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

實踐良好數據管治 —
個人資料私隱管理系統

2023年1月17日

甚麼是個人資料私隱管理系統 (PMP)？

如何設立切合機構日常運作的PMP？

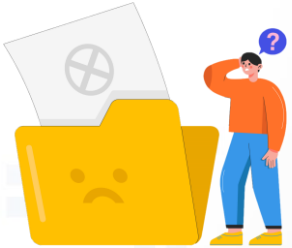
分組討論及分享

甚麼是個人資料私隱管理系統？(PMP)

常見的資料外洩事故種類

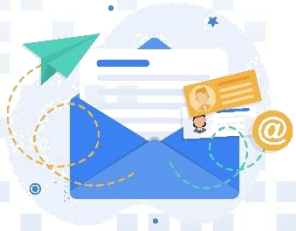
網絡攻擊

系統設置錯誤



遺失實體文件或可攜式裝置

不當或錯誤棄置個人資料



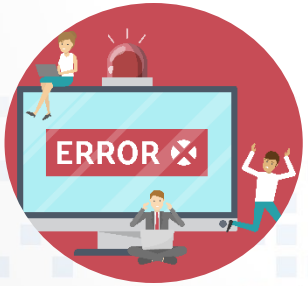
經電郵或郵件的無意披露

職員疏忽 / 行為不當

常見的資料外洩事故種類

網絡攻擊

常見的資料外洩事故種類



系統設置錯誤

懶理是否獲授權　付錢即可5天無限查閱

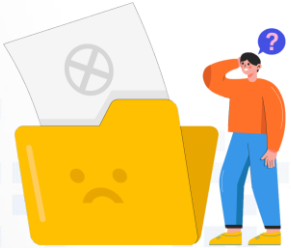
信貸資料庫無王管

財務公司$2任睇

市面上有不少提供借貸服務的財務公司，為方便財務公司評估借款人的還款能力，一個名為TE的信貸資料庫收錄18萬名借款人過往及目前的借貸紀錄。但個人資料私隱專員公署接獲投訴後展開調查，發現即使未有借款人授權，財務公司只需繳付2元，便可於5天內無限次查閱；資料庫營運商也曾接獲66宗投訴，大部分投訴成立，惟營運商未有嚴懲侵權者，削弱阻嚇力。更有5萬多宗已還款的信貸紀錄保存超過5年，違反《私隱條例》，公署已向營運商發出執行通知，要求3個月內糾正，否則考慮作出起訴。公署指出，該資料庫「無王管」，既不受行業公會規管，亦不屬金融行業相關法例監管，建議設立發牌機制。

常見的資料外洩事故種類

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



遺失實體文件或可攜式裝置

處理。(資料圖片)

常見的資料外洩事故種類

不當或錯誤棄置個人資料

獨家消息：病歷當環保紙　大埔醫院疑洩私隱

2014年06月12日(四) 20:45　推介 0　分享　Tweet　分享

294病人私隱當垃圾扔　康健醫療違例

香港文匯報訊（記者 唐文）康健醫療及牙科服務有限公司（康健）旗下位於炮台山的一間醫務中心，於去年3月意外棄置一個載有近300名病人資料的紙箱，竟於事發3個月後才向個人資料私隱專員公署通報有關事故。私隱公署於昨日發表相關調查報告，私隱專員鍾麗玲認為，康健沒有採取所有切實可行的步驟以確保涉事的醫療紀錄受保障，因而違反了《個人資料（私隱）條例》，已向康健送達執行通知，指示其糾正及防止有關違規情況再發生。公署亦正與政府研究修訂《私隱條例》的具體建議，當中包括設立強制性資料外洩通報機制。

私隱公署表示，去年6月2日收到康健的資料外洩事故通報，指該公司旗下一間位於炮台山的醫務中心，在當年3月中旬意外棄置一個載有病人醫療紀錄的紙箱，涉及294名病人的個人資料，包括姓名、電話、身份證號碼、地址、出生日期、診斷紀錄及用藥紀錄等。當時紙箱位於垃圾桶附近，被清潔工誤以為是垃圾丟棄。

經初步研究後，私隱公署認為事件可能涉及違反《私隱條例》，遂於去年7月30日正式展開調查。調查期間，公署對康健處理醫療紀錄的程序及所採取的保安措施進行了6次查訊，亦進行實地視察。

鍾麗玲引述康健曾經表示，紙箱內的物件大部分為過去3年無預約的「不活躍醫療紀錄」，當時收集是為了轉送中央倉庫儲存，事發後康健努力尋找紙箱但不果，並已辭退了涉事清潔工。

至於事發後3個月才作通報，康健指當時已立即展開內部調查，但調查資料未有保存，而處理事件的一名總經理已離職，故未能確定延遲通報的原因。

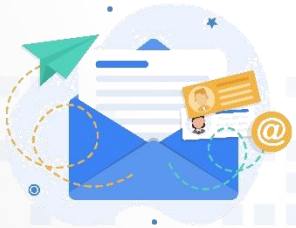
批職員輕率　缺資料保障意識

鍾麗玲表示，調查發現康健在個人資料的保安方面存在嚴重不足，涉事職員做法輕率，欠缺資料保障意識，考慮到洩露的個人資料性質敏感，康健可在更早的時間作出資料外洩事故通報。就意外洩露資料的情況，私隱公署建議機構應委任保障資料主任，監察機構是否遵循《私隱條例》並向高級管理層匯報，同時亦應向僱員提供全面培訓，減低因意識不足而引致的人為錯誤。而當機構懷疑或發現資料外洩事故發生時，應盡快向私隱公署作出通報。

