個人資料去識別化驗證標準規範說明

蔡敦仁
資訊及通信國家標準技術委員會

不斷變化的世界之隱私挑戰

- 開放資料
- 大數據
- 社群網路
- 物聯網(IoT)
- 雲端計算
- Apps
- .....

FB判決掀起隱私大戰

- Maximillian Schrems，登錄為FB用戶，發現如同其他上億的歐盟用戶一樣，他在FB活動的所有資料，無論是個資、留言或照片，被蒐集、儲存在愛爾蘭的歐洲FB公司後，轉傳至美國FB總公司的伺服器儲存
- 此舉可能讓美國情治機構（尤其是NSA）得以「繞過」歐盟隱私保護法規，直接在美國就監控所有歐盟公民的FB資訊
- 2000年時，歐盟執委會與美國政府達成《安全港（Safe Harbor）協議》，概括認定美國是合乎歐盟法要求的第三國
- 歐盟法院(CJEU)裁判，正式確認「安全港根本不安全」，宣告其違反歐盟資料保護法
- 未來位於愛爾蘭的歐洲臉書公司可能無法再將用戶資料悉數傳輸到美國總公司，對FB及其他跨國互聯網企業的衝擊，難以估計

--2015年10月10日蘋果日報，作者：台灣大學法律學院林鈺雄教授

個人資料之定義

- 依個人資料保護法第2條第1款規定，個人資料是指姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料
- 個資法將個人資料區分成兩類：
  - 直接識別之個人資料
  - 間接識別之個人資料

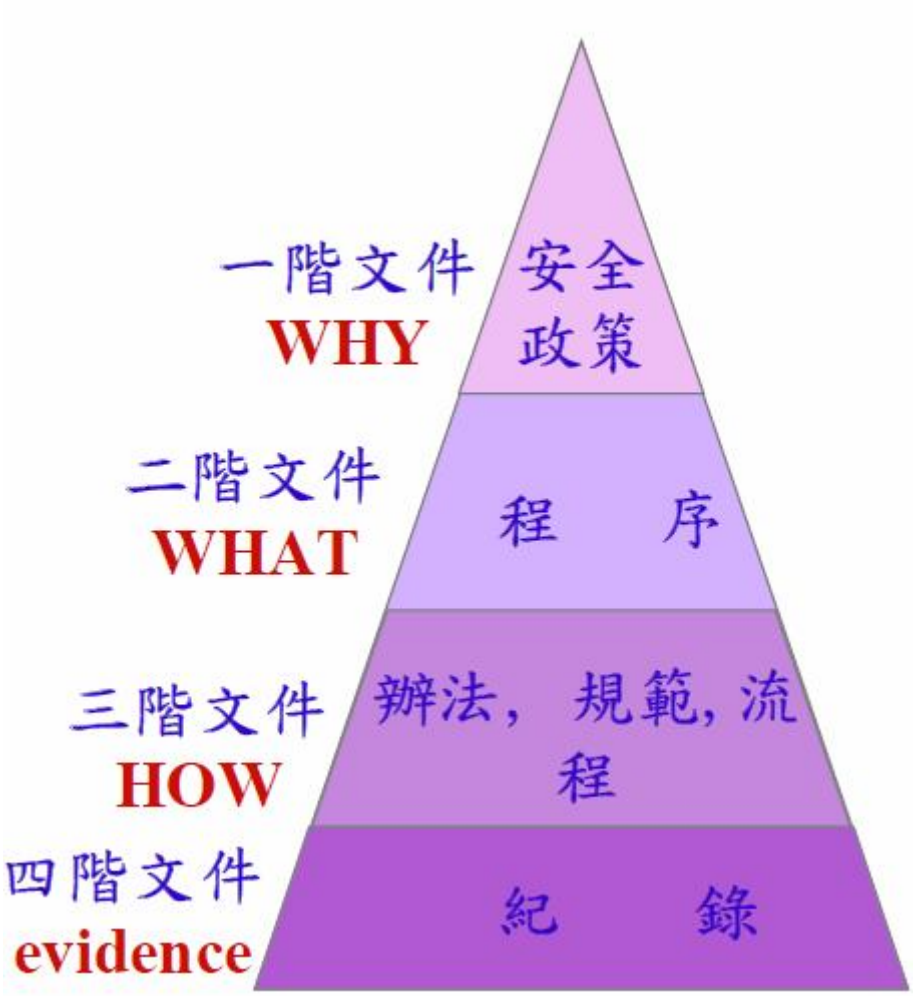
間接識別之個人資料

- 某些資料雖未直接指名道姓，但一經揭露仍足以識別為某一特定人
- 所謂「得以間接方式識別」依個資法施行細則第3條規定，係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人
- 又所謂經由對照、組合、連結等方式識別特定個人，必須是精準且確定地得以識別出特定個人，而非僅是利用專業知識「猜測」、「推測」可能為某人之資料

