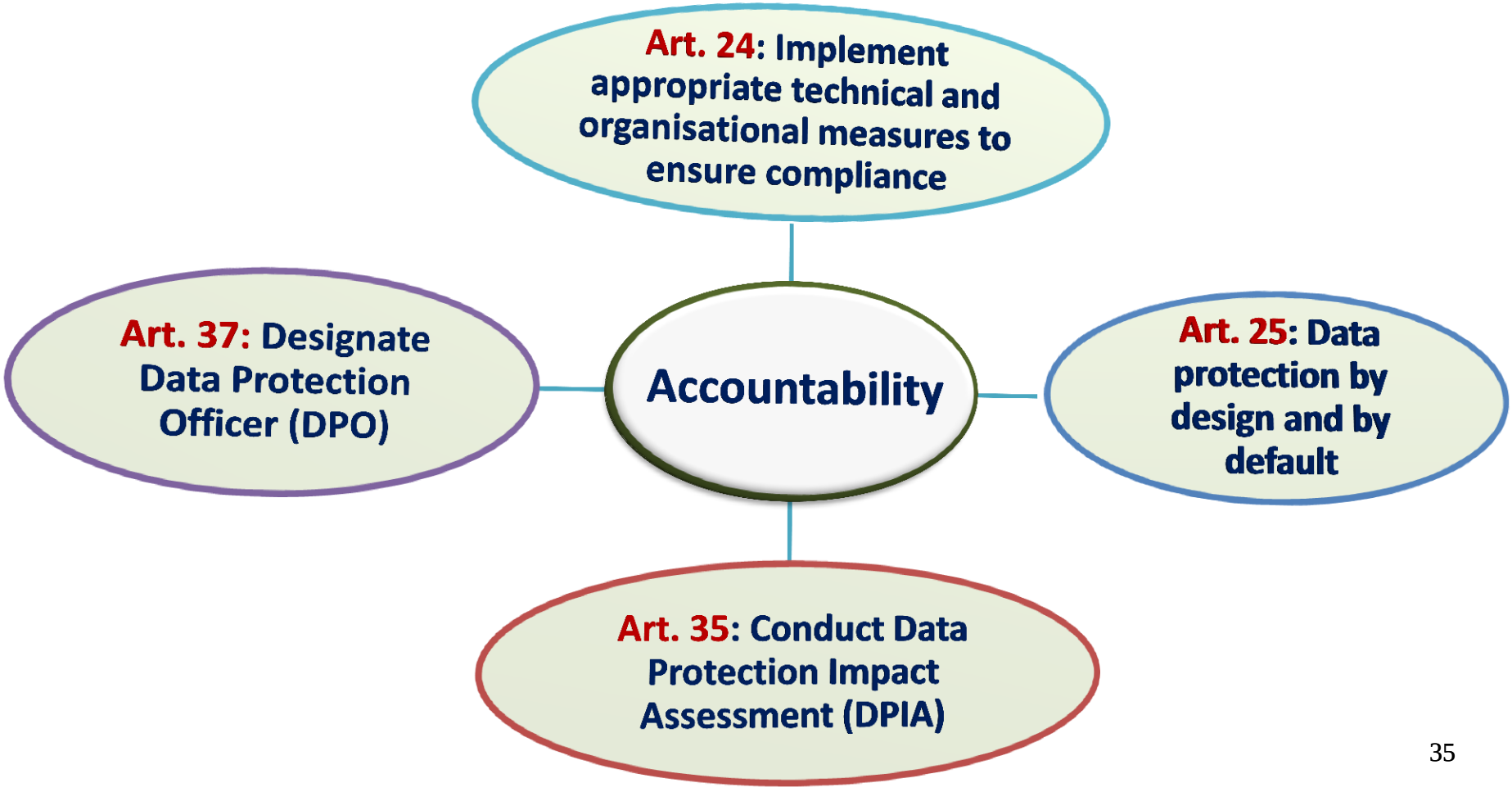
From Compliance, to Accountability… to

Privacy Management Programme (PMP)

- **Accountability Principle in the OECD Privacy Guidelines:**

  a data user (controller) should be accountable for complying with measures which give effect to the data protection principles.

EU General Data Protection Regulation 2018 (GDPR) makes accountability into law



Main Themes of PMP

- "An **accountable organisation** must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management programme."

