個人資料私隱專員公署在協助企業和機構提升數據管治的角色

鍾麗玲
個人資料私隱專員

陳美儀
個人資料私隱專員公署
首席個人資料主任

2022年11月9日

內容

- 關於私隱專員公署
- 資料外洩事故及私隱專員公署的角色
- 應對2019冠狀病毒病所引起的私隱議題
- 人工智能與粵港澳大灣區發展
- 內地及海外保障個人資料的相關法規
- 行業保障私隱活動
- 個人資料私隱管理系統

關於私隱專員公署

職能

個人資料私隱專員公署（**私隱專員公署**）是一個**獨立監管機構**，負責**監察、監管及確保**香港法例第486章《個人資料（私隱）條例》（**《私隱條例》**）獲得遵從。

私隱專員公署於1996年8月成立。

《私隱條例》在1996年12月20日生效。

私隱專員公署的角色

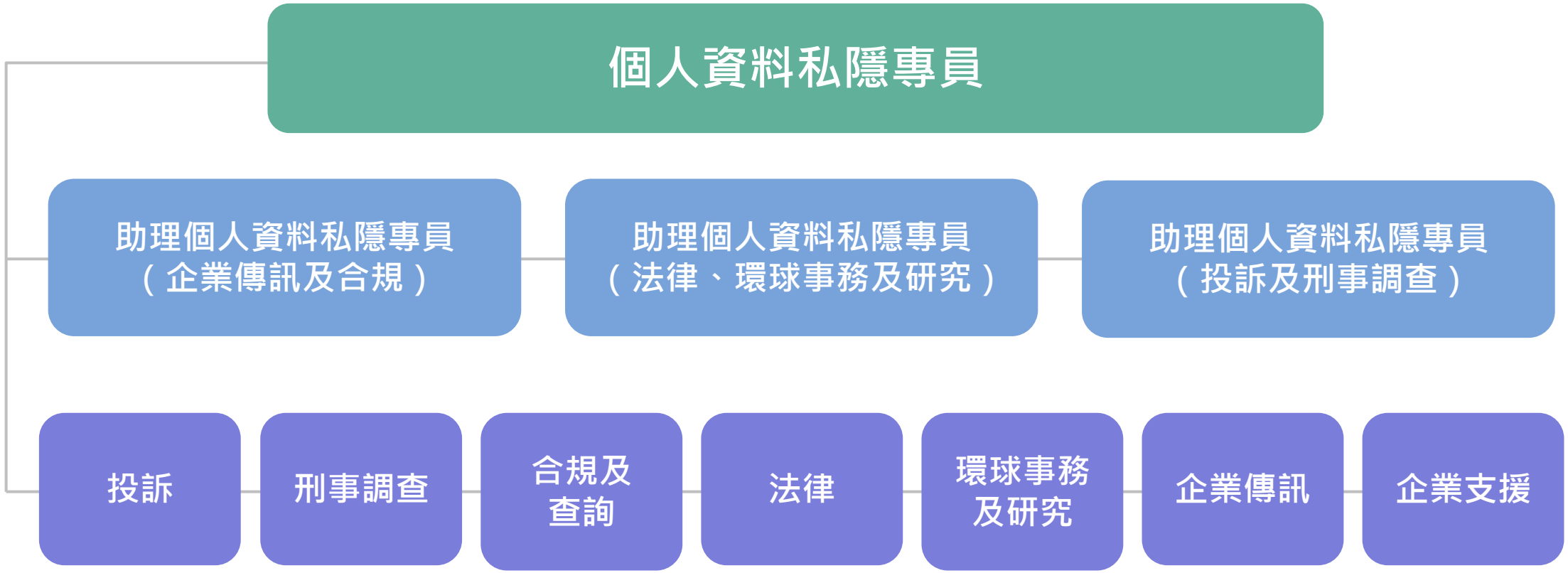
願景

培養及推廣保障與尊重個人資料私隱的文化。

使命

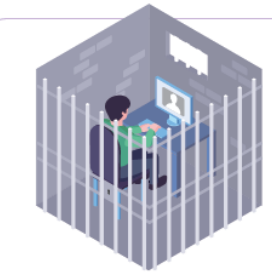
- 透過**宣傳和教育**，推廣保障及尊重個人資料私隱
- 透過**提供指引和最佳行事常規**，促進合法及負責任地使用個人資料
- 透過**有效執法**，監察及監管循規情況
- 透過**持續檢視和優化**，並**參考全球**個人資料私隱保障的**標準**，維持監管機制的效能