個人資料判斷之相對性

- 因得為比對組合之人及資料範圍具有「相對性」，故難有一致性之認定標準，如同個資法施行細則第3條修正理由說明所示：「是否得以直接或間接方式識別者，需從蒐集者本身個別加以判斷，此宜於個案中加以審認，…」
- 換言之，欲判斷一份資料是否為個人資料，對於不同蒐集者而言，即可能會產生不同之判斷結果，蓋蒐集者原先所持有或可能得以獲取之資料範圍有所不同，其與新蒐集之資料，是否得以透過對照、組合、連結等方式識別特定之個人，亦會有不同之結果，自難以一概而論

大家熟知的CNS 27001



- 資訊技術－安全技術－資訊安全管理系統－要求事項
- 資訊安全管理系統(ISMS)
- TAF公布目前我國有377個單位通過驗證

CNS 29100

資訊技術－安全技術－隱私權框架

CNS 29100

- 提供資通訊技術(ICT)系統內保護個人可識別資訊(personally identifiable information, PII)之高階框架
- 提供隱私權框架
  - 規定共同隱私權專門用語
  - 定義處理個人可識別資訊(PII)之行為者與其角色
  - 描述隱私保全考量
  - 對資訊技術之已知隱私權原則提供參考資料
- 個人可識別資訊(personally identifiable information, PII)
  - 所有資訊其能用以識別此類資訊所涉之特定個人， 或係得以直接或間接連結至特定個人

國內目前已有單位開辦29100驗證，但未經TAF認證

行為者及角色

- PII當事人(PII principal)
  - 個人可識別資訊(PII)所關聯之自然人
- PII控制者(PII controller)
  - 判定個人可識別資訊(PII)處理之目的及方法的隱私權相關者，而非就個人目的使用資料的自然人

  備考：PII控制者有時委派他人(例：PII處理者)，代表其處理PII，而處理之責任仍由PII控制者承擔
- PII處理者(PII processor)
  - 代表PII控制者並依其指示，處理個人可識別資訊(PII)之隱私權相關者
- 第三方(third party)
  - 除PII當事人、PII控制者及PII處理者，以及經PII控制者或PII處理者直接授權處理資料之自然人外的隱私權相關者

行為者之互動

(a)PII 當事人提供PII 予PII 控制者
例：於註冊PII 控制者所提供之服務時
(b) PII 控制者提供PII 予PII 處理者，其代表PII 控制者處理該PII
例：作為委外協議之一部分
(c) PII 當事人提供PII 予PII 處理者，其代表PII 控制者處理該PII
(d) PII 控制者提供與該PII 當事人有關之PII 予PII 當事人
例：依PII 當事人之請求
(e) PII 處理者提供PII 予PII 當事人
例：依PII 控制者指示
(f) PII 處理者提供PII 予PII 控制者
例： 於履行所約定服務後
(g) PII 控制者提供PII 予第三方(例：依商業協議)
(h) PII 處理者提供PII 予第三方(例：依PII 控制者指示)

PII 當事人、PII 控制者、PII 處理者及第三方間之PII 流向及其角色

	PII當事人	PII控制者	PII處理者	第三方
情境(a)	PII提供者	PII接收者	—	—
情境(b)	—	PII提供者	PII接收者	—
情境(c)	PII提供者	—	PII接收者	—
情境(d)	PII接收者	PII提供者	—	—
情境(e)	PII接收者	—	PII提供者	—
情境(f)	—	PII接收者	PII提供者	—
情境(g)	—	PII提供者	—	PII接收者
情境(h)	—	—	PII提供者	PII接收者