- encourage organisations to **embrace personal data privacy protection as part of their corporate governance** responsibilities and **apply it as a top-down business imperative** throughout the organisation

Source: Privacy Management Programme - A Best Practice Guide
https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

From Compliance to Accountability

Paradigm Shift

Compliance approach

- passive
- reactive
- remedial
- problem-based
- handled by compliance team
- minimum legal requirement
- bottom-up

Accountability approach

- active
- proactive
- preventative
- based on customer expectation
- directed by top-management
- reputation building
- top-down

Participation in the PMP

Participating sectors that pledged to implement PMP:

- Hong Kong SAR Government
- 25 insurance companies
- 9 telecommunications companies
- 5 organisations from other sectors

The PMP Best Practice Guide does not…

- provide a "one-size-fits-all" solution
- constitute a legal requirement
- provide direct guidance for compliance with specific provisions of the Ordinance
- impose prescriptive obligations

Instead, the PMP is flexible enough for organisations of any size and nature to adopt.

PMP Best Practice Guide - Fundamental Principles

3 Top-down Management Commitment

1. Top-management commitment and buy-in
2. Setting up of a dedicated data protection office or officer
3. Establishing reporting and oversight mechanism

PMP Best Practice Guide - Fundamental Principles

7 Practical Programme Controls

1. Record and maintain **personal data inventory**
2. Establish and maintain data protection and **privacy policies**
3. Develop **risk assessment** tools (e.g. privacy impact assessment)
4. Develop and maintain **training plan** for all relevant staff
5. Establish workable **breach handling** and notification procedures
6. Establish and monitor **data processor** engagement mechanism
7. Establish **communication** so that policies and practice are made known to all stakeholders

PMP Best Practice Guide - Fundamental Principles

Two Review Processes

1

Develop an oversight review plan to check for compliance and effectiveness of the privacy management programme

2

Execute the oversight review plan making sure that any recommendations are followed through

Consultancy on Implementing PMP in the Public Sector

- November 2015 - to facilitate three Hong Kong Government bureaux/departments to implement PMP

- deliverables (toolkits and training) will be beneficial to organisations (public or private) implementing PMP

Tips for Senior Management

- Secure the buy-in from top-management
- Build a culture within organisation to protect privacy
- Keep abreast with new development (PCPD's online resources, Data Protection Officer's Club)
- Prepare organisation to meet new changes through risk assessments, protocols and policies

Recent Developments in the Mainland of China (Cybersecurity Law)

China's Cybersecurity Law

- effective on 1 June 2017

- Purposes: [Art 1]
  - guarantee cybersecurity
  - safeguard cyberspace sovereignty
  - safeguard national security and public interest
  - protect lawful rights and interests of citizens, legal persons and other organisations
  - promote sound development of economic and social informatisation (信息化)

China's Cybersecurity Law

Scope of Application:

- apply to the construction, operation, maintenance and use of the network, and the supervision and administration of cybersecurity within China. [Art 2]

- "network operator" - the owners and administrators of the network as well as network service providers. [Art 76(3)]

- "personal information"- information recorded in electronic or other forms, which can be used, independently or combined with other information, to identify personal identity, e.g. name, date of birth, identity certificate number, biology-identified personal information, address and telephone number. [Art 76(5)]

China's Cybersecurity Law

Data Collection & Use:

- where personal information is collected, explicitly notify users and obtain their consent. [Art 22]
- follow principles of legality, rightfulness and necessity during collection and use, explicitly indicate the purposes, means and scope of collection and use. [Art 41]
- do not collect personal information irrelevant to services provided. [Art 41]
- do not collect or use personal information in violation of any law or administrative regulation or agreement of both parties. [Art 41]

China's Cybersecurity Law

Data Accuracy & Record Retention:

- **not tamper** with personal information collected [Art 42]

- take technical measures to monitor and record the status of network operation and cybersecurity incidents, and **preserve weblogs for not less than 6 months**. [Art 21(3)]

China's Cybersecurity Law

Data Security & Breach Notification:

- strictly keep confidential users' personal information collected, and establish and improve the system for information protection. [Art 40]

- not damage personal information collected, and take technical measures and other necessary measures to ensure security of personal information collected, and prevent information leakage, damage and loss. [Art 42]

