香港中小型律師行協會
18.04.2018

緊貼世界資料保障趨勢

黃繼兒大律師
香港個人資料私隱專員

香港資料保障領域上的最新發展

昔日公佈揀選物業抽籤結果的做法 (1998)

A3 星島日報 一九九八年十一月五日 星期四

敬請留意！

明日公開發售共188個單位

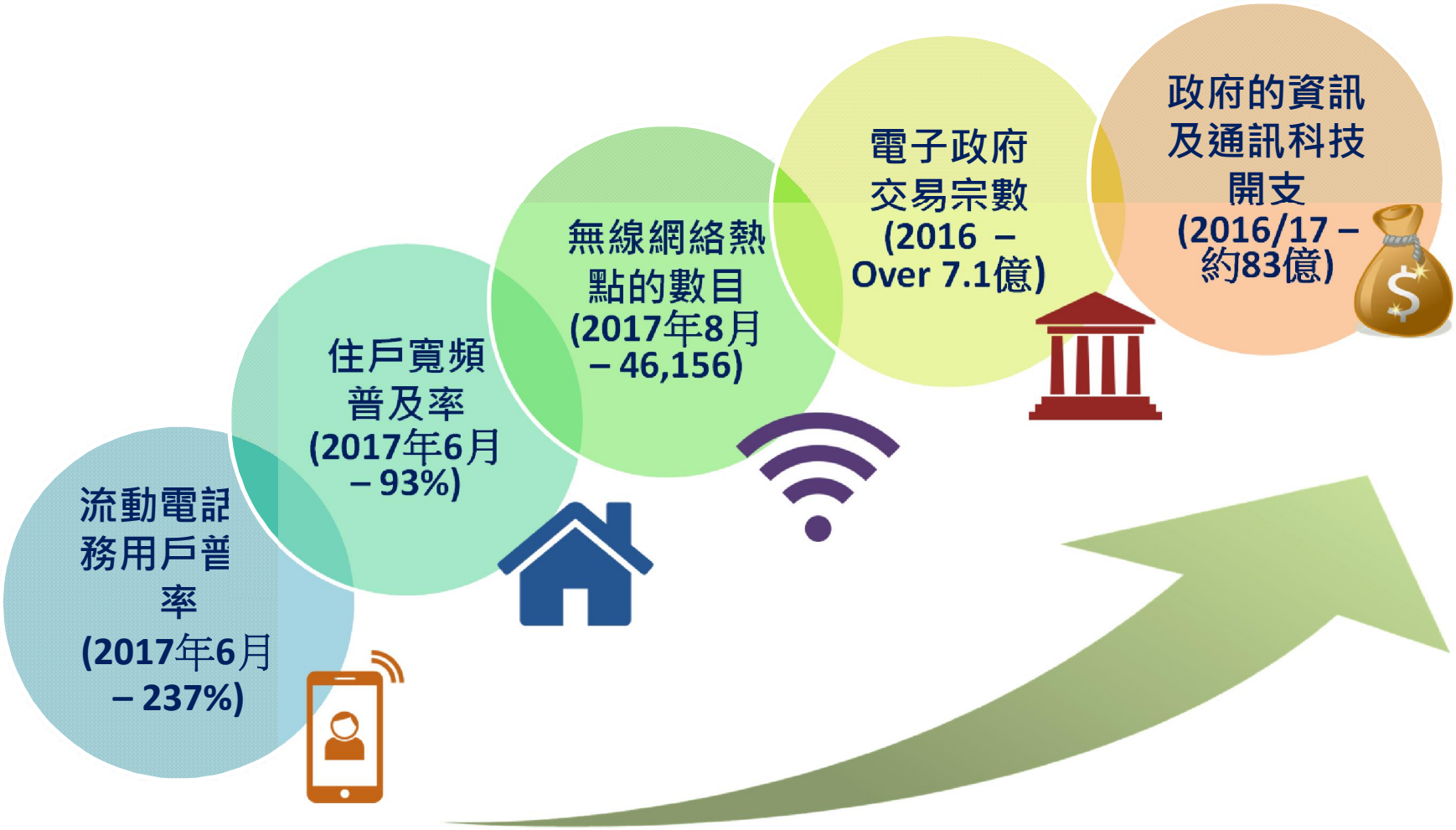
港麗豪園
WATERFRONT SOUTH

由電腦抽籤排列揀樓次序之號碼

申請表號碼	揀樓次序	身份證號碼／商業登記證號碼
SA0808	00764	D670151(6)
SA0809	00701	D394775(1)
SA0810	00475	D433676(4)
SA0811	00559	K185965(A)
SA0812	00153	D525178(9)
SA0813	00871	G285170(8)
SA0814	00891	G080280(7)

香港身份證號碼

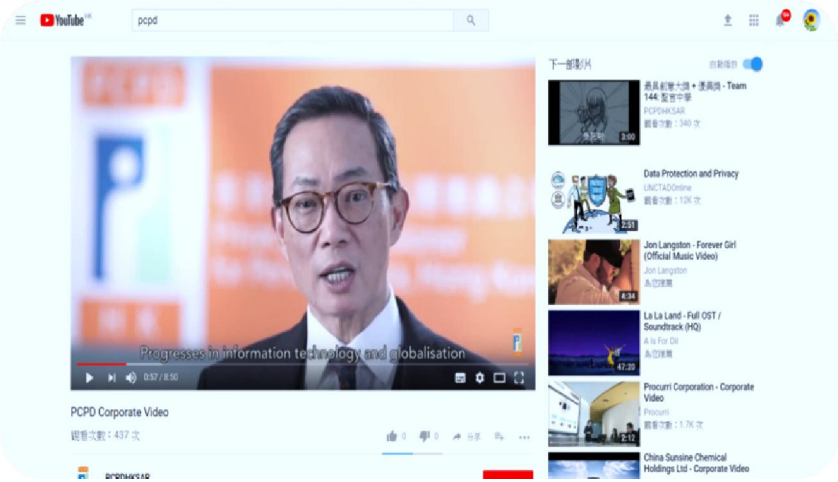
數碼化香港



資料來源: 香港政府「數碼 21」資訊科技策略

香港的數碼熱潮

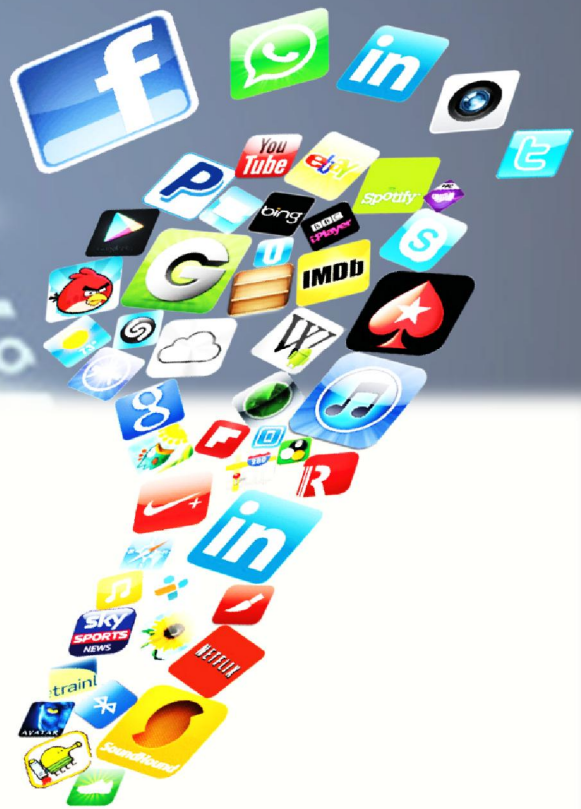
双11来了
2013.11.11 coming soon
不吃不喝买到爽
我来唱
COME ON!
双十一当天
折后再减100元
新品!大牌!
2折起
家装家电



