關注私隱運動2020
「由原則至行動 – 企業保障個人資料」講座

2020年6月24日

黃繼兒大律師
香港個人資料私隱專員

大綱

1. 簡介《私隱條例》
2. 尊重私隱對業務有甚麼好處？
3. 企業十項實務行動
4. 最新私隱議題：疫情下如何保障員工個人資料、使用視像會議軟件與保障私隱
5. 私隱影響評估及貫徹私隱的設計
6. 私隱管理系統及實踐數據道德
7. 國內與私隱相關的最新法規
8. 歐盟《通用數據保障條例》

1.簡介《私隱條例》


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

私隱是甚麼？

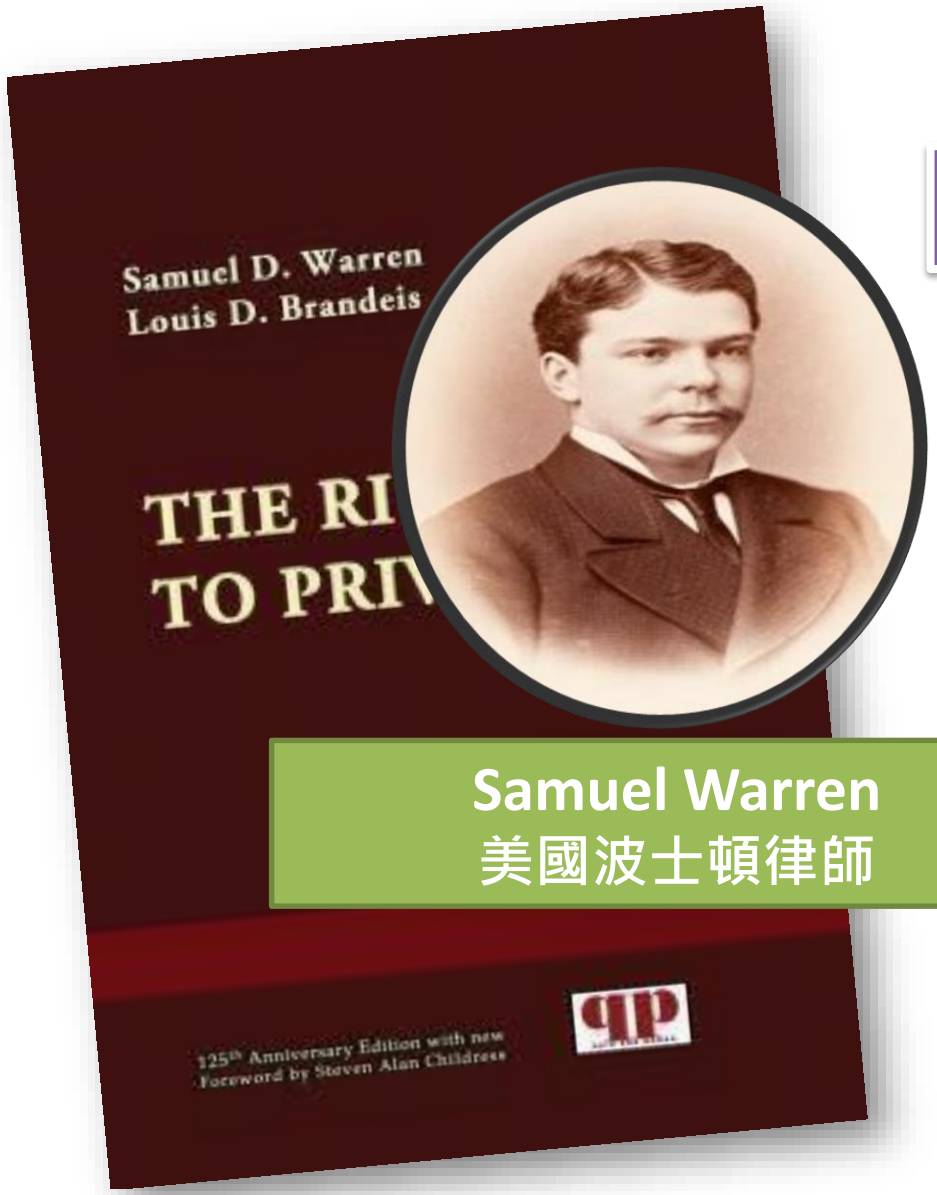
"The state of being alone and not watched or interrupted by other people" 獨處而不被他人看見或打擾的狀態

Oxford Dictionary

「對自主和保護個人尊嚴尤其重要的基本權利，是建立許多其他人權的基礎」

https://www.privacyinternational.org/explainer/56/what-privacy

“Right to be let alone”



1890

Samuel Warren
美國波士頓律師

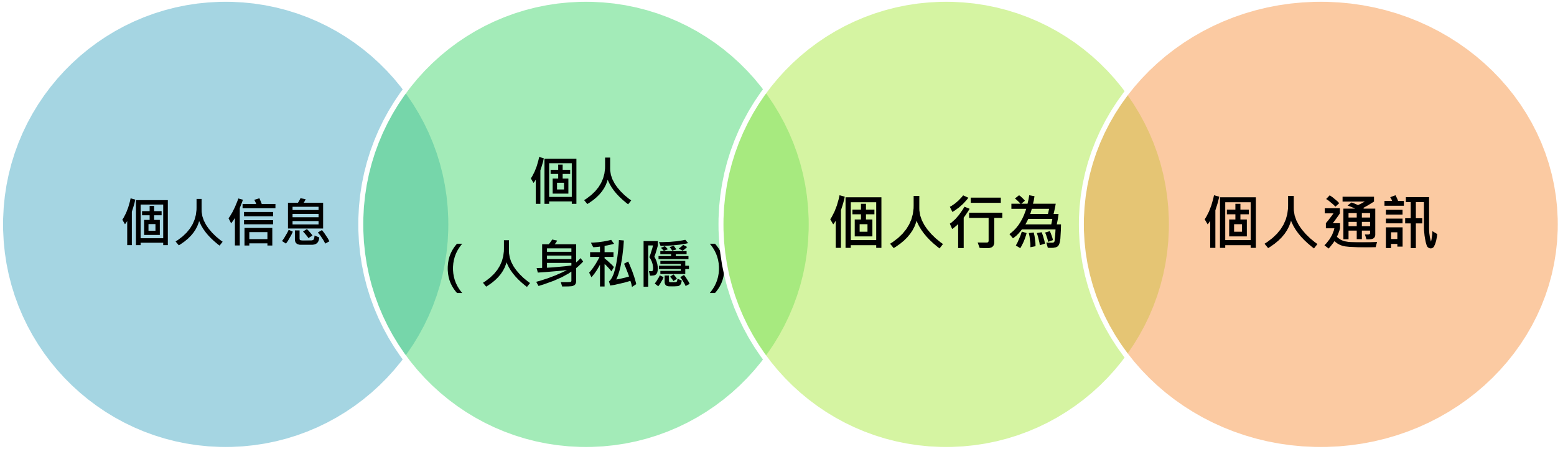
Louis Brandeis
美國律師；由1916年至1939年擔任美國最高法院法官

私隱是甚麼？

「隱私是自然人的私人生活安寧和不願為他人知曉的私密空間、私密活動、私密信息。」

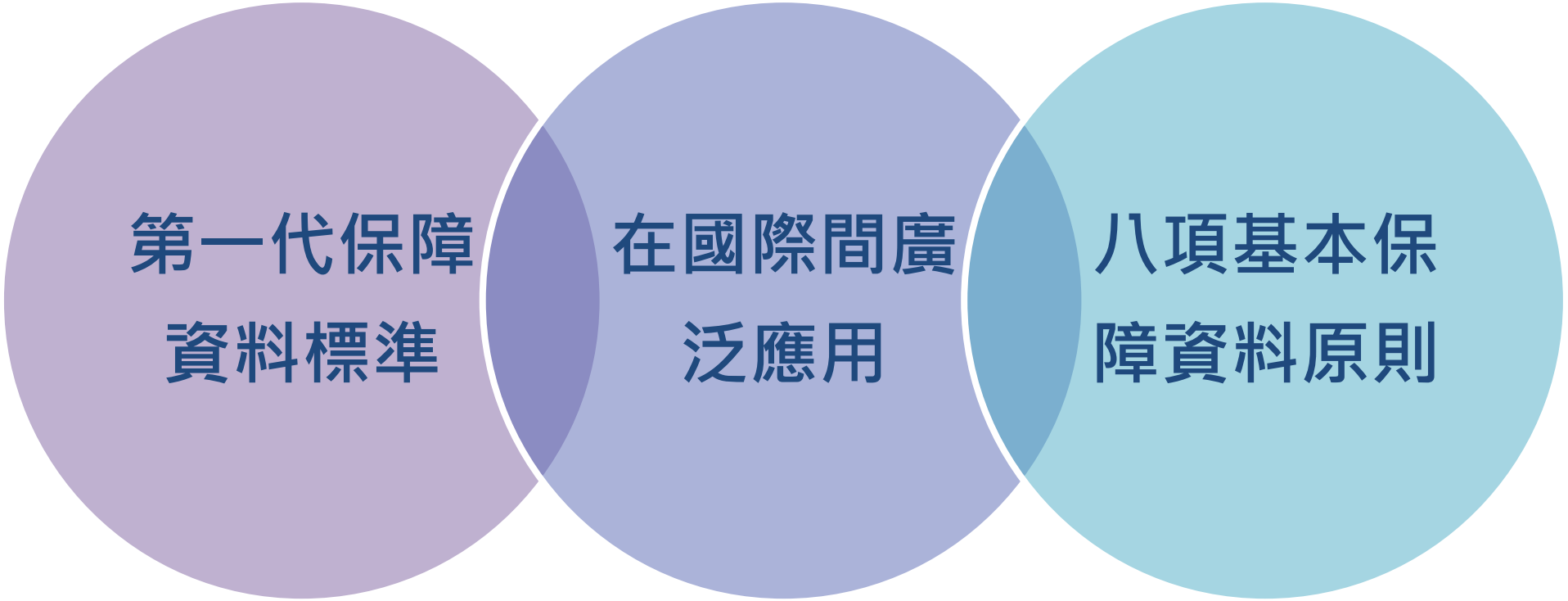
中國《民法典》

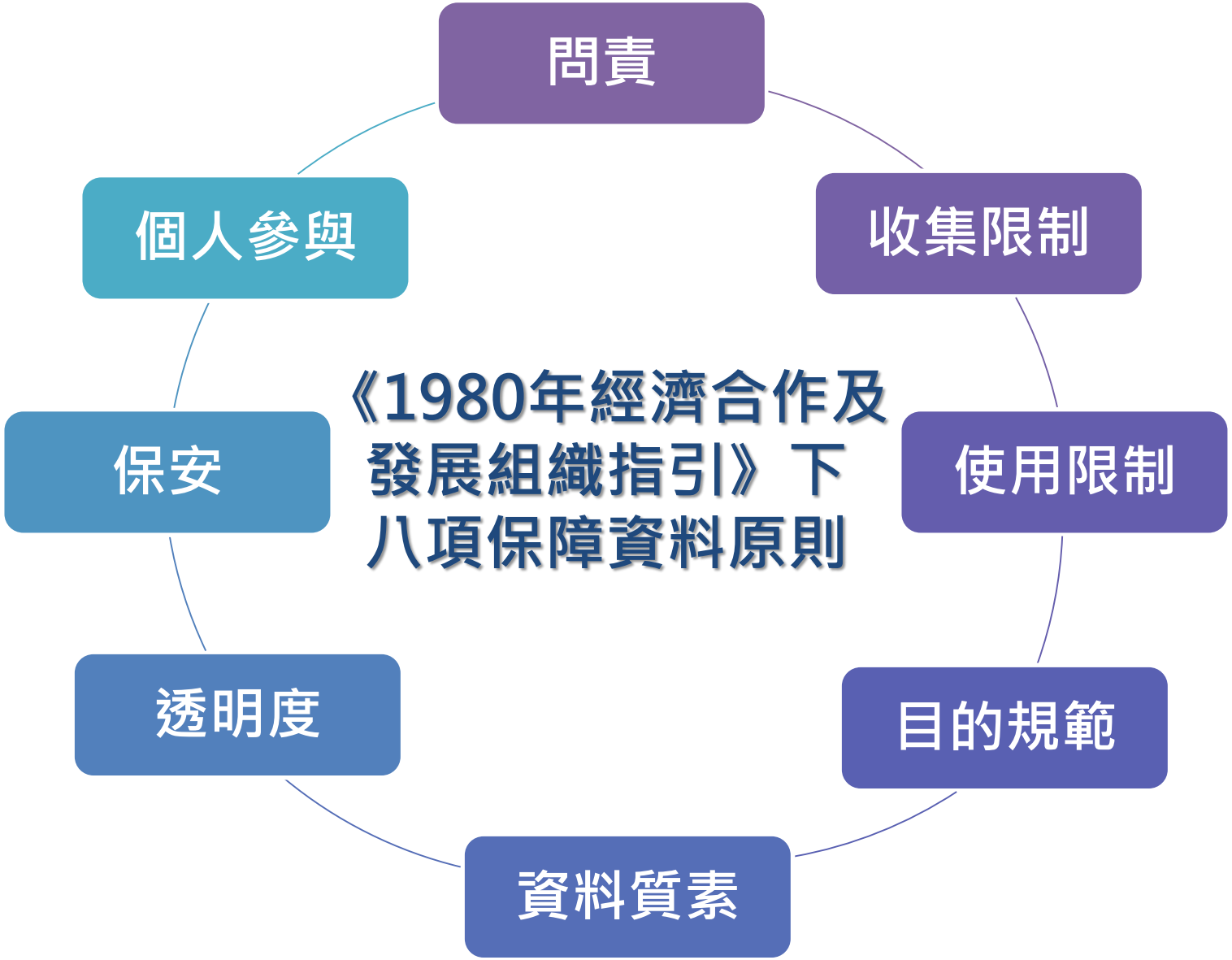
私隱涵蓋...