◆附有294名病人私隱資料的紙箱棄置前的位置（黃圈示）。　私隱公署供圖

常見的資料外洩事故種類

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



經電郵或郵件的無意披露

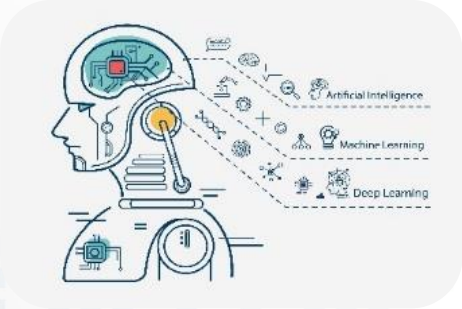
常見的資料外洩事故種類

職員疏忽 / 行為不當

電訊公司職員乘工作之便起底　公開警家屬資料囚24月

2020年11月03日(二) 13:37更新 12:22建立　推介 5,324　分享　Tweet　分享

保障個人資料私隱的挑戰



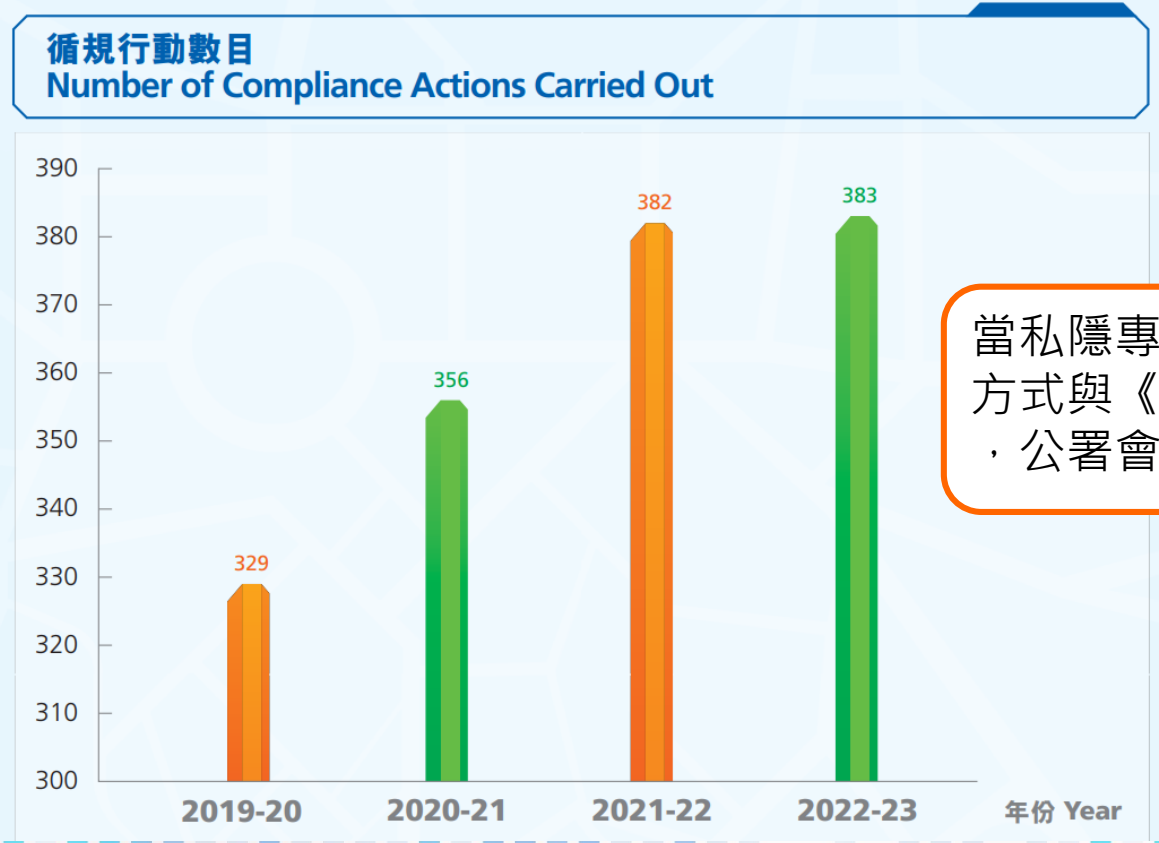
新興科技的掘起

社交媒體的
廣泛應用

生活及工作模式
數碼化

層出不窮的騙案

私隱專員公署循規行動



當私隱專員公署發現有機構的行事方式與《私隱條例》規定不相符時，公署會展開循規審查或調查。

投訴

私隱專員公署在2022-23年度共收到3,644宗投訴及作出主動網上巡查個案，當中包括1,517宗與「起底」相關的個案。撇除「起底」個案，公署在2022-23年度共接獲**2,127宗投訴**。

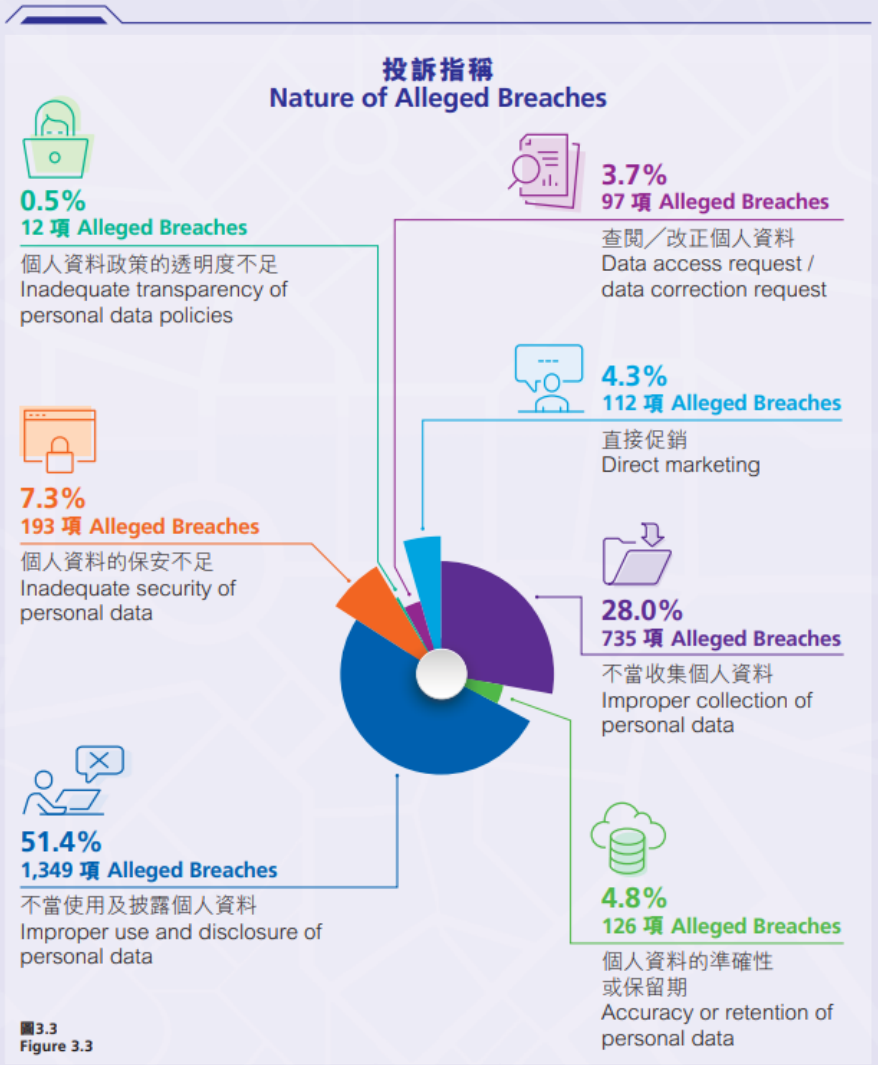


圖3.3
Figure 3.3

個人資料私隱管理系統 (PMP)
Personal Data Privacy Management Programme

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

個人資料私隱管理系統**奉行問責原則**，是一套專為規範個人或機構以負責任的態度收集、持有、處理和使用個人資料而設的管理框架，**以確保機構符合《個人資料（私隱）條例》的規定。**

個人資料私隱管理系統 (PMP)
Personal Data Privacy Management Programme

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

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

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

設立PMP的好處

- 將資料安全相關事故發生的**風險降至最低**；
- 根據既定程序和協定有效處理私隱外洩事故，從而**將損害減至最低**；
- **有效管理**收集所得的個人資料；
- 確保**符合《私隱條例》的規定**；
- 展現樂於履行良好企業管治並與客戶及相關持份者**建立信任的決心**；及
- **提升商譽和競爭優勢**，並開拓潛在商機。

