# 香港中小型律師行協會
# 2019年7月9日

# 如何應對數碼科技對私隱帶來的挑戰？


黃繼兒大律師
香港個人資料私隱專員

# 1

# 議題：數碼時代的資料私隱

# 1.1

# 2018年：資料外洩之年

# 2018全球逾十四億人資料被外洩

| 資料外洩事件涉及的公司 | 涉及數據數量 |
| --- | --- |
| 萬豪酒店 | 3.83億個用户 |
| Twitter (推特社交網站) | 3.3億個用户 |
| My Fitness Pal (食品及營養應用程式 ) | 1.5億個用户 |
| Facebook | 1.47億個用户 |
| Quora (問答網站) | 1億個用户 |
| Firebase （ Google旗下的開發平台 ） | 1億個用户 |
| My Heritage (憑藉DNA測試尋找祖先及家譜) | 9,200萬個用户 |
| Uber (出租車公司) | 5,700萬個賬户 |
| Ticket Fly (活動票務網站) | 2,700萬個賬户 |
| Google+ | 50萬個賬户 |
| 英國航空公司 | 38萬個賬户 |

港聞

國泰940萬乘客私隱外泄違兩私隱原則　遲半年公布未違規 (20:45

2019年6月6日星期四

上一篇　下一篇

# 國泰940萬乘客私隱外泄違兩私隱原則　遲半年公布未違規 (20:45)

讚好 1

圖片來源：明報

# 1.2 數碼科技之廣泛應用與挑戰

# 物聯網


金融科技
Pay
支付宝
ALIPAY
口碑
koubei
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.

# 數碼經濟中的私隱挑戰

- 資料壟斷者濫用主導地位
- 消費者缺乏控制權和真正的選擇

競爭

私隱

- 過度及隱蔽式的資料收集
- 敏感信息曝光
- 非預期，不公平/歧視性地使用資訊
- 沒有意義的同意

資料安全

- 黑客入侵
- 資料外洩

跨範疇和跨境問題

- 消費者保障
- 跨境資料流通

# 1.3 近年資料外洩事故之調查

# 選舉事務處遺失全港選民資料的手提電腦

- 背景：選舉事務處遺失兩部分別載有1,200名選舉委員會委員的姓名以及約378萬名地方選區選民的個人資料(包括姓名、地址及身份證號碼)
- 私隱專員意見:
  - 雖然事故中所涉及的個人資料已經多重加密，但處方應可避免因手提電腦遺失而引起社會對私隱問題產生憂慮
  - 因所聲稱提供查詢服務而備存全體選民資料,此舉帶來的效益與可能產生的風險不合符比例
  - 處方審批查詢系統時非常粗疏,蕭規曹隨,沒有按情況適時檢視或更新，違反資料保安原則