pcpd
Progresses in information technology and globalisation
PCPD Corporate Video
Data Protection and Privacy
Jon Langston - Forever Girl (Official Music Video)
La La Land - Full OST / Soundtrack (HQ)
Procurri Corporation - Corporate Video
China Sunsine Chemical Holdings Ltd - Corporate Video

YAHOO! 拍賣
刊登任何分類都係
立即刊登
全場刊登
刊登任何分類都係
立即刊登
重要消息!
請注意:
Yahoo拍賣平台
「拍賣商店」及「廣告項目」
最新運作公告。
詳情按此

數碼腳印



The Standard

Facebook宣稱在香港擁有500萬用户

Facebook claims 5 million monthly users in HK

Wednesday, September 28, 2016

Facebook announced it has 5 million monthly active users, of with 4.6 million are mobile monthly active users in Hong Kong.

According to the company it also has more than 4 million businesses in world that advertise on Facebook, with more than 70 percent outside of the United States.

大數據、人工智能、物聯網及私隱

內地光棍節

2017天猫双11全球狂欢节
天猫双11全球狂欢节
GLOBAL SHOPPING FESTIVAL 2017
2017.11.11 24:00:00
¥168,269,635,159
$25,386,927,848
Total GMV in USD
无线成交占比
GMV from Mobile
90%
11.11

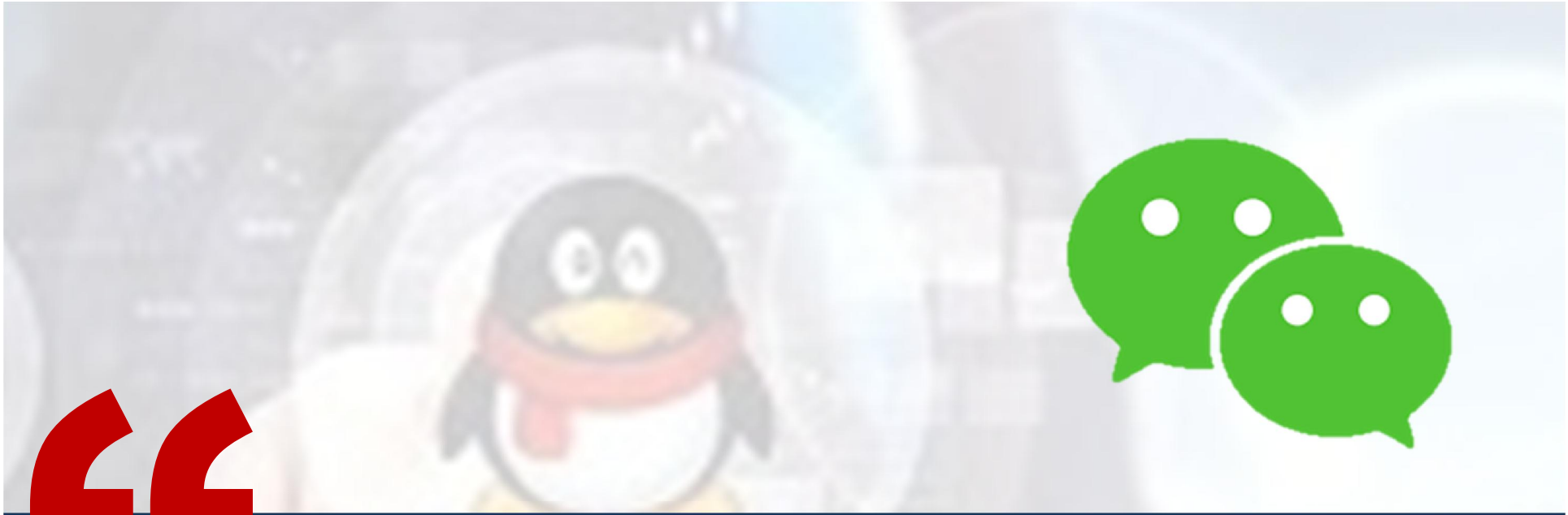
“微信 與 乞討”

金融科技

Pay
支付宝
ALIPAY
口碑
koubei
有优惠，有口碑
本店推荐使用
微信支付
UnionPay
银联
Quick
闪付Pass
欢迎使用云闪付
一挥即付
欢迎使用
禁止外带食物

馬雲金句

我們是通過賣東西收集數據，數據是阿里最值錢的財富。



“我們在馬化騰的眼裏全是裸體的

陶冬(瑞信亞太區私人銀行董事總經理兼大中華區副主席)