私隱專員公署架構


個人資料私隱專員
助理個人資料私隱專員（企業傳訊及合規）
助理個人資料私隱專員（法律、環球事務及研究）
助理個人資料私隱專員（投訴及刑事調查）
投訴
刑事調查
合規及查詢
法律
環球事務及研究
企業傳訊
企業支援

2021-22年度的主要數字

3,368
接獲3,368宗投訴個案
Received 3,368 complaints



1,351
處理1,351宗「起底」個案
Handled 1,351 doxxing cases

96
展開96次調查
Initiated 96 investigations

142
接獲142宗資料外洩事故通報
Received 142 data breach notifications

373
進行373次循規審查
Carried out 373 compliance checks

16,944
接獲16,944宗公眾查詢
Received 16,944 public enquiries

65
展開65次刑事調查
Initiated 65 criminal investigations

註：由2021年4月至2022年3月

2021-22年度的主要數字（續）

33

發布33篇新聞稿
Issued 33 media statements

144

回應144宗傳媒查詢
Responded to 144 media enquiries

2,742

2,742則與私隱公署的工作相關的新聞於不同的傳媒平台報道
2,742 news reports relating to PCPD's work were published on various media channels

296

於社交媒體發表296篇帖文
Published 296 social media posts

32,794

32,794人次參加私隱公署的講座、研習班及工作坊，加強對《私隱條例》的理解及遵從
Recorded 32,794 attendances at PCPD's talks, seminars and workshops to enhance understanding of and compliance with the PDPO

155,901

錄得每月平均155,901人次瀏覽私隱公署網站
Recorded an average of 155,901 visits to the PCPD's website per month

註：由2021年4月至2022年3月

資料外洩事故及私隱專員公署的角色

資料外洩事故有上升趨勢

近年大型資料外洩事故及受影響人數		
2020	Estée Lauder	4.4億
	微軟	2.5億
	Instagram, TikTok, YouTube	2.35億
2019	Capital One（銀行）	1.6億
	Zynga（社交平台遊戲開發商）	2.18億
	Facebook	4.19億
2018	萬豪國際	3.83億
	Twitter	3.3億
	Facebook	1.4億
	Uber	5,700萬
	國泰航空	940萬

2021及2022年大型資料外洩事故

平台	受影響人數	受影響人數（香港）
Facebook	5.33億	293萬
LinkedIn	5億	28萬（所有香港用戶）
Optus	1000萬	-
印度航空	450萬	-

2022年資料外洩事故

香港科技探索有限公司

- 經營網購平台 **HKTVmall**
- 於2022年1月發現電腦系統有異常和可疑的活動
- **438萬**登記用戶資料中，「小部分」資料被取覽

前民政事務局慶典統籌辦公室

- 負責協調2022年7月1日舉行的「香港特別行政區成立25周年慶典」
- 在儀式前向嘉賓發送電郵，告知他們活動期間應遵守的防疫措施
- 但負責的工作人員卻未有使用密件副本（bcc）功能，導致**400多**名嘉賓的電郵地址外洩