明報新聞網

# 黑客盜香港寬頻38萬客資料

**資料外洩事故**
**調查報告**

根據香港法例第 486 章《個人資料(私隱)條例》
第 48(2) 條發表

**國泰航空有限公司**

**及**

**港龍航空有限公司**

**未獲授權取覽或查閱乘客個人資料**

（中文譯本）
（本報告以英文撰寫。如中文譯本與英文報告有歧異，
概以英文為準）

**報告編號：R19 – 15281(c)**
**發表日期：2019 年 6 月 6 日**

港聞

國泰940萬乘客私隱外泄違兩私隱原則　遲半年公布未違規 (20:45

2019年6月6日星期四

上一篇　下一篇

# 國泰940萬乘客私隱外泄違兩私隱原則　遲半年公布未違規 (20:45)

讚好 1

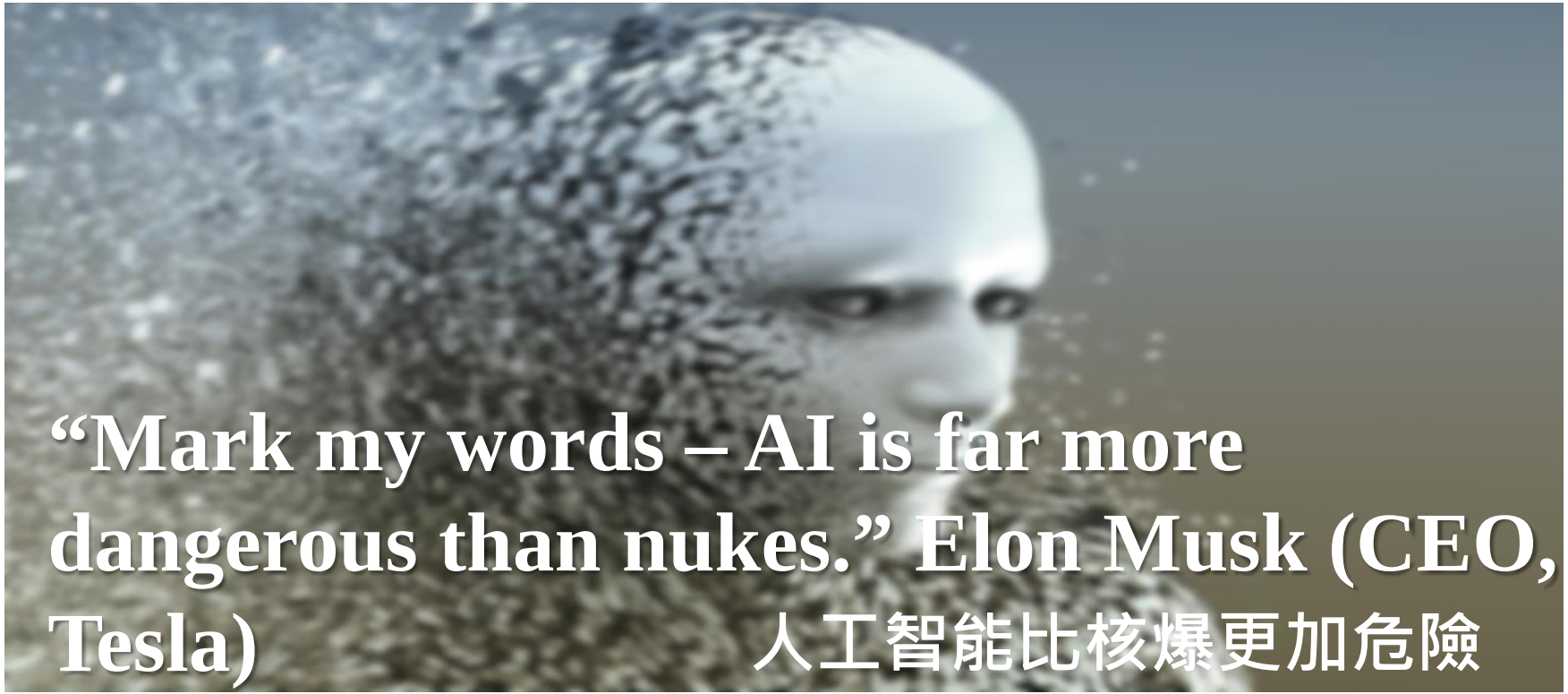
圖片來源：明報




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

# 1.4 人工智能的發展與私隱

# 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

# 數據風險和挑戰

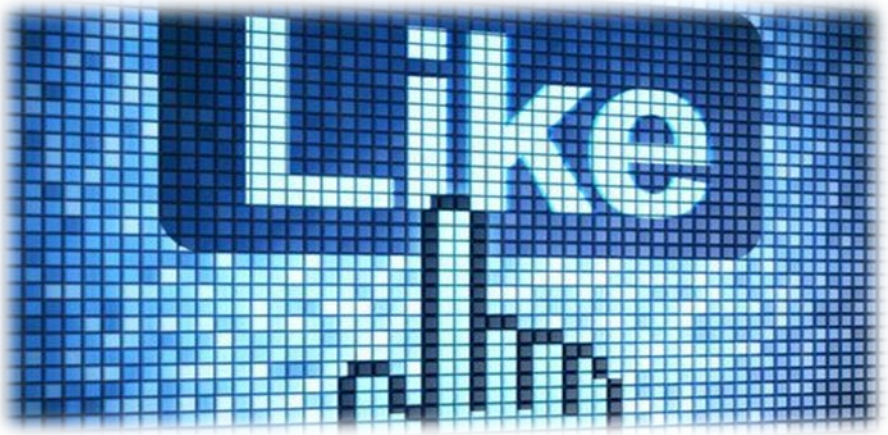
# (1) 資料被暗中收集

- 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

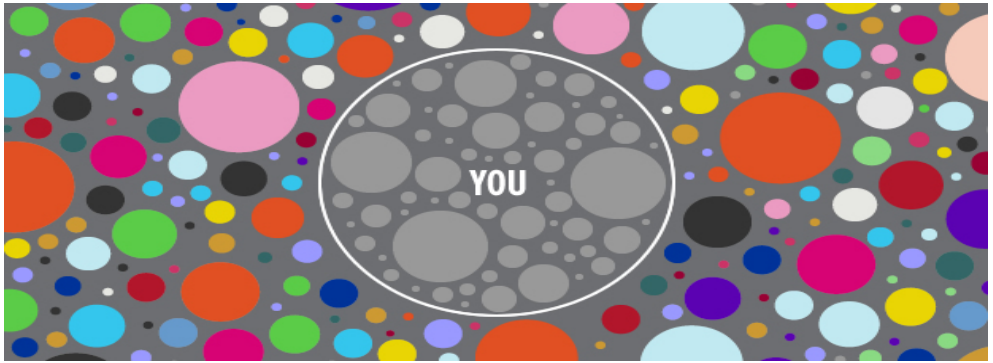
# (5) 難以預測


- 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

# 2 回應：法律與道德

# 2.1 全球私隱保障規範最新發展

# 2.1.1 法律與規則

# 資料保障格局概述

## 歐盟

- 《通用資料保障條例》於2018年5月25日生效
- 嚴格而全面的資料保障法

## 美國

- 聯邦級別沒有全面的資料保護法
- 較強的行業性法規(例如,健康資料信用資料)
- 所有州都有强制性資料外洩通報制度

## 亞洲

- 資料保障法規的數目正增加
- 一般參照歐盟的模式，但相對寬鬆

# GDPR 通用數據保障條例

對自己的個人資料有更多的**控制權**

適用於在歐盟營運的所有公司的**一套規則**

企業受益於**公平的競爭環境**

# GDPR 技術和數據自由流動

## GDPR 序言 6:

*"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. … Technology… should further facilitate the free flow of personal data … while ensuring a high level of the protection of personal data."*

# GDPR – 主要目標

***The digital information ecosystem farms people for their attention, ideas and data in exchange for so called 'free' services. …[The GDPR] aims to restore a sense of trust and control over what happens to our online lives.***

**Giovanni Buttarelli**,
European Data Protection Supervisor

Source:
https://edps.europa.eu/press-publications/press-news/blog/accept-and-continue-billions-are-clocking-digital-sweat-factories_en

# GDPR – 主要目標

*[The GDPR] is about **putting the rights of individuals first** and upgrading the EU data protection rules so that they are efficient and ready for the future.*

**Andrea Jelinek**,
Chair of the European Data Protection Board

Source:
https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en

# GDPR – 主要目標

***The GDPR gives consumers more control over their data. … But arguably the biggest change is around accountability. … The GDPR mandates organisations to put into place comprehensive but proportionate governance measures.***

**Elizabeth Denham**,
Information Commissioner of the UK

Source:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

# GDPR - 將控制權歸還給個人

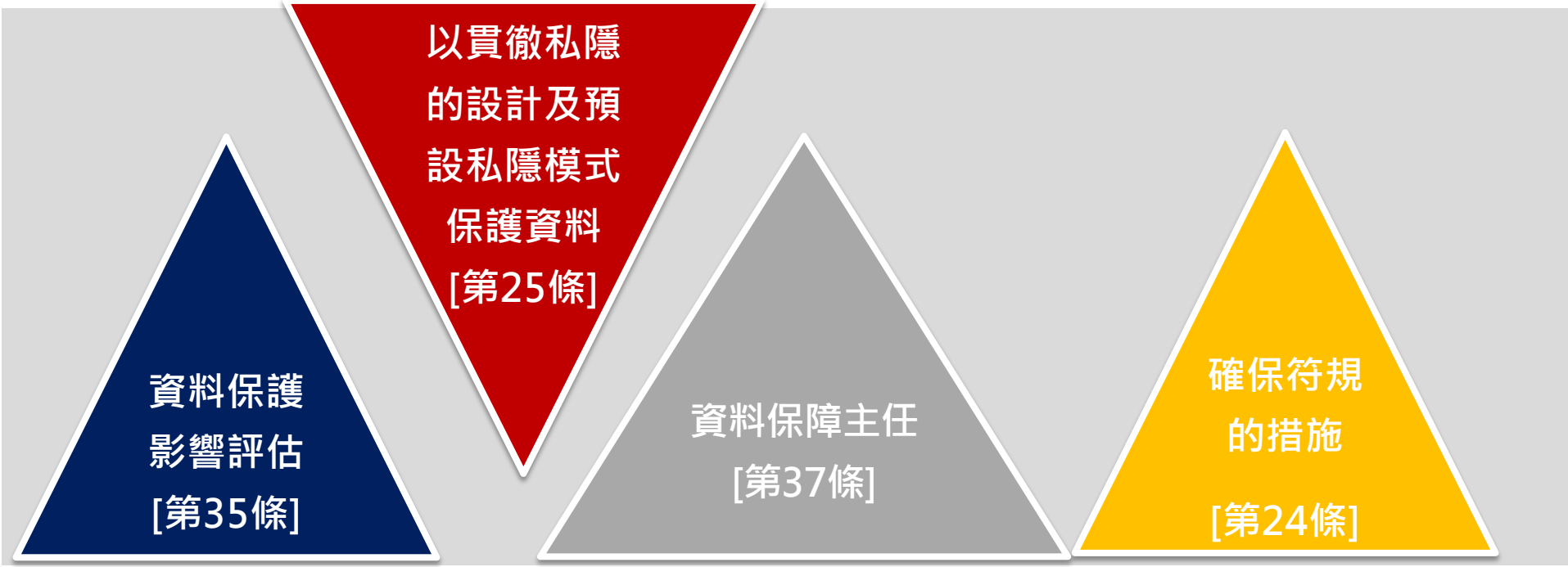
- 被遺忘權
- 資料可攜權
- 反對處理權等

**增強權利**

- 知情
- 明確
- 自願給予
- 具體

**加強同意**

# GDPR - 問責性


以貫徹私隱的設計及預設私隱模式保護資料[第25條]
資料保護影響評估[第35條]
資料保障主任[第37條]
確保符規的措施[第24條]