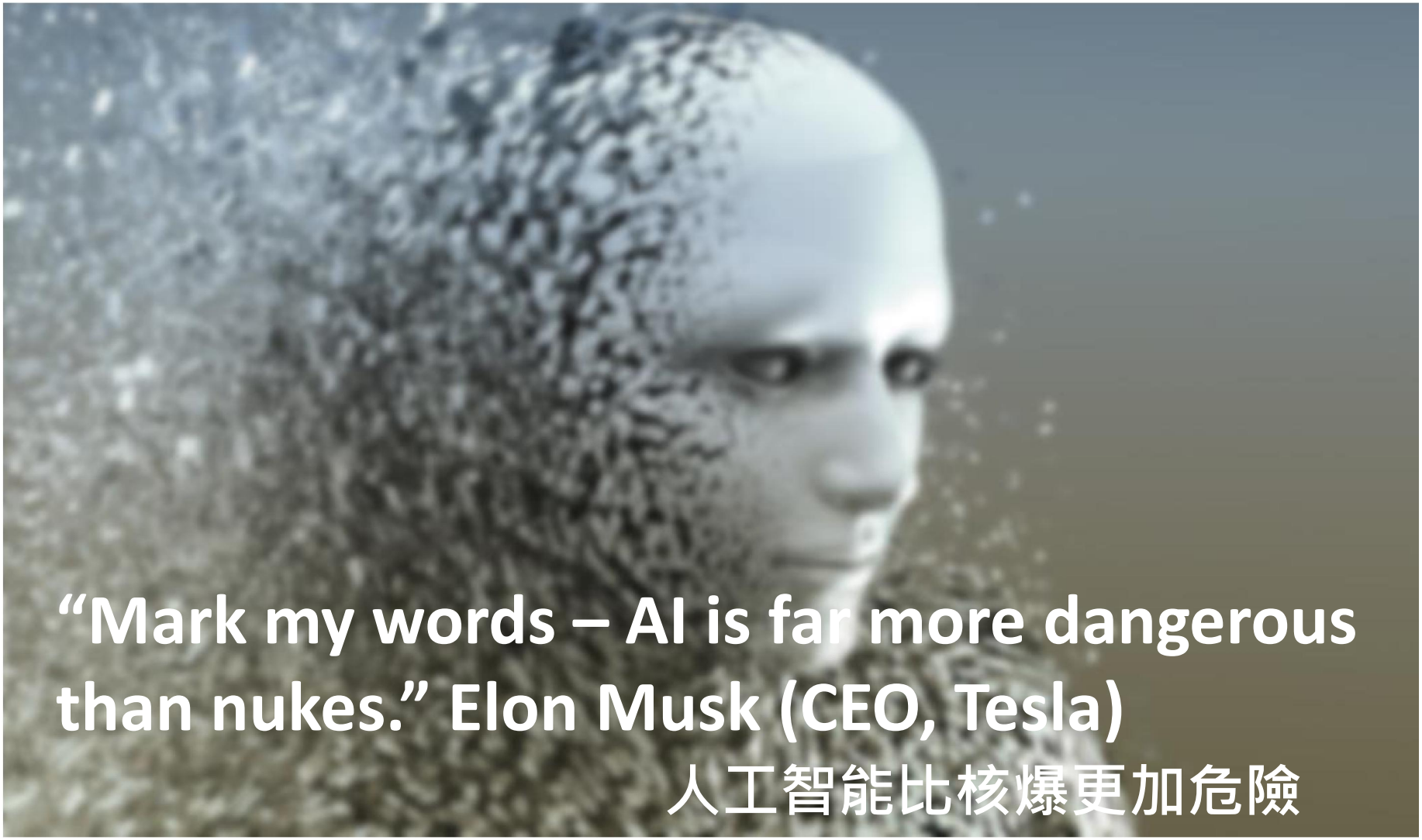
大數據

大規模收集、處理、整合及匯集非結構性的資料

大數據分析

"Information is the oil of the 21st century, and analytics is the combustion engine."
資料是21世紀的石油
數據演算則為燃燒引擎
– Peter Sondergaard, Senior Vice President, Gartner Research.

人工智能


“Mark my words – AI is far more dangerous than nukes.” Elon Musk (CEO, Tesla)
人工智能比核爆更加危險

物聯網

Wi-Fi 連通城市

智能運輸系統
及交通管理

數碼個人身分
eID

大數據分析

金融科技

香港智慧城市

智慧旅遊

多功能智慧燈柱

Hong Kong
Smart City

開放數據

數碼支付

來源：創科局及政府資訊科技總監辦公室 – 香港智慧城市藍圖

數據的風險和挑戰

(1) 資料被暗中收集

- 大量資料可從多種來源收集
- 線上及線下追踪
- 資料當事人可能未必察覺到其資料被收集和使用
- 通知及同意是否具意義?

(2) 超出資料使用的預期

- 企業可能會對看起來平平無奇的數據作出分析，並從中推斷出用戶不想公開的敏感資料
- 相互關係(並非因果關係)
- 用戶會對預測感到驚訝

(2) 超出資料使用的預期

- 研究員利用算式分析 “likes” 以推論敏感的個人資料包括宗教、政治取向、種族及性取向

(3) 身份重新識辨

- 匿名化的資料可藉由推測資料之間的關係或連結而被還原

(4) 個人概況彙編會否構成不公平及歧視？

- 個人概況彙編以推算或預測個人的喜好、健康狀況、工作表現、信用度、犯罪傾向等...

(4) 個人概況彙編會否構成不公平及歧視？

- 信貸機構基於其他客人與借款人在同一商戶購物時的不良還款紀錄而下調借款人的信貸額
- 是否公平?