PMP的主要組件

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

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

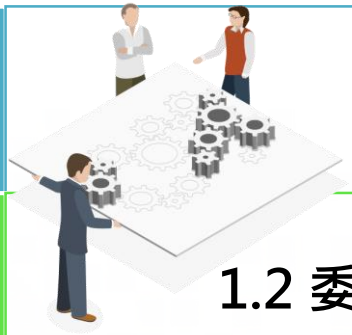
3. 持續評估及修訂

- 3.1 制定監督及檢討計劃
- 3.2 評估及修訂系統管控措施

PMP的主要組件

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

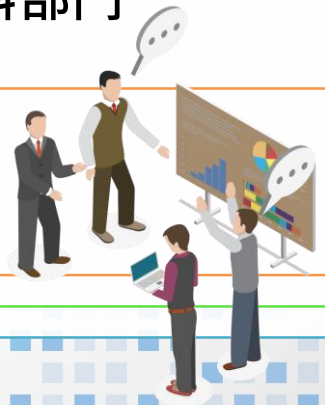
1. 機構的決心



1.1 最高管理層的支持

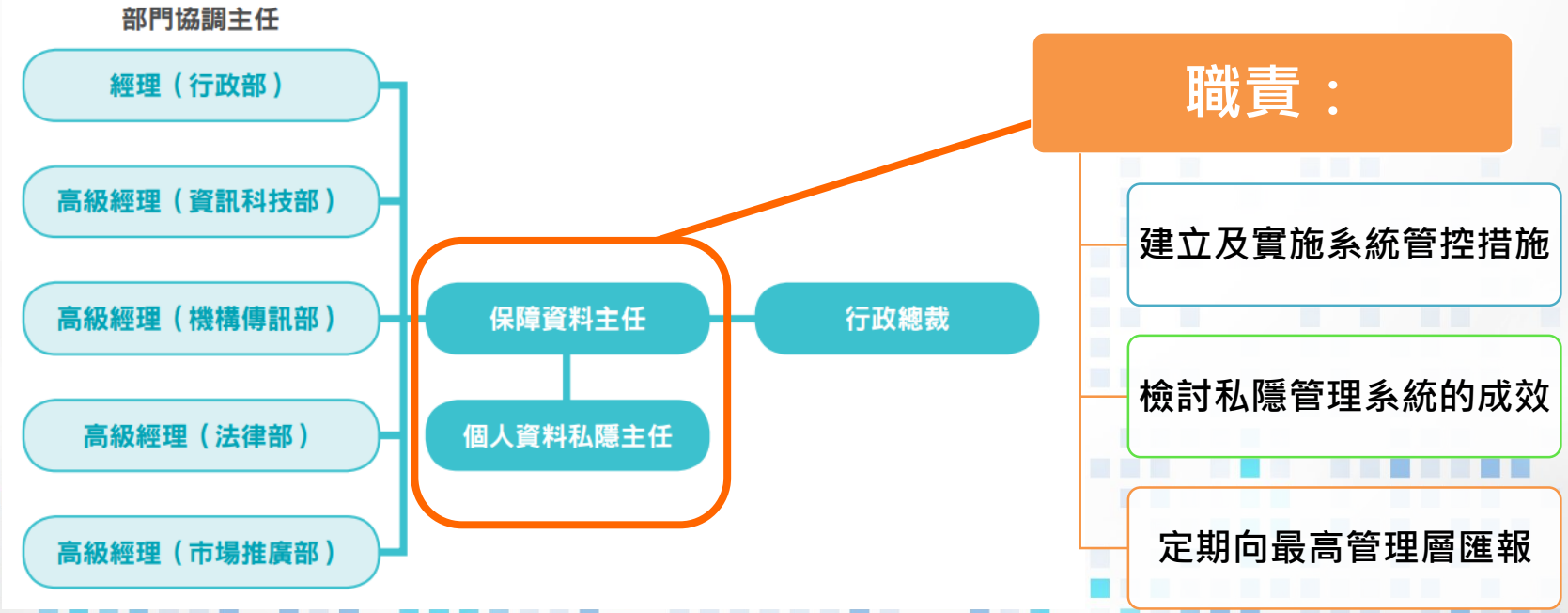
1.2 委任保障資料主任 / 設立保障資料部門

1.3 建立匯報機制



PMP的主要組件

1. 機構的決心　1.2 委任保障資料主任 / 設立保障資料部門



PMP的主要組件

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

2.系統管控措施

PMP的主要組件

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

2.系統管控措施　2.1 個人資料庫存

個人資料庫存有助機構:

a) 了解應向資料當事人徵求何種方式的同意；

b) 決定如何保護有關資料；

c) 依從查閱及改正資料要求；及

d) 有效地應對資料外洩事故。

建議機構每年要求各部門更新其個人資料庫存，並將已更新的個人資料庫存交予保障資料主任審閱及存檔。

PMP的主要組件

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

2.系統管控措施　2.1 個人資料庫存

部門	行政部	市場推廣部
紀錄的種類	人事檔案	會員檔案
所載有的個人資料	僱員的個人資料： - 姓名 - 身份證副本 - 聯絡資料（包括地址、手提電話號碼及電郵地址）	會員的個人資料： - 姓名 - 聯絡資料（包括地址、手提電話號碼及電郵地址）
收集資料的方法 / 途徑	僱員資料表格	會員申請表
收集及使用資料的目的	處理與僱傭有關的事宜	處理與向會員提供產品服務有關的事宜
資料的保留期間	有關員工離職日期起計 7 年	有關會員取消會籍後 1 年
資料的儲存地點	實體檔案： 人事檔案室內的文件櫃	實體檔案： 市場推廣部的文件櫃 電子檔案： 市場推廣部的電腦網路硬碟

樣本

是否會披露予第三者（包括資料處理者）及該第三者的名稱和相關資料（是 / 否）	否	資料會交予服務承辦商進行電話推廣
資料可能會被轉移至何處（例如雲端的位置）	不適用	服務承辦商的電腦網路硬碟
有關資料披露的目的及是否符合《個人資料（私隱）條例》的規定	不適用	進行電話推廣（已取得資料當事人的同意可進行直接促銷）
資料處理者退回或銷毀有關資料的日期（如適用）	不適用	服務承辦商會在合約期屆滿後 7 日內銷毀有關資料
所採用的保安措施	文件櫃已上鎖，只有人力資源部總經理及人事主任才持有該文件櫃的鑰匙	市場推廣部的文件櫃已上鎖，只有市場推廣部的職員才持有該文件櫃的鑰匙 市場推廣部的電腦網路硬碟只有市場推廣部的職員才獲授權查閱

PMP的主要組件

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

2.系統管控措施 2.2 處理個人資料的內部政策

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

資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil 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 practicable 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。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the 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.

PMP的主要組件

2.系統管控措施 2.3 風險評估工具

(i) 定期私隱風險評估

保障資料主任向部門協調主任提供風險評估問卷

部門協調主任填妥問卷

保障資料主任檢視填妥的問卷，評估是否有不合規的地方

部門協調主任為已識別的風險制定相應緩解措施

如風險已被緩解，保障資料主任簽署問卷並將其存檔

PMP的主要組件

2.系統管控措施　2.3 風險評估工具

(ii) 私隱影響評估

進行評估的時機:

- 規管個人資料的法規或機構的現行個人資料程序出現重大改動
- 機構引入新的處理個人資料程序
- 機構擬委託資料處理者代為處理個人資料

機構應:

- 就私隱影響評估訂明內部政策及程序
- 在可行情況下將私隱影響評估內容上載到機構網頁，以增加透明度

私隱影響評估 – 樣本節錄

甲部：擬進行的改動 / 計劃之背景資料	
計劃名稱	
組別 / 部門	
負責同事（姓名及職位）	
預計實行時間	
描述收集有關個人資料的目的及處理流程	
擬收集的個人資料種類（如：姓名、出生日期、身份證號碼、地址、電話號碼等）	
預計涉及的資料當事人數目	
是否涉及資料處理者？如「是」，是否已採取合約規範方式或其他方法以確保資料處理者已對有關個人資料採取相應的保安措施，並請詳細描述相關措施。如「否」，請詳述理由。	( ) 是 ( ) 否
是否涉及跨境個人資料轉移？如「是」，請具體說明轉移的目的地及轉移的目的。	( ) 是 ( ) 否