GDPR

# 強制資料外洩通報

- 風險為本

- 72小時內

GDPR

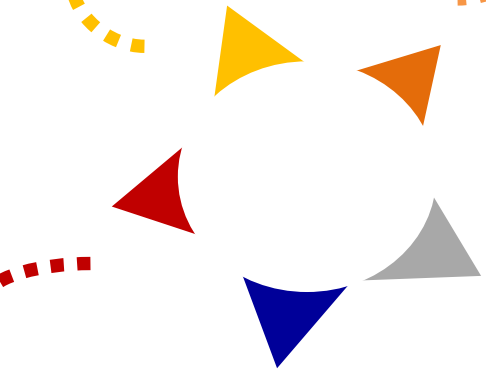
# 行政 罰款

最高為營業額的4% 或

2000萬歐元

# USA - 加州消費者私隱法案

自2020年1月1日起生效



個人權利：
- 查閱及刪除資料、資料可攜權
- 反對出售個人資料

民事處罰:
- 每項違規最高可達7,500美元

民事索賠:
- 每個事件每個消費者最多750美元, 或實際損失

- 迄今為止美國最全面的資料保障法規
- 以「同意」為本的歐洲模式

域外效力

# 聯邦資料保障法?

- 美國科技公司正在呼籲制定聯邦資料保障法
- 谷歌于2018年9月發佈了一套私隱原則,強調透明度,個人的控制權和機構的問責性
- 蘋果公司行政總裁 庫克: 聯邦資料保護法應該包括:
  - 資料最少化的權利
  - 通知權
  - 查閱權
  - 保安權

# 印度 - 2018年個人資料保障法案

遵循印度最高法院的判決（2017年）：

私隱是個人的基本權利

原則性及全面的保障

參考中國，歐盟和美國的數據保障法規

印度塑造21世紀全球數碼格局的必要原素

# 印度 - 2018年個人資料保障法案

**規定：**

- 域外效力
- 資料本地化：至少應儲存一份個人資料在印度
- 透明度和問責性
- 個人權利：
  - ✓ 查閱和更正資料
  - ✓ 數據可攜權
  - ✓ 被遺忘權
- 違規行政罰款：
  - ✓ 最多為全球年營業額的4%或1.5億盧比（約200萬美元）

# 其他亞洲資料保障法

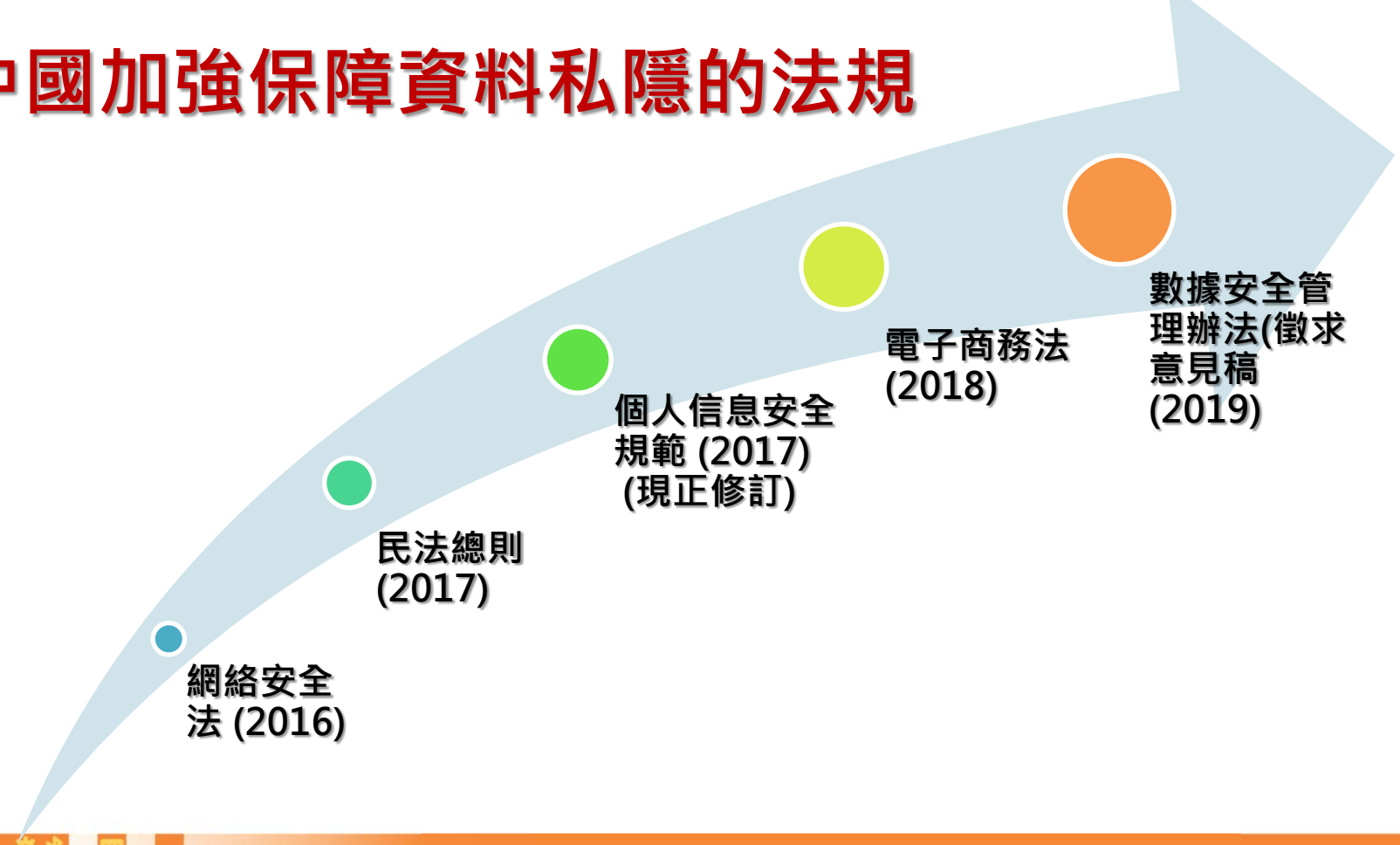
- 國務院正在審議資料保障法草案
- 遵循國際數據保障標準，尤其是GDPR
- 原則性
- 域外效力
- 限制跨境數據傳輸