(4) 個人概況彙編會否構成不公平及歧視？

- 運輸應用程度透過建立個人資料檔案拒絕向疑似執法人員的客人提供服務

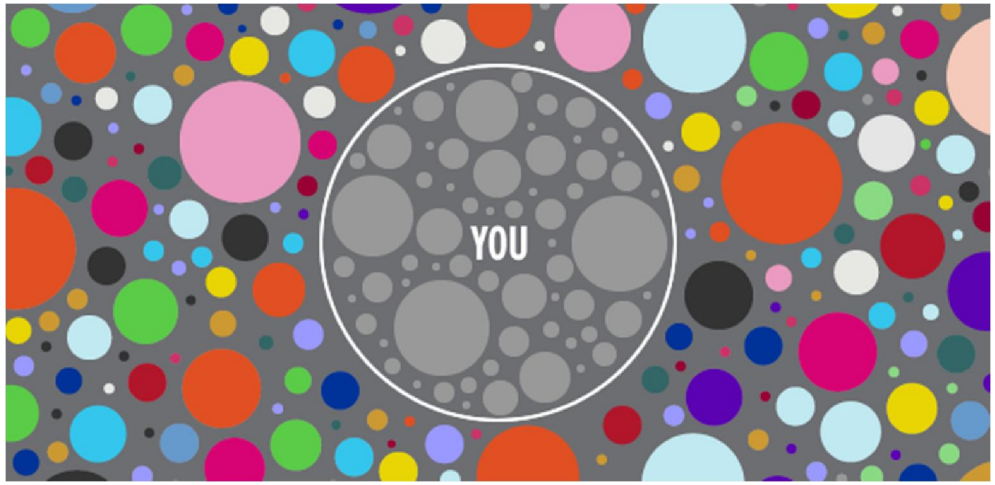
(5) 難以預測

- 自我演化
- 不遵循工程師的邏輯
- DeepMind's 的人工智能只需以極少的人力協助，便學會了49個經典視頻遊戲

(6) 透明度

- 有機會無法述明收集資料目的
- 低透明度
- 黑箱算法，不透明及複雜

(7) 過濾氣泡效應



- 訊息供給及影片推薦變得異常個人化
- 個人化資料過濾

(8) 被大數據及人工智能控制

- 人們被大數據及人工智能控制
- 失去自主進程
- 極權社會

以私隱為本的解決方法

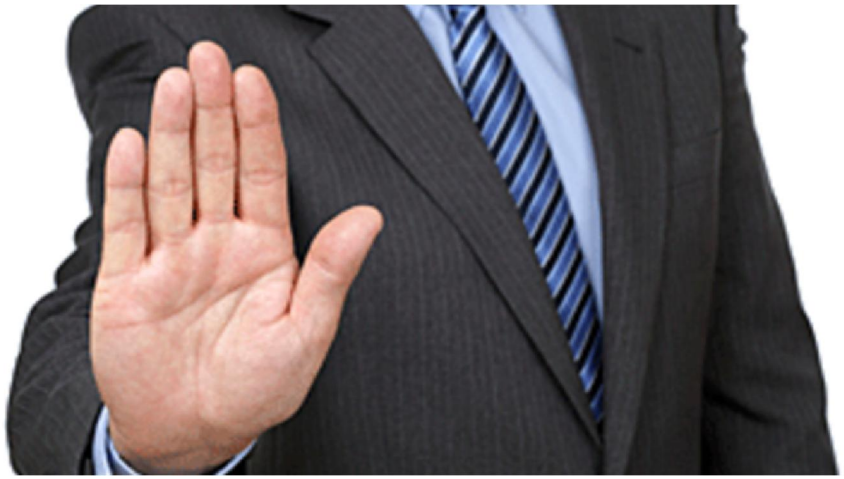
問責

- 保障、尊重個人資料
- 管理層孕育及推動尊重私隱
- 採取措施保障私隱
- 實行私隱管理系統
- 貫徹私隱的設計及預設私隱模式

透明度

- 2 “Ts” ： 透明度及信任
- 透明度可提升信任
- 解釋收集哪些資料及使用目的
- 解釋決定背後的邏輯及原因

具意義的選擇



- 准許當事人反對個人概況彙編
- 准許當事人反對對其有重大影響的決定

保障、尊重個人資料

- 《私隱條例》是科技中立，原則性的法例
- 平衡私隱及資訊自由流通
- 當事人獲告知收集及使用資料的目的及取得有意義的同意

簡介歐盟的《通用數據保障條例 》及其與《個人資料(私隱)條例》的比較

六項保障資料原則

6 保障資料原則 Data Protection Principles

PCPD.org.hk

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

PCPD HK

PCPD.org.hk

est.1996

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

六項保障資料原則

DPP1 – 收集

✓不過量

✓ 合法及公平

✓充份的通知

DPP2 – 準確性及保留時間

✓ 使用前確保資料準確

✓ 完成收集資料目的後銷毀資料

DPP3 – 使用

✓ 沒有資料當事人的同意，個人資料不可用於新目的

六項保障資料原則

DPP4 –
保安

✓ 採取切實可行的步驟避免資料外洩

DPP5 –
公開及透明

✓須具有私隱政策及常規

DPP6 –
查閱及改正

✓容許資料當事人查閱及改正資料

個案分享

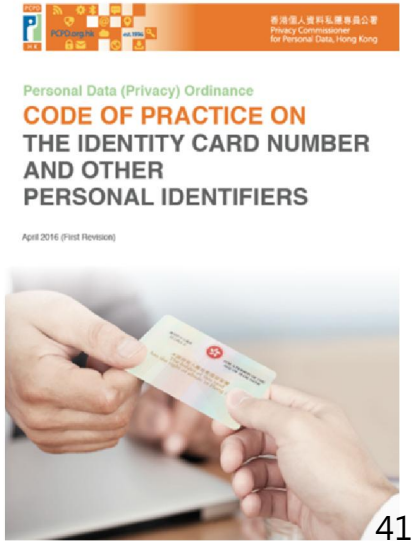
個案一：收集非賬戶持有人的身份證明文件號碼

- 投訴人(非賬戶持有人)到銀行將$500港元紙幣兑換為5張$100港元紙幣
- 櫃檯職員根據銀行政策記錄他的姓名及香港身份證號碼
- 沒有表面證據顯示涉及洗錢或恐怖分子資金籌集，加上交易金額不高

個案分享

- 《身份證號碼及其他身份代號實務守則》
  - 第 2.2.1 段 – 應容許使用其他身份代號辯識，如護照號碼
  - 第 2.3.1 段 – 除非根據法定條文而獲授權，否則不可收取身份證號碼

- 私隱專員認為銀行違反守則及第1原則



個案分享

個案二：保險公司無限期地保留不成功投保人士的個人資料

- 保險公司提供的原因
  - ~ 保留賬簿的法律規定
  - ~ 監管機構的指引及通告
  - ~ 可能的訴訟、查詢及投訴
  - ~ 與日後的申請作比對

個案分享

- 私隱專員的決定
  - ❖ 涉及金錢交易 – 7年
  - ❖ 不涉及金錢交易 – 2年
  - ❖ 除非涉及特別情況

- 保險公司遵從專員的執行通知，銷毀超過 7,000份紀錄

近期的網絡保安事故

source: https://goo.gl/oY6ArS

港聞

【縱橫遊翻版】入侵大航金怡數據庫索比特幣　數萬客戶資料外洩

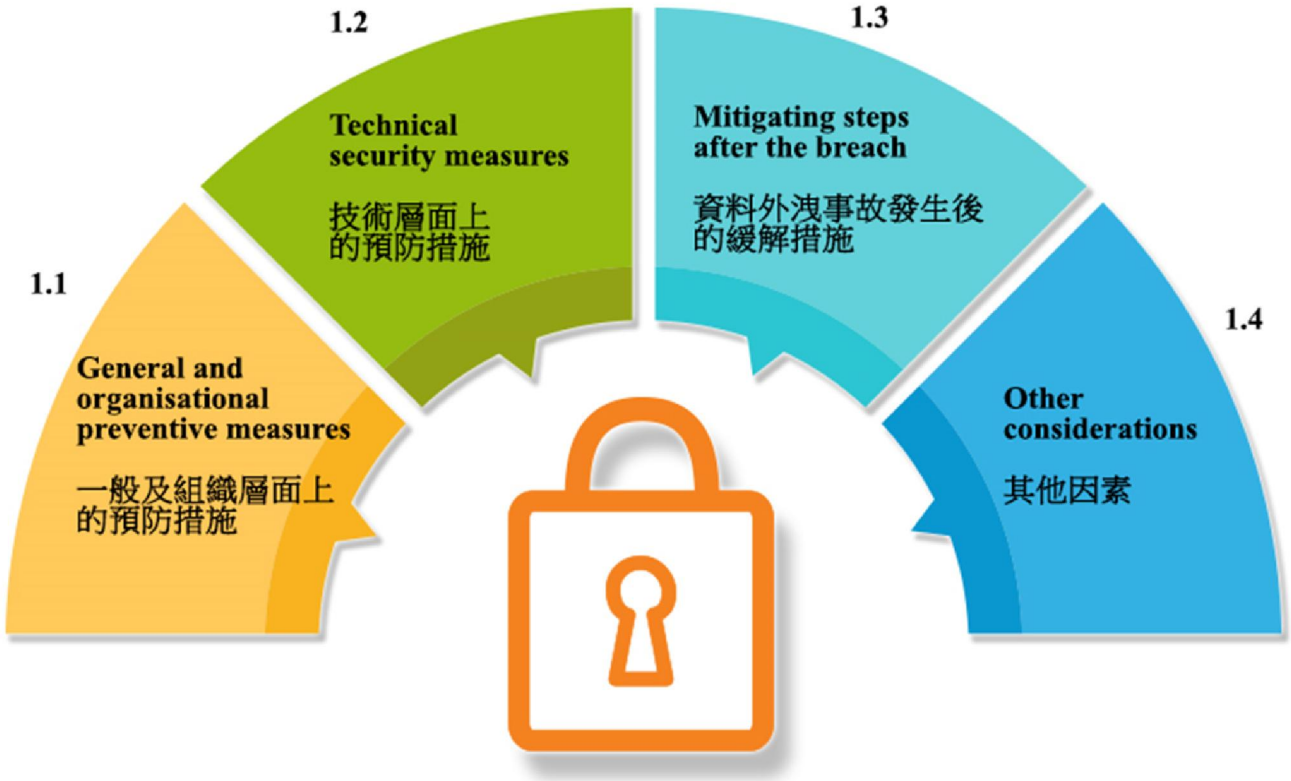
撰文：鄭詠中　蔡正邦　林振華　發佈日期：2018-01-04 15:38　最後更新日期：2018-01-05 00:30