乙部：私隱風險分析		
範圍	私隱影響評估問題	組別 / 部門的回應
保障資料第 1 原則 — 收集個人資料的目的及方式 ▸ 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。 ▸ 須採取所有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予甚麼類別的人。 ▸ 收集的資料是必須，但不超乎適度。	是否會告知資料當事人收集其個人資料的目的？如「否」，請說明理由。	( ) 是 ( ) 否
	是否只收集最少的個人資料（即不會收集超乎適度的資料）？ 請說明收集敏感個人資料的理由（包括但不限於）： ▸ 身份證號碼及其他身份代號（如護照號碼）[13] ▸ 生物特徵資料（如指紋）[14]	( ) 是 ( ) 否。收集敏感個人資料的理由： _____ _____ _____
	是否會在收集資料當事人的個人資料之前或之時，告知他他有責任提供個人資料抑或是可自願提供有關資料？如「否」，請說明理由。	( ) 是 ( ) 否，_____
	如資料當事人有責任提供有關個人資料，是否會告知他如不提供有關資料便會承受的後果？如「是」，請述明有關情況。如「否」，請說明理由。	( ) 是，_____ ( ) 否，_____ ( ) 不適用（資料當事人可自願提供有關個人資料）
	是否會將資料當事人的個人資料轉移或披露予第三者？	( ) 是 ( ) 否
	若有關個人資料會轉移予第三者或資料處理者，是否會告知資料當事人其個人資料會被轉移予甚麼類別的人？如「否」，請說明理由。	( ) 是 ( ) 否，_____ ( ) 不適用（有關個人資料不會披露予第三者）

PMP的主要組件

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

2.系統管控措施　2.3 風險評估工具

「貫徹私隱設計」（Privacy by Design）

歐盟的《通用數據保障條例》 (GDPR)要求 資料控制者(data controller)在處理資料時採取**貫徹私隱設計**

私隱公署與新加坡個人資料保護委員會聯合出版的指引列出**貫徹私隱設計**的7項基本原則

2.3 風險評估工具

貫徹私隱設計

1.主動及預防 (Proactive and preventive)

主動評估私隱風險，並採取措施預防或減低有關風險

例子：進行私隱風險評估 (Privacy Impact Assessment)

2. 將資料保障定為預設 (Data protection as the default)

在開發和設計系統的過程中加入資料保障措施，並將有關措施定為預設，無需用戶自行啟動

例子：第三方追蹤的Cookies預設為不啟用

3. 端對端保安 (End-to-end security)

從個人資料的收集直至銷毀整個過程的每一步都須考慮資料保安

例子：個人資料的儲存和傳輸都應加密

4. 收集最少量資料 (Data minimisation)

只收集及儲存對使用目的而言屬最少和必要的個人資料

例子：對收集的個人資料進行假名化(Psudonymisation) 或匿名化處理 (Anonymisation)

2.3 風險評估工具

5. 以用戶為中心 (User-centric)

設計和操作系統時以用戶為中心，提供方便的介面讓用戶調整設定，時刻謹記保障用戶 個人資料私隱

例子：容許用戶透過網上平台檢視及管理機構如何使用其個人資料

6. 透明度 (Transparency)

主動及適時通知用戶有關其個人資料的收集、使用及如何被分享至第三方

例子：適時向用戶提供清晰易明的個人資料收集聲明

貫徹私隱設計

在設計以至使用系統的每個階段識別並減低資料保障風險

例子：設計系統或程式時加入合適的保安措施，並定期檢視及更新措施

7. 減低風險 (Risk minimisation)


香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong
合乎道德標準的
人工智能
3
三項數據管理價值
• 尊重
• 互惠
• 公平
7
七項人工智能的道德原則
• 問責
• 人為監督
• 透明度與可解釋性
• 數據私隱
• 公平
• 有益的人工智能
• 可靠、穩健及安全
4
四項主要業務流程
• 人工智能策略及管治
• 風險評估及人為監督
• 人工智能模型的開發及人工智能系統的管理
• 與持份者的溝通及交流


開發及使用
人工智能道德標準指引
AI
PCPD.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

PMP的主要組件

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

2.系統管控措施 2.4 培訓及教育推廣

- 了解機構的PMP
- 了解條例的規定
- 新發出/修訂的政策及指引
- 個案分享
- 私隱影響評估結果

PMP的主要組件

2.系統管控措施 2.4 培訓及教育推廣

私隱專員公署發表的調查報告 / 視察報告

發表日期	報告題目	報告編號	報告類別
2023年12月21日	僱主不當保留及使用僱員 / 前僱員個人資料	R23 - 18465	調查報告
2023年12月21日	Carousell 用戶的個人資料 遭未獲准許的擷取	R23 - 0665	調查報告
2023年10月9日	眾安銀行有限公司的客戶個人資料系統	R23 - 20950	視察報告
2023年9月20日	選舉事務處的個人資料系統（只有英文）	R23 - 1738	視察報告
2023年6月1日	未經授權查閱TE信貸資料庫的信貸資料	R23 - 21242	調查報告
2023年2月9日	香港銀行學會伺服器遭勒索軟件攻擊	R23 - 6319	調查報告

PMP的主要組件

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

2.系統管控措施 2.4 培訓及教育推廣

個案簡述

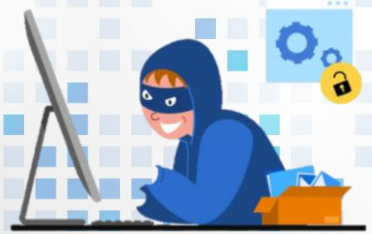
資源中心

PMP的主要組件

2.系統管控措施　2.4 培訓及教育推廣

加強員工對網絡釣魚攻擊的警覺性

- 根據美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA），勒索軟件（ransomware）通常**透過網路釣魚電郵**或**「路過式下載」**（drive-by downloads）傳播。



PMP的主要組件

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

2.系統管控措施 2.4 培訓及教育推廣

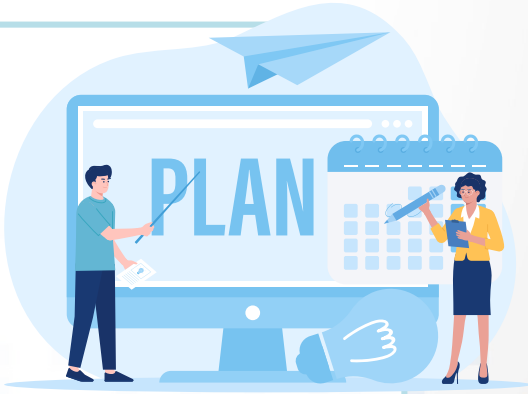
工作人員應在入職時及往後**定期接受足夠培訓**，培訓類型可包括:

PMP的主要組件

2.系統管控措施 2.5 資料外洩事故的處理

沒有訂立資料外洩事故處理程序可能帶來的問題

「事故發生前」–資料外洩事故應變計劃



- 載列機構一旦發生資料外洩時會**如何應對的文件**
- 有助機構快速應對及有效管理事故
- 資料外洩事故應變計劃應：
  - ① 概述發生事故後**須執行的程序**
  - ② 資料使用者由事故開始到完結就**識別**、**遏止**、**評估**以至**管理**事故所帶來的影響的策略
- 計劃主要涵蓋範疇包括：外洩事故的**定義**、**通報**程序、應變小組的**角色及責任**、**風險評估**工作流程、**遏止**策略、**調查**程序、**紀錄**政策、事後**檢討**機制、**培訓或演習**計劃等

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

「事故發生後」—處理資料外洩事故5大步驟

步驟 1 ：立即收集重要資料

- 事故於**何時及哪裏**發生？
- 事故**如何被發現**及由**誰人發現**？
- 導致事故的**原因**是甚麼？
- 涉及**甚麼種類**的個人資料？
- **有多少個**可能受影響的資料當事人？
- 可能對受影響人士造成甚麼**傷害**？