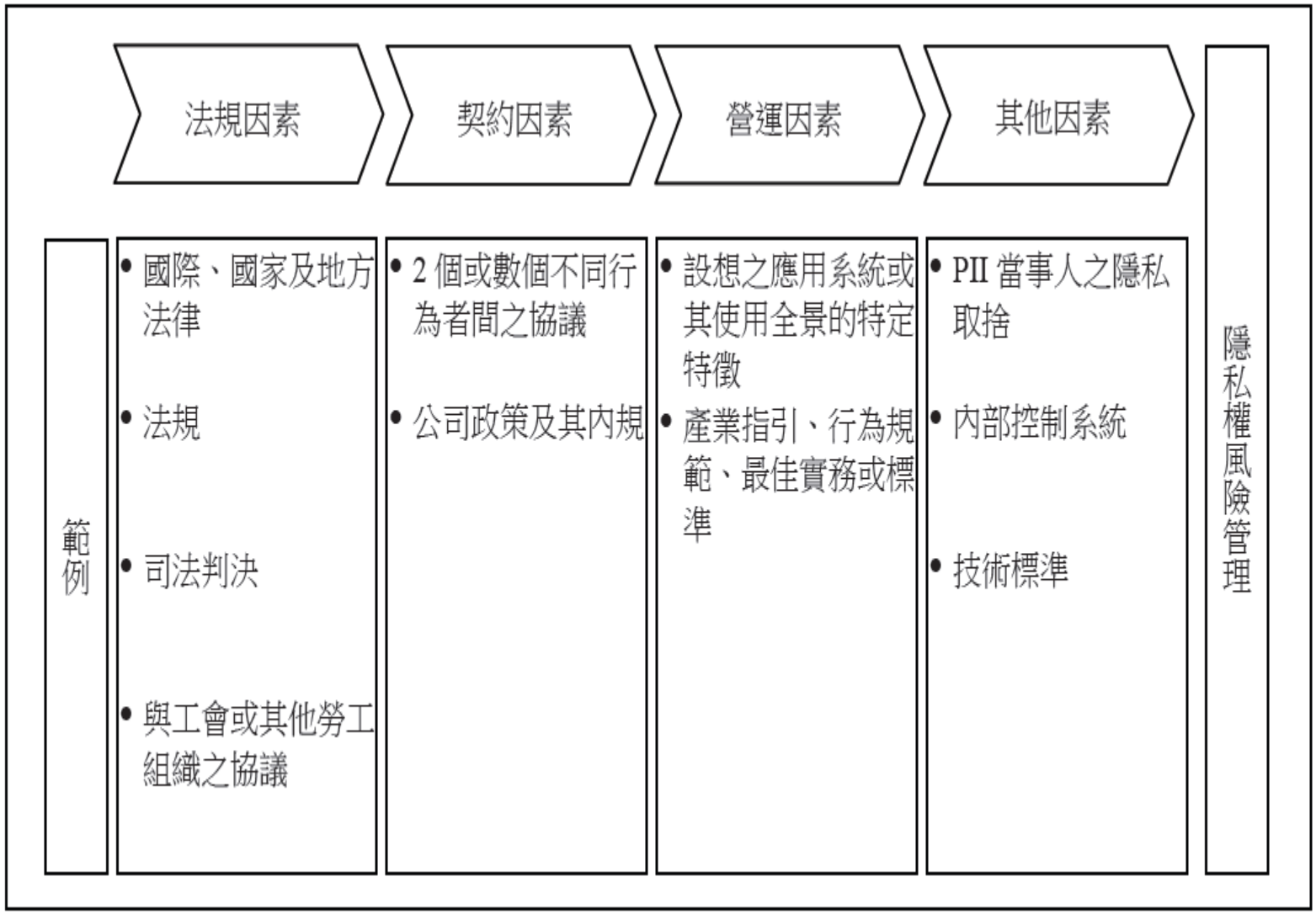
可用以識別自然人之屬性範例

- 身弱自然人之年齡或特別需求
- 犯罪前科
- 醫療服務所蒐集之任何資訊
- 銀行帳號或信用卡號碼
- 生物量測識別符(例：指紋)
- 信用卡帳單
- 刑事判決或罪行
- 刑事調查報告
- 客戶編號
- 生日
- 健檢資訊
- 身心障礙
- 醫療帳單
- 員工薪資及人力資源檔案
- 財務狀況
- 性別
- GPS 位置
- GPS 行蹤
- 住家地址
- IP 位址
- 電信系統導出之位置
- 病歷
- 姓名
- 國家賦予之識別碼(例：護照號碼)
- 個人電子郵件位址
- 個人識別碼(PIN)或通行碼
- 追蹤網際網路網站使用所導出之個人興趣
- 個人或行為剖繪
- 個人電話號碼
- 可識別自然人之照片或視訊
- 產品及服務偏好
- 種族或族裔
- 宗教或哲學信仰
- 性向
- 工會會員
- 公用事業帳單

隱私保全要求事項

- 隱私風險管理過程包含下列過程。
  - 建立全景，其藉瞭解組織(例：PII 處理、責任)、技術環境及影響隱私風險管理之因素(亦即法規因素、契約因素、營運因素及其他因素)達成
  - 風險評鑑，其藉識別、分析及評估PII原則之風險(可能有負面影響之風險)達成
  - 風險處理，其藉定義隱私保全要求事項、識別及實作隱私控制措施以避免或減少PII原則之風險達成
  - 溝通及諮詢，其藉從關注各方得到資訊、對每一風險管理過程獲得共識，以及通知PII當事人並與其溝通風險及控制措施達成
  - 監視及審查，其藉追查風險及控制措施，以及改善過程達成

影響隱私風險管理之因素



隱私權政策

- 涉及PII處理之組織高階管理者宜建立隱私權政策
- 隱私權政策宜如下
  - 合於組織目的
  - 提供設定目標之框架
  - 包括滿足適用之隱私保全要求事項的承諾
  - 包括持續改善之承諾
  - 於組織內傳達
  - 相關各方可適時取得
- 組織宜以書面載明其隱私權政策
- 當組織因處理PII而成為PII處理者時，該等政策主要由PII 控制者決定