讚好 25 分享

source: https://goo.gl/9sSQHN

source: https://goo.gl/1ZVttD

何謂「切實可行的步驟」？



DPP4 & Data Security

保障資料第4原則及資料保安

何謂「切實可行的步驟」？

在企業管治方面貫徹執行個人資料私隱保障，
涵蓋業務常規、操作程序、政策、培訓等

有整全的檢討及監察程序，
建立健全的私隱保障基建

一般及組織層面上的預防措施

公開和具透明度的
資訊私隱政策和常規

由管理層開始，
從上而下推

何謂「切實可行的步驟」？

技術層面上的預防措施

硬件方面的保安工作，如資訊系統、網絡基礎設施等

保安系統的定期審視政策和程序

在進入系統、資料傳送和保存方面的保安措施和步驟，以及採用國際間接受的準則和技術，如轉為亂碼 (hashed)、加密等

何謂「切實可行的步驟」？

何謂「切實可行的步驟」？

其他因素

- 資料使用者的規模、性質及資源
- 受影響人士可能遭受的不利後果
- 資料使用者的業務或經營模式的複雜性
- 個人資料的數量及敏感度

豁免

S.51A - 執行司法職能
S.52 - 家居用途
S.53 - 僱傭- 職工策劃
S.54 - 僱傭- 過渡性條文
S.55 - 有關程序
S.56 - 個人評介
S.57 - 關於香港保安等
S.58 - 罪行

豁免

S.58A - 《截取通訊及監察條例》所指的受保護成果及有關紀錄
S.59 - 健康
S.59A - 未成年人的照顧及監護
S.60 - 法律專業保密權
S.60A - 導致自己入罪
S.60B - 法律程序等
S.61 - 新聞

豁免

S.62 - 統計及研究
S.63 - 第18(1)(a)條的豁免
S.63A - 人類胚胎等
S.63B - 盡職審查
S.63C - 危急處境
S.63D - 轉移紀錄予政府檔案處

直接促銷

直接促銷的新規管機制

- 直接促銷的新規管機制於2013年4月1日起正式生效

- 「直接促銷方法」指藉郵件、圖文傳真、電子郵件或其他形式的傳訊，向指名特定人士送交資訊或貨品；或以特定人士為致電對象的電話通話。

直接促銷的條文要求

擬用客戶個人資料作直銷用途或轉交另他人作直銷用途

資料使用者

通知

資料當事人

同意

提交個人資料

提供「訂明資訊」及回應途徑，讓資料當事人選擇同意個人資料被用作直銷 通知必須清楚易明	同意必須自願和清晰作出

直接促銷的條文要求

- 如當事人表示拒絕再接收有關的直銷資料，資料使用者須在不收費的情況下照辦

- 資料使用者如違反關於直接促銷的規定，屬刑事罪行

與直銷有關的定罪個案

時期	個案	罰則
2015年9月 (屬首宗定罪個案)	• 一間電訊公司沒有依從客戶的拒收直銷訊息要求	被判罰款三萬元
2015年9月	• 一間儲存服務供應商在直接促銷前未有採取指明行動通知當事人及取得其同意	被判罰款一萬元
2015年11月	• 一間體檢服務公司沒有依從客戶的拒收直銷訊息要求	被判罰款一萬元

與直銷有關的定罪個案

時期	個案	罰則
2015年12月	• 一名人士在未有採取指明行動通知當事人及取得其同意前,將個人資料提供予第三者作直接促銷	被判罰款五千元
2016年4月	• 一名保險代理人在直接促銷前未有採取指明行動通知當事人及取得其同意；及 • 在首次使用個人資料作直接促銷時，未有告知資料當事人他有權提出拒收直銷訊息要求	被判罰每項控罪各80小時社會服務令

與直銷有關的定罪個案

時期	個案	罰則
2016年5月	• 一間銷售推廣公司在直接促銷前未有採取指明行動通知客戶及取得其同意；及 • 沒有依從拒收直銷訊息要求	每項控罪分別被判 罰款八千元
2016年12月	• 一間鐘錶公司在直接促銷前未有採取指明行動通知當事人及取得其同意；及 • 在首次使用個人資料作直接促銷時，未有告知資料當事人他有權提出拒收直銷訊息要求	每項控罪分別被判 罰款八千元

與直銷有關的定罪個案

時期	個案	罰則
2017年1月	• 一間銀行沒有依從客戶的拒收直銷訊息要求	被判罰款一萬元
2017年11月	• 一名理財顧問在直接促銷前未有採取指明行動通知當事人及取得其同意；及 • 在首次使用個人資料作直接促銷時，未有告知資料當事人他有權提出拒收直銷訊息要求	每項控罪分別被判 罰款一萬元
2017年12月	• 一間健身公司沒有依從客戶的拒收直銷訊息要求	被判罰款七千元
2018年1月	• 一間超級市場在未獲資料當事人同意下，將其個人資料使用於直接促銷	被判罰款三千元

跨境資料轉移

除非符合條例列明的6種情況，條例第33條禁止轉移個人資料至香港以外地區

立法目的:
確保轉移香港以外的個人資料獲得相當於在條例下所提供的保障

跨境資料轉移

條例下「轉移」指：

將個人資料由香港轉移至境外

在兩個其他司法區之間轉移個人資料，該轉移是由香港的資料使用者所控制

跨境資料轉移

除非符合以下其中一項條件，資料使用者不得將個人資料轉移至香港以外地區:-

第33(2)(a)條	• 符合白名單列出的其中一個司法管轄區 (該地區實施的有關個人資料保障法律，與條例大致上相似)
第33(2)(b)條	• 資料使用者自行評估該地方有與條例大體上相似或達致與條例的目的相同的目的之法律正在生效
第33(2)(c)條	• 資料當事人已以書面同意有關轉移