《1980年經濟合作及發展組織指引》

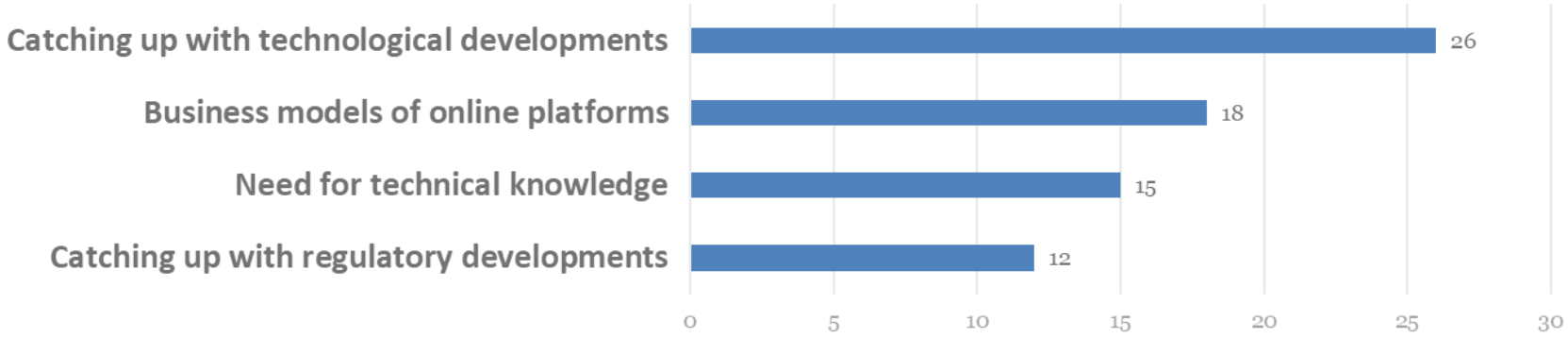
Organisation for Economic Co-operation and Development (OECD)



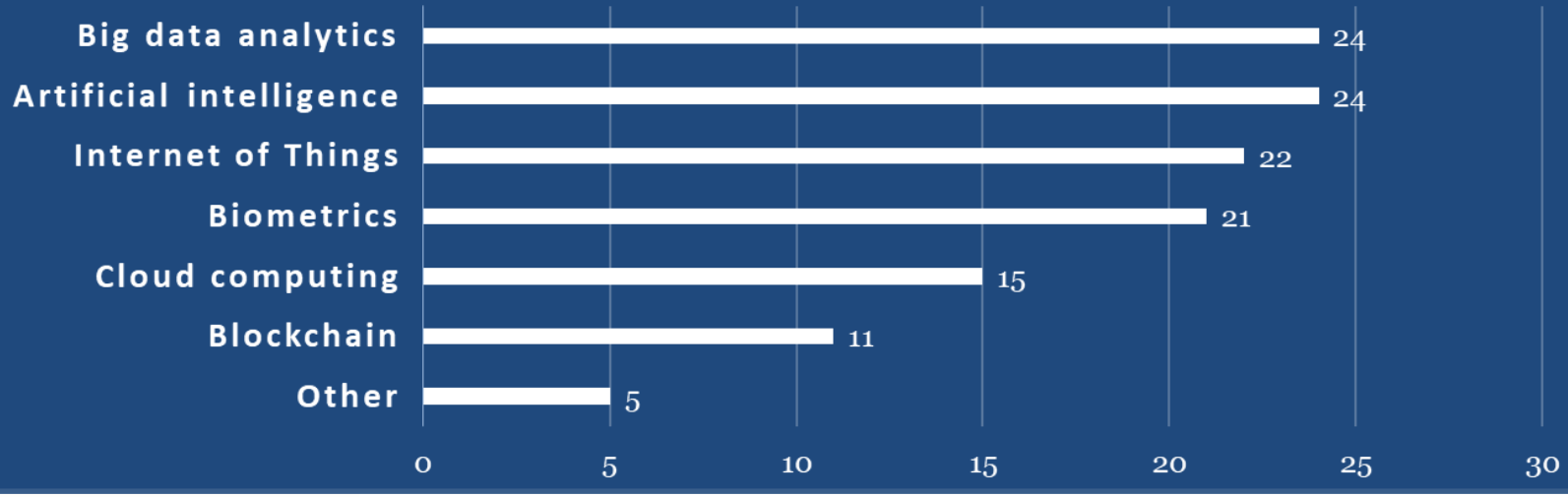

問責
收集限制
使用限制
目的規範
資料質素
透明度
保安
個人參與
《1980年經濟合作及發展組織指引》下八項保障資料原則

But challenges remain for countries implementing their privacy and data protection frameworks

Main challenges to implementation of regulatory frameworks



Emerging technologies that pose the main challenges to the frameworks



資料來源:
OECD

《1995年歐盟資料保護指令》

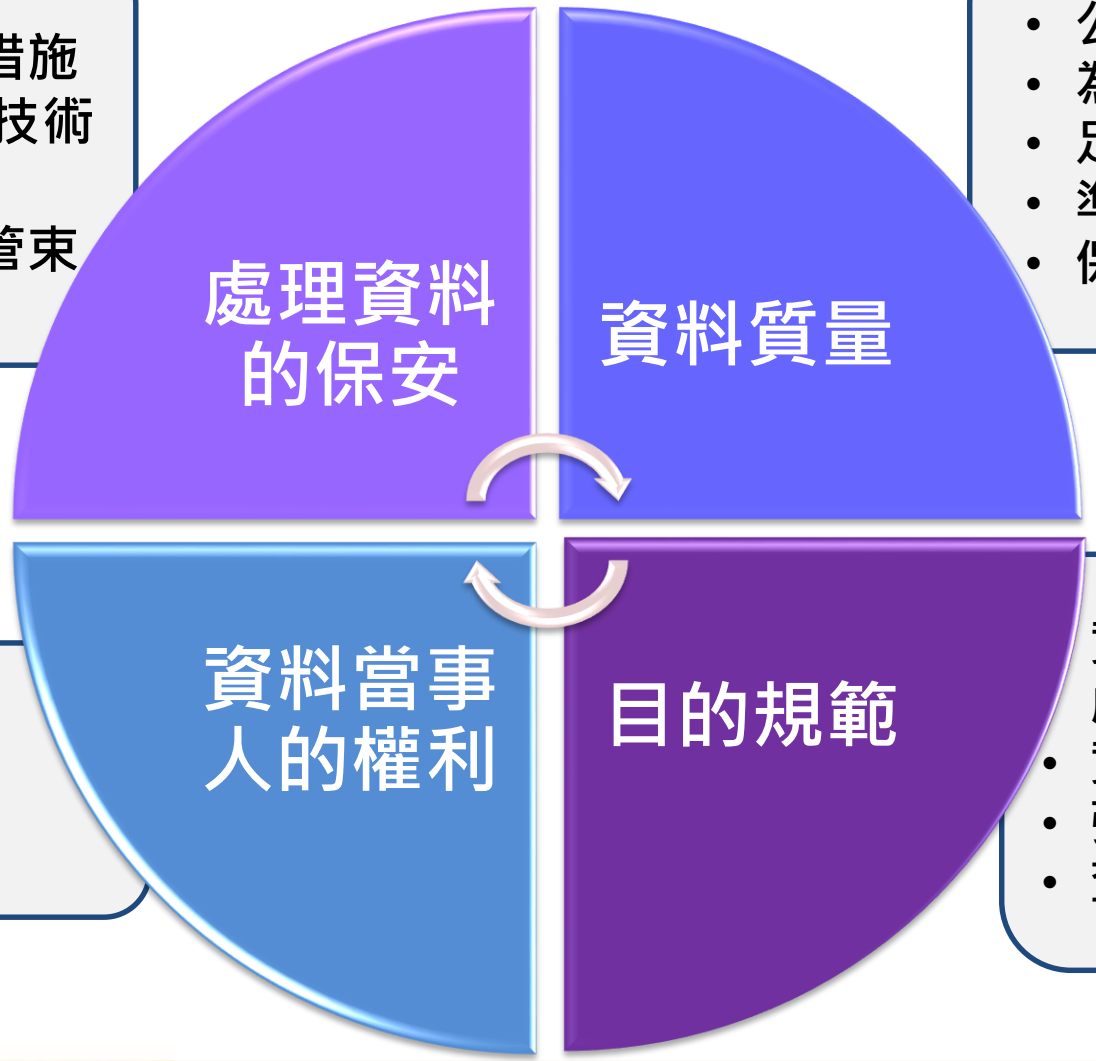
第二代保障資料標準

為所有歐洲國家法律制定法律框架

在2018年被《通用數據保障條例》取代(*第三代保障資料標準*)

《1995年歐盟資料保護指令》

- 實施適當的技術和架構措施
- 對資料處理者所提供的技術安全措施有充分的保證
- 資料處理者必須受合約管束



- 公平及合法地處理
- 為特定，明確和合法目的而收集
- 足夠、相關及不過度收集
- 準確
- 保留時間不超過實際所需

- 查閱權利
- 改正權利
- 反對處理權利

資料控制者的身份
處理的目的
- 資料接收人或資料接收人的類別
- 強制性或自願性
- 查閱及改正資料的權利

全球資料保障形勢

截至2019年4月

134 個

國家或地區擁有資料保障法例

30+

法案等待頒布

Source:
https://gallery.mailchimp.com/1072135a1de8b1660644928a6/files/da8fb6f6-ade4-45c3-9eaf-7f13c8b12316/INT159.pdf

私隱權在香港屬基本人權

International Covenant on Civil and Political Rights

《公民權利和政治權利國際公約》

該條約的適用範圍於1976年擴展至香港

「(一) 任何人之私生活、家庭、住宅或通信，不得無理或非法侵擾，其名譽及信用，亦不得非法破壞。」[第十七條]

基本法（1990）

第三十九條

《公民權利和政治權利國際公約》、《經濟、社會與文化權利的國際公約》和國際勞工公約適用於香港的有關規定繼續有效，通過香港特別行政區的法律予以實施。

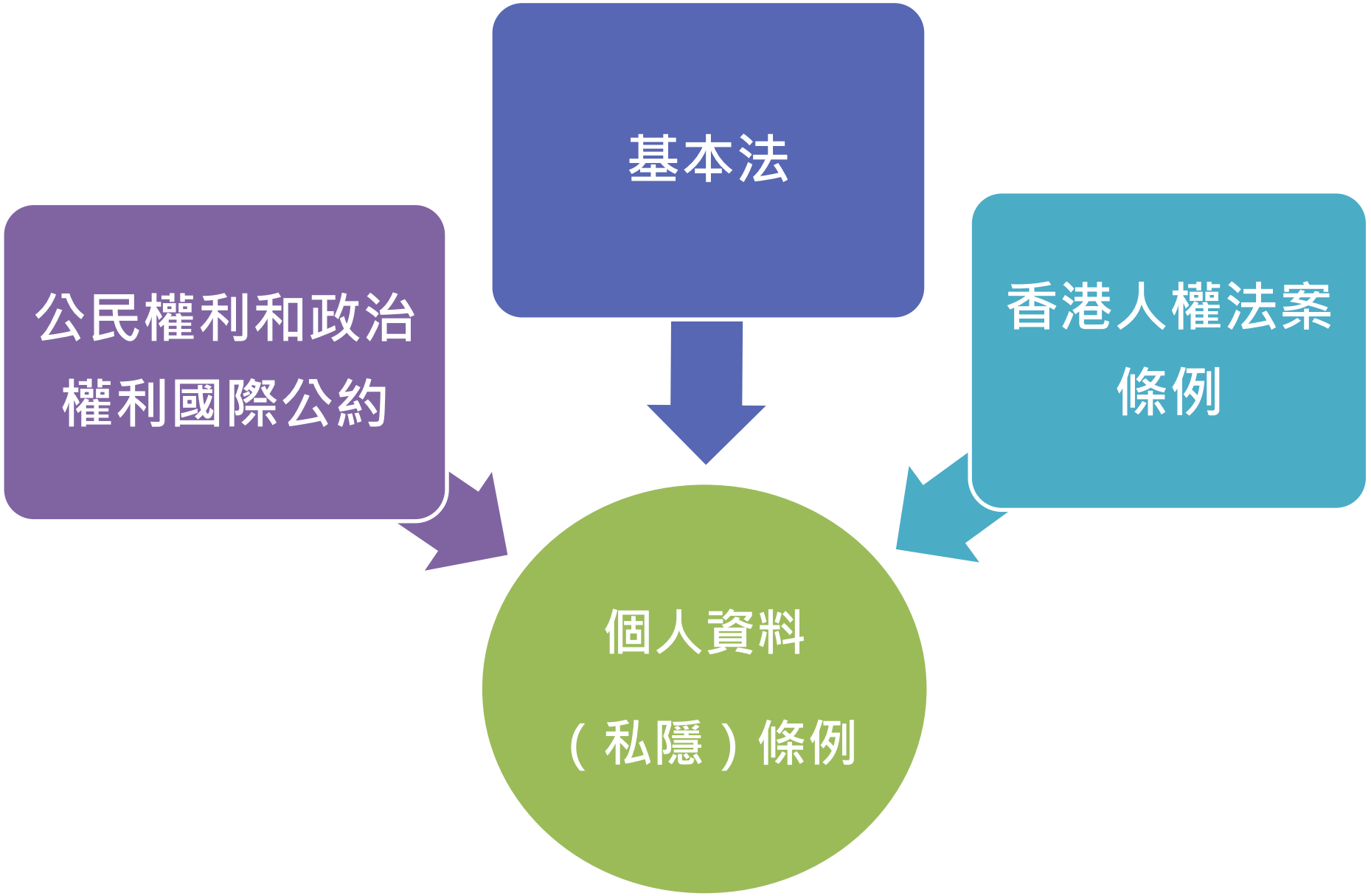
香港居民享有的權利和自由，除依法規定外不得限制，此種限制不得與本條第一款規定抵觸。

