The Hong Kong Institute of Chartered Secretaries:
18th Annual Corporate and Regulatory Update
2 June 2017

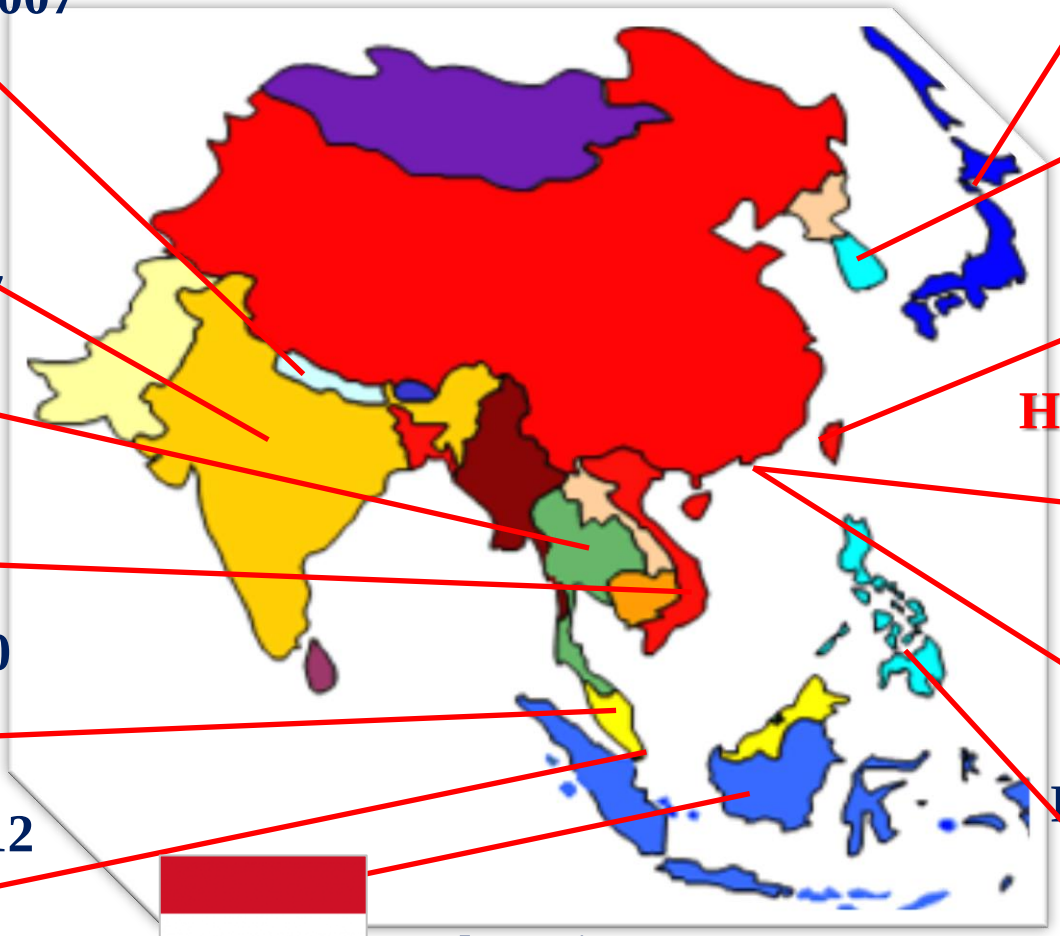
Personal Data Protection and Data Governance: Points to Note for Senior Management

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

Today's presentation will cover…

- an overview of the Personal Data (Privacy) Ordinance
- several real life examples of personal data incidents
- accountability principle in personal data protection, and the Privacy Management Programme
- key impact of the EU GDPR 2018