跨境資料轉移

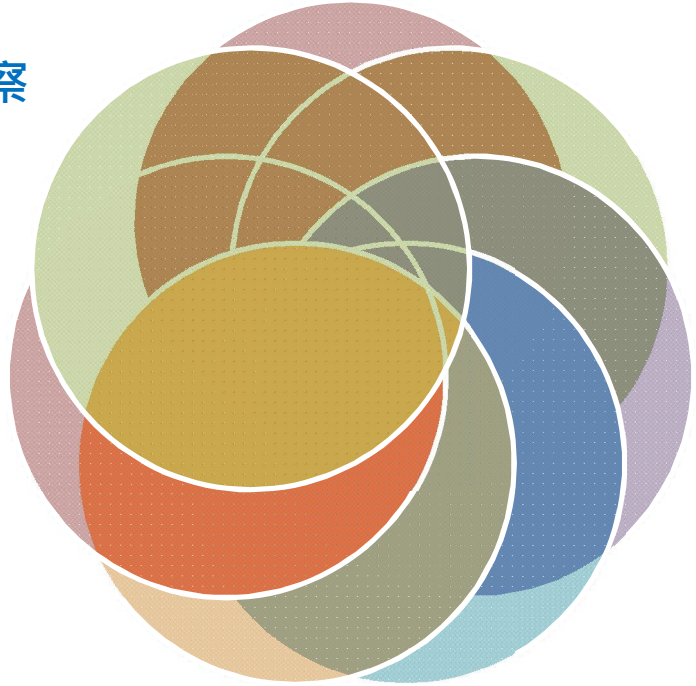
第33(2)(d)條	• 避免針對資料當事人的不利行動或減輕該等行動
第33(2)(e)條	• 條例第8部份下的豁免保障資料第3原則的條款適用
第33(2)(f)條	• 資料使用者已採取所有合理措施及作出所有相應努力確保資料被轉移後的處理不違反條例規定（「克盡職責的規定」）

跨境資料轉移的實用提示

檢討資料轉移安排

進行定期審核及視察

控制涉及無意或不必要的
跨境資料流動活動



保持透明度

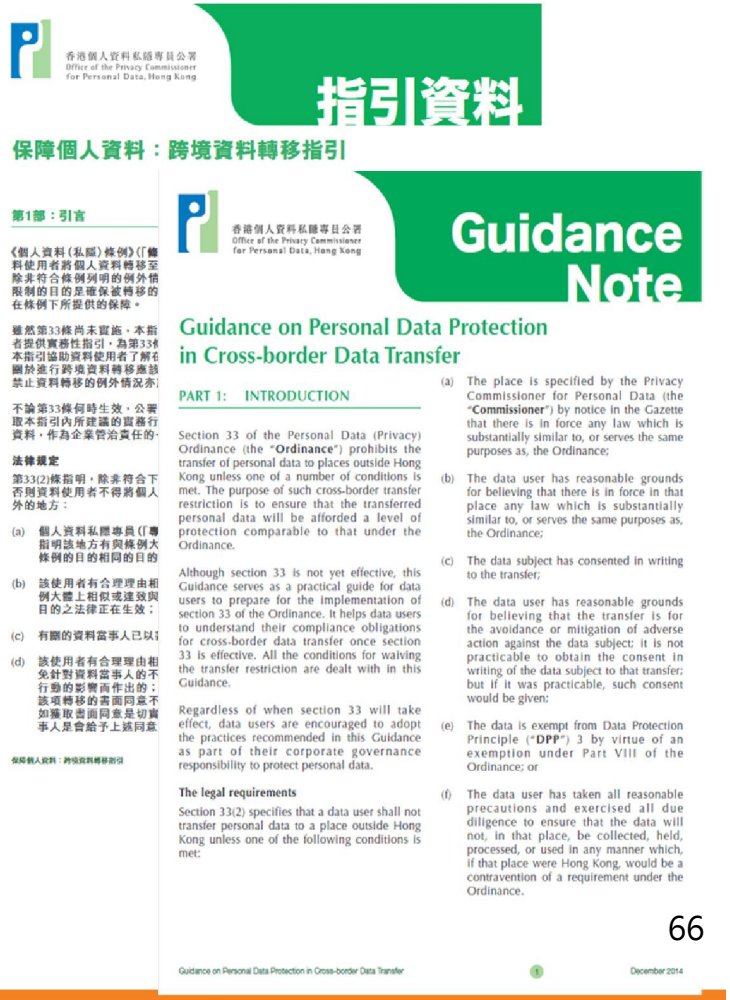
檢查白名單 (當正式生效時)

備存個人資料庫存

採取更多措施提高保障

保障個人資料: 跨境資料轉移指引

- 雖然第33條尚未實施，有關指引旨在向資料使用者提供實務性指引，以協助他們:
  - 了解應該遵守的義務;
  - 採取指引內所建議的實務行事方式以保障個人資料，作為企業管治責任的一部份;
  - 考慮在資料轉移協議內改編/ 採納指引內列出之「建議範本條文」



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

指引資料

保障個人資料：跨境資料轉移指引

第1部：引言

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 Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

The legal requirements

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

(a) The place is specified by the Privacy Commissioner for Personal Data (the "**Commissioner**") by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(c) The data subject has consented in writing to the transfer;

(d) The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;

(e) The data is exempt from Data Protection Principle ("**DPP**") 3 by virtue of an exemption under Part VIII of the Ordinance; or

(f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

Guidance on Personal Data Protection in Cross-border Data Transfer 1 December 2014

其他與資料轉移有關的保障資料原則

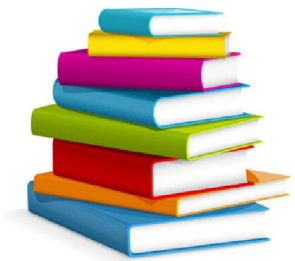
如資料使用者聘用資料處理者處理個人資料，須透過合約規範或其他方法 -

原則 2(3)

- 防止轉移予資料處理者處理的個人資料被保存超過所需時間

原則 4(2)

- 防止轉移予資料處理者處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用



《私隱條例 》– 《通用數據保障條例》比較研究

背景

- 使《私隱條例》能緊貼全球私隱法規的發展
- 評估《通用數據保障條例》對企業(尤其跨國企業)的影響
- 法例框架比較便利資訊自由流通及促進商貿活動

《私隱條例 》– 《通用數據保障條例》比較研究

歐盟的《通用數據保障條例》及香港的《個人資料(私隱)條例》 的主要分別:

	歐盟	香港
應用	資料處理者或控制者： • 在歐盟設立公司，或 • 在歐盟以外設立公司，提供貨品或服務，或監察歐盟人士的行為。 [第3條]	資料使用者指獨自或聯同其他人或與其他人在/從香港共同控制該資料的收集、持有、處理或使用的人 [第2(1)條]

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
個人資料	「個人資料」為： • 任何有關一名已被識別或可被識別的自然人的資訊；而一名可被識別的自然人是指可直接或間接地被識別的。 • 可被明確地識別身份的個人資料的例子延伸至包括位置資料及網上識別符。[第4(1)條]	「個人資料」為指符合以下說明的任何資料： • 直接或間接與一名在世的個人有關的； • 從該資料直接或間接地確定有關的個人的身分是切實可行的；及 • 該資料的存在形式令予以查閱及處理均是切實可行的。 [第2(1)條]