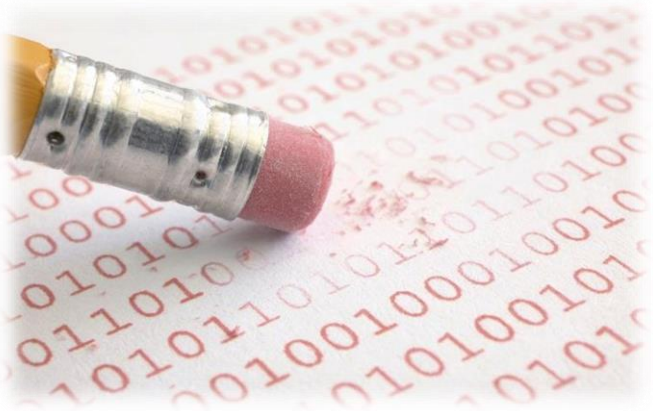
- where personal information has been or is likely to be divulged, damaged or lost, take remedial measures, inform users, and report to regulatory authority. [Art 42]

China's Cybersecurity Law

Data Deletion & Correction:

- individual can request network operator to delete his personal information, if the operator collects or uses information in violation of any law, administrative regulation or agreement of both parties. [Art 43]

- individual can request network operator to correct his personal information collected or stored if there is any error. [Art 43]



China's Cybersecurity Law

Data Localisation & Cross-Border Data Transfer:

- higher standard of care for "critical information infrastructure" (CII)

- CII examples: public communications and information services, energy, transport, water conservancy, finance, public services, e-government affairs, and CII that will result in serious damage to state security, national economy and people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. [Art 31]

China's Cybersecurity Law

Data Localisation & Cross-Border Data Transfer:

- **personal information and important data** collected and produced by CII operators during their operations within China shall be **stored within China**. [Art 37]

- if CII operators need to provide such information and data to overseas parties due to business requirements, they shall conduct **security assessment according to the measures developed by the Cyberspace Administration of China (CAC)** and relevant departments of State Council, unless otherwise prescribed. [Art 37]

- operators other than CII operators are encouraged to **voluntarily participate** in the CII protection system. [Art 31]

China's Cybersecurity Law

Sanctions and Fines:

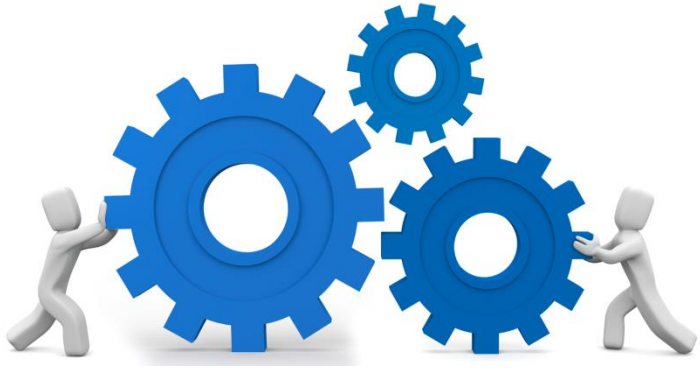
- **Breach of Collection, Use, Security, Breach Notification, Deletion & Correction requirements:**
  - **corrective action**
  - **warning, confiscate illegal income, impose fine between 1 and 10 times such income**
  - **if no illegal income, impose fine < RMB 1 million, and impose fine between RMB 10,000 and 100,000 on directly responsible person in charge and other directly liable persons**
  - **in serious cases, suspend or cease business operation for rectification, or close down website, or revoke business permit or license. [Art 64]**

China's Cybersecurity Law

- **Breach of Data Localisation Requirements:**
  - corrective action; and
  - warning, confiscate illegal income, and impose fine between RMB 50,000 and 500,000; and
  - suspend or cease business operation for rectification, or close down website, or revoke business permit or license; and
  - impose fine between RMB 10,000 and 100,000 on directly responsible person in charge and other directly liable persons. [Art 66]

"Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data" (《個人信息和重要數據出境安全評估辦法》)

- **Purposes: implement data localisation and security assessment requirements under China's Cybersecurity Law**
- **1st Draft Measures issued on 11 April 2017; consultation ended on 11 May 2017**
- **date of implementation is uncertain**



The New York Times | https://nyti.ms/2vbooTd

BUSINESS DAY

Apple Opening Data Center in China to Comply With Cybersecurity Law

点击查看本文中文版

By PAUL MOZUR, DAISUKE WAKABAYASHI and NICK WINGFIELD JULY 12, 2017

SHANGHAI — Apple said Wednesday that it would open its first data center in China, joining a parade of technology companies responding to growing global demands to build facilities that store online data closer to customers.