《私隱條例》的相關規定

有關個人資料保安的規定　*保障資料第4原則：*

4　保安措施 Security

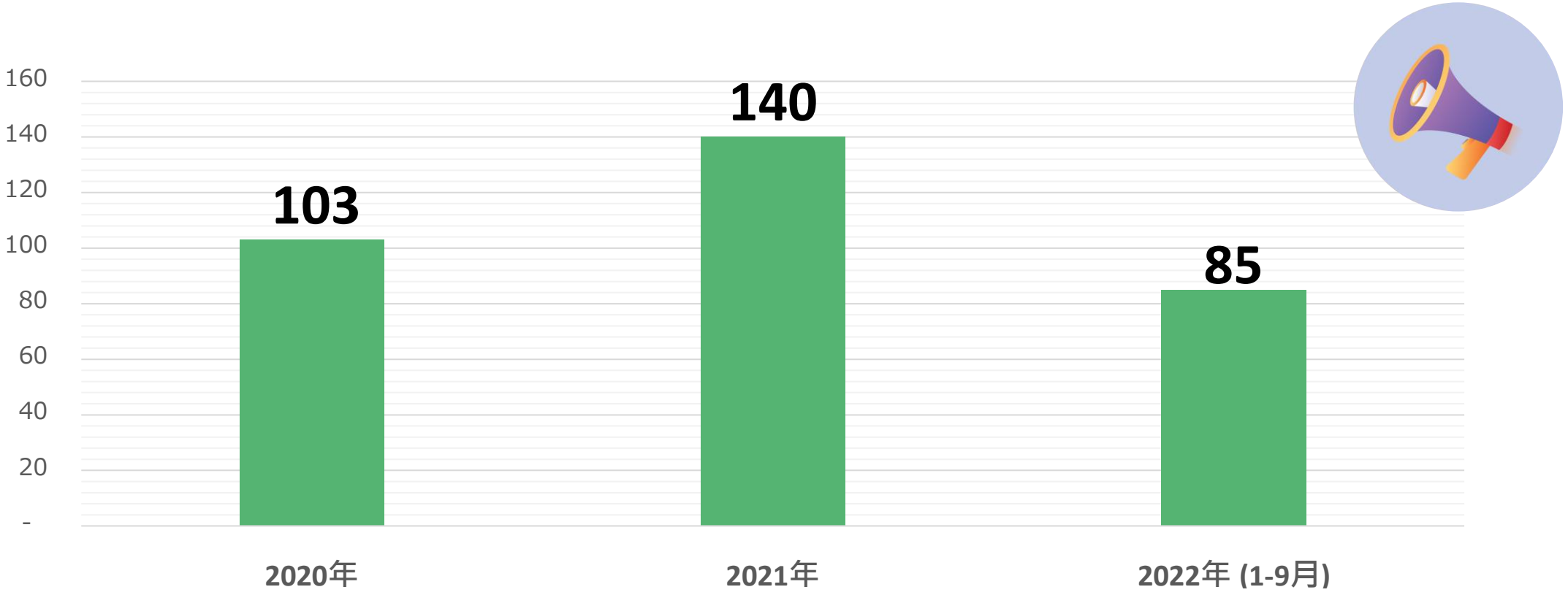
資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

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

NOTE

資料外洩事故一般是指因資料使用者的保安不足或存有漏洞，從而引致個人資料被人未經授權或意外地查閱、處理、刪除、喪失或使用，因此有關事故有可能構成違反保障資料第4原則的規定。