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
問責與管治	以風險為本；資料控制者須： • 實施技術性及機構性措施以確保循規 [第24條]； • 採取預設貫徹私隱的設計及預設 [第25條]； • 為高風險的處理活動進行資料保障評估 [第35條]；及 • （若屬某些類型的機構）委任保障資料主任 [第37條]。	沒有明確列明問責原則及相關的私隱管理措施。 私隱專員倡議採納私隱管理系統以顯示問責原則。委任保障資料主任及進行私隱影響評估是為達致問責而建議的良好行事方式。

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
敏感個人資料	敏感個人資料的類別被擴大。 只在特定情況下才容許處理敏感個人資料。 [第9條]	沒有以任何目的區分敏感及非敏感個人資料。

《私隱條例 》– 《通用數據保障條例》比較研究

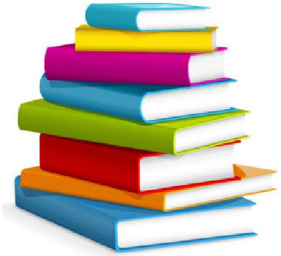
	歐盟	香港
同意	同意必須是 • 自願給予、具體及知情； • 以聲明或清晰明確的行動不含糊地指明資料當事人的意願，表示同意處理其個人資料[第4(1)條]；及 • 由16歲（或13歲）以下兒童給予的同意須有家長授權。	同意不是收集個人資料的先決條件，除非個人資料是用於新目的。[保障資料第1及3原則] 在其他情況，若須徵求同意，同意是指自願作出的明示同意。 沒有規定需要家長同意。

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
通報資料外洩事故	資料控制者須向監管機構通報資料外洩事故，不可不當地延誤（例外情況適用）。如事故很可能對資料當事人的權利及利益造成高度風險，資料控制者須通知受影響的資料當事人，除非例外情況適用。[第33-34條]	沒有強制性規定，但考慮到所有持份者包括資料使用者 / 控制者 / 當事人的利益，應通報私隱專員（及資料當事人，如適用）。

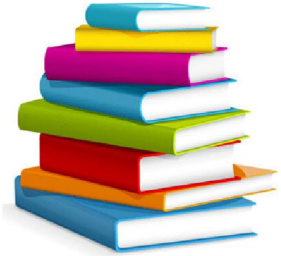
《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
資料處理者	資料處理者負上額外責任以保存處理記錄、確保處理安全、通報資料外洩事故、委任保障資料主任等。[第30, 32-33, 37條]	資料處理者不是直接受規管。[第2(12)條] 資料使用者須採取合約或其他方式以確保資料處理者循規。[保障資料第2(3) 及4(2)原則]



《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
資料當事人新增及提升的權利	• 就資料處理獲通知的權利 [第13-14條] • 刪除個人資料權（「被遺忘權」）[第17條]	• 對資料使用者 / 控制者就通知的要求相對未有如此廣泛 • 沒有刪除權，但資料不得保留超過所需的時間 [第26條及保障資料第2(2)原則]



《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
資料當事人新增及提升的權利 (續)	• 限制處理及資料可攜權 [第18及20條] • 反對處理（包括個人概況彙編）的權利 [第21條]	• 就資料處理沒有限制及沒有資料可攜權，但需遵從查閱資料及改正資料的權利 [保障資料第6原則，第5部] • 沒有反對處理資料的權利（包括個人概況彙編），但可拒絕直銷活動 [第35G及35L條]，而《條例》中亦有條文規管資料核對程序 [第30-31條]

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
認證、印章及行為守則	設有明確認可機制以證明資料控制者及處理者合規。[第42條]	沒有正式的認證或私隱印章機制以證明合規。私隱專員在諮詢後可核准實務守則。[第12條]

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
司法管轄區之間的資料轉移	述明認證及依從核准的行為守則 作為其中一項資料轉移的法律基礎。[第46條]	認證制度及依從實務守則未有明確定為法律基礎。

《私隱條例 》– 《通用數據保障條例》比較研究

	歐盟	香港
懲罰	資料保障機構獲授權可判處資料控制者及處理者行政罰款。[第58條] 視乎違規的性質，罰款可達二千萬歐元或全球年度總營業額的4%。[第83條]	私隱專員沒有獲賦權施加行政罰款或刑罰。 私隱專員可向資料使用者送達執行通知，在完成司法程序後違法者可能被判罰。[第50條]

歐洲聯盟《通用數據保障條例 2016 》小冊子

www.pcpd.org.hk//tc_chi/resources_centre/publications/files/eugdpr_c.pdf

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

內地網絡安全法

- 於2017年6月1 日生效
- 不適用於香港

內地網絡安全法

適用範圍：

- 適用於國家境內建設，運營，維護和使用網絡以及網絡安全的監督管理 [第2條]
- 規管網絡運營者，即網絡的所有者，管理者和網絡服務提供者 [第76(3)條]
  - 不只限於科技公司，例如金融機構在其運營中使用計算機網絡的也是“網絡運營商”
- 保障個人信息

PCPD HK
PCPD.org.hk
est.1996
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

內地網絡安全法如何影響香港企業

除非

- 以香港為基地處理個人資料的企業受到個人資料私隱條例所監管，並非網絡安全法

便會

- 處理個人資料亦涉及建設、營運、維修或使用內地的網絡

- 處理個人資料將可能受到兩項法例所監管

PCPD HK
PCPD.org.hk
est.1996
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

內地網絡安全法與私隱條例的比較

收集及使用

內地網絡安全法	香港私隱條例
第41條 (收集及使用)	保障資料第1原則 (收集)
• 遵循合法、正當及必要的原則 • 取得當事人同意 • 不得收集與其提供的服務無關的個人信息 • 公開相關政策及措施 • 明示收集，使用信息的目的，方式和範圍不得違反法律，行政法規的規定和雙方的約定收集，使用個人信息	• 不需要同意 • 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。收集的資料是有實際需要的，而不超乎適度 • 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

內地網絡安全法與私隱條例的比較

收集及使用

內地網絡安全法	香港私隱條例
第42條 (披露)	保障資料第3原則 (使用, 包括轉移)
• 未經資料當事人同意，不得向他人提供個人信息。	• 除非得到資料當事人的訂明同意，個人資料不可用於新目的。

內地網絡安全法與私隱條例的比較

準確性、保留及刪除

內地網絡安全法	香港私隱條例
準確性	保障資料第2(1)原則) (準確性)
• 沒有明確條文要求 • 但第42條要求資料處理者不得篡改個人信息	• 採取切實可行的步驟以確保持有的個人資料準確無誤

內地網絡安全法與私隱條例的比較

準確性、保留及刪除

內地網絡安全法	香港私隱條例
保留	保障資料第2(2)原則及第26條 (保留及刪除)
• 沒有明確條文要求 • 但第21(3)條採取監測，記錄網絡運行狀態，網絡安全事件的技術措施並按照規定留存相關的網絡日誌不少於六個月;	• 採取切實可行的步驟以確保資料的保留時間不應超過達致原來目的的實際所需