The move is a response to a strict new law in China that requires companies to store users' data in the country. The new data center, in Guizhou, a province in southwest China, is part of a $1 billion investment in the province and will be operated in partnership with a local data management company, Apple said.

The move is part of a worldwide trend regarding the security and sovereignty of digital data. Microsoft, Amazon and Facebook are among the big American technology companies plowing billions of dollars into building data centers in Germany, the Netherlands, France and other countries. While some of the expansion is for technical reasons — the online services operate faster when they are near customers — the companies are also reacting to growing pressure from European governments and customers to maintain some control over their data.

As is the case with many laws, the digital security regulations approved last month in China were vaguely worded, leaving many foreign companies uncertain about which parts would be enforced and how. Already, Amazon, Microsoft and IBM have formed partnerships with Chinese companies to offer cloud computing services

https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html?mkt_tok=eyJpIjoiTTJaak16STFOR1V6WW1RMyIsInQiOiIz... 1/4

Apple Opening Data Centre in China to Comply With Cybersecurity Law

Source: The New York Times 12 July 2017

Major Impact of the 2018

Hong Kong – European Union Trade Relationships

- EU is Hong Kong's second major trading partner after China
- EU has been a major source of foreign direct investment in Hong Kong
- In 2015, EU was Hong Kong's second largest supplier of goods after China
- In 2015, EU was Hong Kong's third largest market of goods after China and the USA

Sources: HK Trade and Industry Department, European Commission

EU General Data Protection Regulation (GDPR)

- approved by EU Parliament on 14 April 2016
- will be enforced on 25 May 2018
- replaces the 1995 EU Data Protection Directive (95/46/EC)
- harmonises data protection laws across Europe

GDPR – Extra-Territoriality

GDPR applies to data controllers (i.e. data users) and data processors:

- **with an establishment in the EU; or**
- **without an establishment in the EU, but offer goods or services to data subjects in the EU, or monitor their behaviours in the EU. [Art 3]**

GDPR – Significant Changes

Accountability - Commitment to privacy impact assessment, privacy by design etc.

Children's Protection - Parental consent is needed for processing children's personal data

Data Breach Notification - Mandatory breach notification

Data Processor Obligations - Processors to implement technical and organisational measures to ensure security

Data Protection Officers - Appointment of DPO in specified circumstances

GDPR – Significant Changes

Sensitive Personal Data – Sensitive personal data is defined and can only be processed upon explicit consent

Data Protection Seals – Encourage the establishment of data protection seals and marks

Right to be Forgotten & Data Portability – Individuals have right to request erasure and certain right to port their personal data from one controller to another in a common format

Fining power – Up to 4% global annual turnover

GDPR – Cross-Border Data Transfer

Personal data may be transferred outside the EU in limited circumstances, which include:

- transfer to countries with "adequate" level of data protection [Art 45]
- European Commission shall consider the following elements when assessing the adequacy level: [Art 45(2)]
  a. the rule of law, respect for human rights and fundamental freedoms, as well as the implementation of relevant legislation and rules;
  b. the existence and effective functioning of one or more independent data protection authorities, including adequate enforcement powers; and
  c. the international commitments the third country has entered into, or other obligations arising from legally binding conventions or instruments.

GDPR – Cross-Border Data Transfer

- In the absence of an adequacy decision, organisations in the EU may still transfer personal data to a third country on the following bases:
  - legally binding and enforceable instrument between public authorities or bodies [Art 46(2)(a)];
  - binding corporate rules [Arts 46(2)(b) and 47];
  - standard contract clauses [Art 46(2)(c) & (d)];
  - codes of conduct approved by the European Commission or data protection authorities of the EU Member States [Arts 40 and 46(2)(e)];
  - certification mechanism approved by the European Commission or data protection authorities of the EU Member States [Arts 42 and 46(2)(f)];
  - derogations for specific situations (e.g. informed and explicit consent from data subject; necessity for the conclusion or performance of contract; necessity for important public interest; etc.) [Art 49(1)]; etc.