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

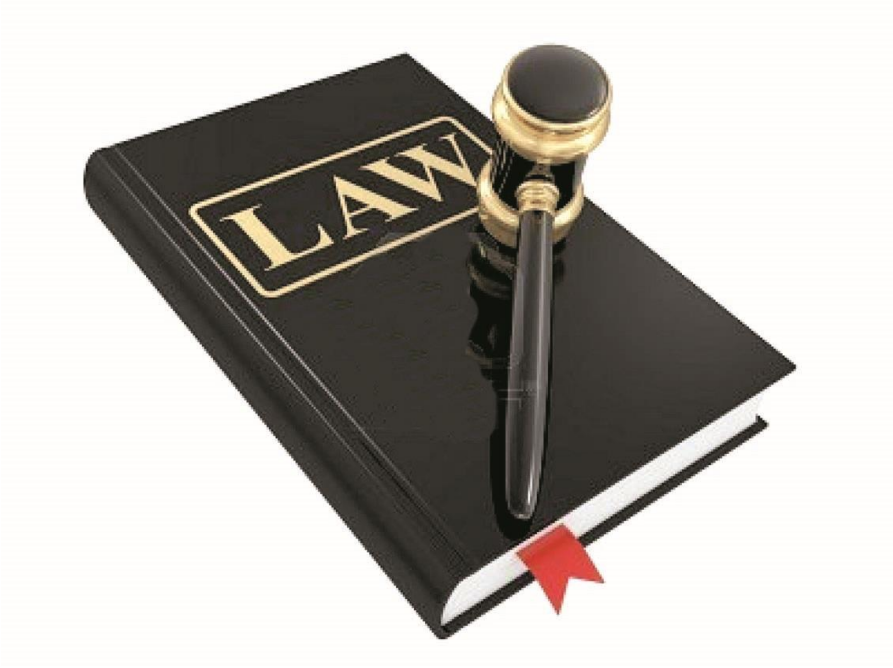
Taiwan - 2010

Hong Kong - 1995

Macau - 2005

Philippines - 2012

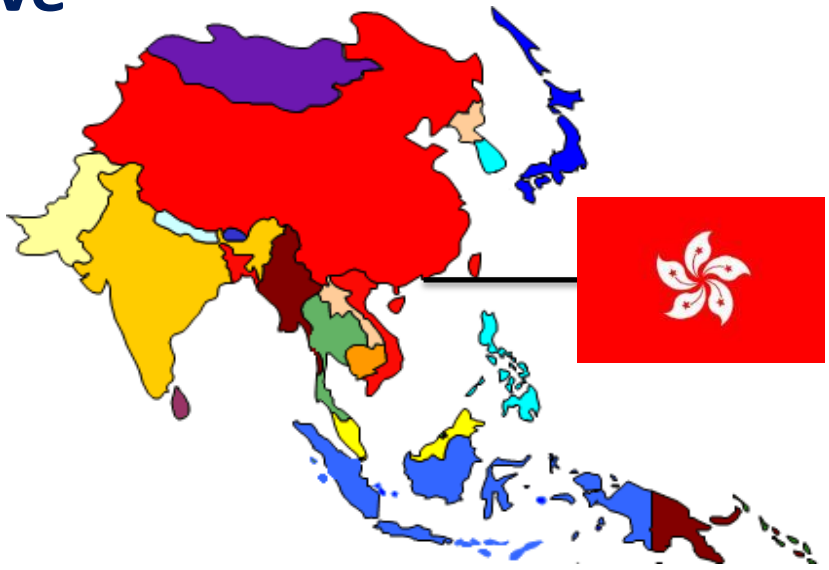
Overview of
Personal Data (Privacy) Ordinance



Personal Data (Privacy) Ordinance

- **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" 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;*

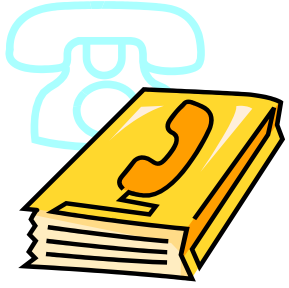
*(b) from which it is practicable for the **identity** of the individual to be directly or indirectly ascertained; and*