泰國

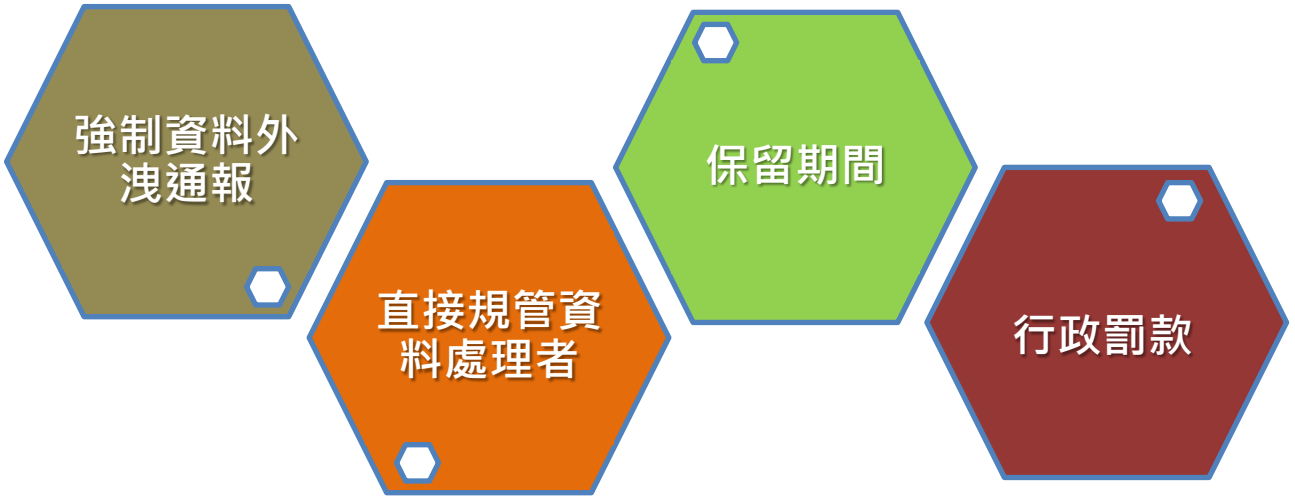
- 初稿於2015年出版
- 不在2018年的立法議程中
- 主要遵循歐洲模式
- 限制跨境數據傳輸

印尼

# 中國加強保障資料私隱的法規



# 檢討香港私隱條例的方向



# 2.1.2 指引

# ICDPPC 人工智能道德與資料保障宣言Declaration on Ethics and Data Protection in Artificial Intelligence (2018):

## 六個核心原則


Declaration on Ethics and Data Protection in Artificial Intelligence

ICDPPC
International Conference of Data Protection & Privacy Commissioners

**DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE**
40th International Conference of Data Protection and Privacy Commissioners
Tuesday 23rd October 2018, Brussels

AUTHORS:
- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- European Data Protection Supervisor (EDPS), European Union
- Garante per la protezione dei dati personali, Italy

CO-SPONSORS:
- Agencia de Acceso a la Información Pública, Argentina
- Commission d'accès à l'information, Québec, Canada
- Datatilsynet (Data Inspectorate), Norway
- Information Commissioner's Office (ICO), United Kingdom
- Préposé fédéral à la protection des données et à la transparence, Switzerland
- Privacy Commissioner for Personal Data, Hong Kong
- Data protection Authority, Belgium
- Data protection Commission, Ireland
- Data Protection Office, Poland
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mexico
- National Authority for Data Protection and Freedom of Information, Hungary
- Federal Commissioner for Data Protection and Freedom of Information, Germany
- Office of the Privacy Commissioner (OPC), Canada
- National Privacy Commission, Philippines

1 | Page

公平原則
**Fairness principle**

減少偏見與歧視
**Reducing biases or discriminations**

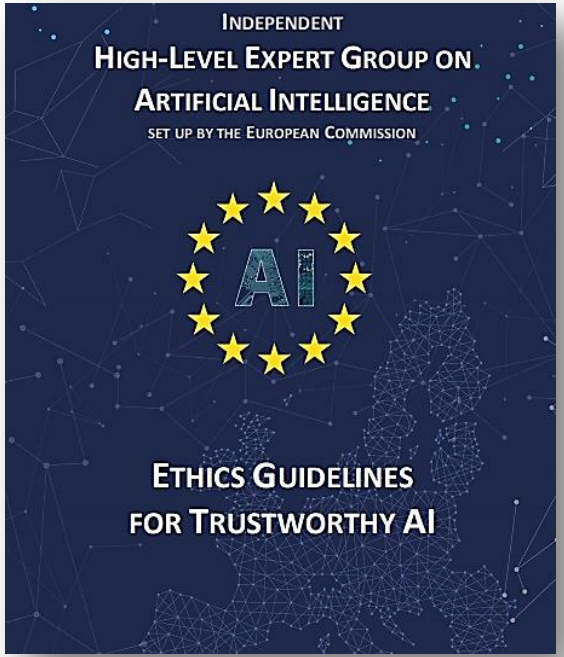
為每個人充權
**Empowerment of every individual**

持續關注與警惕
**Continued attention and vigilance**

系統透明度與清晰度
**Systems transparency and intelligibility**

貫切道德的設計
**Ethics by design**

# 歐盟人工智能道德指引 (2019)




七大關鍵要求：

1. 人類能動性及監察 Human agency and oversight
2. 穩健及安全 Technical robustness and safety
3. 私隱與數據管理 Privacy and data governance
4. 透明度 Transparency
5. 多元、不歧視和公平 Diversity, non-discrimination and fairness
6. 社會及環境福祉 Societal and environmental well-being
7. 問責 Accountability

# 2.2 數據道德的重要性

# 解決方案：問責和倫理道德


以風險為本的問責

「GDPR 帶來的最大變化是圍繞問責」
Elizabeth Denham, Information Commissioner of the UK

「GDPR旨在恢復我們對網絡生活中所發生的事情的信任和控制」
Giovanni Buttarelli, European Data Protection Supervisor

# 道德與信任

# 提倡道德：處理數據的正當性計劃

**目標**

- 何謂有道德的數據處理
- 公平的數據處理的標準為何
- 公平/有道德的資料處理與法律規定間直接或間接聯繫為何?資料道德管理在哪些方面超出法律範圍?
- 什麼誘因驅使企業採用道德資料影響評估,以及當中的原則和標準?