最先發現事故的職員應考慮是否依從資料外洩事故應變計劃所訂的程序向專責應變小組／高級管理層／保障資料主任通報事故

步驟 2：遏止事件擴大

機構可視乎所涉及個人資料的類別及事故的嚴重性，考慮採取以下的遏止措施：

- 要求錯誤接收有關電郵 / 信件 / 傳真的人士**銷毀或交回誤發的文件**
- **關閉或隔離**受損 / 遭破壞的系統 / 伺服器
- **修復**導致事故的**漏洞或錯誤**
- **更改用戶密碼及系統配置**
- **移除**涉嫌造成或引致資料外洩的**用戶的查閱權**
- 如已發生或可能發生身分盜竊或其他犯罪活動，應**通知有關執法部門**

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

步驟 3：評估事件可造成的損害

資料外洩事故可導致的損害包括：

- 人身安全受到威脅
- 身分盜竊
- 財務損失
- 受辱或喪失尊嚴、名譽或關係受損
- 失去生意或聘用機會

因資料外洩而可能蒙受的傷害程度取決於：

例如：

- 外洩個人資料的**種類**、**敏感程度**及**數量**
- 資料外洩的情況
- 傷害的性質
- **身分盜竊**或**詐騙**的可能性
- 遺失的資料**有否備份**
- 外洩資料有否進行足夠的**加密**、**匿名化**或其他保障措施
- 資料外洩**持續的時間**

步驟 4：考慮作出資料外洩通報

資料使用者在決定是否把事故通知受影響資料當事人、私隱專員公署及其他執法部門時，應考慮：

- 事故可能對受影響人士**造成的影響**
- 影響**有多嚴重**或重大
- 發生的**可能性**
- **不作出通知的後果**

如資料外洩事故相當可能對受影響資料當事人有構成實質傷害的風險，資料使用者應在知道發生資料外洩後在切實可行的情況下**盡快通知私隱專員公署及受影響資料當事人**

步驟 5：記錄事故

- 資料使用者必須**完整地記錄事故**，包括事故的**詳情、影響，資料使用者所採取的遏止措施和補救行動**
- 機構如須依從其他司法管轄區的法例及規例，亦應留意有關法例及規例下的**強制記錄要求**

例如歐洲聯盟的《通用數據保障條例》規定資料控制者記錄所有資料外洩事故並保存有關紀錄

PMP的主要組件

2.系統管控措施

2.5 資料外洩事故的處理

下載指引

下載指引

下載小冊子

下載小冊子

PMP的主要組件

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

2.系統管控措施 2.5 資料外洩事故的處理

資料外洩通報：
dbn@pcpd.org.hk

專題網頁
QR Code:

PMP的主要組件

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

2.系統管控措施 2.6 對資料處理者的管理

資料使用者在聘用資料處理者時可考慮：

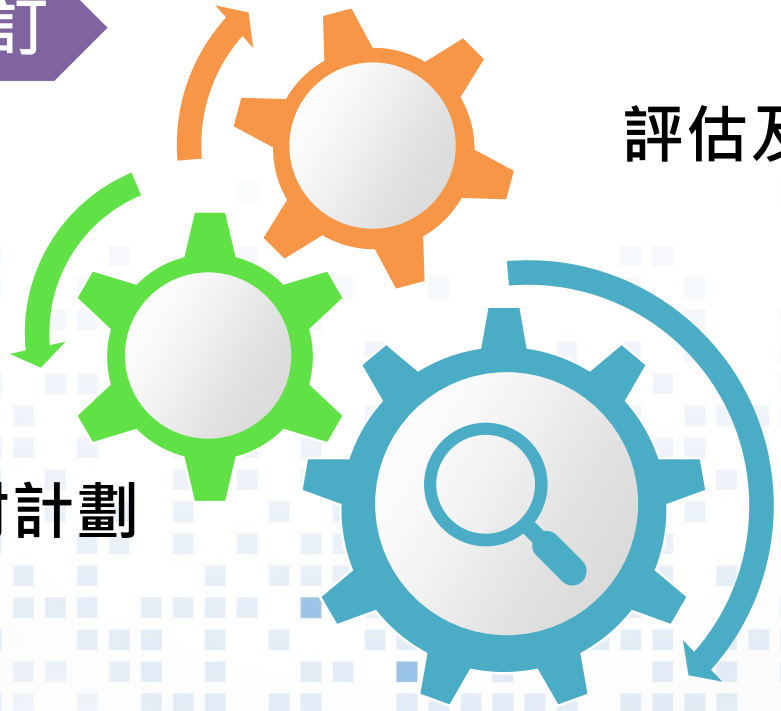
- 實施政策及程序確保**只聘用稱職且可靠**的資料處理者
- 進行評估**確保只有必要的個人資料轉移**至資料處理者
- 於合同**明確規定**資料處理者須採取的**保安措施**
- 要求資料處理者在發生資料保安事故時**立即作出通知**
- **進行現場審核**以確保資料處理者遵守資料處理合同的要求

根據《私隱條例》第65(2)條，資料使用者須對其代理人（包括資料處理者）的行為負責

PMP的主要組件

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

3.持續評估及修訂



制定監督及檢討計劃

評估及修訂系統管控措施

PMP的主要組件

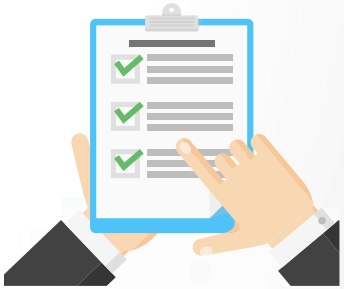
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

3.持續評估及修訂 3.1 制定監督及檢討計劃

月份	監督及檢討活動
擬備監督及檢討計劃	
1 至 4	▸ 更新個人資料庫存 ▸ 檢視機構對資料處理者的管理 ▸ 進行定期風險評估 ▸ 更新培訓內容及培訓計劃
5 至 7	評估各項系統管控措施的成效，並作出相關修訂
8 至 10	檢視及修訂私隱管理系統操作手冊，及其他與個人資料私隱有關的政策和指引
11	向員工傳閱私隱管理系統操作手冊及其他與個人資料私隱有關的政策和指引
12	檢視監督及檢討計劃的執行，並擬備來年的監督及檢討計劃

PMP的主要組件

3.持續評估及修訂　3.2 評估及修訂系統管控措施



在決定系統管控措施是否有需要作出修訂前，機構可考慮以下因素：

- 有甚麼**新的威脅**及風險？
- 系統管控措施是否可以應付新的威脅和顧及**最近的投訴或審核結果**，或**私隱專員發出的指引**？
- 機構有沒有提供**新的服務**使個人資料收集、使用或披露有所增加？
- 是否**需要提供培訓**？如「是」的話，有沒有推行？是否有效？政策及程序是否獲得依從？系統是否切合最新情況？

如何設立切合機構日常運作的PMP？

關鍵步驟

關鍵步驟

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

1.設立團隊

- 委任**具經驗的專責人員**擔任保障資料主任 / 設立保障資料部門，以全面監督機構的私隱管理系統
- 確保**最高管理層**透過保障資料主任進行**監督**
- 可邀請人力資源、風險管理、內部合規和 IT **部門參與**，支援保障資料主任，以充分掌握機構在處理個人資料的實際運作
- 可尋求私隱專家協助