Sanctions

Maximum administrative fine:

- **€10 million or 2% of global annual turnover for less serious contravention, e.g. failure to notify data breach, appoint data protection officer, conduct data protection impact assessment, etc.**

- **€20 million or 4% of global annual turnover for more serious contravention, e.g. processing without lawful basis, failure to comply with individuals' request to erasure, failure to comply with cross-border data transfer requirements, etc. [Article 83]**

The Belt and Road Initiative: Hong Kong As a Bridge in Cross-Border Data Transfers Between Hong Kong, Mainland of China & EU

The Belt and Road Initiative

- cover more than 60 countries and regions from Asia to Europe via China, Southeast Asia, Europe, Africa and the Middle East

China – European Union Trade Relationships

- EU is China's largest trading partner, largest supplier of goods and second largest market of goods

- China and EU cooperate in areas of energy, technology, finance, industry and agriculture

Source : Ministry of Foreign Affairs of the People's Republic of China

Hong Kong's Unique Advantages

"Hong Kong…has many unique advantages…for instance, free and open economy, efficient business environment, advanced professional services sector, well-established infrastructure and facilities, internationally recognised legal system, free flow of information and large supply of quality professionals…"

Mr Zhang Dejiang,
Member of the Standing Committee of the Political Bureau of the Communist Party of China Central Committee;
Chairman of the Standing Committee of the National People's Congress of the People's Republic of China
Keynote Speech,
Belt and Road Summit, 18 May 2016

Hong Kong's Unique Advantages

"With the combined advantages of 'one country' and 'two systems,' Hong Kong can serve as a 'super-connector' (超級聯繫人) between the Mainland of China and the rest of the world. In areas such as finance, investment, professional services, trade, logistics, culture, creativity, innovation and technology, Hong Kong's unique 'super connector' role can bring together the strengths of Belt and Road economies."

The Hon C Y Leung, GBM, GBS, JP
Former Chief Executive, Hong Kong SAR
Opening Remarks
Belt and Road Summit, 18 May 2016

Hong Kong – Asia's Leading Data Hub

- **2016 Cloud Readiness Index Overall Ranking # 1:**
  - International Connectivity #1
  - Data Centre Safety #1
  - Privacy #1
  - Broadband Quality #2
  - Power Grid, Green Policy & Sustainability #2

Secretary for Innovation and Technology Mr Nicholas Yang's Speech at 2nd Phase NTT Communications Hong Kong Financial Data Center Opening Ceremony (9 Dec 2015):

"Hong Kong…well-positioned to…secure data centre services…Our robust information infrastructure is among the most sophisticated and advanced, with submarine and overland cable systems connected to other parts of the world. We have a highly stable power supply, with reliability exceeding 99.999 per cent. Our Internet connection speed ranked second in the world…Hong Kong…offer effective protection of data privacy and information security."

Source: Innovation and Technology Bureau (9 Dec 2015)

Support of Hong Kong Government

Hong Kong Government fully supports developing Hong Kong into Asia's Leading Data Hub:

"**Data centres are an essential infrastructure** to support pillar sectors like financial services, trading and logistics as well as other economic sectors. Data centres also provide the **catalyst for the development of new content and applications**, as well as cloud computing services… **the Government fully supports** the **development of data centres** in Hong Kong as the backbone to our economic growth…"

Source : Hong Kong Office of the Government Chief Information Officer

Hong Kong Government Policy

- Set up a Data Centre Facilitation Unit and a thematic information portal, to provide coordinated services to interested developers and investors on matters related to setting up of data centres in Hong Kong
- Step up promotion to position Hong Kong as a prime location for data centres in the Asia Pacific region;
- Promote the incentive measures that optimise the use of industrial buildings for the benefit of developing data centres; and
- Identify sites for development of high-tier data centres and appropriate land disposal arrangements.

Source : Hong Kong Office of the Government Chief Information Officer

Hong Kong – Reputable Legal System

- The Rule of Law
- Common Law Jurisdiction
- Strong Commercial and Property Law
- Independence of the Judiciary
- Arbitration and Mediation