私隱專員公署接獲的個人資料外洩事故通報



私隱專員公署針對個人資料外洩事故採取的跟進行動

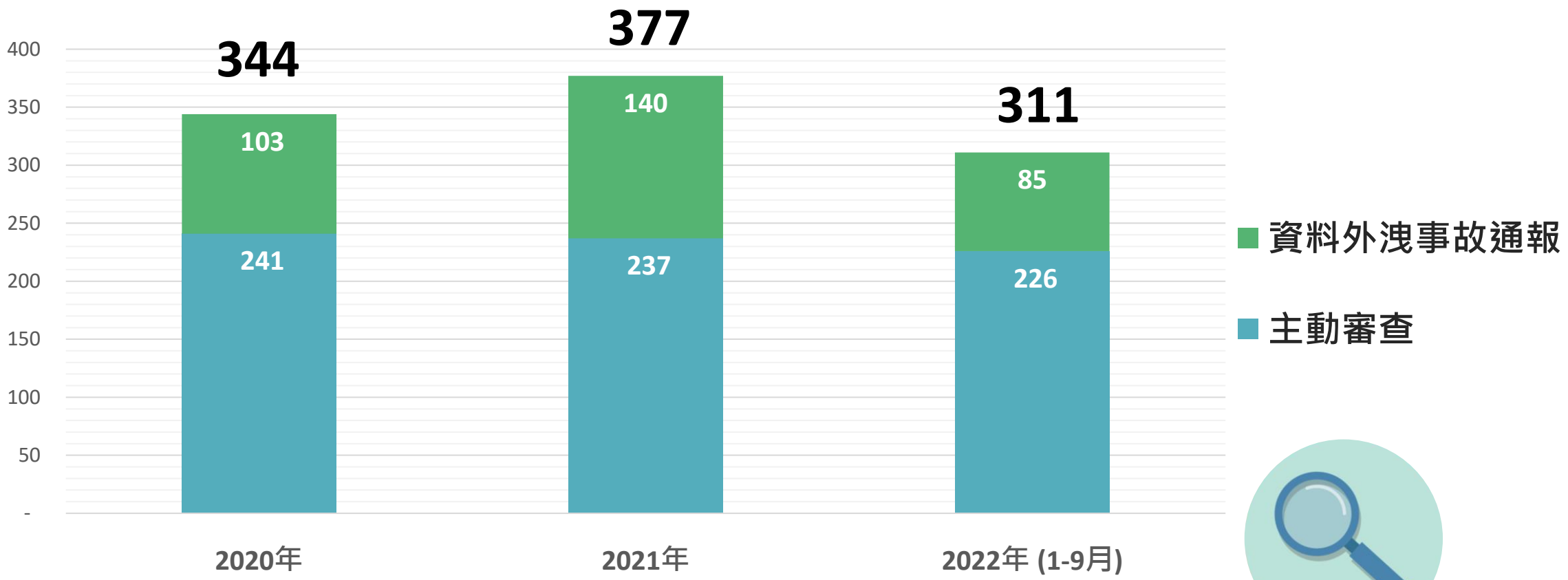
若發生資料外洩事故，機構的**商譽**或會受損，
並失去客戶的**信任**

向私隱專員公署**作出通報**

私隱專員公署可就處理資料外洩**作出建議**

注意： **不論機構有否就資料外洩事故作出通報**，
私隱專員公署也可能就事故進行調查

循規審查


400
350
300
250
200
150
100
50
-
344
103
241
377
140
237
311
85
226
2020年
2021年
2022年 (1-9月)
資料外洩事故通報
主動審查

《私隱條例》的相關規定

有關專員的職能及權力 *第8(1)條：*

私隱專員須就遵守《私隱條例》條文作出監察及監管，並促進對《私隱條例》的認識及理解以及遵守。

發現機構的行事方式與《私隱條例》規定不相符

考慮對有關機構展開循規審查或調查

指出明顯的不足之處並建議補救措施

發出執行通知

《私隱條例》的相關規定

有關個人資料系統的視察 *第36條：*

賦權專員對資料使用者，或屬於某類別的資料使用者所使用的任何個人資料系統進行視察，並向資料使用者作出建議。

私隱專員公署一直致力就各界遵守《私隱條例》條文作出監察及監管，包括行使《私隱條例》第36條的權力，到持有大量市民個人資料的機構就資料系統進行實地視察。公署會按個別情況建議有關機構加強保障客戶個人資料私隱。