# 顧問公司的研究方向(2018年10月23日 在比利時布魯塞爾發佈)

找出數據道德的含義及核心價值

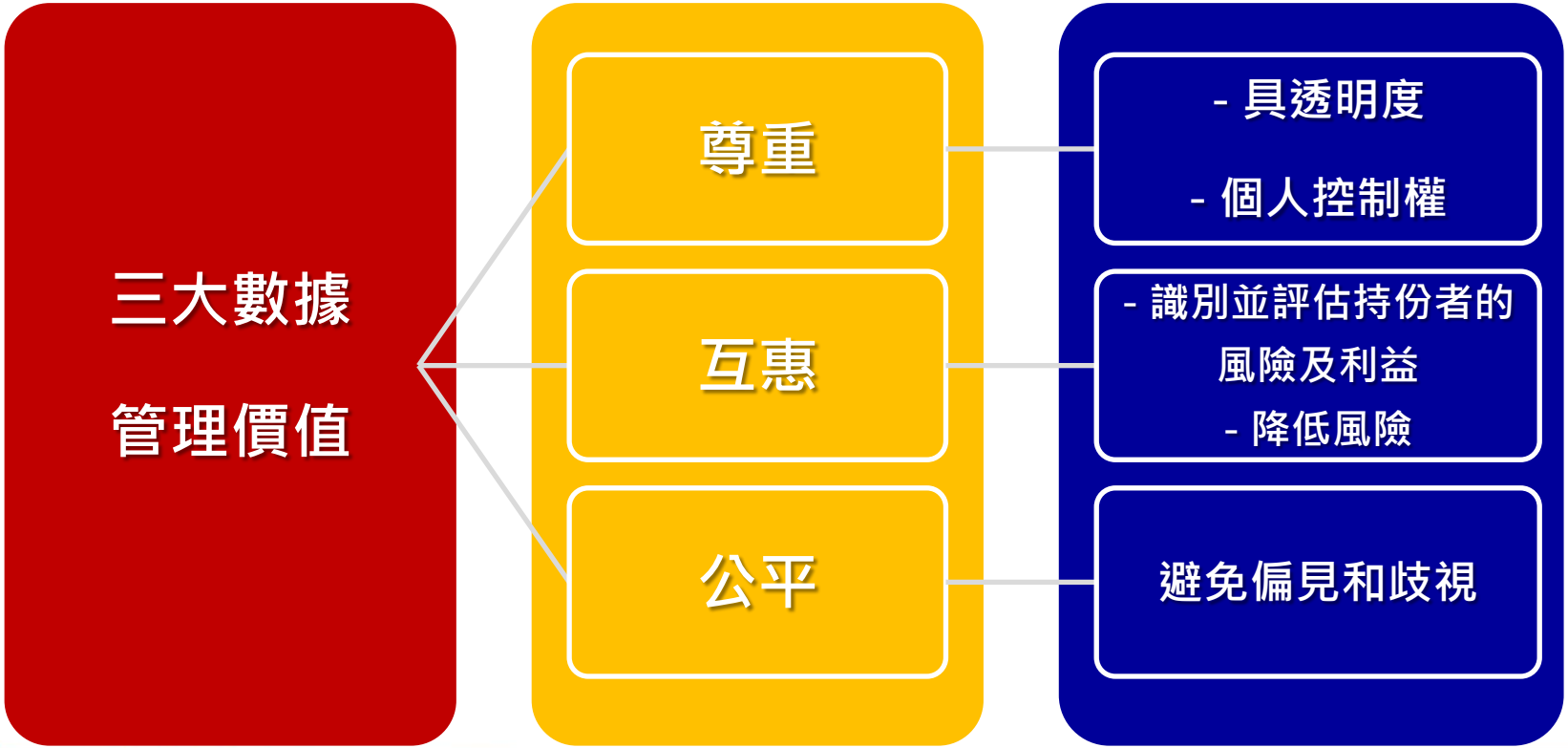
提供將數據道德核心價值付諸實踐的工具

鼓勵企業在日常運營中恪守數據道德

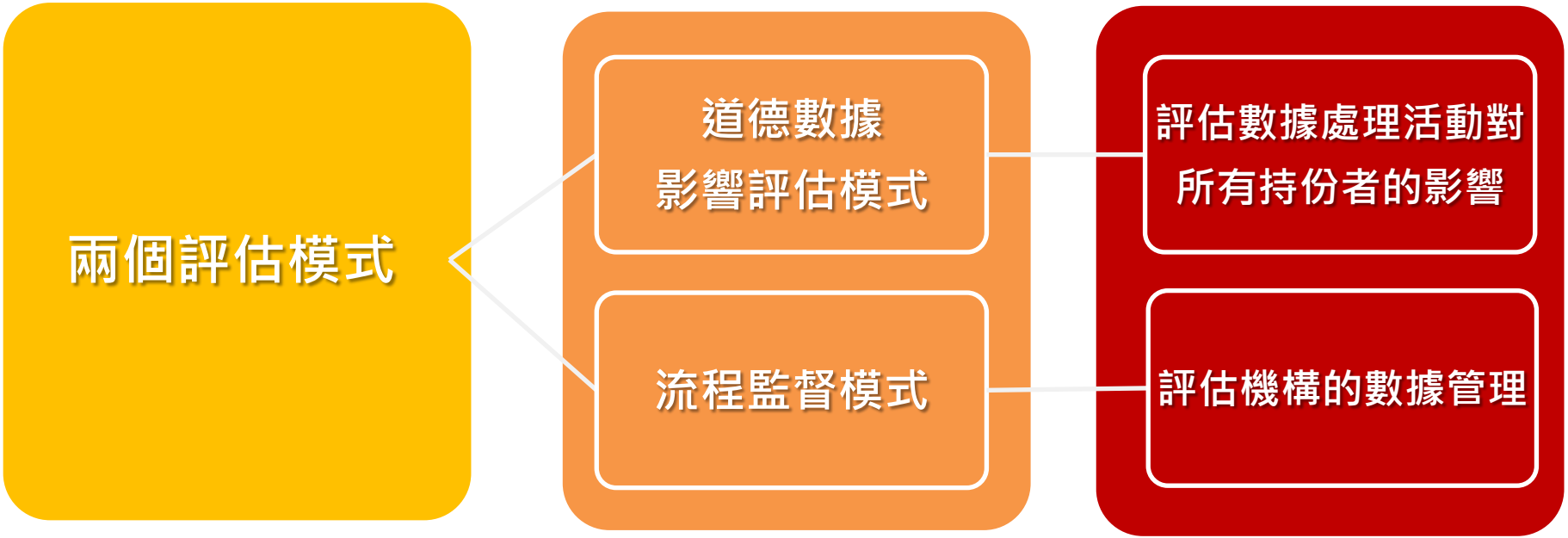
| | |
|---|---|
| 道德 | • 一套文化規範,當中結合群體的共同價值和指導信念 |
| 價值 | • 個人及社會秉持及使用的核心信念和理想 — 以商業機構而言,則為其經營的目標 |
| 原則 | • 在營商或投資策略的環境下的價值觀表述,並會引申為機構的政策及營運指引 |
| 執行 | • 政策、程式、培訓、工具、行為/實務守則 |
| 核實 | 道德數據影響評估模式 / 流程監督模式 |

有道德的數據管理問責

# 核心價值



# 實用工具



- 「我們必須確保科技是為人類服務,而非相反情況。」
- 「沒有人民對科技的完全信任, 我們永遠不能獲取科技的真正潛能。」
- 「我們不應因為有須要做而做, 我們因為應當做所以才去做。」