關鍵步驟

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

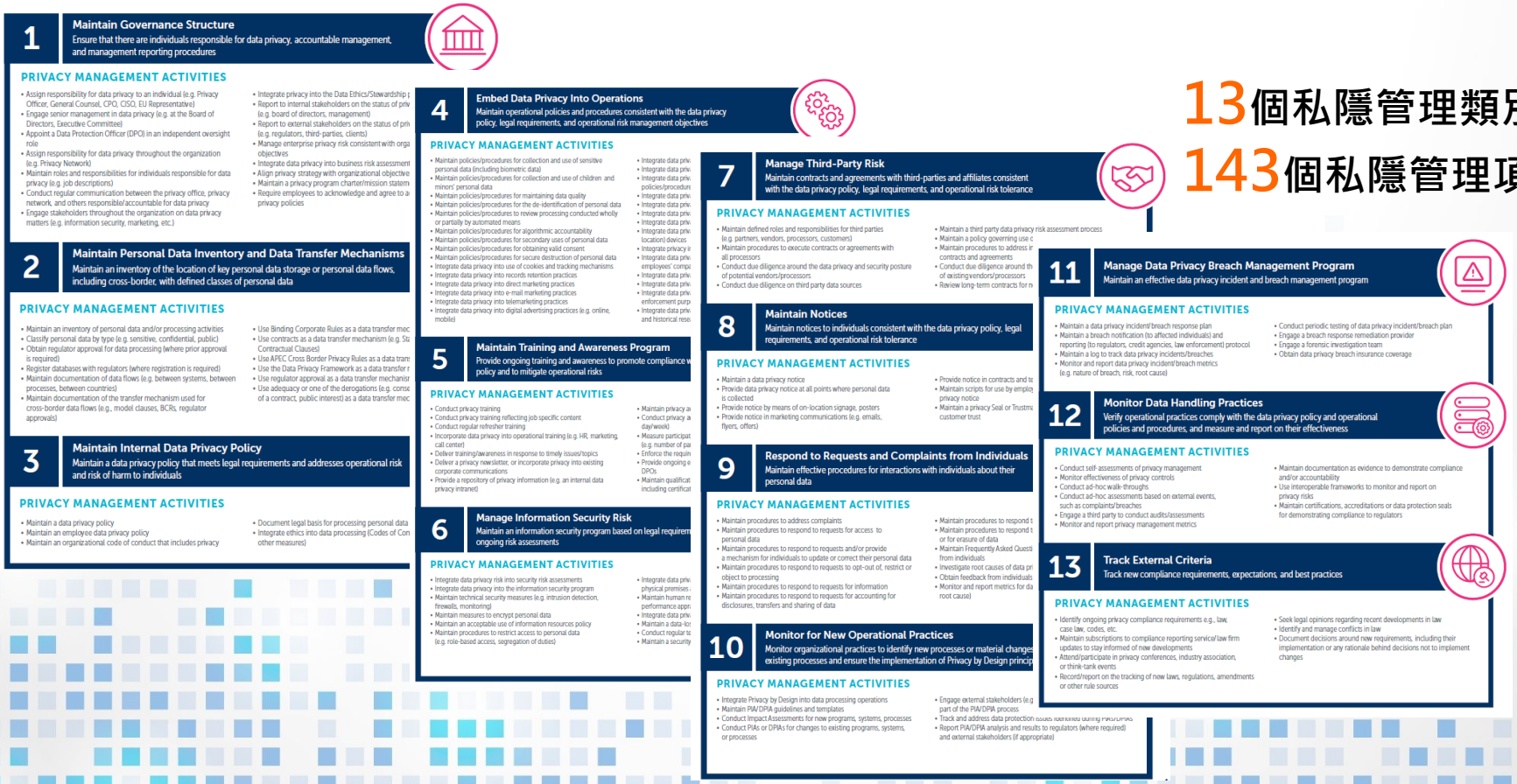
2.制定框架

- 除了私隱專員公署的指引，亦可參考海外的保障資料機構或非執法機構的指引：
  - 加拿大 — *Getting Accountability Right with a Privacy Management Program*
  - 澳洲 — *Privacy Management Framework*
  - Centre for Information Policy Leadership — *Accountability: Data Governance for the Evolving Digital Marketplace*
  - TrustArc — *TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks*

TrustArc — *TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks*

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

13個私隱管理類別及
143個私隱管理項目



1 Maintain Governance Structure

Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

PRIVACY MANAGEMENT ACTIVITIES

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network, and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Integrate privacy into the Data Ethics/Stewardship p
- Report to internal stakeholders on the status of priv (e.g. board of directors, management)
- Report to external stakeholders on the status of pri (e.g. regulators, third-parties, clients)
- Manage enterprise privacy risk consistent with orga objectives
- Integrate data privacy into business risk assessment
- Align privacy strategy with organizational objective
- Maintain a privacy program charter/mission statem
- Require employees to acknowledge and agree to a privacy policies

2 Maintain Personal Data Inventory and Data Transfer Mechanisms

Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

PRIVACY MANAGEMENT ACTIVITIES

- Maintain an inventory of personal data and/or processing activities
- Classify personal data by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain documentation of data flows (e.g. between systems, between processes, between countries)
- Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, regulator approvals)
- Use Binding Corporate Rules as a data transfer mec
- Use contracts as a data transfer mechanism (e.g. Stz Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data trans
- Use the Data Privacy Framework as a data transfer r
- Use regulator approval as a data transfer mechanisr
- Use adequacy or one of the derogations (e.g. conse of a contract, public interest) as a data transfer mec

3 Maintain Internal Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Con other measures)

4 Embed Data Privacy Into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

PRIVACY MANAGEMENT ACTIVITIES

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for algorithmic accountability
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data priv
- Integrate data priv
- Integrate data priv policies/procedure
- Integrate data priv
- Integrate data priv
- Integrate data priv
- Integrate data priv
- Integrate data priv
- Integrate data priv location) devices
- Integrate privacy i
- Integrate data priv
- Integrate data priv employees' compa
- Integrate data priv
- Integrate data priv
- Integrate data priv enforcement purp
- Integrate data priv and historical rese

5 Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance w policy and to mitigate operational risks

PRIVACY MANAGEMENT ACTIVITIES

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training (e.g. HR, marketing, call center)
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy a
- Conduct privacy a day/weeks)
- Measure participat (e.g. number of pa
- Enforce the requin
- Provide ongoing e DPOs
- Maintain qualificat including certificat

6 Manage Information Security Risk

Maintain an information security program based on legal requirem ongoing risk assessments

PRIVACY MANAGEMENT ACTIVITIES

- Integrate data privacy into security risk assessments
- Integrate data privacy into the information security program
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data priv physical premises
- Maintain humans re performance appr
- Integrate data priv
- Maintain a data-lo
- Conduct regular te
- Maintain a security

7 Manage Third-Party Risk

Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

PRIVACY MANAGEMENT ACTIVITIES

- Maintain defined roles and responsibilities for third parties (e.g. partners, vendors, processors, customers)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a third party data privacy risk assessment process
- Maintain a policy governing use c
- Maintain procedures to address ir contracts and agreements
- Conduct due diligence around th of existing vendors/processors
- Review long-term contracts for n

8 Maintain Notices

Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy notice
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in contracts and te
- Maintain scripts for use by employ privacy notice
- Maintain a privacy Seal or Trustm customer trust

9 Respond to Requests and Complaints from Individuals

Maintain effective procedures for interactions with individuals about their personal data

PRIVACY MANAGEMENT ACTIVITIES

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for accounting for disclosures, transfers and sharing of data
- Maintain procedures to respond t
- Maintain procedures to respond t or for erasure of data
- Maintain Frequently Asked Questi from individuals
- Investigate root causes of data pr
- Obtain feedback from individuals
- Monitor and report metrics for da root cause)

10 Monitor for New Operational Practices

Monitor organizational practices to identify new processes or material changes existing processes and ensure the implementation of Privacy by Design princip

PRIVACY MANAGEMENT ACTIVITIES

- Integrate Privacy by Design into data processing operations
- Maintain PIA/DPIA guidelines and templates
- Conduct Impact Assessments for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

11 Manage Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

12 Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

PRIVACY MANAGEMENT ACTIVITIES

- Conduct self-assessments of privacy management
- Monitor effectiveness of privacy controls
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Use interoperable frameworks to monitor and report on privacy risks
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