香港人權法案條例（1991）

香港人權法案第十四條
（比照《公民權利和政治權利國際公約》第十七條）

對私生活、家庭、住宅、通信、名譽及信用的保護

（一）任何人之私生活、家庭、住宅或通信，不得無理或非法侵擾，其名譽及信用，亦不得非法破壞。


基本法
公民權利和政治權利國際公約
香港人權法案條例
個人資料（私隱）條例

《個人資料（私隱）條例》

《個人資料（私隱）條例》

亞洲區內最早的全面保障個人資料私隱的法例之一

《私隱條例》
立法背景

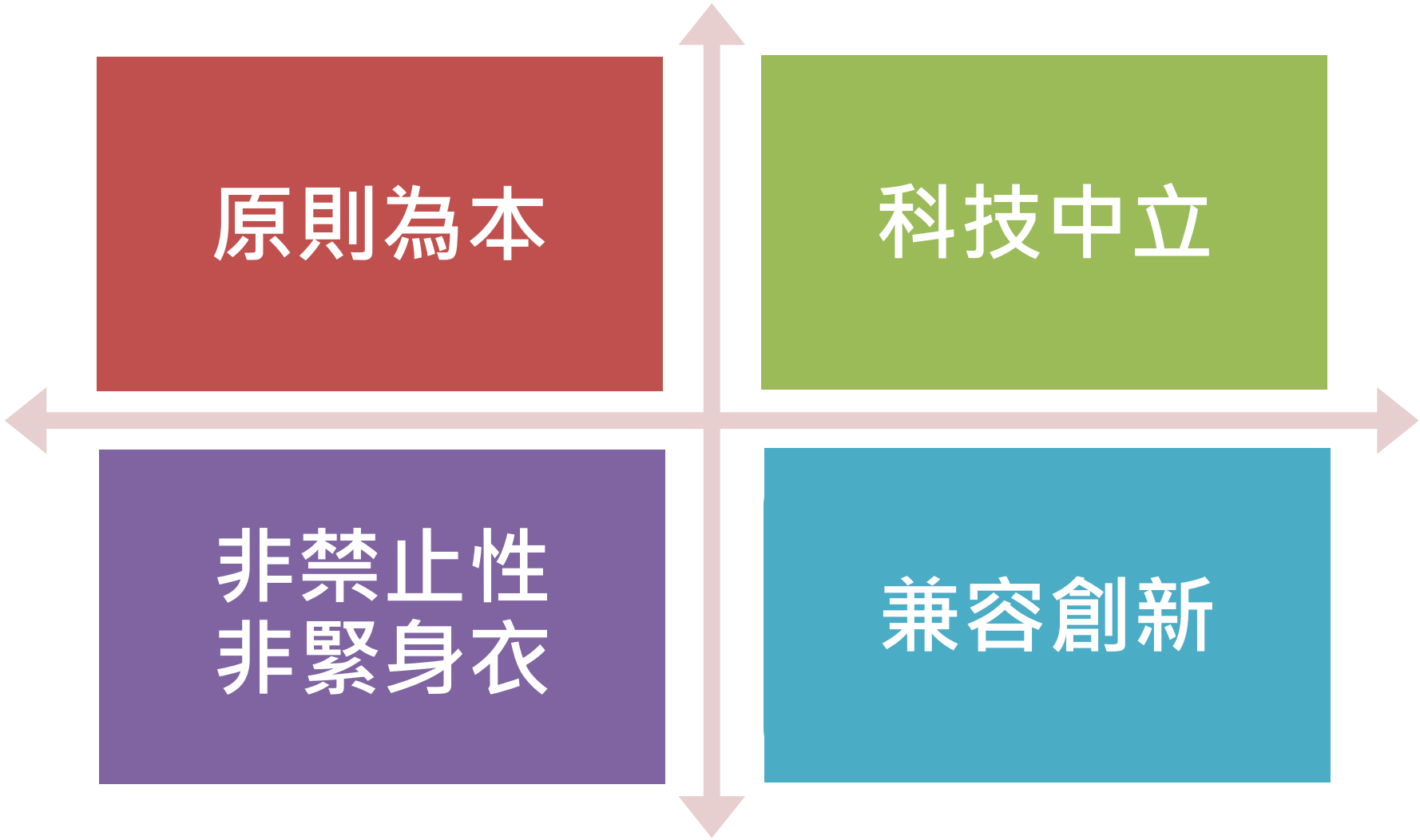
商業

- 便利營商環境
- 維持香港作為金融和貿易中心的地位

人權

- 保障個人資料私隱

《私隱條例》的特點



《私隱條例》主要內容

- 個人資料的定義
- 《私隱條例》的規定涵蓋個人資料由收集、保存、使用以至銷毀的整個生命周期
- 直接促銷
- 豁免
- 跨境資料轉移

《私隱條例》主要規管範疇

甚麼是「個人資料」？

「個人資料」須符合以下三項條件：

1. 直接或間接與一名在世人士有關
2. 從該等資料直接或間接地確定有關的個人的身分是切實可行的；而
3. 該等資料的存在形式令予以「查閱」及「處理」均是切實可行的

直接促銷規管機制

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

- 提供「訂明資訊」及回應途徑，讓資料當事人選擇同意或表示「不反對」個人資料被用作直銷
- 通知必須清楚易明

資料當事人同意

- 必須自願和清晰作出
- 不反對也屬同意

提交個人資料

《私隱條例》下的刑事罪行—直接促銷的規定

	最高罰款(港幣)	監禁最高年期
未依例行事(條例第 35C, 35E, 35F 及 35G條)	500,000	3 年
賣資料予他人直銷用途，而未有依例行事(條例第35J, 35K 及 35L條)	1,000,000	5 年

《私隱條例》下的刑事罪行

違反保障資料原則	• 不是罪行 • 可發出執行通知要求資料使用者採取步驟糾正違規行為
不遵從執行通知	• 刑事罪行 • 罰款$50,000及監禁兩年
重複違反執行通知	• 罰款$100,000及監禁2年 • 持續罪行，每日罰款$2,000
第二次相同違規行為	• 罰款$50,000及監禁兩年

《私隱條例》下的刑事罪行

第64條：披露未經資料使用者同意而取得的個人資料

(1)任何人披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料，而該項披露是出於以下意圖的，該人即屬犯罪 ——

(a) 獲取金錢得益或其他財產得益，不論是為了令該人或另一人受惠而獲取；或

(b) 導致該當事人蒙受金錢損失或其他財產損失。

(2) 如 ——

(a) 任何人披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料；而

(b) 該項披露導致該當事人蒙受心理傷害， 該人即屬犯罪。

一經定罪，可處罰款 $1,000,000 及監禁 5 年。

違反第64條的例子

未經同意下在互聯網上以欺凌、煽動和恐嚇等非法目的披露個人資料

僱員未經公司同意出售公司客戶的個人資料，並從買方那裡獲得款項。

某銀行的前僱員代表另一金融機構（他的新僱主）致電該銀行的客戶推廣貸款產品。

電腦維修公司人員未經一位名人的同意下，從筆記本電腦中取得名人的私密照片，並將照片上傳到互聯網，對該名人造成了心理傷害。

豁免條文（《私隱條例》第8部)

以下情況的個人資料可獲豁免依從保障資料原則：

	情況	保障資料原則
第57條	政府為維護香港安全、防衛或國際關係而持有的個人資料	保障資料第3 及第 6原則
第58條	為預防、偵查犯罪或糾正嚴重不當行為而持有的個人資料	保障資料第3 及第 6原則
第59條	與資料當事人的身體或精神健康有關	保障資料第3 及第 6原則
第60條	法律專業保密權	保障資料第6原則
第60B條	法律程序	保障資料第3原則
第61條	業務或部分業務包含新聞活動的資料使用者持有	保障資料第3及第 6原則
第62條	用於準備統計數據或進行研究，而研究結果無法識別資料當事人	保障資料第3原則

法例檢討

1. 強制性資料外洩通報機制
2. 資料保留時限
3. 懲處權
4. 直接規管資料處理者
5. 「個人資料」的定義
6. 規管披露屬於其他資料當事人的個人資料的行為
7. 刑事調查及檢控權

2. 尊重私隱對業務有甚麼好處？

營商環境不斷改變

資源有限

企業管治架構薄弱

支援不足

員工培訓不足

缺乏接收資訊渠道

Present situation of SME and their concerns
中小企業的現狀及面對的挑戰

尊重私隱對業務的好處

- 客戶對個人資料私隱保障的期望與日俱增
- 積極主動保障個人資料私隱、實踐數據道德管治、確保個人資料獲妥善保存及管理
- 私隱為本、「數碼榮譽」
- 贏取客戶信任，提升商譽及競爭優勢

3. 企業十項實務行動

由原則至行動—中小企保障個人資料實務手冊

目的

- 提升中小企對保障和尊重個人資料的認知
- 提供實用資訊
- 有系統地協助中小企依從《私隱條例》的規定和實踐數據道德

實務手冊內容簡介

- 《私隱條例》主要釋義
- 十項實務行動
- 實用工具和清單
- 直接促銷、人力資源管理
- 便攜式「中小企十項實務行動重點提示卡」

按部就班向企業解釋循規要求

01 

認識《私隱條例》

先對《私隱條例》及其保障資料原則作基本認識，以作為你的企業在處理個人資料方面合規的依據。 ▷ 頁 17

02 

為何要收集這些個人資料？

在收集個人資料前，確定你收集該等資料的目的，以檢討和確定處理資料程序的私隱風險。 ▷ 頁 22

03 

有否清晰地通知個別人士收集其個人資料的目的？

在收集個人資料時或之前，清晰告訴相關人士為何你需要他們的個人資料，及你將如何使用該等資料。 ▷ 頁 23

04 

持有個人資料的期限和準確性

確保你的企業持有的個人資料準確無誤，以及保留時間不會超過達致原來目的的實際所需。 ▷ 頁 25

05 

如何使用收集所得的個人資料？

檢討資料收集目的，若打算使用於新目的時，須在使用前確保已取得相關人士的訂明同意。 ▷ 頁 27

按部就班向企業解釋循規要求

06

檢視資料保安

確保所持有的個人資料的安全，不會未經授權或意外被查閱、處理、刪除、喪失或使用。 ▷ 頁 30

07

建立資料外洩事故通報程序

確保你的企業已採取良好行事方式，訂立程序以偵測、匯報和調查資料外洩事故。 ▷ 頁 32

08

處理查閱和改正個人資料要求

確保你的企業已訂立程序，回應個別人士提出的相關要求，提供及更新個人資料。 ▷ 頁 34

09

委聘資料處理者

採用合約或其他方式以令資料處理者承擔責任 。 ▷ 頁 39

10

私隱影響評估

使個人資料私隱成為將來業務項目的核心元素。 ▷ 頁 41

- 流程圖作指引以協助企業學習如何保障客戶和員工的個人資料

- 提供範本讓企業參考

樣本一：
訂購產品和
服務

收集個人資料聲明(範本)

ABC 公司
收集個人資料聲明

本公司向你收集的資料會用以處理你的訂單，以及管理你在本公司開設的帳戶。

你必須在訂單上註明（*）的欄目提供所需的個人資料。如你未能提供，我們未必可以處理你的訂單或向你提供我們的產品或服務。

你有權隨時查閱及改正本公司持有關於你的個人資料。如要欲行使上述權利或改正你的個人資料，請透過_____（公司地址）或電郵_____與本公司的保障資料人員聯絡。

樣本二：
招聘員工

收集個人資料聲明（範本）

ABC 公司
收集個人資料聲明

本公司透過本申請表所收集的個人資料，將會用於評估你是否適合擔任所申請的職位，以及在你獲挑選出任該職位時，用作與你商討初步的薪酬、花紅及福利。

申請表中有（*）號的項目是挑選合適入選者所必須考慮的資料。求職者如不提供此等資料，會對申請的處理及結果有所影響。

本公司的政策是為日後的招聘活動保留落選者的個人資料兩年。如本公司的附屬或聯營機構在此期間出現職位空缺，本公司或會將你的申請資料轉交有關機構考慮。

根據《個人資料（私隱）條例》，你有權要求查閱及改正申請表上所填報的個人資料。如你欲行使這項權利，請填妥本公司的《查閱資料要求表格》，並透過郵寄表格至_____（公司地址）或電郵_____，交回人力資源部的資料保障主任辦理。

由原則至行動—中小企保障個人資料實務手冊

便攜式「中小企十項實務行動提示卡」

- 重點提示
- 易於攜帶

- “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

私隱公署如何協助企業

- 投放資源協助本港企業（尤其中小企）加強保障個人資料，推廣「尊重」個人資料私隱的企業文化
- 舉辦不同講座及研討會，為中小企提供適切的訓練
- 出版與中小企有關的刊物，加強網上培訓工具
- 設立中小企專用的諮詢熱線（2110 1155）和電郵（sme@pcpd.org.hk），為中小企提供便捷的查詢渠道