- 隱私權政策宜依不同隱私權利害相關者， 補充更詳細之PII 處理規則及義務(例：特定部門或員工之程序)
- 此外，宜載明特殊設定下(例：存取控制、告知條款、稽核等)，用以增強隱私權政策之控制措施

隱私權政策

- 〝隱私權政策〞用語常意指內部及外部兩者之隱私權政策
- 內部隱私權政策載明組織採用之目標、規則、義務、限制及/或控制措施，以滿足與其PII 處理有關之隱私保全要求事項
  - 〝隱私權政策〞用語意指組織之內部隱私權政策
- 外部之隱私權政策提供外部人員對組織隱私權實務作法聲明，以及其他相關資訊，如PII 控制者之身分及辦公室地址、PII 當事人可能取得額外資訊之連絡窗口等
  - 外部隱私權政策稱為告知

隱私控制措施

- 組織宜識別及實作隱私控制措施以符合隱私風險評鑑及處理過程所識別之隱私保全要求事項
- 已識別及實作之隱私控制措施宜作為組織隱私風險評鑑之一部分予以記載
- 隱私風險評鑑可協助組織，以識別涉及設想運作之違反隱私權的特定風險
- 隱私遵循宜於PII處理之系統設計時期即納入考量，而非於後續階段方納入
- 並非所有PII處理均要求相同保護等級或型式
  - 組織宜依其面對之特定風險在PII 處理運作之間區分，以協助決定在何種情況下，適合採取何種資訊安全控制措施
- 風險管理係此過程之核心方法

隱私權原則

1.同意及選擇
2.目的適法性及規定
3.蒐集限制
4.資料極小化
5.利用、持有及揭露限制
6.準確性及品質
7.公開、透明及告知
8.個人參與及存取
9.可歸責性
10.資訊安全
11.隱私遵循

隱私權原則概觀

- 標準中描述之隱私權原則，係由若干國家及國際組織所發展之既存原則衍生而出
- 此框架聚焦於ICT內隱私權原則之實作，以及將實作於組織ICT系統內之隱私管理系統的發展
- 此等隱私權原則宜用以指導隱私權政策及隱私控制措施之設計、發展及實作
- 其可做為組織於監視及量測隱私管理方案之執行績效、評效及稽核層面時之基準
- 儘管社會、文化、法律及經濟因素之差異於某些情況下，可能限制此等原則之使用，但仍建議使用本標準所定義之所有原則
- 此等原則之例外情形宜限制之