資訊及通訊科技的保安措施指引

資料保安建議措施 *七大建議措施一覽*

1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

應對2019冠狀病毒病所引起的私隱議題

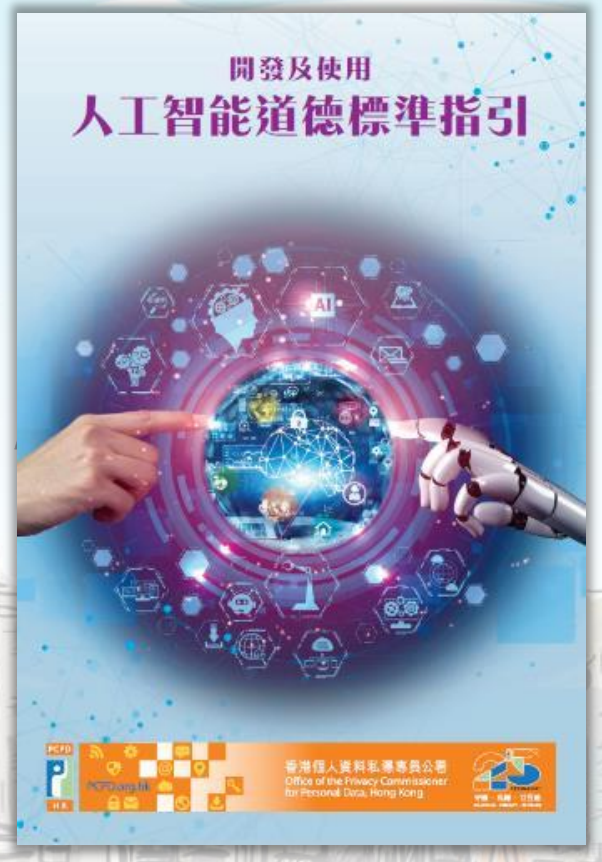
私隱專員公署就2019冠狀病毒病大流行所引起的個人資料私隱議題**發出23份指引 / 新聞稿**，包括：

- 《僱主在2019冠狀病毒病疫情期間收集及使用僱員個人資料的指引》
- 「在家工作安排下的個人資料保障」系列指引及單張：(1) 機構篇、(2) 僱員篇及 (3) 使用視像會議軟件

人工智能與粵港澳大灣區發展

《開發及使用人工智能道德標準指引》的目標

- 協助機構在開發及使用人工智能時明白及遵從《私隱條例》的規定，同時合乎良好數據道德標準
- 促進香港人工智能的循規發展及使用
- 配合《粵港澳大灣區發展規劃綱要》，促進香港成為區內的創科中心及世界級的智慧城市



《開發及使用人工智能道德標準指引》

七個道德原則

問責
機構應：
- 對其作為負責
- 能夠就其行為提供充份的理據

透明度與可解釋性
機構應：
- 披露它們使用人工智能及相關的政策
- 致力改善自動化決策的可解釋性

公平
機構應：
- 在使用人工智能時避免偏見及歧視

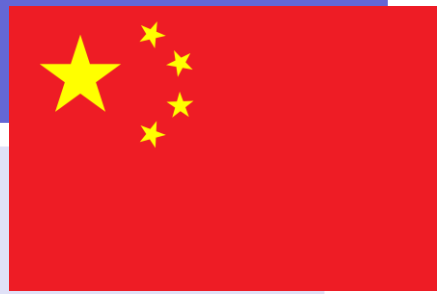
可靠、穩健及安全
人工智能系統應：
- 能可靠地運作
- 能夠處理錯誤
- 得到保護而免受攻擊

人為監督
人為參與的程度應：
- 與使用人工智能的風險及影響相稱

數據私隱
機構應：
- 具備有效的數據管治以保障個人資料私隱

有益的人工智能
使用人工智能應：
- 帶來益處
- 減低對持份者造成的傷害

內地《個人信息保護法》



- 於2021年11月1日實施
- 內地**首部**針對個人信息保護而訂立的法律
- 確立以個人的同意為處理個人信息的主要法律基礎，規定處理個人信息須遵循**合法**、**正當**、**誠信**、**最少必要**以及**公開透明**的原則，並且須具有**明確**、**合理的目的**。
- 具**境外效力**，境外機構如符合以下情況，亦須遵守《個人信息保護法》的規定，及在境內設立專門機構或代表：
  ① 為向境內自然人提供產品或者服務，或
  ② 為分析、評估境內自然人的行為等而處理境內自然人的個人信息