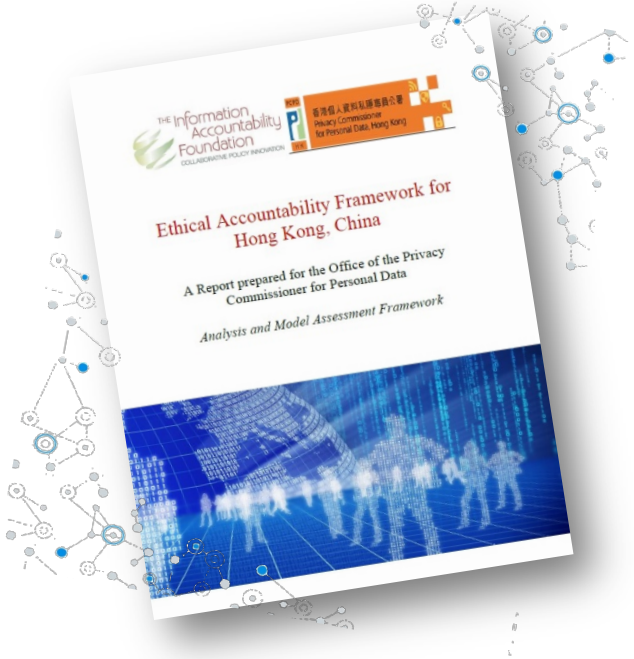
蘋果公司首席執行官 庫克
第四十屆國際資料保障及私隱專員會議(布魯塞爾)演說

「信任是新的黃金」

**Andrea Jelinek,**
**Chair of European Data Protection Board**

# “Ethical Accountability Framework for Hong Kong, China” (2018)

## REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT




Download >>

# 2.3 實施數據道德：私隱管理系統

# 問責：私隱管理系統（PMP）

好處


- 有效管理個人資料
- 最大限度地降低私隱風險
- 有效處理資料外洩事件
- 展示符規和問責性

# PMP – 主要組件

**1. 機構的決心**

- **1.1** 最高管理層的支持
- **1.2** 委任保障資料主任 / 設立保障資料部門
- **1.3** 建立匯報機制

# PMP – 主要組件

## 2. 系統管控措施

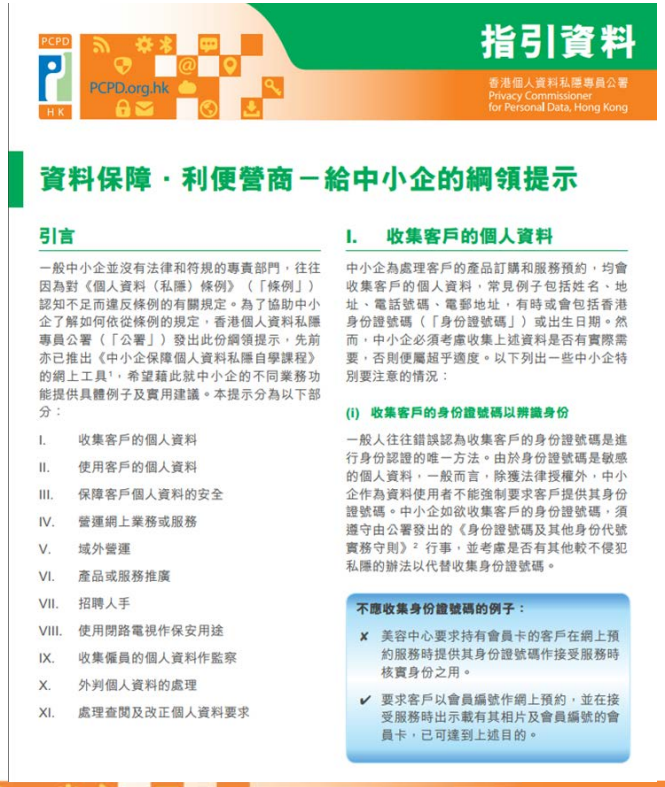
- **2.1** 個人資料庫存
- **2.2** 處理個人資料的內部政策
- **2.3** 風險評估工具
- **2.4** 培訓及教育推廣
- **2.5** 資料外洩事故的處理
- **2.6** 對資料處理者的管理
- **2.7** 溝通

# PMP – 主要組件

## 3. 持續評估及修訂

3.1 制定監督及檢討計劃 …… 3.2 評估及修訂系統管控措施

# 《資料保障 利便營商 — 給中小企的綱領提示》



PCPD.org.hk

指引資料

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

## 資料保障・利便營商－給中小企的綱領提示

### 引言

一般中小企並沒有法律和符規的專責部門，往往因為對《個人資料（私隱）條例》（「條例」）認知不足而違反條例的有關規定。為了協助中小企了解如何依從條例的規定，香港個人資料私隱專員公署（「公署」）發出此份綱領提示，先前亦已推出《中小企保障個人資料私隱自學課程》的網上工具[1]，希望藉此就中小企的不同業務功能提供具體例子及實用建議。本提示分為以下部分：

I. 收集客戶的個人資料
II. 使用客戶的個人資料
III. 保障客戶個人資料的安全
IV. 營運網上業務或服務
V. 域外營運
VI. 產品或服務推廣
VII. 招聘人手
VIII. 使用閉路電視作保安用途
IX. 收集僱員的個人資料作監察
X. 外判個人資料的處理
XI. 處理查閱及改正個人資料要求

### I. 收集客戶的個人資料

中小企為處理客戶的產品訂購和服務預約，均會收集客戶的個人資料，常見例子包括姓名、地址、電話號碼、電郵地址，有時或會包括香港身份證號碼（「身份證號碼」）或出生日期。然而，中小企必須考慮收集上述資料是否有實際需要，否則便屬超乎適度。以下列出一些中小企特別要注意的情況：

#### (i) 收集客戶的身份證號碼以辨識身份

一般人往往錯誤認為收集客戶的身份證號碼是進行身份認證的唯一方法。由於身份證號碼是敏感的個人資料，一般而言，除獲法律授權外，中小企作為資料使用者不能強制要求客戶提供其身份證號碼。中小企如欲收集客戶的身份證號碼，須遵守由公署發出的《身份證號碼及其他身份代號實務守則》[2] 行事，並考慮是否有其他較不侵犯私隱的辦法以代替收集身份證號碼。