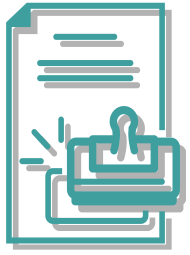
*(c) in a **form** in which access to or processing of the data is practicable.*

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

Examples of Personal Data used in everyday life

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





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

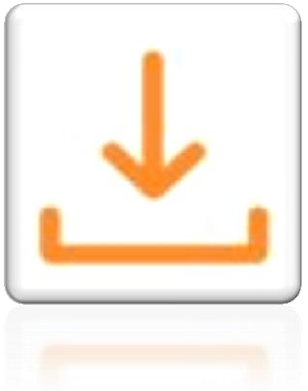
資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

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 and 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 and 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 – 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

Direct Marketing Requirements

- The new provisions on regulation of direct marketing activities 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

Data User
資料使用者
Notification
通知

Data Subject
資料當事人
Consent
同意

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

- If a data subject submits an opt-out request, the data user must comply with the request without charge

- Criminal sanctions may apply if a data user fails to comply with the requirements on notification, consent and opt-out request

Direct Marketing Conviction Cases

Date	Case	Penalty
Sep 2015 *(1st conviction after the 2012 amendments)*	• **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**
Sep 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 *(Note: Appeal trial in progress)*	• 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. The appeal trial is in progress.	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 the 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 the claimants equal 25% of the relevant profits, total $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

Impact of inadequate data protection

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.

REO 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

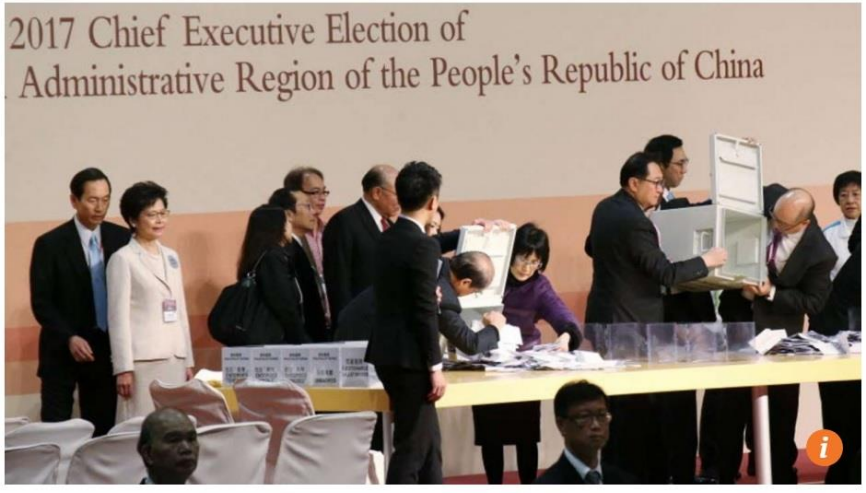
NOW READING Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive e