問 《私隱條例》是甚麼？

- 旨在保障在世人士的個人資料私隱權，屬科技中立和原則性的條例，在科技發展和創新，與保障和尊重個人資料之間取得平衡

答

問 企業收集個人資料時需注意甚麼？

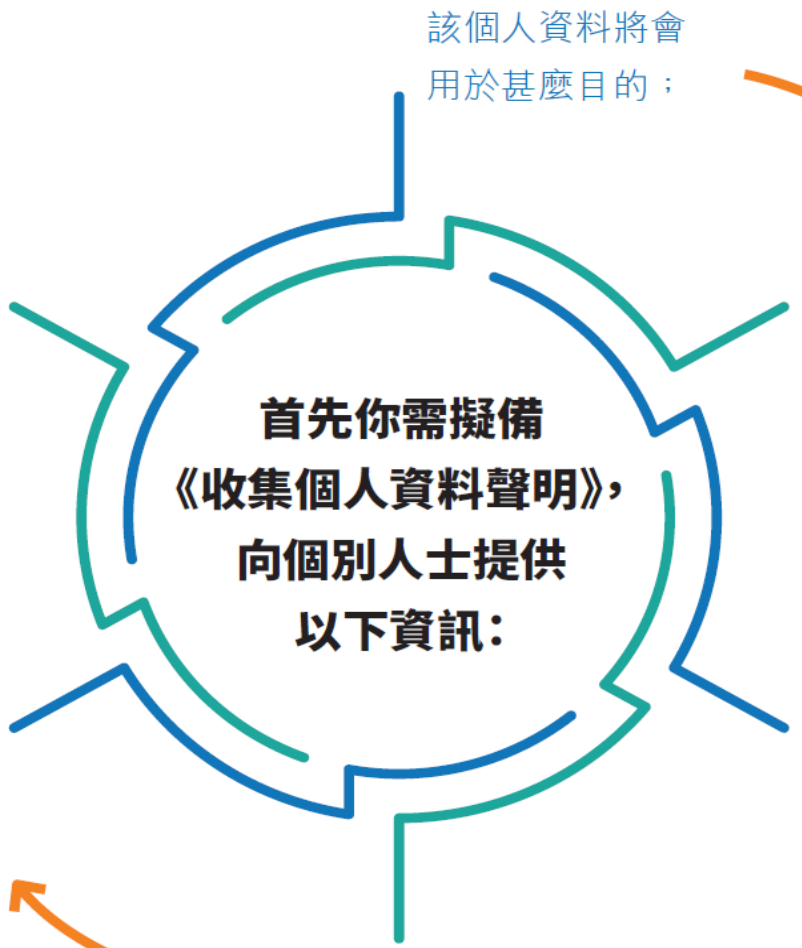
- 當企業收集個人資料時，應只收集對收集目的而言是必須及足夠的資料，但不要超乎適度

答

問

收集個人資料之前或之時，企業應怎樣做去告知資料當事人收集其資料的目的？

答



問 企業應保留個人資料多久？

- 《私隱條例》沒訂明確實個人資料的保留時限
- 企業應確保個人資料不會保留超過達原來目的的實際所需，並刪除已不再需要的個人資料
- 企業應採取良好的行事方式，制定個人資料政策（包括檢視時間表和程序），詳細列明保留的個人資料的安排

答

問 如何使用收集所得的個人資料？

- 使用收集所得的個人資料時，需參考相關的收集目的，並定期進行檢視，確保資料用於收集資料時述明的目的或直接有關的目的

- 若用於新目的，之前須獲得個人自願給予的明示同意

答

問 企業應怎樣做保障所持有的個人資料？

企業可：

- 制定和實施企業內部的保安措施
- 使用合適的保安措施以保障不同形式的個人資料
- 定期檢視相關的保安政策和措施以確保資料是最新的
- 提供相關的僱員培訓，確保僱員對資料保安的認知
- 採取合約方式以避免轉移予外判商的個人資料被未經授權而被查閱、處理、刪除、喪失或使用

答

問 若發生資料外洩事故，企業應如何處理？

- 若發生資料外洩事故，企業可根據企業所制定的資料外洩處理政策 / 程序，搜集必需資料，考慮盡快採取良好行事方式向受影響人士及監管機構作出通報

答

資料外洩事故

信貸資料公司網上認證程式存在漏洞

背景

- 本地報章於2018年11月通過公司的網上認證程式，取得數名公眾人士的信貸報告
- 事故發生時，個人可透過公司的網站及其五個夥伴的網站 / 手機程式申請及查取信貸報告

信貸資料公司網上認證程式存在漏洞

調查發現

- 個人所輸入的全名和出生日期無須與信貸資料公司料庫的紀錄完全脗合
- 「基於知識的認證」採用了 (a) 與個人信貸無關的問題（如年齡範圍及生肖），及 (b) 過時並且容易被排除的答案
- 其他網站 / 手機程式的查取途徑沒有因個人未能通過另一網站 / 手機程式的認證程式而被封鎖
- 非所有申請均使用雙重認證

信貸資料公司網上認證程式存在漏洞

調查結果

- 沒有採取所有切實可行的步驟確保個人資料不受未獲准許的查閱
- 違反《私隱條例》保障資料第4(1)原則（資料保安）

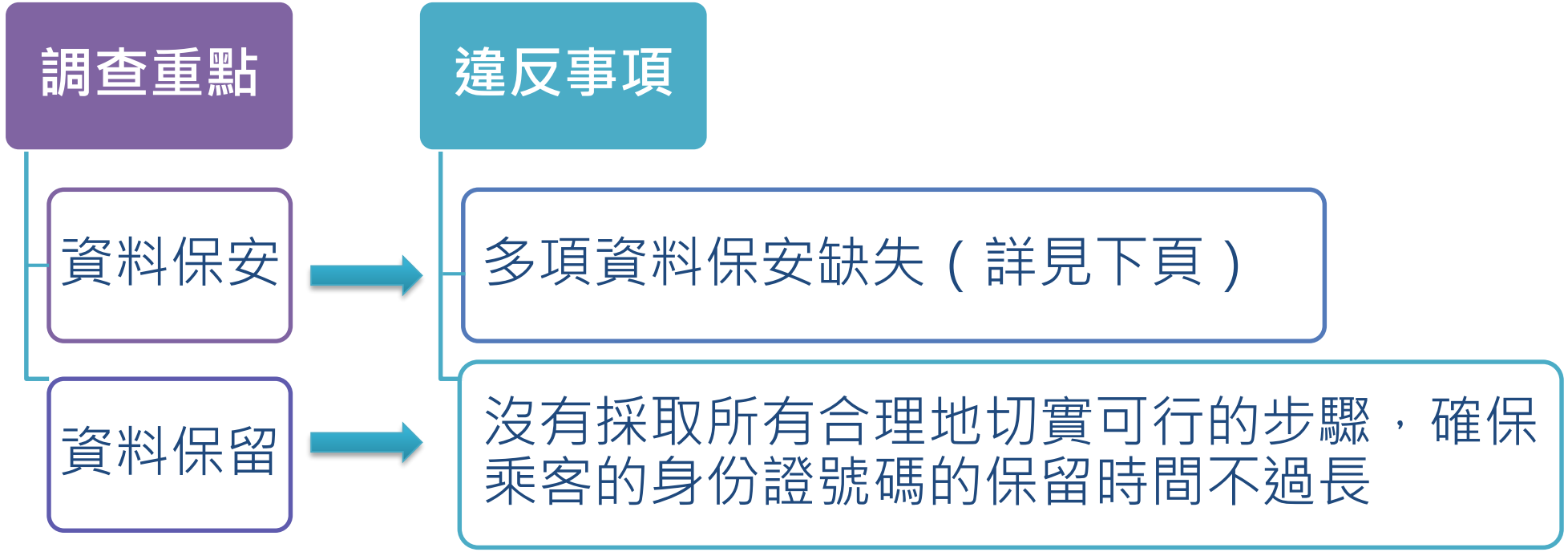
航空公司資料外洩事故

背景

- 航空公司於2018年3月首次在系統中發現可疑活動跡象
- 私隱專員於2018年10月24日收到資料外洩通報
- 940萬名乘客的個人資料曾被未獲授權而取覽，涉及超過260個國家 / 司法管轄區 / 地區的乘客
- 涉事的個人資料包括姓名、航班編號及日期、會員編號、電郵地址、住址、電話號碼

航空公司資料外洩事故

調查結果



航空公司資料外洩事故

資料保安缺失

管治問題

- 對風險的警覺性低
- 未有建立有效的個人資料庫存以涵蓋所有載有個人資料的系統

風險評估 / 防治問題

- 未能識辨某個廣為人知及可被加以利用的保安漏洞
- 只為伺服器每年進行一次漏洞掃描（頻率不足）
- 沒有避免伺服器的管理員控制台埠曝露於互聯網

保安措施問題

- 為了方便遷移資料中心而建立未經加密的資料庫備份檔案
- 未有對資訊系統的所有遙距使用者實施有效的多重身份認證

航空公司資料外洩事故

執行通知

- 聘請獨立的資料保安專家徹底檢修系統
- 實施有效的多重身份認證
- 進行有效的漏洞掃描
- 聘請獨立的資料保安專家定期對網路的保安進行檢視 / 測試
- 制定清晰的資料保留政策，並實施有效措施以確保政策獲有效執行
- 徹底銷毀不必要的身份證號碼

問 處理客戶的查閱和改正個人資料要求時需注意的事項？

- 查閱資料要求者無權查閱不屬個人資料，亦無權要求查閱不屬於他的個人資料
- 企業須從所要求的資料複本中刪除第三者的個人資料，才向查閱資料要求者提供其個人資料複本

答

問 處理改正個人資料要求時需注意的事項？

- 企業應分辨哪些是「可被核實的事項」和「意見表達」：
  - **可被核實的事項**指以客觀現實、紀錄或數據為基準評定有關資料是否準確的事項
  - **意見表達**指不能核實的、或在有關個案的所有情況下予以核實不是切實可行的事實的陳述。若資料涉及專業判斷，一般情況下私隱專員不會介入要求專業人士改正其作出的專業判斷的個案

答

問 企業若委聘資料處理者，需要注意甚麼？

- 只向資料處理者提供最低限度的個人資料
- 採取合約或其他規範方式以保障交託予資料處理者的個人資料
- 定期進行檢討，確保已採取足夠和全面的措施管理資料處理者

答

問 企業何時需要進行私隱影響評估？

- 當規管個人資料私隱的法規有重大改動時
- 企業對現行的處理個人資料程序作出重大改動時
- 企業引入新的個人資料種類
- 企業擬委託資料處理者代表處理個人資料時

答

4. 最新私隱議題

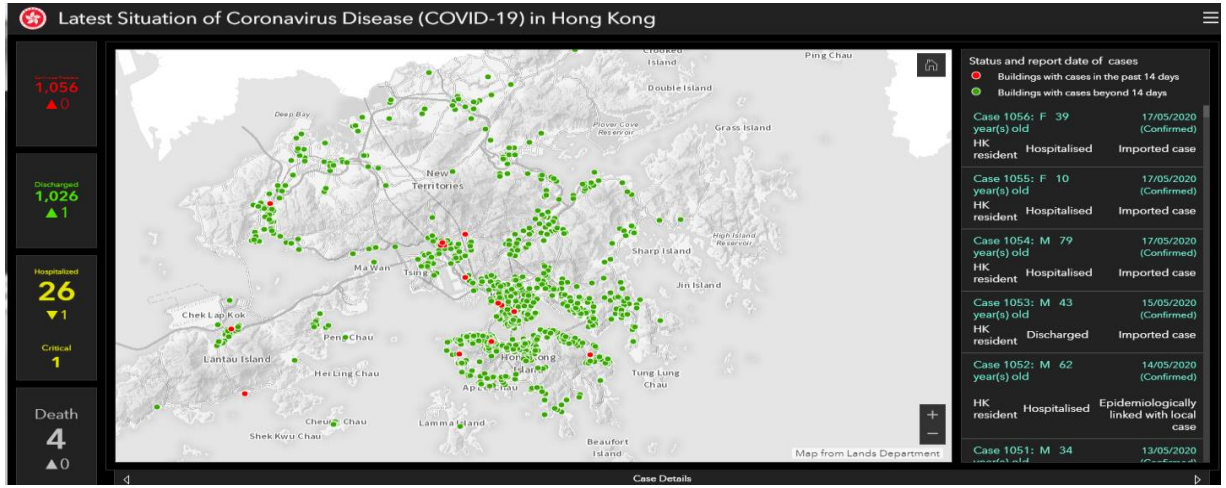
2019冠狀病毒病疫情引發的私隱議題

- 自2020年1月起就政府考慮推行的抗疫措施向政府提供有關個人資料私隱範疇的意見
- 回應傳媒 / 發出新聞稿共34次
- 媒體訪問 4 次

(1) 電子監察手環 + 手機應用程式

- 電子監察手環與手機應用程式「居安抗疫」一併使用 – 實施家居隔離
- 向所有入境人士實施（包括香港居民）
- 電子監察手環沒有定位設備
- 手機程式不會收集地理位置數據
- 通過分析環境通信信號（例如藍牙、Wi-Fi 和地理空間信號）確認一個人待在家裡

(2) 本地情況互動地圖



資料來源:
https://chp-dashboard.geodata.gov.hk/covid-19/en.html

- 列出已確診或疑似個案曾居住/到訪的建築物和乘搭過的航班/火車/船名單
- 列出已確診個案的狀況，包括性別和年齡
- 不會披露能夠識別確診者的資料
- 在保障私隱和資訊透明度之間取得良好平衡

(3) 追蹤密切接觸者的措施

- 口頭詢問

- 以重大事件調查及災難支援系(MIIDSS)，俗稱「超級電腦」和大數據分析以追蹤密切接觸者

條例下的豁免條文

- 第59(2)條 健康 -
  使用身份資料及位置資料在條例下可獲得豁免

- 第60B條 –法律程序
  如根據《預防及控制疾病(披露資料)規例》所規定的
  披露可獲得豁免

而不受第 3 保障資料原則的條文所管限

(4) 八達通向香港大學研究人員提供提供有關八達通卡的聚合資料，以遏止2019冠狀病毒病的傳播

- 利用八達通卡使用情況的統計資料來追蹤病毒的傳播，並確定香港各地區的感染風險，包括香港居民在不同地區接觸模式和密集度的資訊
- 不包含姓名、身份證號碼、電話號碼，卡識別碼等
- 無法確定任何人身份的資料