Hong Kong – Legal Professionals

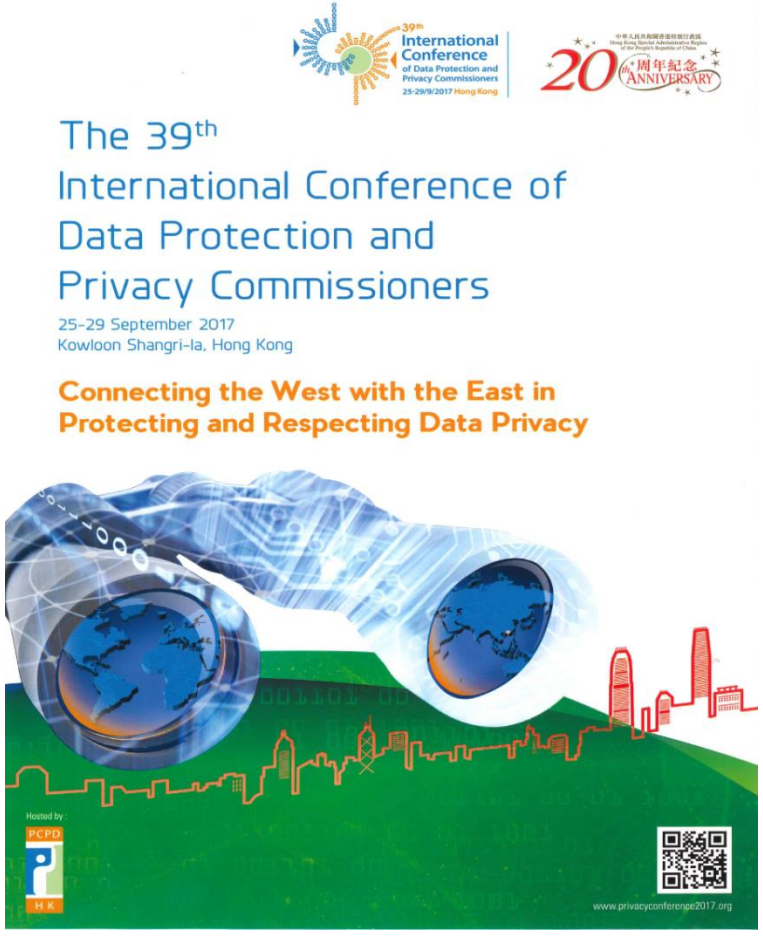
- International Trade
- Intellectual Property
- International Arbitration
- Professional Knowledge
- Diverse Cultures
- International Vision

Hong Kong's comprehensive data protection regime

- **Personal Data (Privacy) Ordinance**: A comprehensive data protection law in line with international standards
- **Office of the Privacy Commissioner for Personal Data**: independent, fair and reliable enforcement agency trusted by local citizens and overseas enforcement agencies

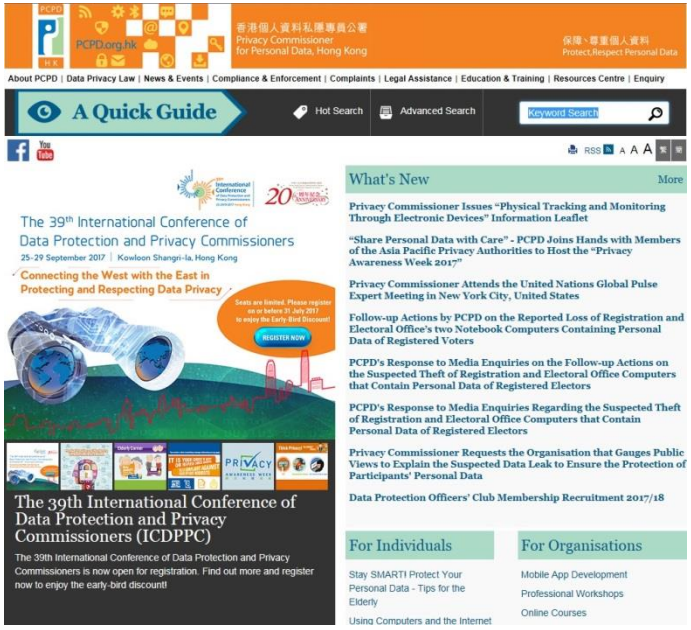
39th International Conference of Data Protection and Privacy Commissioners

- **East Meets West**
- **meet over 110 data protection authorities from over 70 countries/regions**
- **local, the Mainland of China and international corporations will participate**



Stay tuned for updates on
www.privacyconference2017.org

Contact Us



- ❑ **Hotline** 2827 2827
- ❑ **Fax** 2877 7026
- ❑ **Website** www.pcpd.org.hk
- ❑ **E-mail** enquiry@pcpd.org.hk
- ❑ **Address** 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, HK