**不應收集身份證號碼的例子：**

✘ 美容中心要求持有會員卡的客戶在網上預約服務時提供其身份證號碼作接受服務時核實身份之用。

✔ 要求客戶以會員編號作網上預約，並在接受服務時出示載有其相片及會員編號的會員卡，已可達到上述目的。

- 協助中小企瞭解私隱條例的規定
- 深入淺出解釋相關法規
- 提供切合中小企運作模式的具體合規例子和實用建議

# 3

# 展望：香港智慧城市發展與大灣區機遇

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*

# 粵港澳大灣區倡議：

橫跨香港，澳門和珠江三角洲九個城市的城市群;
面積56,000平方公里;
7500萬人口和10萬億人民幣GDP

Source: bayarea.gov.hk

# 香港 – 「五流」匯聚之地

# 香港的優勢

先進的基礎設施

自由開放的體制

自由流通的信息

便利的營商環境

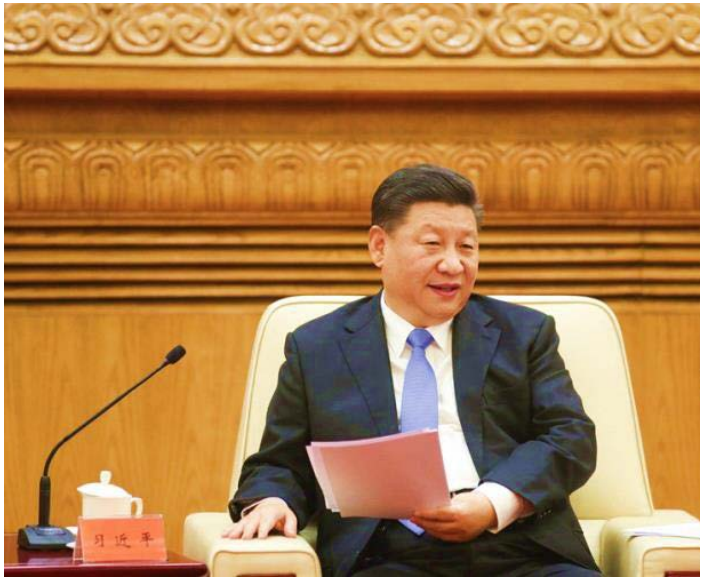
國際接軌的法治

廣泛的國際聯繫

發達的服務業

眾多高質素人才

中共中央政治局常委、
全國人大常委會委員長
張德江2016年5月18日
出席香港「一帶一路高
峰論壇」演講



*"在新時期的國家改革開放中，香港和澳門仍然具有特殊地位和獨特優勢及不可替代的作用"*

**國家主席習近平**
在北京人民大會堂會見
香港澳門各界慶祝國家改革開放40週年訪問團
2018年11月12日

# 香港獨特和不可替代的優勢

自由流動的信息

普通法制度和法治

*(在2019年法治指數126個轄區中排名第16位，高於美國)*

全面的個人資料保障法

*即《個人資料（私隱）條例》（香港法例第486章)*

中國唯一一個以英語為官方語言的地區

# 法律的優勢

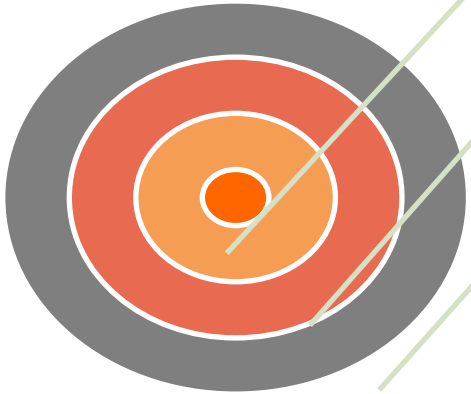
- 大量法律專業人才
- 健全的普通法制度
- 律師、法官具雙語優勢及豐富經驗
- 人權保障

# 《粵港澳大灣區發展規劃綱要》

## 香港的角色

# 《粵港澳大灣區發展規劃綱要》

## 與數據相關的區域合作



促進人員，貨物，資本和信息的跨境和區域流動

共同開發大灣區大數據中心

制定計劃，加強醫療數據和生物樣本跨境使用的管理

探索建立通用標準，開放數據端口，開發互聯的公共應用平台

# 智庫：**香港可以成為大灣區的全球數據中心**

依賴大數據的全球企業需要一個「中立」的中心來幫助彌合中國數碼系統的分歧...香港擁有一個顯而易見的地位。


馮國經, 2022基金會主席

香港已經制定了大陸和國際企業可以信任的嚴格的個人資料私隱法律和法律保護

Source: The Standard (29 March 2019)
http://www.thestandard.com.hk/breaking-news.php?id=125179&sid=4