資料來源: 八達通卡有限公司

(5) 其他救助及保障措施

- **派發可重用口罩**

  個人資料的收集和使用的目的必需是合理的， 而收集的資料為足夠但不超乎適度

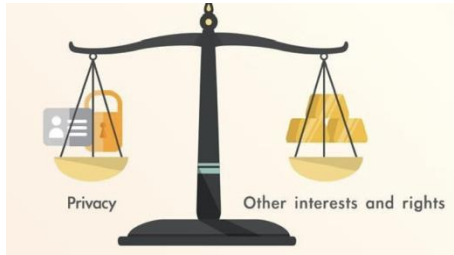
- **現金發放計劃**

  政府事前已與私隱公署作出溝通和交換意見，
  收集的個人資料實屬最少和必須，使用個人資料亦受適當的限制，並已確保在處理個人資料的過程中達致方便、快捷、安全、穩妥，符合條例的規定

資料來源: https://www.qmask.gov.hk/
https://www.cashpayout.gov.hk/eng/index.html

推行抗疫措施的考慮因素

- 私隱權**並非絕對**，須與其他利益或權利平衡
- 需衡量措施是否**必要或相稱**
- 措施是否合符**控制和預防冠狀病毒病傳播並拯救公眾生命的正當目的**
- 實行措施是否合理地與該正當目的有所關聯
- 措施帶來的限制**不能超越達到合法目的所需的程度**（即只會披露必須及不超乎適度的資料）
- 是否已在該措施帶來的社會利益與憲法保障的個人權利之間**取得合理平衡**，尤其是對社會利益的追求是否導致個人承擔過於嚴苛的負擔



問

疫情下僱主可收集僱員的健康數據 / 外遊資料嗎？

<u>僱主須平衡公共衞生和個人資料私隱：</u>

- 收集員工的健康數據或屬2019冠狀病毒病醫學症狀的有限資訊，一般情況屬合理做法
- 沒禁止任何機構收集他人的外遊資料

答

問 僱主可收集哪類個人資料，及如何正確地收集？

- 收集的資料是必要、適當及與達到的目的相稱
- 匿名或刪除可識別資料的方式處理
- 自我申報機制收集資料

答

疫情下保障員工個人資料

問

僱主可把收集的個人資料向其他人披露、或用作其他目的嗎？

- 除非得到相關人士自願給予的明示同意或《私隱條例》下的豁免適用
- 向政府或衞生機構披露他人身份、健康狀況及位置資訊作追蹤和治療感染者，不會被視為違反《私隱條例》
- 不透露感染者的個人身份信息作出通知

答

問 收集有關僱員的醫療及健康數據可被保留多久？

- 已達致收集目的後，經過一段合理時間亦沒證據說明僱員感染2019冠狀病毒病，或與感染者有密切接觸，僱主應永久銷毀為有關個人資料

答

疫情下保障員工個人資料

問

如實施在家工作安排，僱主或僱員可採取甚麼安全措施保障個人資料私隱？

問 在家工作應採取的安全措施

1. 由辦公室**轉移文件或電腦檔案**至家中前：

- 採取所有可行的步驟，防止個人資料外洩，尤其須注意：
  - 資料的種類及可能造成的損害
  - 資料存放的實體地點
  - 存放資料的設備是否已採取任何保安措施
  - 任何確保能查閱資料的人員具備良好操守、審慎態度及辦事能力的措施
  - 任何可確保安全傳送資料的措施
- 避免將個人資料 / 保密資料移離辦公室
- 先向上司尋求指示或批准，盡量減少轉移至外間的資料
- 將資料加密
- 運送期間小心保管資料
- 記錄資料的轉移歷程並保存記錄

答

問 在家工作應採取的安全措施

2. 在家工作並使用自己的裝置的僱員，要小心留意有關網絡保安以防資料外洩，應：

- 使用多重身份認證
- 不要和其他人共用工作裝置的帳戶
- 確保無線網絡安全（如加密數據）
- 定期更改裝置密碼
- 安裝適合的防病毒軟件
- 為裝置定期進行系統更新
- 勿點擊或開啟可疑網站及電郵
- 在發送或上載文件之前，仔細檢查要發送的內容和收件人的身份
- 使用在線會議工具時做好私隱及保安設定

答

問 如何安全使用VPN（虛擬私人網路）？

- ✓ 選擇有良好的私隱保護和數據安全往績的VPN供應商
- ✓ 留意VPN供應商所在的司法管轄區及其伺服器的位置，相關的資料保障法律法規可能會有所不同
- ✓ 選擇有高度加密功能的VPN供應商
- ✓ 了解VPN供應商記錄的資料種類，例如瀏覽過的網頁（ 記錄越少，私隱保障越好）
- ✓ 了解VPN供應商與第三方分享的用戶數據（分享越少，私隱保障越好）
- ✓ 了解並評估VPN應用程式的權限，並拒絕不必要的訪問權限要求

答

問

如公司使用視像會議軟件主持會議，應採取甚麼安全措施？

問 如何安全地使用視像會議工具？

- 將手機或電腦的應用程式更新到最新版本
- 使用專為使用視像會議工具而建立的電郵帳戶登入，避免使用現有的其他電郵帳戶登入
- 為會議設置一次性密碼，只提供會議密碼及連結給參加者
- 禁止電話撥入、禁止參與者早於主持人加入會議、並在參加者進入會議後鎖上會議，防止第三者的干擾
- 禁用視頻錄影功能、禁止文件傳輸，僅限主持人共享屏幕
- 參與者應使用耳機及在無必要時關閉攝錄鏡頭和麥克風，並避免談論非必要的私人資料
- 如果使用電腦及網絡瀏覽器進行視頻會議，應打開一個新視窗，並關閉其他應用程式
- 密切注意帳戶任何異常活動
- 保留所造成的任何損失的紀錄，以便將來有需要跟進時，仍有紀錄可循

答

5. 私隱影響評估及貫徹私隱的設計

私隱影響評估
(Privacy Impact Assessment)

- 私隱影響評估一般被視為可融合於決策過程的系統性風險評估工具

- 是一個系統性過程，用以評估一項計劃對個人資料私隱的影響，以達致避免或減低不利影響

私隱影響評估
(Privacy Impact Assessment)

1. 資料處理周期分析:

審視計劃背後的目的和理念 - 預算收集的個人資料種類、數量及程度是否必需

2. 私隱風險分析 :

識辨私隱關注的主要範疇，並集中處理

3.避免或減低私隱風險:

應採取適當的緩減措施，以保障個人資料被未經准許的查閱、使用、披露或喪失

4. 私隱影響評估報告:

應以報告形式清楚羅列評估結果、建議及採用的私隱保障措施

貫徹私隱的設計(Privacy by Design)

- 充分考慮保障私隱的需要
- 七項基本原則

貫徹私隱的設計

1. 主動和預防 (Proactive and preventive)
2. 預設資料保障 (Data protection as the default)
3. 端到端安全 (End-to-end security)
4. 收集最少量的個人資料 (Data minimisation)
5. 以使用者為中心(User-centric)
6. 具透明度(Transparency)
7. 風險最小化(Risk minimisation)

貫徹私隱的設計 (Privacy by Design)

- 《資訊及通訊科技系統的貫徹數據保障設計指引》與新加坡个人资料保护委员会共同製作（Guide to Data Protection by Design for ICT Systems）

貫徹私隱的設計 - 正面例子

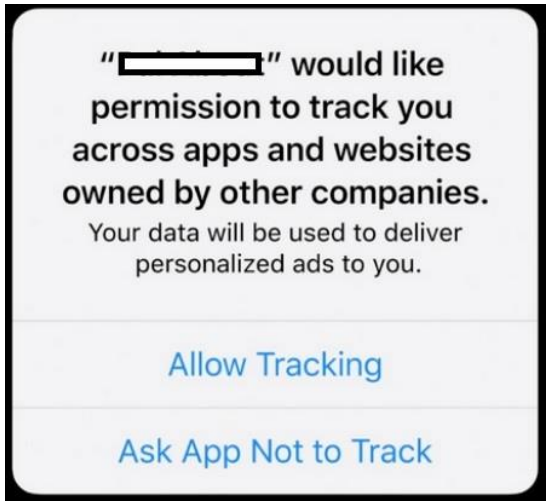
智能電話操作平台最新公布的私隱保障功能：

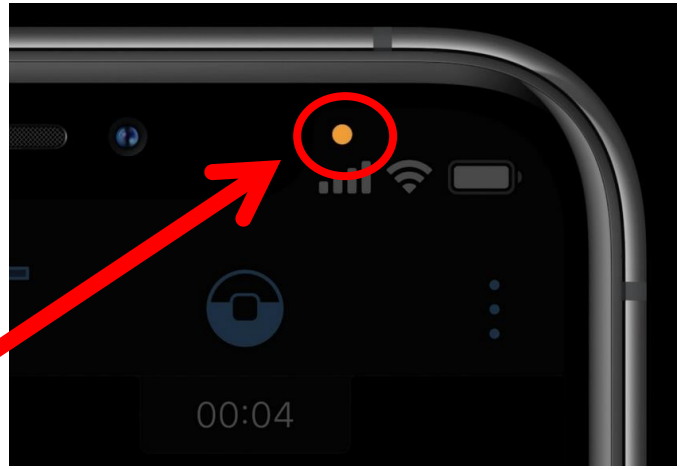
1. 清晰告知用户apps可能會收集哪些資料，及用甚麼資料追蹤用戶的網上行為

2. Apps進行跨網頁 / 跨app 的行為追蹤前要取得用戶的同意

3. 容許用戶向apps分享大概地理位置，而非確實位置

4. 當攝錄鏡頭 / 收音器正被使用時，會亮起訊號，防止apps偷拍 / 竊聽





資料來源：ZDNet (22/6/2020)

貫徹私隱的設計 - 反面例子

私隱政策不清晰

問題
1. 私隱政策分散於不同網頁，用戶難以全面理解
2. 徵求用戶同意時所展示的私隱政策撮要含糊、不夠詳盡
3. 因此，徵得的用戶同意無效

資料來源：Global Data Review (19/6/2020)

某視像會議應用程式的私隱及保安問題

問題: 容許主持人暗中監察與會者是否專注

改善措施: 永久移除相關功能

問題: 未得與會者同意下，從社交網站搜集其個人簡介，供其他與會者查閱

改善措施: 永久移除相關功能

問題: 暗中與社交網站分享用戶的資料

改善措施:
- 停止與有關社交網站分享「不必要」的用戶資料
- 更新私隱政策，提高透明度

問題: 未獲邀請者可闖進會議，散播不良資訊

改善措施:
- 要求用戶開設會議時設立會議密碼
- 預設啟動「等候室」功能以驗證與會者
- 身份

問題:

改善措施:

利用被視為較缺乏資料保障的地區的伺服器傳輸會議數據

- 容許付費用戶選擇數據傳輸的地區
- 承諾免費用戶的數據只會經由其所處地區的伺服器傳輸

訛稱使用「端對端」加密

- 澄清加密方式
- 即將推出「端對端」加密

問題:

改善措施:

$

拒絕為免費用戶提供新的「端對端」加密功能

- 承諾向所有用戶提供「端對端」加密功能，但免費用戶須提供額外資料（如電話號碼）以驗證身份
- 「端對端」加密功能並非預設的設定

其他潛在風險

- 停止開發新功能90天
- 集中資源處理現有問題

從該視像會議應用程式汲取的教訓

- 防患勝於未然，須採取貫徹私隱保障的設計
- 縱有補救措施，但損害已經造成（包括用戶私隱和機構聲譽）
- 須保持私隱政策的高透明度及高解釋度
- 私隱保障、資訊保安應大眾共享，非付費者的專利
- 良好私隱保障和資訊保安是營銷策略，更是良好管治行為、企業的社會責任

重新探索私隱管理模式

全球企業意見調查顯示：

- 遵守私隱法例不容易
- 新冠肺炎期間收集更多個人資料、使用更多通訊科技，符規更具挑戰
- 只有17%受訪企業使用私隱管理軟件
- 17%受訪企業仍在使用試算表（spreadsheet）管理個人資料

建議：

- 制訂全面、協調一致的私隱管理模式，
- 簡化、自動化私隱管理流程

資料來源：TrustArc (17/6/2020)

6. 私隱管理系統及實踐數據道德

數據經濟中的私隱挑戰

- “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

- 駭客入侵
- 資料外泄

跨範疇和跨境問題

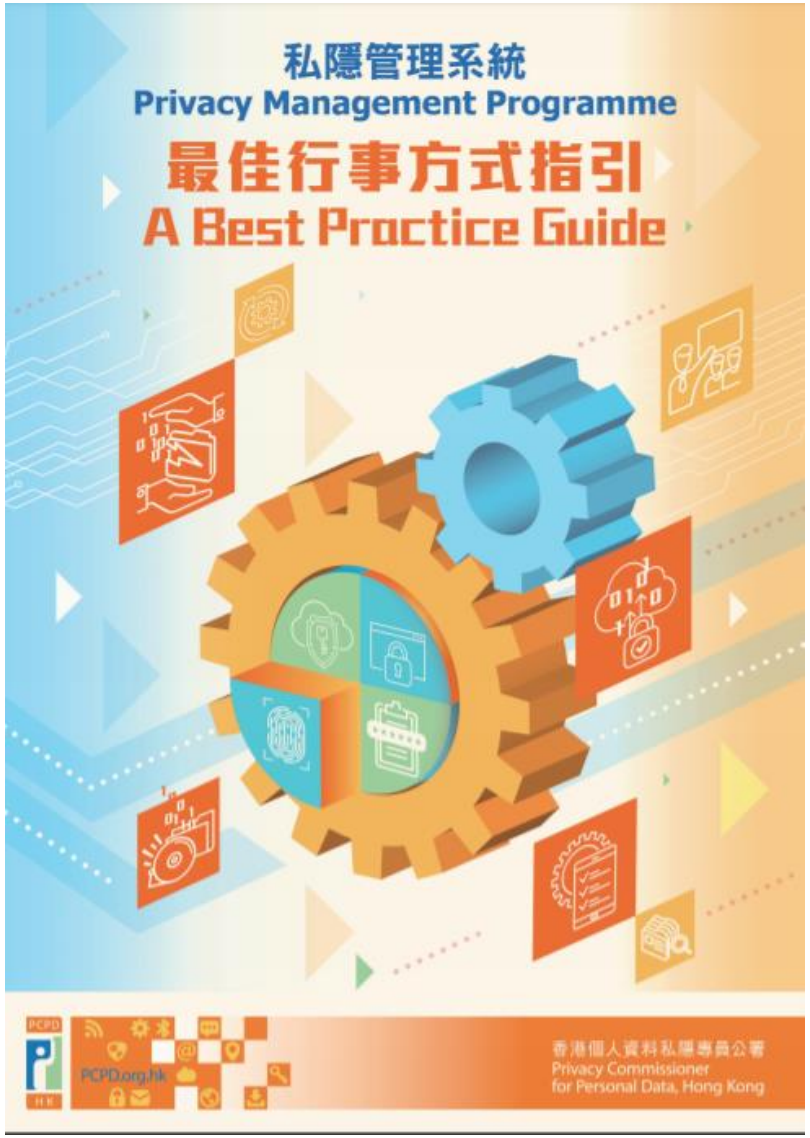
- 消費者保護
- 跨境資料流程通

解決方案：問責制和倫理道德

以風險為本的問責制

"GDPR 帶來的最大變化是圍繞**問責制**"
Elizabeth Denham, Information Commissioner of the UK

"GDPR旨在恢復我們對網路生活中所發生的事情的**信任**和**控制**."
Giovanni Buttarelli, European Data Protection Supervisor