香港的機構及企業必須根據其業務情況，確定《個人信息保護法》是否適用於它們，並遵從有關規定

其他相關法規：內地《數據出境安全評估辦法》

- 於2022年9月1日實施
- 數據處理者向境外提供數據，如有指明情形之一，須**開展數據出境風險自評估**，並須**通過所在地省級網信部門向國家網信部門申報**數據出境安全評估：

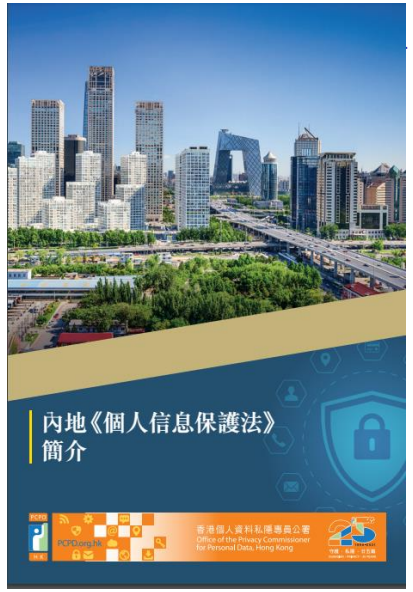
(1)	數據處理者向境外提供重要數據
(2)	關鍵信息基礎設施運營者和處理100萬人以上個人信息的數據處理者向境外提供個人信息
(3)	自上年1月1日起累計向境外提供10萬人個人信息或1萬人敏感個人信息的數據處理者向境外提供個人信息
(4)	國家網信部門規定的其他需要申報數據出境安全評估的情形

歐洲聯盟《通用數據保障條例》

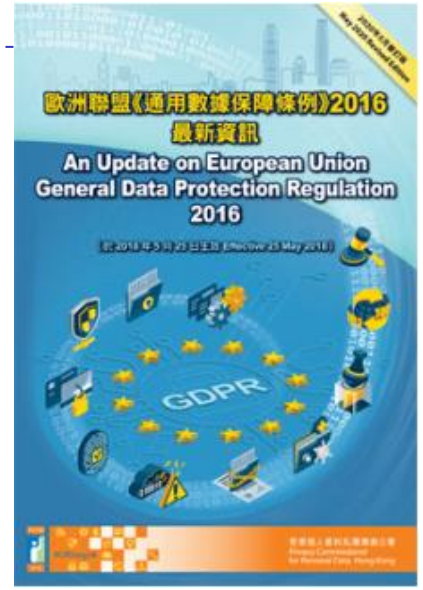
- 於2018年5月25日實施
- 條例明確規定，**在非歐盟法域管轄區內成立**的機構，在特定的情況下須遵從條例的規定
- 由於業務或交易模式多樣化（例如網上交易），香港的機構及企業必須確定《通用數據保障條例》是否對它們適用，並予以遵從
- 香港的機構或企業在以下情況下可能需要遵從《通用數據保障條例》的規定：

(1)	在歐盟設立機關，而該機關的活動涉及處理個人資料，不論是否確實在歐盟境內處理資料；或
(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。

公署的宣傳及教育 – 刊物及文章



《個人信息保護法》及相關法規	《通用數據保障條例》
刊物： ➢ 內地《個人信息保護法》簡介	**刊物：** ➢ 歐洲聯盟《通用數據保障條例》2016 最新資訊
文章： ➢ 在公署的電子通訊發表**專欄**「**Mainland Corner**」，**每月**向讀者簡介內地個人信息保護法規的最新發展 ➢ 在**專業團體會刊**（例如香港律師會）及**報章**發表文章，概述內地《個人信息保護法》對個人信息從內地轉移至其他司法管轄區的要求	**文章：** ➢ 在**專業團體會刊**（例如香港律師會）發表文章，介紹《通用數據保障條例》的相關規定及討論該法例與《私隱條例》的分別