13 Track External Criteria

Track new compliance requirements, expectations, and best practices

PRIVACY MANAGEMENT ACTIVITIES

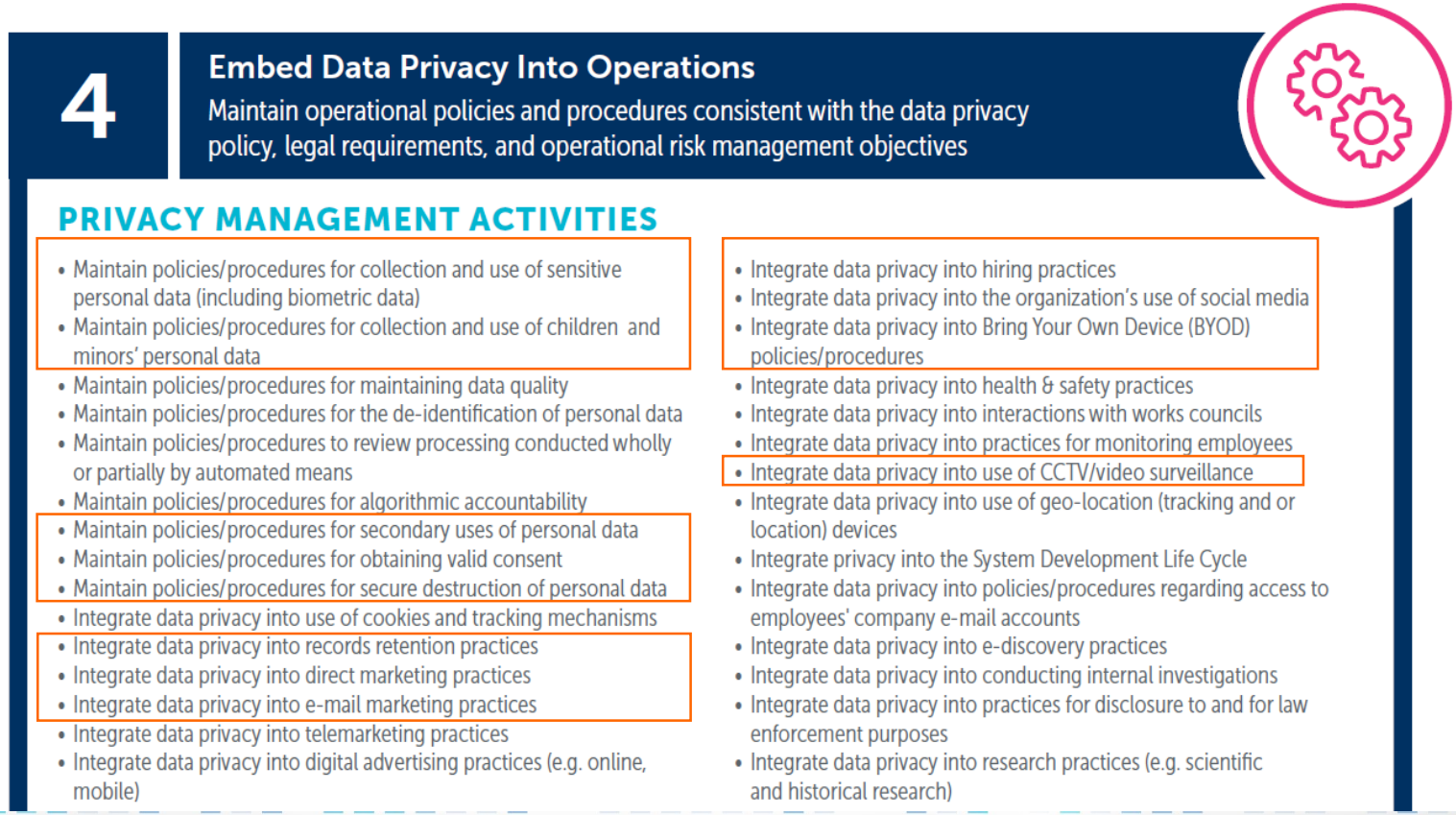
- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

關鍵步驟

3.計劃細節

- 進行**差距分析** (Gap analysis)
- 根據機構的性質、規模、持有個人資料的種類等，判斷哪些是**必要項目**，哪些是**可取項目**：
  - 必要項目的例子：定期檢討和更新隱私權政策；為員工提供定期培訓
  - 可取項目的例子：舉辦年度資料私隱週；聘請第三方進行審核和評估
- 為各個項目**制定執行細節及時間表**
- 確定由**誰來實施變革**

TrustArc — *TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks*



4 Embed Data Privacy Into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

PRIVACY MANAGEMENT ACTIVITIES

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for algorithmic accountability
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate privacy into the System Development Life Cycle
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)

TrustArc — *TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks*

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

5 Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

PRIVACY MANAGEMENT ACTIVITIES

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training (e.g. HR, marketing, call center)
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain qualifications for individuals responsible for data privacy, including certifications

TrustArc — *TrustArc-Nymity integrated Privacy and Data Governance Accountability Frameworks*

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

11 Manage Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

PRIVACY MANAGEMENT ACTIVITIES

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

關鍵步驟

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

4.落實執行

- 分配資源
- 訂立溝通計劃
- 執行及培訓
- 持續監察及評估成效，並持續改善

關鍵步驟

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

4.落實執行

框架	政策	指引、樣本、程序文件
處理個人資料的內部政策	收集個人資料聲明	用於招聘的相關樣本 / 用於收集服務使用者的個人資料之相關樣本
	資料保留及刪除政策	不同工作項目的資料刪除時間表 / 指引

數據安全建議措施

- **使用網站安全掃描服務，定期掃描以偵測最新的已知或潛在的網絡安全風險**
  - 香港互聯網註冊管理有限公司的免費網站安全掃描服務 *https://www.hkirc.hk/zh-hant/public_mission/cybersecurity/free_web_scan_services/*

數據安全建議措施

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

- 留意最新網絡威脅資訊：
  - 守網者
    https://cyberdefender.hk/
  - 網絡安全資訊共享夥伴計劃
    https://www.cybersechub.hk/
  - 香港電腦保安事故協調中心
    https://www.hkcert.org/

私隱管理工具

同意管理
Consent Management

網站掃瞄
Website Scanning

風險評估
Assessment Manager

資料發現及數據映射
Data Discovery and Data Mapping

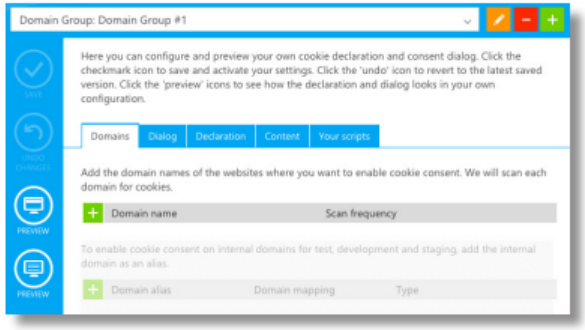
處理資料當事人查詢
Data Subject Requests

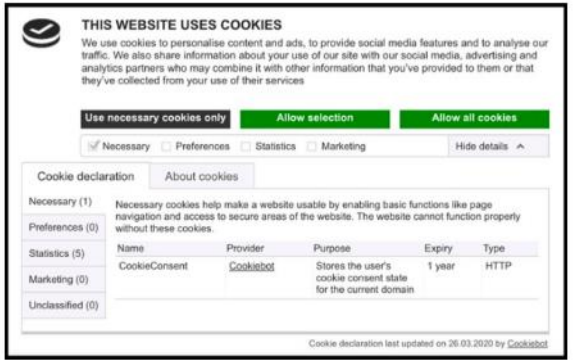
私隱管理工具

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

同意管理

- 與收集用戶資料平台融合
- 管理從收集到撤回的整個處理同意的生命週期
- 設立處理同意的中央資料庫
- 建立同意聲明和選擇退出
- 收集有效的用戶同意





(Source: Cookiebot)