私隱管理系統
(Privacy Management Programme)

- 由符規躍升為問責的保障個人資料策略
- 提倡企業把保障個人資料提升為良好的管治必要責任
- 由上而下貫徹地在企業中執行

甚麼是私隱管理系統？

合規方式

- 被動
- 補救
- 以解決問題為本
- 由合規部門處理
- 符合法律的最低要求
- 由下而上

模式轉變

問責方式

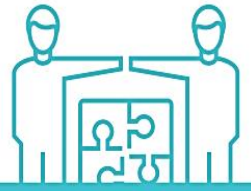
- 主動
- 預防
- 以符合客戶期望為本
- 由最高管理層指派
- 建立商譽
- 由上而下

問責制：私隱管理系統（PMP）

好處

- 有效管理個人資料
- 最大限度地降低隱私風險
- 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

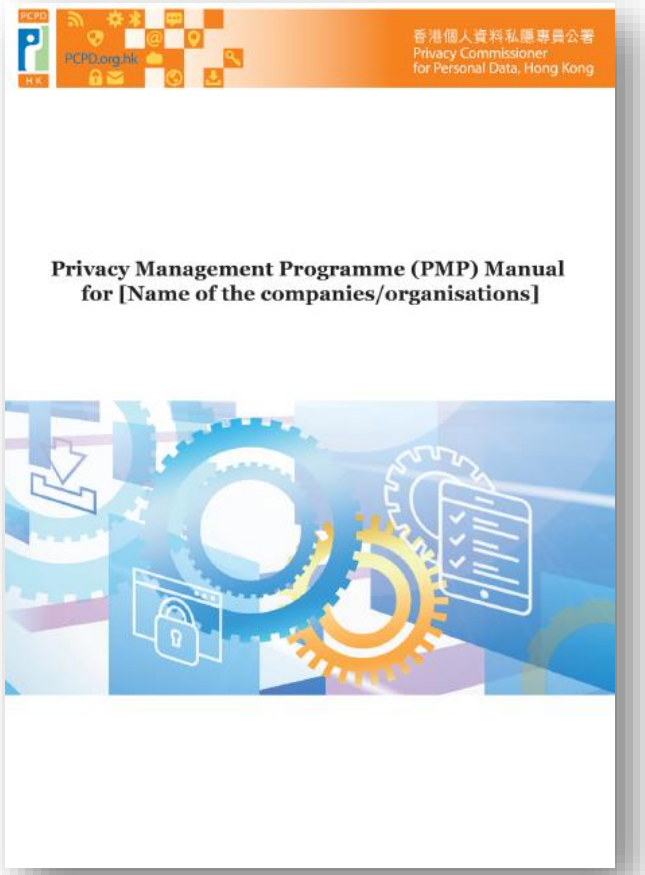
- **2.1** 個人資料庫存
- **2.2** 處理個人資料的內部政策
- **2.3** 風險評估工具
- **2.4** 培訓及教育推廣
- **2.5** 資料外洩事故的處理
- **2.6** 對資料處理者的管理
- **2.7** 溝通

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

General Reference Guide-Privacy Management Programme Manual (for Private Sector) (只提供英文版本)



- 概述企業處理個人資料的政策、做法、要求和指南，可作為企業開發和實施PMP的參考

數據道德 (Data Ethics)

- 積極推動將數據道德納入為數據管理問責要素（Data Stewardship Accountability Elements）
- 提倡尊重、互惠、公平的數據道德管理價值和模式

倫理道德與信任

數據

消費者

企業

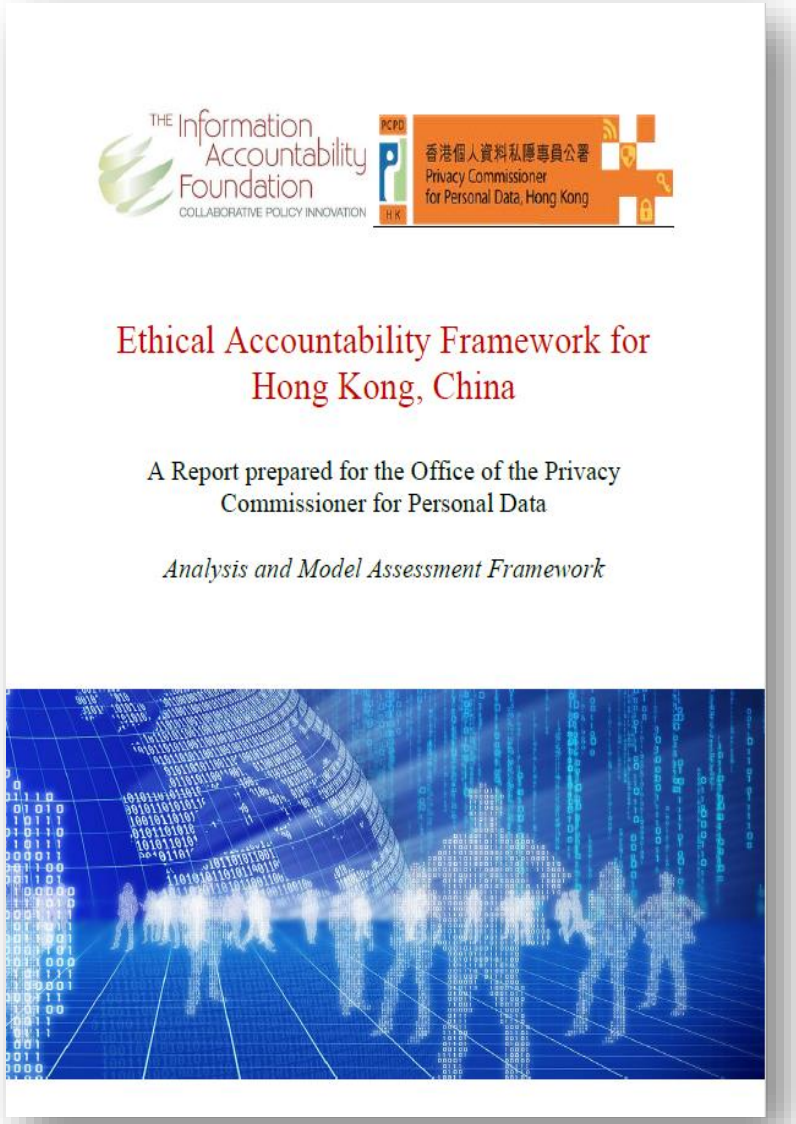
倫理道德義務

提倡道德：處理數據的正當性計劃

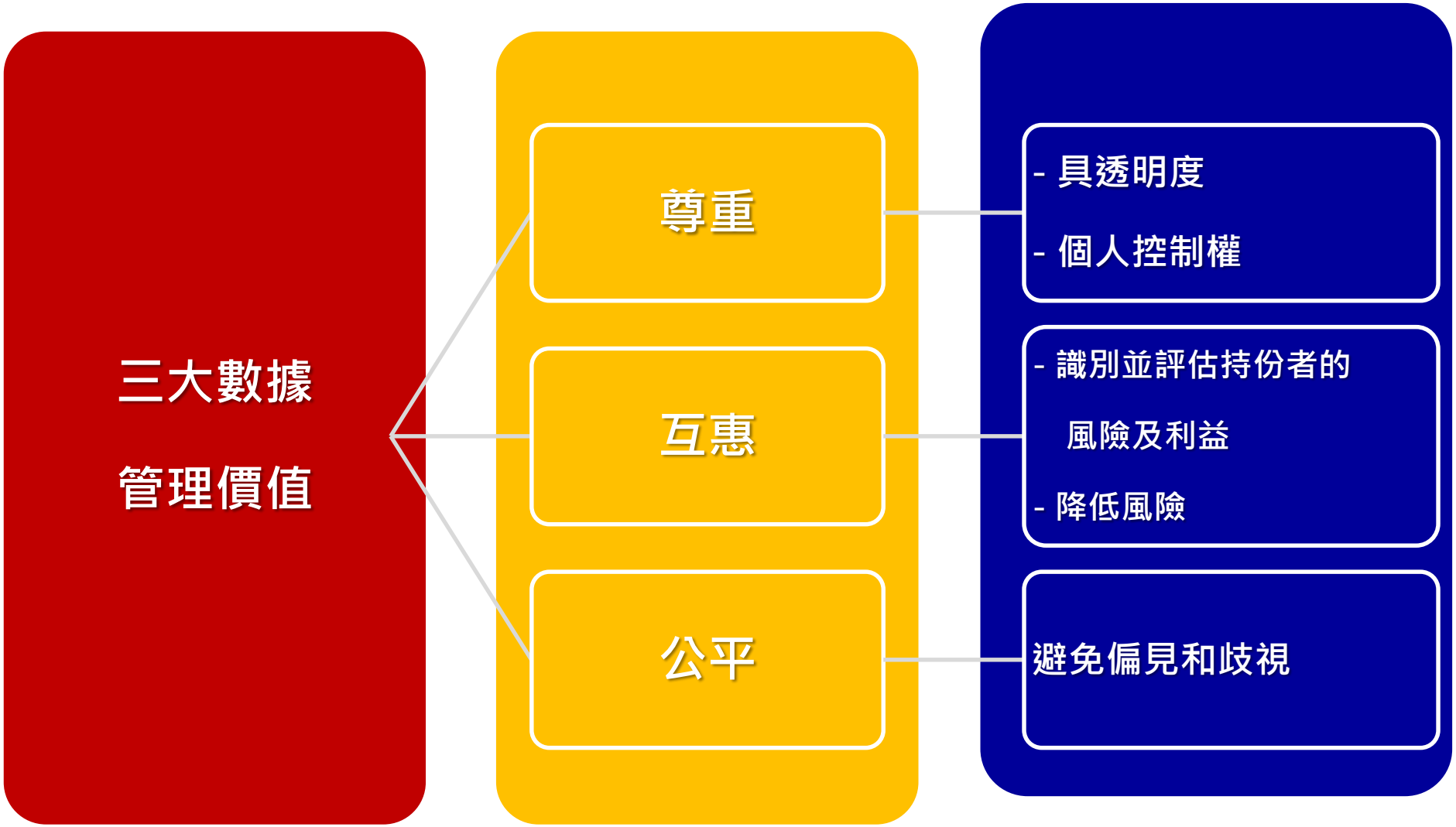
目標

- 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?
- 甚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?

2018年10月發布的顧問研究報告



核心價值



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、程序、培訓、工具、行為/實務守則
審核	道德數據影響評估 / 內部監控

有道德的數據管理問責

實踐數據道德
良好例子

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

1 HOW WE COLLECT AND STORE YOUR DATA

We collect your data

- when you interact with us and use our products and services
- visit our websites (see our Use of cookies policy on our website for details of how we use cookies)
- from other people and companies, including other HSBC group companies

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

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

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

2 WHAT WE USE YOUR DATA FOR

We use your data

- to send you direct marketing if you've consented to it
- to improve our products, services and marketing
- to help us comply with laws, regulations and requirements, including our internal policies, in or outside Hong Kong
- to detect, investigate and prevent financial crimes
- for the other purposes set out in section B

The Hongkong and Shanghai Banking Corporation Limited 115

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

3 WHO WE SHARE YOUR DATA WITH

We share your data with

- other HSBC group companies
- third parties who help us to provide services to you or who act for us
- third parties who you consent to us sharing your data with
- local or overseas law enforcement agencies, industry bodies, regulators or authorities
- the other third parties set out in section C

We may share your data locally or overseas.

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

You can access your data

You can request access to the data we store about you. We may charge a fee for this.

You can also ask us to

- correct or update your data
- explain our data policies and practices

You control your marketing preferences

You control what marketing you receive from us and how you receive it.

You can change this at any time by contacting us or updating your preferences on internet banking.

You can contact us

dfv.enquiry@hsbc.com.hk

The Data Protection Officer HSBC, PO Box 72677, Kowloon Central Post Office, Hong Kong

The Hongkong and Shanghai Banking Corporation Limited

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

A Collect and store

We may collect

- biometric data such as your voice ID, thumb print and facial recognition data
- your geographic data and location data based on your mobile or other electronic device
- data from people who act for you or who you deal with through our services
- data from public sources, credit reference, debt collection and fraud prevention agencies, and other aggregators

If you don't give us data then we may be unable to provide products or services.