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

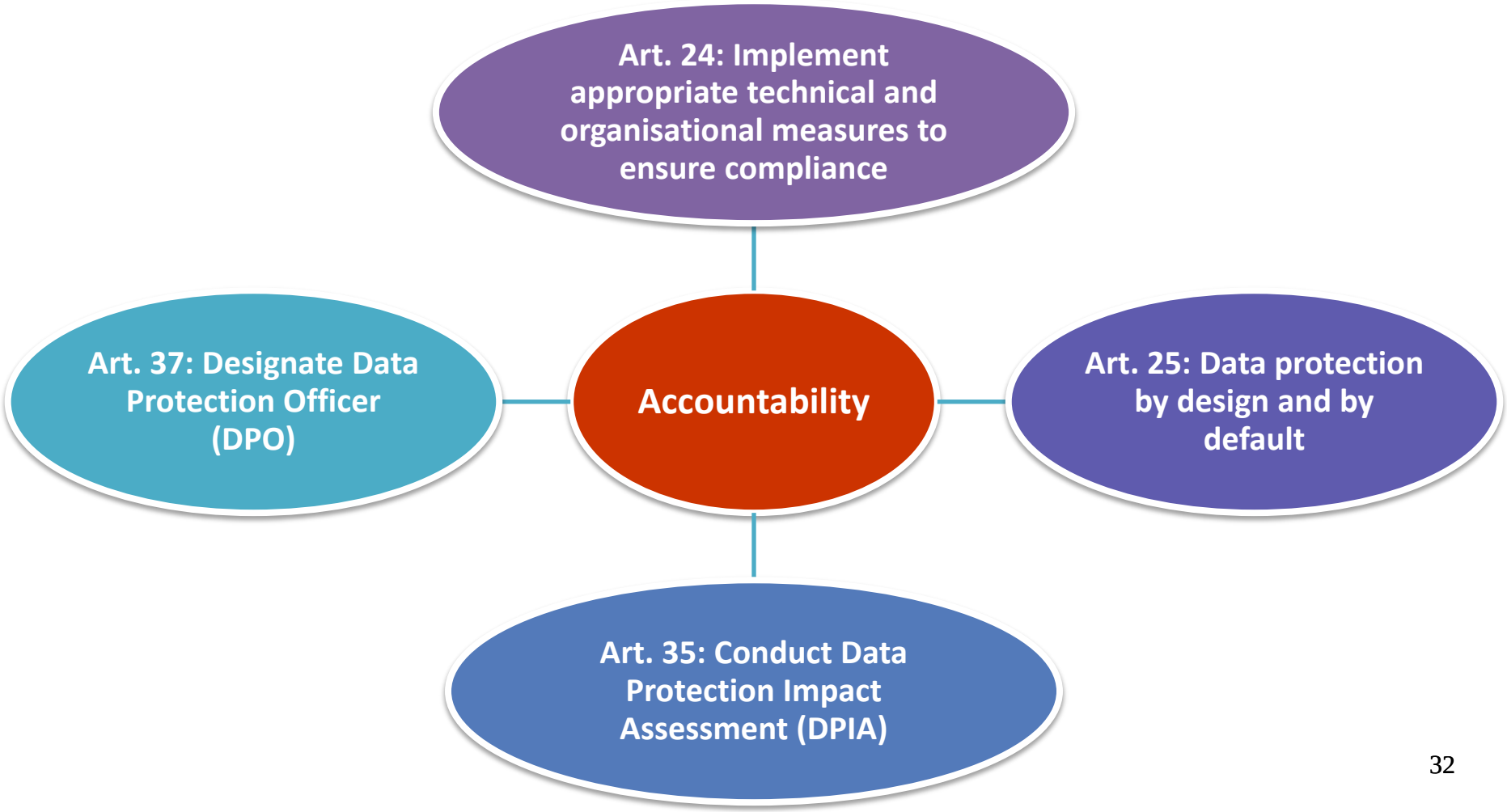
From compliance, to accountability… to

Privacy Management Programme (PMP)

Accountability Principle under OECD Privacy Guideline:

- **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 a 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

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 adapt to.

PMP Best Practice Guide - Fundamental Principles

3 top-down management commitments

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

PMP Best Practice Guide - Fundamental Principles

2 review processes

1. **Development** of an **oversight review plan** to check for compliance and effectiveness of the privacy management programme

2. **Execution** of 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 Company Secretaries

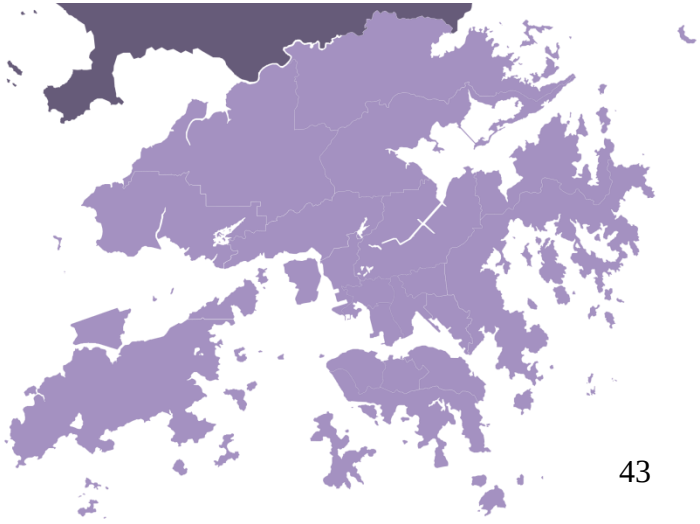
Key Impact of the 2018

Extra-territoriality of GDPR

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 individuals in the EU, or monitor the individuals behaviour.