公署的宣傳及教育 – 網上資源及講座

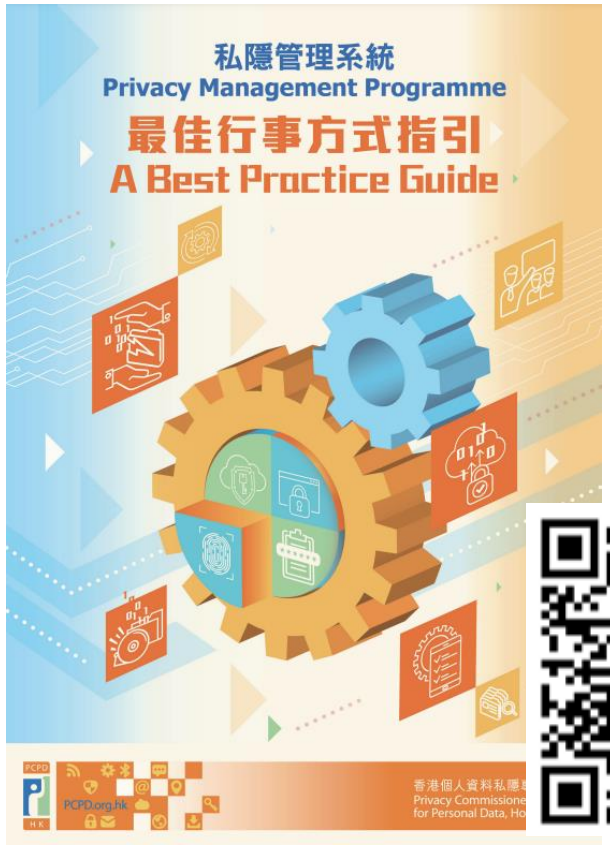
《個人信息保護法》及相關法規	《通用數據保障條例》
專題網站： https://www.pcpd.org.hk/tc_chi/data_privacy_law/mainland_law/mainland_law.html	**專題網站：** https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html
網上講座： ➢ 2021年10月28日：「內地《個人信息保護法》」網上講座 ➢ 2022年9月29日：「內地《數據出境安全評估辦法》」網上講座	**網上講座：** ➢ 2021年9月6日：「歐盟的新版標準合約條款下從歐盟轉移個人資料至非歐盟地區」網上講座
其他： ➢ 透過公署**「最新消息」**介紹《個人信息保護法》的重點 ➢ 透過**新聞稿**介紹《數據出境安全評估辦法》的重點	**其他：** ➢ 發布有關「了解歐盟委員會有關由歐盟地區轉移個人資料至非歐盟地區的新版標準合約條款」的**常見問題資料**

行業保障私隱活動

2022年	行業保障私隱活動
9月26日	舉辦「網絡世界中的數據安全管理 — 個人資料保安及事故應變實用貼士」網上講座
7月27日及 9月20日	舉辦「物業管理界別：保障個人資料私隱」網上講座
1月24日	擔任香港社會服務聯會「ITRC 研討會2022」的主講嘉賓，向社福機構講解雲端平台上的資料保障
全年	舉辦專題講座（包括銀行、保險、法律界別），以及為不同機構提供度身訂造的培訓課程

實施個人資料私隱管理系統 (PMP) 的好處

- 有助遵從《私隱條例》的規定
- 最大限度地降低私隱風險
- 有效處理資料外洩事故
- 展示符規和問責性，決心體現良好數據管治



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

PMP – 主要組件

1. 機構的決心

- 最高管理職的支持
- 委任保障資料主任 / 設立保障資料部門
- 建立匯報機制

PMP – 主要組件

2. 系統管控措施

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

保障資料主任 (Data Protection Officer)

- 私隱專員公署於2000年成立**保障資料主任聯會**
- 為公私營機構的保障資料人員提供有效的培訓和經驗交流平台，**增加對資料私隱合規的認識**和**促進企業合規實踐**
- 聯會會員分別來自人力資源管理及培訓、循規、法律、規管和執法等多元背景
- 會員人數**超過500名***

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

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

* 截至2022年9月底

問答環節

聯絡我們

2827 2827

2877 7026

www.pcpd.org.hk

communications@pcpd.org.hk

香港灣仔皇后大道東248號大新金融中心13樓1303室

追蹤公署社交平台