We may also generate data about you

- by combining information that we and other HSBC group companies have collected about you
- based on the analysis of your interactions with us
- through the use of cookies and similar technology when you access our website or apps

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

B Use

We use your data to

- provide products and services to you including conducting credit checks
- provide personalised advertising to you on third party websites (this may involve us aggregating your data with data of others)
- help us to comply with requirements or requests that we or the HSBC group have or receive such as legal or regulatory in or outside Hong Kong . Sometimes we may have to comply and other times we may choose to voluntarily comply
- manage our business, including exercising our legal rights
- other uses relating to the above or to which you have consented

If you provide data about others

If you provide data to us about another person you should tell that person how we will collect, use and share their data as explained in this notice.

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

C Share

We share your data with

- local or overseas bodies or authorities such as legal, regulatory, law enforcement, government and tax and any partnerships between law enforcement and the financial sector
- any person who you hold a joint account with, people who can give instructions for you and anyone who is giving (or may give) security for your loans
- any third party who we may transfer our business or assets to so it can evaluate our business and use your data after any transfer
- partners and providers of reward, co-branding or loyalty programs, charities or non-profit organisations
- social media advertising partners (who can check if you hold an account with us and send our adverts to you and advertise to people who have a similar profile to you)

We may share your anonymised data with other parties not listed above. If we do this you won't be identifiable from this data.

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

D Direct Marketing

This is when we use your data to send you details about financial, insurance or related products, services and offers provided by us or our co-branding, rewards or loyalty programme partners or charities.

We may use data such as your demographics, the products and services that you're interested in, transaction behaviour, portfolio information, location data, social media data, analytics and information from third parties when we market to you.

We don't give your data to others for them to market their products and services to you. If we ever wanted to do this, we'd get your separate consent.

Data Privacy Notice

Notice relating to the Personal Data (Privacy) Ordinance

We protect your privacy. Read this notice to find out how we collect, store, use and share your personal data.

E Your Credit Information

If you apply for, have, or have had, a loan including a home loan

We'll perform credit checks on you which may involve us providing your loan data to a credit reference agency (CRA). The CRA will add this data to their database, which is available to other credit providers to help them assess whether to provide you with credit.

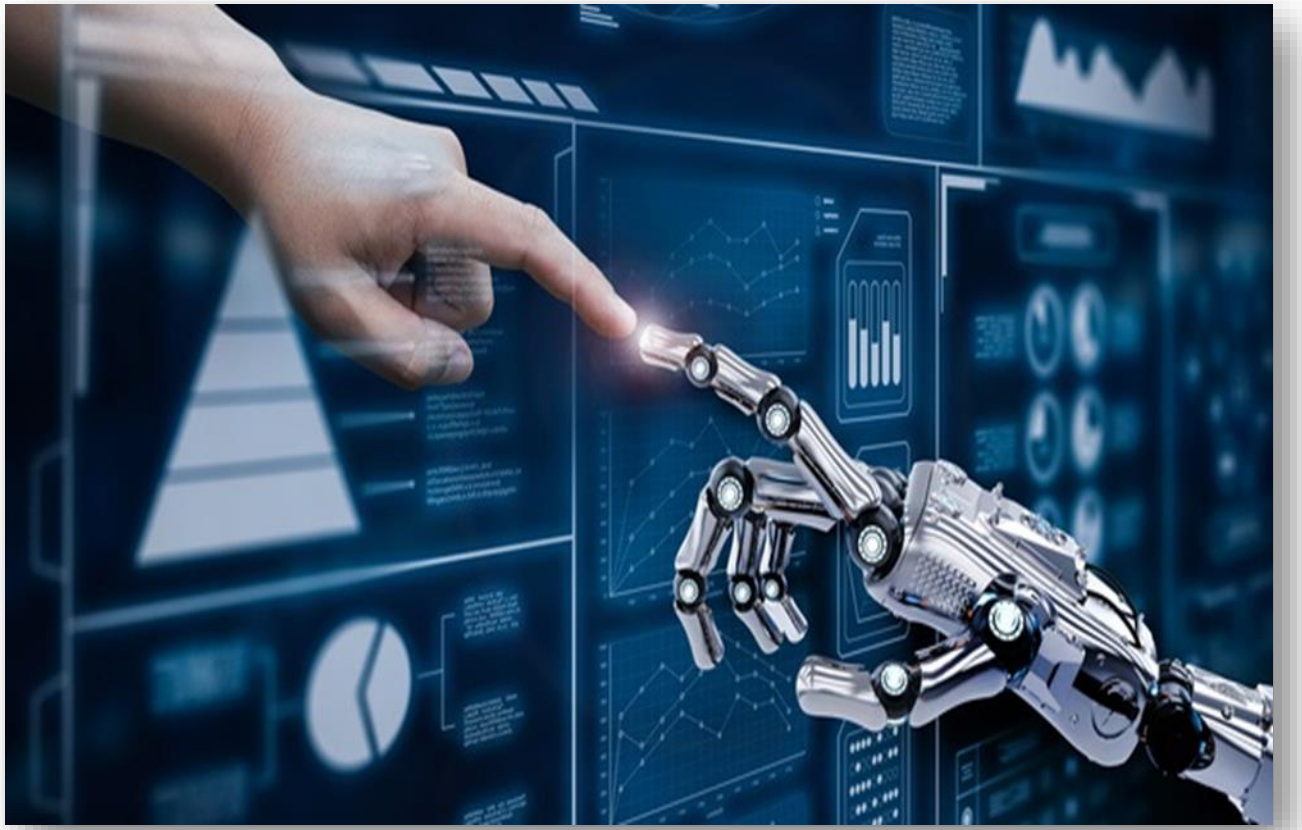
The CRA will keep your data. You can request that we ask the CRA to delete it once you've fully repaid your loan. They will only do this if:

- none of your payments were more than 60 days overdue in the 5 years before you fully repaid your loan. If they were, the CRA will keep your data for 5 years from the date you fully paid that missed payment
- you're not declared bankrupt with an amount under your loan being written off. If you are, the CRA will delete that record after 5 years from the date you're discharged from bankruptcy (you must tell them when this happens) or 5 years from the date you fully repay the overdue loan amount

If you have a home loan, we'll ask for your consent to share previous home loan data with CRAs.

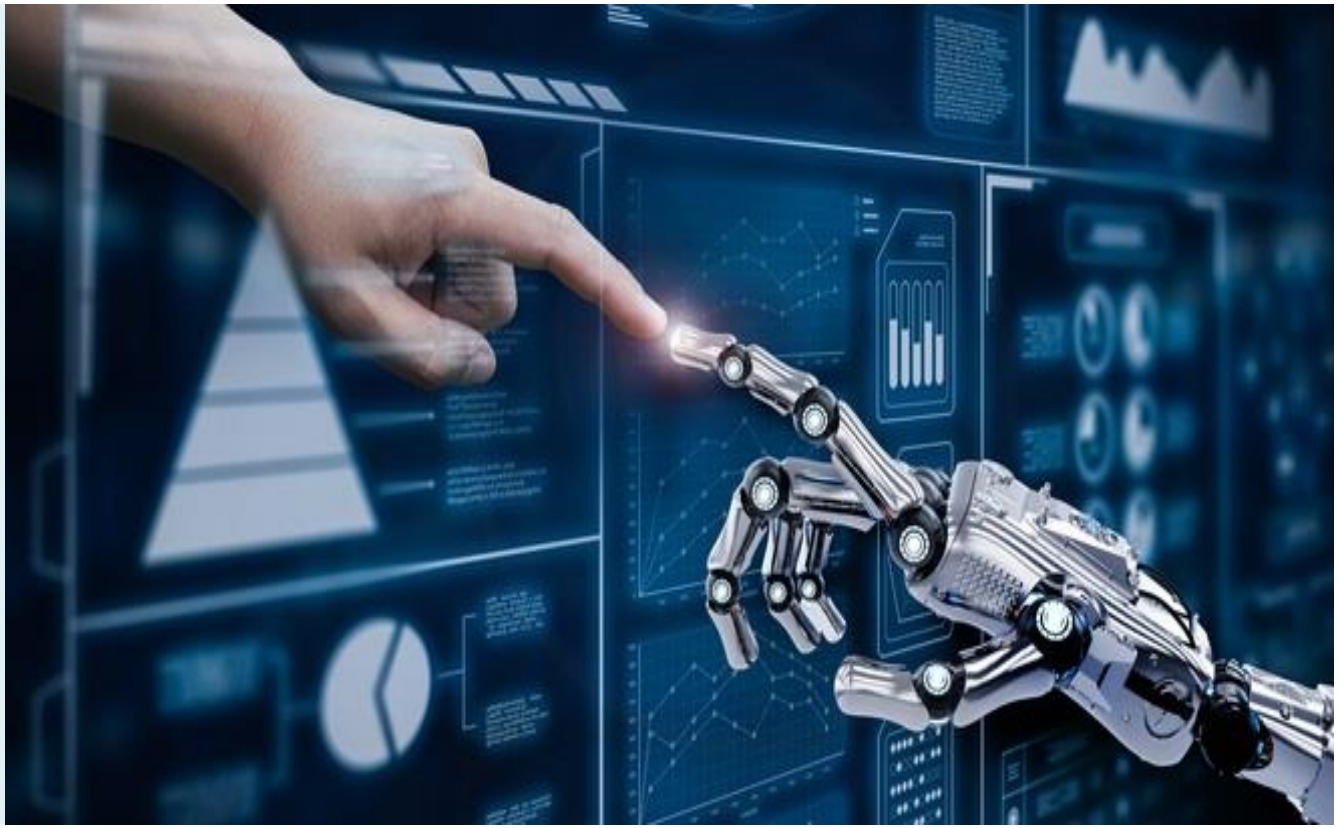
This notice will apply for as long as we store your data. We'll send you the latest version at least once a year. If we use your data for a new purpose, we'll get your consent.

人工智能與數據道德



歐盟《值得信賴的人工智能的道德準則》（“Ethics Guidelines for Trustworthy AI”）

目標：
建立以人為本的人工智能



資料來源：https://ec.europa.eu/futurium/en/ai-alliance-consultation

第40屆“國際資料保障及私隱專員會議”

(2018年10 月22-26日)

《人工智慧中的道德規範和資料保護宣言》

人工智慧開發的六個主要原則：

1. 公平原則
2. 持續關注和警惕
3. 系統透明度和清晰度
4. 貫徹道德的設計 (Ethics by Design)
5. 賦予每個人權力
6. 減少偏見或歧視

- 私隱專員擔任環球私隱議會人工智能的道德與資料保障工作常設工作小組聯席主席

- 小組現正進行十項工作計劃
- 私隱專員在環球私隱議會2020年6月電子通訊撰文

Working Group highlights

Ethics and Data Protection in Artificial Intelligence Working Group

The Chairs of the Working Group highlight progress in promoting implementation of the Declaration on Ethics and Data Protection in Artificial Intelligence

This permanent Working Group was established after the adoption of the Declaration on Ethics and Data Protection in Artificial Intelligence in October 2018, at the 40th ICDPPC. The aim of the Working Group is to promote the understanding of, and respect for, the guiding principles of the Declaration by all relevant parties involved in the development of AI systems, including; governments and public authorities; standardisation bodies; AI system designers; providers and researchers; companies; citizens and end-users of AI systems.

> It will not be long before the guiding principles of the Declaration create a flow-on effect on the general GPA community

The guiding principles of the Declaration include fairness, privacy by design and by default as part of ethics by design, reducing biases and discrimination, individual empowerment, continued attention and vigilance, system transparency and intelligibility.

After the adoption of the Declaration, the Executive Committee Secretariat launched a public consultation, which received a number of responses from different social and economic stakeholders. We have published a report on the responses to this public consultation, including the principles which might require more specific guidance.

While all respondents generally supported the six principles and the broad values presented in the Declaration, some respondents (mainly private enterprises) were of the opinion that ethical considerations should be flexible enough to cater for different types of AI use. One-size-fits-all approaches are not recommended by respondents. Feedback will be reflected in the future practical guidance. During the consultation period and after it, Working Group members also had direct exchanges with stakeholders, e.g., at the RightsCon in Tunis in 2019.

Current priorities

The Working Group currently has a 10-item work programme, which includes, but is not limited to, the following significant and far-reaching projects, on which the members and observers are currently working:

- Statement on the relationship between ethics, human rights, and data protection in AI;
- Statement on the need for demonstrable accountability for AI systems;
- Planned resolution on how data protection and privacy is essential to sustainable digital growth and AI innovation; and
- Member survey on the capacity and expertise of authorities in addressing ethical and data protection issues in AI systems – a starting point towards a gap analysis.

The Working Group invites all members and observers of the GPA to contribute to two repositories, which it has set up. One includes policy documents and legal instruments, adopted by privacy and data protection authorities or relevant legislative bodies at national, supranational, or subnational level. The other repository collects real life cases of applications of AI, in particular where GPA members or observers have observed or assessed their impacts. The Working Group welcomes submissions to its Secretariat and will make the collected material available to the GPA membership.

Adapting to new considerations

In light of the "White Paper on Artificial Intelligence – A European approach to excellence and trust" (the White Paper) released by the European Commission in February 2020, members of the Working Group are discussing the issues raised in the White Paper and plan to submit a collective and well-balanced response to the European Commission.