[Article 3]



What does GDPR apply to?

GDPR applies to personal data, which is defined as:

> ***"any information relating to an identified or identifiable natural person..."*** **[Article 4(1)]**

- **May include location data and online identifier**
- **A wider definition than the Hong Kong Personal Data (Privacy) Ordinance**

Consent

- One of the lawful bases for processing of personal data. [Article 6]
- Consent must be:
  - freely given, specific and informed; and
  - provided by an unambiguous indication.

- '*Processing*' includes collection, use and retention.

Mandatory data breach notification

- Data controller must notify, without undue delay:
  - the supervisory authority, unless the breach is unlikely to result in a risk to the rights or freedoms of individuals; and
  - the affected individuals, if the data breach is likely to result in a "*high risk to the rights and freedoms*" of individuals.
- Data processor shall notify its data controller without undue delay.

[Articles 33-34]

Individuals' rights

New rights to individuals, include:

- **right to erasure; [Article 17]**
- **right to data portability; [Article 20]**
- **right to object to processing. [Article 21]**

Accountability

- Implement appropriate technical and organisational measures to ensure compliance [Article 24]
- Data protection by design and by default [Article 25]
- Conduct Data Protection Impact Assessment [Article 35]
- Designate Data Protection Officer [Article 37]

Cross-border transfer

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

- **transfer to countries with 'adequate' level of data protection;**
- **use of 'standard contract clauses' or 'binding corporate rules';**
- **use of approved codes of conduct or certification.**

[Articles 44-47]

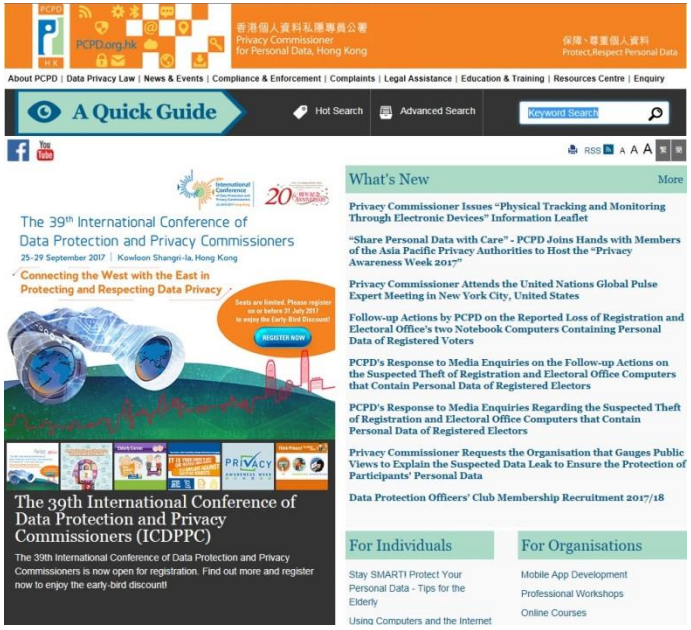
Sanctions

Maximum administrative fine:

- **€10 million or 2% of global annual turnover for less serious contravention, like failure to make data breach notification, appoint data protection officer, or conduct data protection impact assessment;**
- **€20 million or 4% of global annual turnover for more serious contravention, like processing not under a lawful basis, failure to comply with individuals request to erasure.**

[Article 83]

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

39th International Conference of Data Protection and Privacy Commissioners

Stay tuned for updates on
www.privacyconference2017.org

Thank You!