內地網絡安全法與私隱條例的比較

資料保安及資料外洩通報

內地網絡安全法	香港私隱條例
第42條 (資料保安及通報)	保障資料第4原則 (資料保安)
• 應當採取技術措施和其他必要措施確保其收集的個人信息安全，防止信息洩露、毀損、丟失 • 在發生或者可能發生個人信息洩露時，應當立即採取補救措施，按照規定及時告知用戶並向有關主管部門報告	• 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 • 沒有強制性規定作出資料外洩通報

內地網絡安全法與私隱條例的比較

公開性及透明度

內地網絡安全法	香港私隱條例
• 對個人信息處理方面的政策和措施沒有一般的公開性及透明度的要求持開放和透明的一般要求 • 第41條只要求在收集和使用個人信息時披露相關政策和做法	保障資料第5原則 (公開性) • 資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途

內地網絡安全法與私隱條例的比較

查閱、改正及刪除

內地網絡安全法	香港私隱條例
• 資料當事人沒被賦予查閱其個人資料的權利	第18-25條及保障資料第6原則 (查閱及改正)
第43條 (改正及刪除) • 資料當事人如發現網絡運營者違反法律，行政法規的規定或者雙方的約定，有權要求網絡營運者: ▪ 改正其個人信息; 及 ▪ 刪除其個人信息	• 資料當事人可要求取得其個人資料的複本 (除豁免情況外) • 如資料當事人認為資料使用者所持有其個人資料不準確，可要求資料使用者作出改正 (除豁免情況外) • 資料當事人沒被賦予刪除其個人資料的權利，但資料使用者不可保留個人資料超過實際所需的時間 [第26條及保障資料第2(2)原則]

內地網絡安全法與私隱條例的比較

問責

內地網絡安全法	香港私隱條例
第40條 網絡運營者應當對其收集的用戶信息嚴格保密，並建立健全用戶信息保護制度	• 沒有資料使用者問責規定

如何孕育尊重個人資料私隱的企業文化

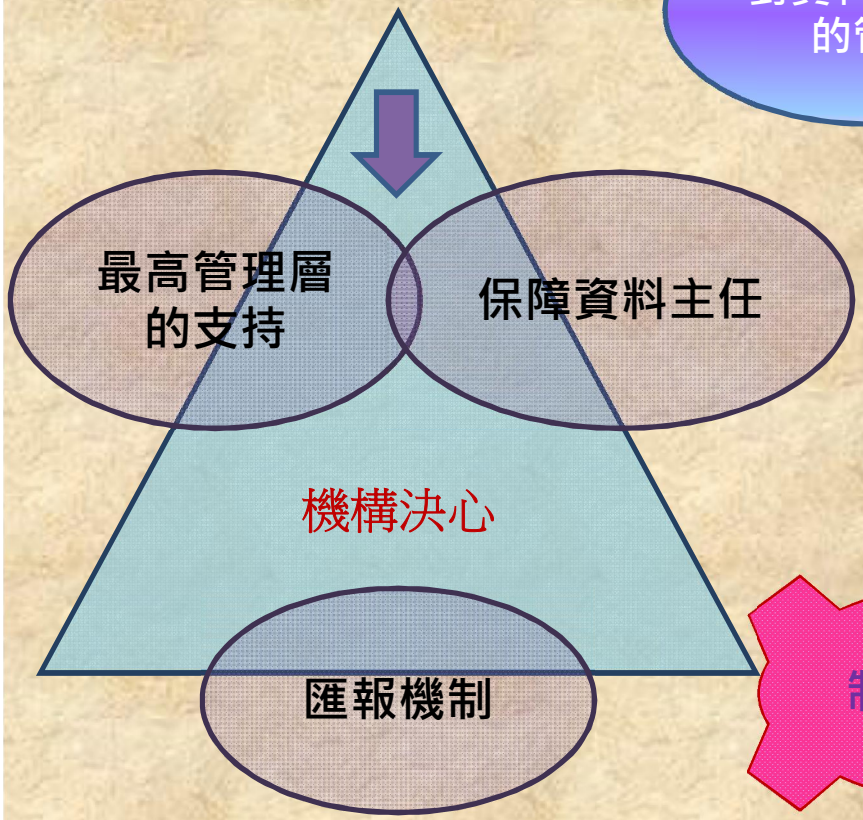
Privacy Management Programme

From Compliance to *Accountability*

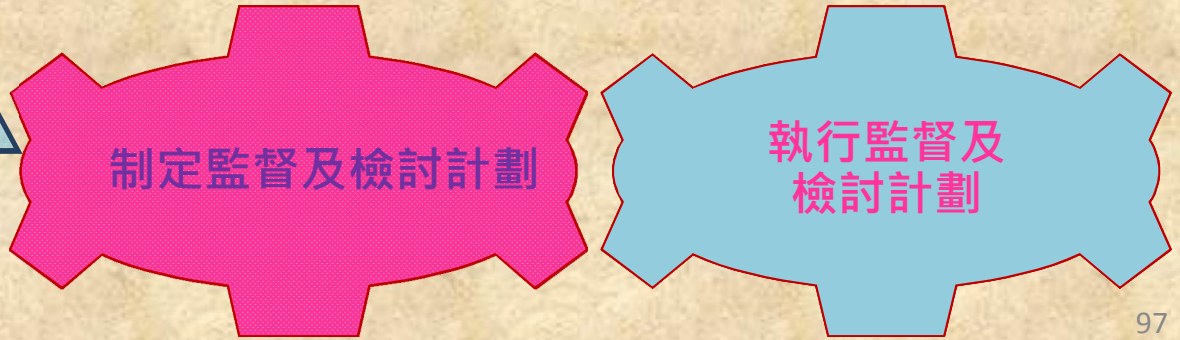
甚麼是私隱管理系統
模式轉變

符規方式	問責方式
• 被動	主動
• 消極	積極
• 補救	預防
• 以解決問題為本	以符合客戶期望為本
• 由合規部門處理	由最高管理層指派
• 符合法律的最低要求	建立商譽
• 由下而上	由上而下

私隱管理系統組件



持續評估及修訂



參與私隱管理系統

承諾機構

- ✓ 76個政府政策局及部門
- ✓ 25間保險公司
- ✓ 9間電訊公司
- ✓ 5間其他行業機構

政府就實施私隱管理系統的顧問項目

聘請外間顧問協助政府決策局及部門實施私隱管理系統

公署建議

私隱管理系統手冊
(今年內完成)

培訓

公署未來工作

為機構舉辦專業研習班

鼓勵資料使用者推行私隱管理系統

嘉獎

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

歐洲聯盟
《通用數據保障條例 2016 》
小冊子 – 中文版

歐洲聯盟
《通用數據保障條例 2016 》
小冊子 – 英文版

PCPD
HK

PCPD.org.hk

保障、尊重個人資料
Protect,Respect Personal Data