私隱管理工具

資料發現及數據映射

- 監查系統以確定個人資料所在位置
- 根據預定標準自動對個人資料進行分類
- 建立資料映射將機構內部和外部的個人資料流向影像化
- 產生即時、最新的處理活動記錄

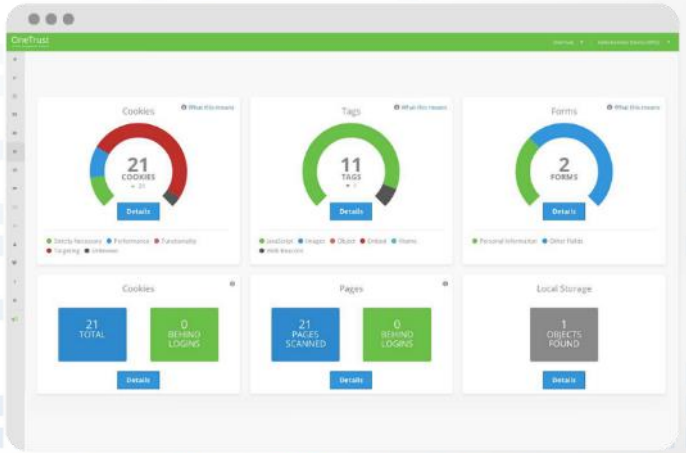
(Source: AvePoint, TrustArc)

私隱管理工具

網站掃瞄

掃描網站以確定嵌入了哪些cookies、網絡信標和其他追蹤器

確保遵守各種與cookies相關的法規



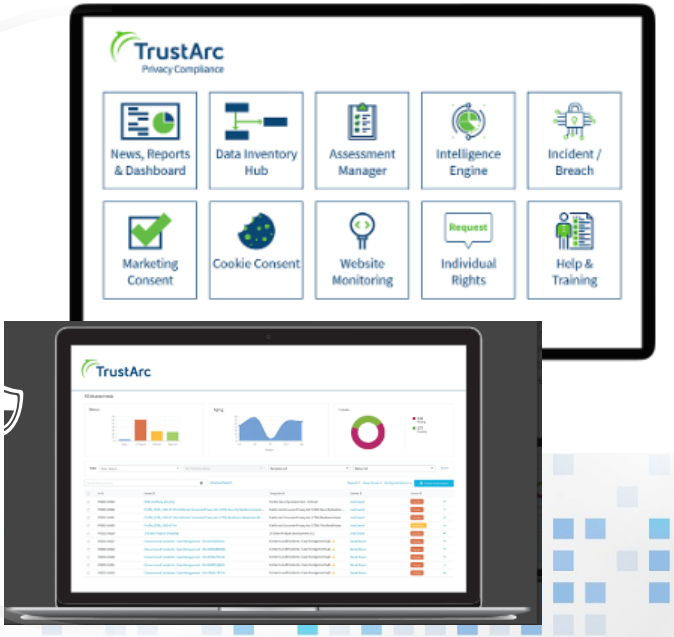
(Source: OneTrust)

私隱管理工具

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

風險評估

- 用於風險評估的自動化範本和清單
- 找出風險差距和補救建議
- 實施隱私影響評估
- 展示合規性
- 協助資料保障主任擴展需要電子表格的複雜項目



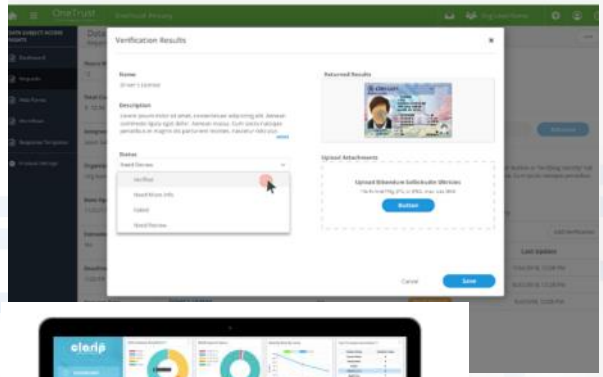
(Source: TrustArc)

私隱管理工具

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

處理資料當事人查詢

- 快速驗證請求者身分以驗證請求
- 使用範本以簡化流程
- 及時、準確地執行用戶請求
- 保存全面的記錄



(Source: OneTrust, Clarip)

道德與信任

三項數據管理價值

尊重

尊重持份者的權利、利益及合理期望

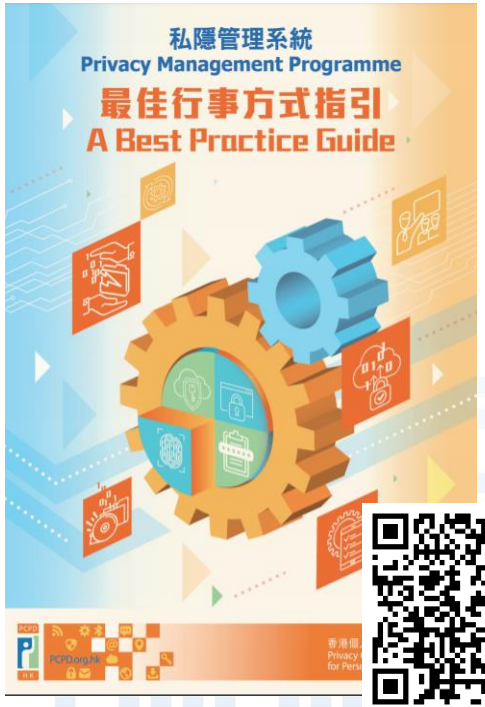
互惠

為持份者帶來益處及減低對持份者造成的傷害

公平

避免偏見及歧視

https://www.pcpd.org.hk//english/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf



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

https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/GN_biometric_c.pdf

聯絡我們

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

查詢 2827 2827　傳真 2877 7026

網址 www.pcpd.org.hk

電郵 communications@pcpd.org.hk

地址 香港皇后大道中248號大新金融中心13樓1303室

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

追蹤我們最新資訊

答問時間

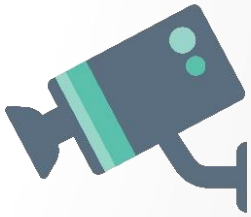
謝謝！Thank you!

分組討論及分享

分組討論及分享

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

討論題目（一）



假設你要為一間兒童及青少年服務中心設立保障資料部門.....

- 為了**保障服務使用者（兒童、青少年、家長等）**的個人資料私隱，討論須制定**哪些個人資料的內部政策**以符合《私隱條例》下六項保障資料原則的規定

六項保障資料原則

分組討論及分享

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

討論題目（二）

「早期抑鬱症篩查AI系統」可透過分析求助者的說話聲線、情緒和關鍵詞等，評估情緒困擾及患上抑鬱症的程度及風險。假設你有意引進這個AI系統，並希望事前先進行**私隱影響評估**.....

- 根據私隱影響評估問卷樣本，討論當中**潛在風險及解決方法**

私隱影響評估範本
(P.17-20)

分組討論及分享

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

討論題目（三）

最近黑客攻擊及詐騙個人資料的個案頻生，假設你是一間長者服務機構的負責人，希望訂立**資料外洩事故應變計劃**.....

- 針對黑客入侵機構電腦系統的應變計劃，討論需涵蓋哪些範疇及具體建議

計劃範疇 (P.3)