CNS 29100概念與CNS 27000概念比對

CNS 29100概念	CNS 27000概念
隱私權相關者	利害相關者
PII	資訊資產
隱私權違反	資訊安全事故
隱私控制措施	控制措施
隱私風險	風險
隱私風險管理	風險管理
隱私保全要求事項	控制目標

CNS 29191

資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項

CNS 29191

- 目前先進之個體鑑別技術，要求揭露待鑑別個體的可識別資訊
- 於許多交易中，傾向於將個體保持匿名及去連結
  - 意即當履行2個交易時，難以區別該等交易係由同一使用者或由不同使用者所履行
- 於某些具正當理由之情況下，可後續啟動重新識別(例：確認可歸責性時)
- 〝部分匿名及部分去連結〞意謂事先指定開啟者，且僅該指定開啟者，可識別該鑑別之個體
  - 例：圖書館可能需要識別未歸還所借書籍之個體，以便發送逾期通知予該個體。
  - 目前之密碼學技術可用以提供部分匿名及部分去連結之鑑別
- 此標準規定部分匿名及部分去連結鑑別之框架及其要求事項

一般(1/2)

- 現今有許多密碼式機 制可用以改進鑑別過程 之安全性
- 此等機制對於使用某授權過程成功鑑別後，賦予個體存取受保護資源之適切權限，產生較大信任
  - 注意，授權細節非屬本標準之範圍， 故以括號標記之
- 典型之鑑別及授權模型， 包含下列步驟(而各步驟通常包含數個子步驟， 諸多此等步驟描述於ISO/IEC 29115中)

  (a) 註冊

  (b) 鑑別

  (c) (授權)
- 目前大多數使用中之密碼式機制，要求揭露可識別資訊，並使個體能被跨交易追蹤
  - 例：使用公開金鑰可隱藏個體之真實姓名
- 然而，若多個鑑別使用同一公開金鑰或擬匿名(pseudonym)，則該公開金鑰或擬匿名可被用以連結關於個體之跨多項交易的資訊， 並據以建立剖繪

一般(2/2)

- 但並非所有情況皆希望使用完全匿名性或完全去連結性
  - 例：個體可用匿名性以逃避非法使用系統後之處罰
- 雖然匿名性及去連結性可能適用於某些情境，然而於某些情況中，或須賦予某些機關(構)能重新識別個體之能力
- 為達成部分匿名及部分去連結鑑別之目的，過程步驟如下

  (a)註冊，包括設置資訊以達成匿名性

  (b)鑑別

  (c)(授權)

  (d)重新識別(適當時)

定義4 個角色

- 核發者－ 核發信符予宣稱者之個體
- 宣稱者－ 待查證者(verifier)鑑別之個體
- 查證者－ 查核宣稱者是否擁有有效信符之個體
- 指定開啟者－ 可重新識別宣稱者之個體