「*香港在大灣區擁有獨特的功能。……支持香港成為國際創新中心。……香港應該把它的優勢應用於大灣區發展的專業服務。*」

**韓正**國務院副總理; 2019年3月


Source: xinhuanet.com; March 2019

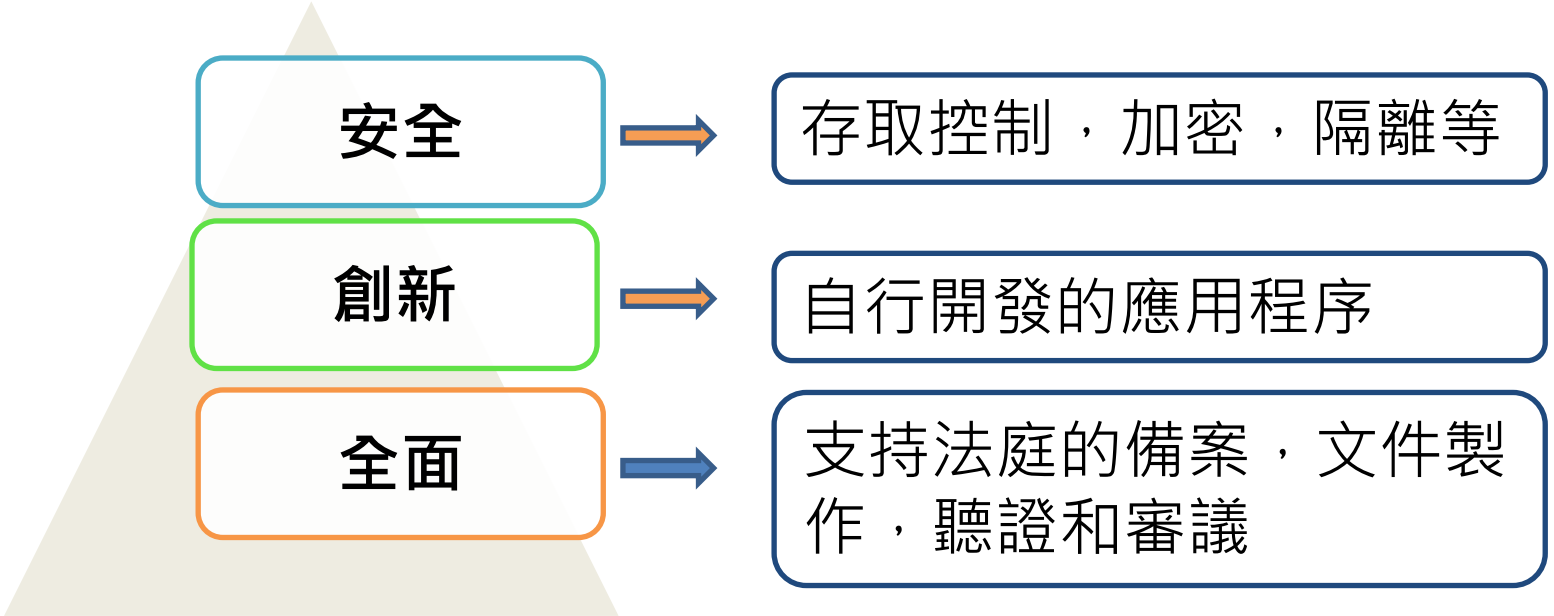
# eBRAM Centre一帶一路仲裁與調解電子平台

充分發揮香港的特質

擔任一帶一路倡議的爭議解決者

提供在線爭議解決平台

# eBRAM 的在線爭議解決平台



# 香港作為區域數據中心的角色

沒有國界的個人數據流動

＋

促進技術發展（例如人工智能，大數據等）

→

加強數據保障的重要性

# 香港作為區域數據中心的角色

在處理向歐盟/美國的數據傳輸方面擁有豐富的經驗

受一國兩制支持

一帶一路倡議

香港有條件成為大灣區的區域數據中心和國際數據中心

# 香港作為數據中心的優勢

國際連通性蟬聯第一

數據中心安全性第一

寬頻品質第二

私隱保障第一

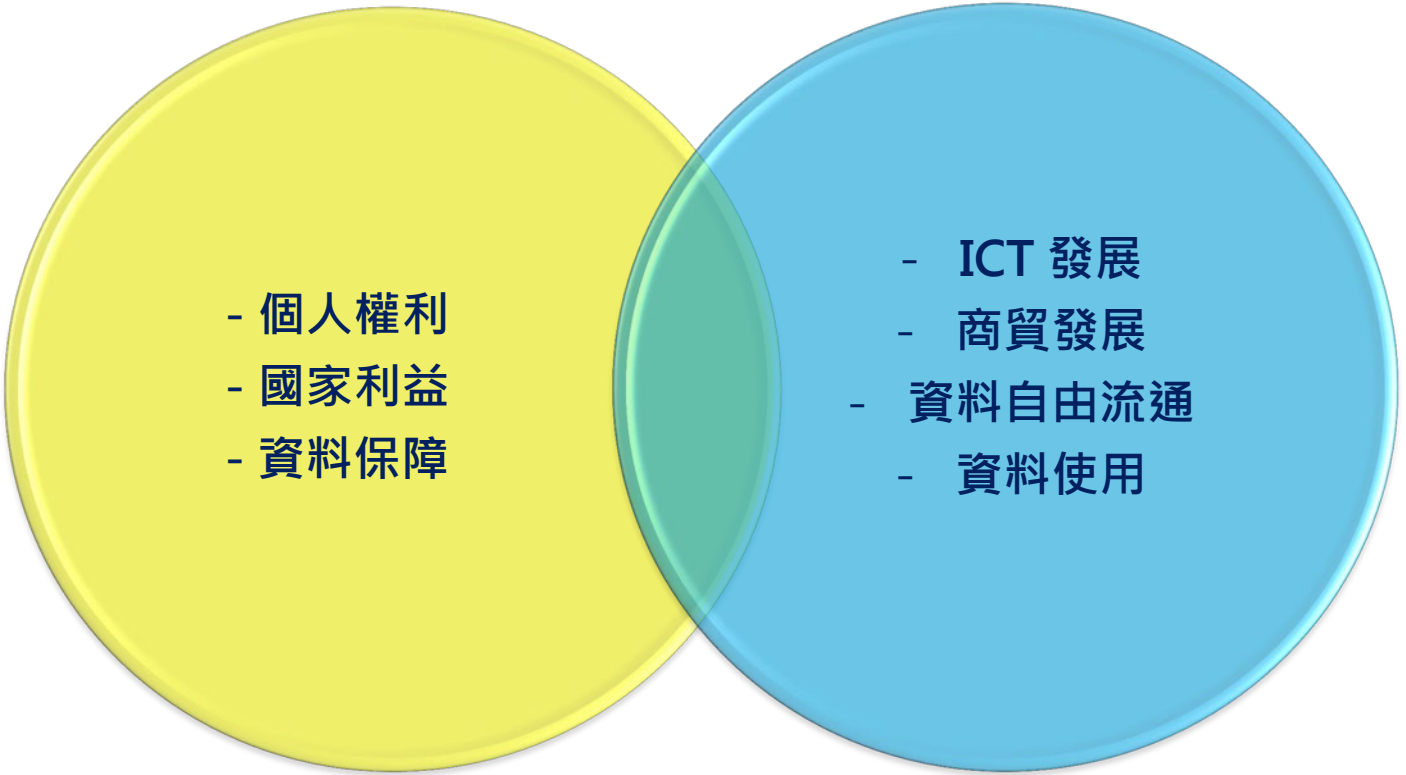
# 公署的策略重點

推動、鼓勵

提供誘因


尊重私隱文化

# 平衡各方權益



# 私隱專員於香港律師會會刊《香港律師》之專欄文章

- 2月：數碼革命中的資料保護
- 3月：物聯網如何揭露你的私隱
- 4月：人工智慧對私隱的影響
- 5月：容貌辨識與閉路電視監控
- 6月：指紋掃描的私隱問題

HONG KONG LAWYER 香港律師 • June 2019

DATA PRIVACY

## Privacy Issues of Fingerprints Scanning

**More affordable and efficient fingerprinting hardware and applications are conducive to the wide adoption of fingerprint scanners for attendance record management and access control.**

**Recent complaint cases processed by my office (PCPD) serve to illustrate how organisations can adopt good practices to respect and protect consumers' personal data when using fingerprint scanners.**

The Personal Data (Privacy) Ordinance (the "Ordinance") is technology neutral. Data Protection Principle 1 in Schedule 1 to the Ordinance provides that the collection of personal data must be "necessary for or directly related to" the stated purpose of collection, and "not excessive" in relation to that purpose. It must also be collected by means "which are fair in the circumstances".

When using fingerprint scanners, organisations should consider offering less privacy-intrusive options, or adopt technical measures that minimise data collection.

**Less Privacy-Intrusive Alternatives**

In a recent case handled by the PCPD, a client paying a site-visit to a cloud storage data centre was required by the data centre to submit his fingerprint for registration as a condition of entry.

According to the Personal Information Collection Statement provided by the data centre, the purpose of the fingerprint registration was to strengthen the physical security of the premises, and also to allow registered visitors to walk unescorted and to conveniently gain entry by fingerprint-scan verification. The fingerprint data would be erased upon the client's departure from the data centre.

Upon the recommendations of the PCPD, the data centre agreed to provide a less privacy-intrusive option to visitors who do not wish to submit their fingerprints, such as using security staff to escort the visitor to designated locations on the premises.

**Alternative Technical Measures**

In another case, an employer collected its employee's fingerprint data through a fingerprint scanner on her first day of work. The system was installed for staff attendance and security purposes because the business involved the sale and display of high-value fashion merchandise.

After conducting an investigation prompted by a complaint, the PCPD concluded that the collection of fingerprint data was unnecessary and excessive in the circumstances because the employer could record staff attendance and control access to the premises by the use of smartcards and passwords.

Another alternative was to control entry by the combined use of a **smartcard and fingerprint-scan device**. The employee's fingerprint data would be stored in a company-issued smartcard, carried by the employee himself – no fingerprint data would be stored by the

56 www.hk-lawyer.org


私隱管理系統
Privacy Management Programme
最佳行事方式指引
A Best Practice Guide
「处理数据的正当性」
研究报告
欧洲联盟
《通用数据保障条例》
2016
6 保障資料原則
Data Protection Principles
PCPD.org.hk
1 收集目的及方式 Collection Purpose & Means
2 準確性、儲存及保留 Accuracy & Retention
3 使用 Use
4 保安措施 Security
5 透明度 Openness
6 查閱及更正 Data Access & Correction
「处理数据的正当性」
新闻稿

# 謝謝！

# Data Protection Officers' Club

## (Membership 2019-2020)

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

**By becoming a DPOC member, you will:**

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

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

# JOIN today!