The thrust of the White Paper is the importance of human-centric development for trustworthy and transparent AI, which fits well with the principles that the Working Group is aiming for. The Working Group will carefully consider the suggestions in the White Paper to further promote the Working Group's main objectives and proactively support an active public debate on digital ethics

10

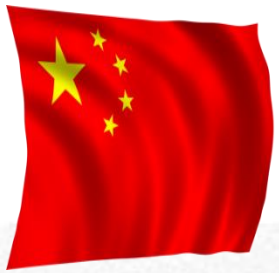
歐盟《值得信賴的人工智能的道德準則》

七個關鍵要求：

- 人力資源和監督
- 技術穩健性和安全性
- 隱私和資料治理
- 透明度
- 多樣性，非歧視和公平
- 社會和環境福祉
- 問責制

資料來源：https://ec.europa.eu/futurium/en/ai-alliance-consultation

國家對大數據和人工智能的政策



《国家信息化发展战略纲要》绘十年产业蓝图

2016年09月12日 17:43:37　来源：《网络传播》7月刊　【打印】【纠错】

重点是发展核心技术、夯实基础设施、开发信息资源、优化人才队伍、深化合作交流

主要是落实“五位一体”总体布局，对培育信息经济、深化电子政务、繁荣网络文化、创新公共服务、服务生态文明建设作出安排，并首次将信息强军的内容纳入信息化战略

强调要保障信息化有序健康安全发展，明确信息化法治建设、网络生态治理和维护网络空间安全的主要任务

- 加強互聯網管治
- 保障公民的法律權利

資料來源: 中央網路安全和資訊化委員會辦公室 (2016年9 月12日)

國家對大數據和人工智能的政策

中國科學技術部於2019年2月成立的人工智慧治理專家委員會

於2019年6月發佈「新一代人工智能的治理原則」

八個原則:

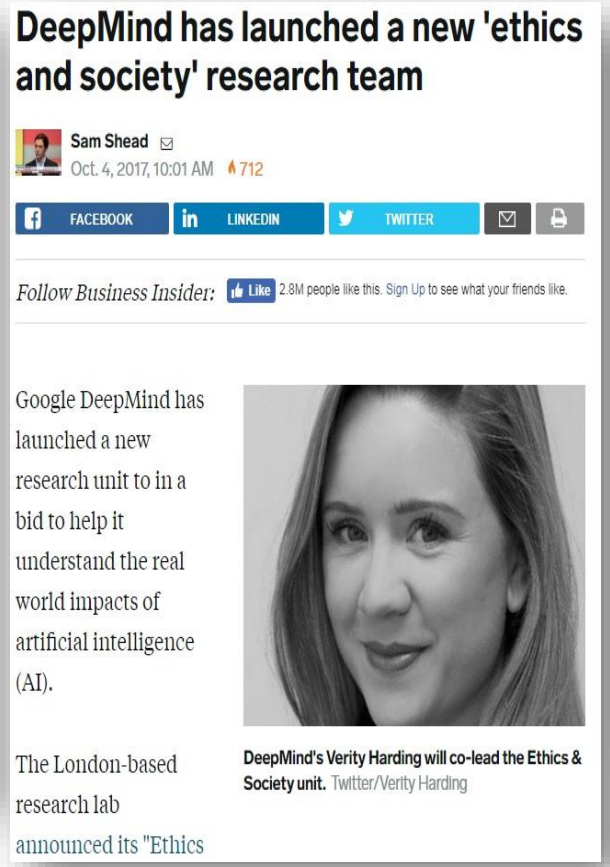
1. 和諧友好
2. 公平公正
3. 包容共享
4. 尊重私隱
5. 安全可控
6. 共同責任
7. 開放協作
8. 敏捷治理

商界的回應

Gartner picks digital ethics and privacy as a strategic trend for 2019

Natasha Lomas @riptari / 1 month ago

資料來源: 2018年10月15日
《 TechCrunch 》



DeepMind has launched a new 'ethics and society' research team

Sam Shead
Oct. 4, 2017, 10:01 AM 712

FACEBOOK LINKEDIN TWITTER

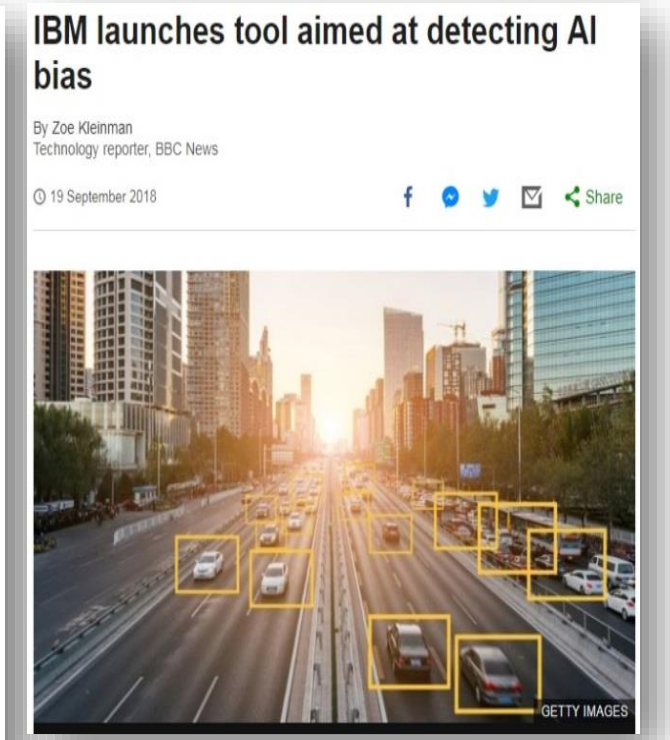
Follow Business Insider: Like 2.8M people like this. Sign Up to see what your friends like.

Google DeepMind has launched a new research unit to in a bid to help it understand the real world impacts of artificial intelligence (AI).

The London-based research lab announced its "Ethics

DeepMind's Verity Harding will co-lead the Ethics & Society unit. Twitter/Verity Harding

資料來源: 2017年10月4日
《 Business Insider》



IBM launches tool aimed at detecting AI bias

By Zoe Kleinman
Technology reporter, BBC News

19 September 2018 Share

GETTY IMAGES

資料來源: 2018年9月19 日
《BBC》

7.國內與私隱相關的最新法規

《中華人民共和國民法典》提升私隱和個人信息保護

《中華人民共和國民法典》

- 基本民事法律
- 2020年5月28日十三屆人大會議通過
- 2021年1月1日生效
- 當中《人格權篇》有關隱私權和個人信息保護條文

《民法典》-「人格權篇」

- 保留《網路安全法》對個人資訊保護的法律原則
- 「隱私」的定義結合中國古代「不願為他人知曉」和「私密」等表述

《民法典》-「人格權篇」

- 自然人享有隱私權
- 隱私是自然人的私人生活安寧和不願為他人知曉的私密空間、私密活動、私密信息
- 任何組織或者個人不得以刺探、侵擾、洩露、公開等方式侵害他人的隱私權

（第1032條）

- 自然人的個人信息受法律保護

- 處理個人信息應當遵循合法、正當、必要原則，不得過度處理，並符合一系列的條件，如具透明度和獲得當事人的同意

（第1034條）

《個人信息保護法》將出台

- 十三屆人大會議公佈工作計劃包括制定《個人資訊保護法》和《 數據安全法》
- 全國政協委員、北京國際城市發展研究院院長連玉明建議：
  - 應盡快建立個人資訊保護監管機構
  - 借鑒香港個人資料私隱專員公署

8.歐盟《通用數據保障條例》

歐洲聯盟《通用數據保障條例》

- 於2018年5月25日生效
- 代替1995年的資料保障指令（歐盟指令）

為何《通用數據保障條例》與香港的企業有關？

- 草擬《私隱條例》時曾參考歐盟指令

- 企業在以下情況下可能需要遵從《通用數據保障條例》的規定：

  (1) 在歐盟設立機關，而該機關的活動涉及處理個人資料
  (2) 在歐盟沒有設立機關，但向歐盟人士提供貨品或服務或監察他們的行為

私隱公署就《通用數據保障條例》收到的查詢數字

關注範疇	查詢數字
《通用數據保障條例》的範圍和適用性	163
《通用數據保障條例》的要求	74
私隱公署有關《通用數據保障條例》的指引/研討會	21
比較《通用數據保障條例》與《私隱條例》	15
私隱公署在《通用數據保障條例》中的角色	11
總數	284

私隱公署就《通用數據保障條例》收到的投訴數字

- 五宗
- 在港的歐盟人士，誤以為一些公司在香港就他們的個人資料在香港的處理，受《通用數據保障條例》管轄
- 在歐盟人士向私隱公署投訴一間本地公司有資料外洩

《歐洲聯盟《通用數據保障條例》2016 最新資訊》

- 2018年版本的「加強版」
- 涵蓋《通用數據保障條例》兩年來的實踐經驗和個案
- 協助機構及企業更深入了解該條例的實施情況

https://www.pcpd.org.hk/tc_chi/data_privacy_law/eu/files/eugdpr_c.pdf

《通用數據保障條例》有以下的主要目標：

- 協調及簡化現時的數碼單一市場的框架；
- 讓個人掌握他們的資料；
- 制定現代化的保障資料規範；及
- 基於問責原則的管治。

《通用數據保障條例》的重點：

《通用數據保障條例》

- 已有違反《通用數據保障條例》而被罰款的案例
- 預期日後更多罰款情況

- ❖ 一個網上搜尋引擎在使用個人資料作個人化廣告時欠缺透明度及有效同意，被法國監管機構判罰5,000萬歐元
- ❖ 該搜尋引擎在提供個人化廣告方面的資訊不清晰、不全面，個別用戶不易查閱
- ❖ 顯示「用戶同意」的格子是預先加上剔號

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（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	資料使用者（控制者／處理者）： • 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、處理或使用的人個人資料
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	「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； • 從該資料直接或間接地確定有關的個人的身分；及 • 該資料的存在形式令予以查閱及處理均是切實可行的

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	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 • 採取預設貫徹私隱的設計及預設 • 為高風險的處理活動進行資料保障評估；及 • 委任保障資料主任	• 沒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
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	沒有以任何目的區分敏感及非敏感個人資料

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	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 • 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 • 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

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	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	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）
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	• 資料處理者不是直接受規管 • 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

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	歐盟	香港
資料當事人增及提升的權利 	• 就資料處理獲通知的權利 • 刪除個人資料權（「被遺忘權」） • 限制處理及資料可攜權 • 反對處理（包括個人概況彙編）的權利	• 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 • 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 • 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，而《條例》中亦有條文規管資料核對程序

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	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	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
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	認證制度及依從實務守則未有明確定為法律基礎
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 • 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%	• 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

參加

保障資料主任聯會

(會籍申請)

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

成為會員，你可以 ：

- 透過經驗分享和出席公署舉辦的培訓活動，增加對資料私隱合規的認識和促進企業合規實踐
- 報讀公署專業研習班，報名費享有八折優惠
- 透過公署出版的電子通訊接收資料私隱的最新發展資訊

成為保障資料主任聯會會員後，公署會把貴公司名稱刊登在公署網頁內「保障資料主任聯會會員列表」

年費：港幣 $350*

查詢： dpoc@pcpd.org.hk

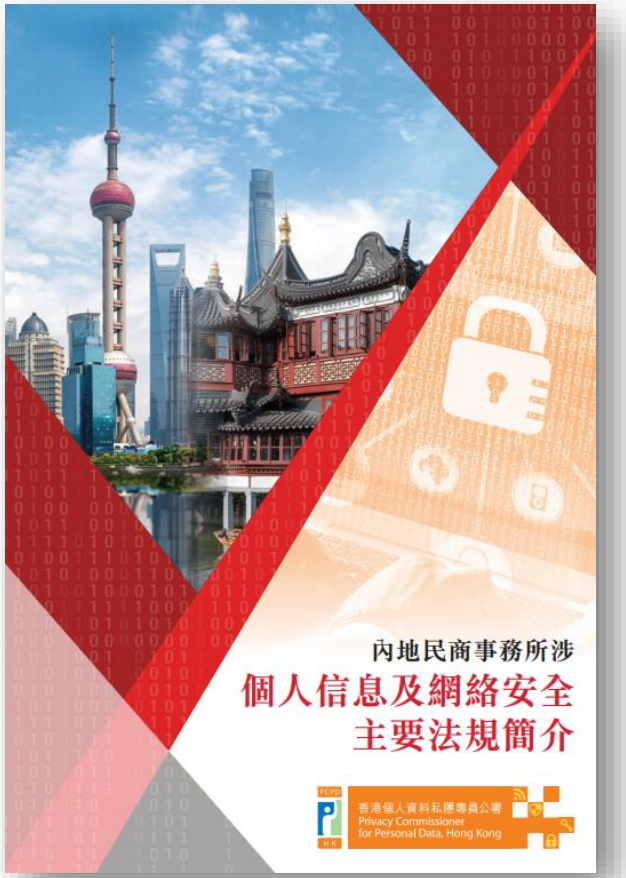
https://www.pcpd.org.hk/misc/dpoc/files/AppForm_1920_NewMembers.pdf

*八折
2020年6月30日前入會

關注私隱運動2020
海報

《由原則至行動 – 中小企
保障個人資料實務手冊》

《內地民商事務所涉個人信息
及網絡安全主要法規簡介》



《歐洲聯盟《通用數據保障條例》
2016 最新資訊》小冊子

派發安排：

請於2020年6月24日起親臨個人資料私隱專員公署接待處領取

聯絡我們

查詢熱線	2827 2827
傳真	2877 7026
網址	www.pcpd.org.hk
電郵	enquiry@pcpd.org.hk
地址	香港皇后大道東248號 陽光中心13樓1303室

WEBINAR "WORKING OUT FOR THE NEW DATA ECOSYSTEM AND LEGAL FRAMEWORKS"

SPEAKER

MR STEPHEN KAI-YI WONG, BARRISTER,
PRIVACY COMMISSIONER FOR PERSONAL DATA,
HONG KONG

KEY TAKE-AWAYS

- Overview of the global development in personal data protection
- EU GDPR two years on
- Stepping up privacy and personal information protection in the mainland of China
- Other international development in the post-GDPR era: Singapore, India, and the United States
- Global convergence towards higher watermark in personal data protection
- Amendment of the Hong Kong Personal Data (Privacy) Ordinance

DATE: 28 JULY 2020
TIME: 2:30PM - 5:30PM
MODE: ONLINE
CPD POINTS: 3
www.pcpd.org.hk

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

問與答

www.PCPD.org.hk

下載本簡報