4 項基本操作

(1)信符核發過程：核發者與宣稱者間進行信符核發之過程

- 完成本過程後，宣稱者始具有信符

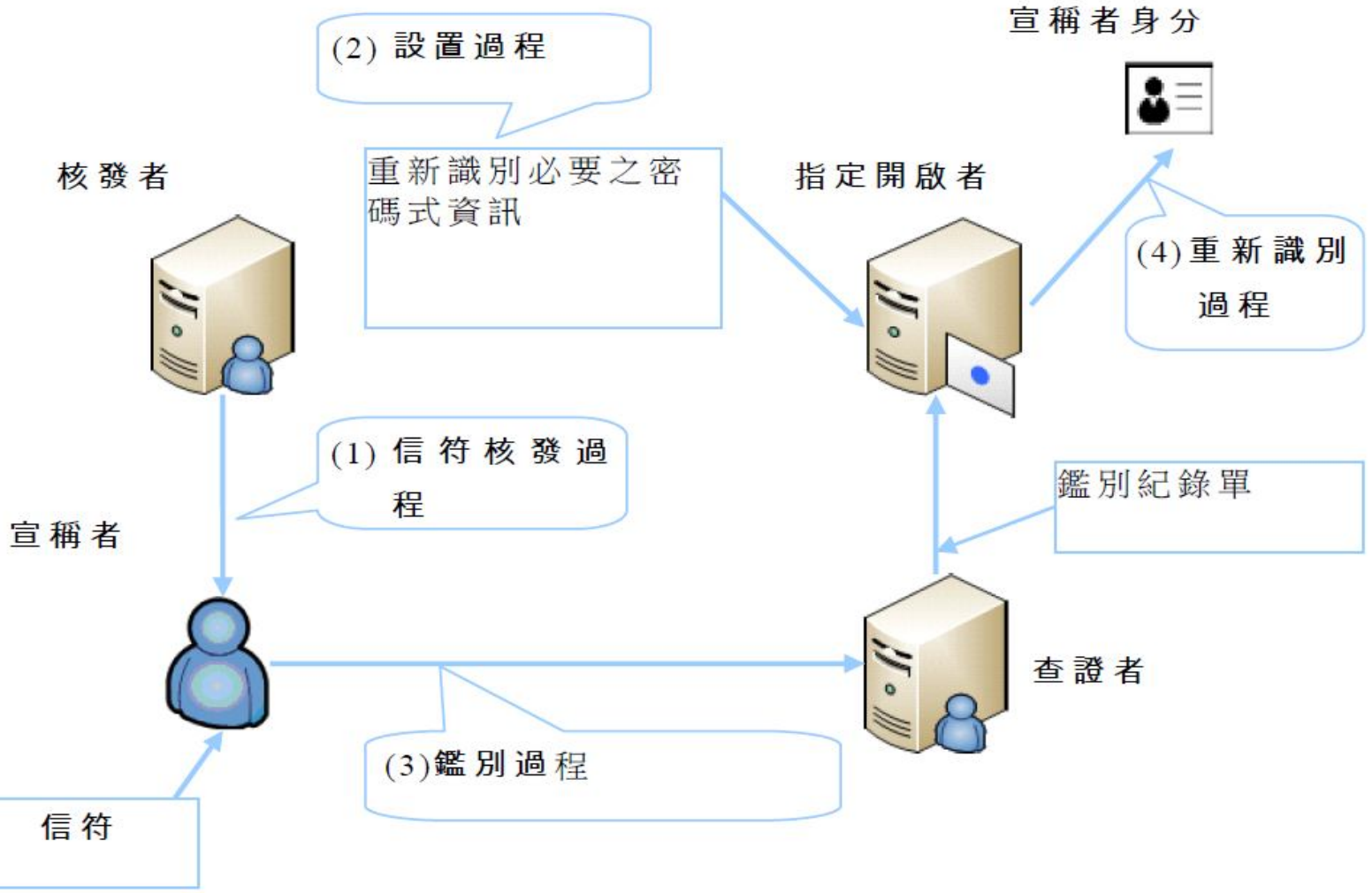
(2) 設置過程：指定開啟者設置對重新識別為必要之密碼式資訊的過程

(3) 鑑別過程：宣稱者與查證者間， 進行鑑別並產生鑑別紀錄單之過程

- 若查證者判定宣稱者持有有效信符， 則鑑別成功

(4) 重新識別過程： 指定開啟者由鑑別紀錄單識別宣稱者之過程。於此過程中，指定開啟者使用鑑別紀錄單， 且於適當時可使用其他資訊， 進行重新識別

部分匿名及部分去連結鑑別之框架



要求事項

(a)宣稱者應由查證者鑑別，而不能由查證者識別

- 對於向查證者保持匿名之宣稱者，其交易不應提供任何可用以識別宣稱者之資訊，但允許查證者證實宣稱者持有有效之信符

(b)鑑別紀錄單本身不得提供能連結同一宣稱者多項鑑別交易之資訊

- 對於向查證者保持不可連結之宣稱者，其交易不得提供可連結同一宣稱者履行之多項交易的任何資訊

(c)鑑別紀錄單應包含供指定開啟者重新識別宣稱者之必要資訊

- 為使指定開啟者之後能重新識別宣稱者，成功交易產生之紀錄單應提供識別宣稱者之資訊。注意，於適當情況下，指定開啟者可使用其他資訊以進行重新識別

(d)指定開啟者應能提供所宣稱身分為正確之證據

- 為避免指定開啟者之不誠實宣稱，指定開啟者應能提供重新識別程序已正當履行之證據

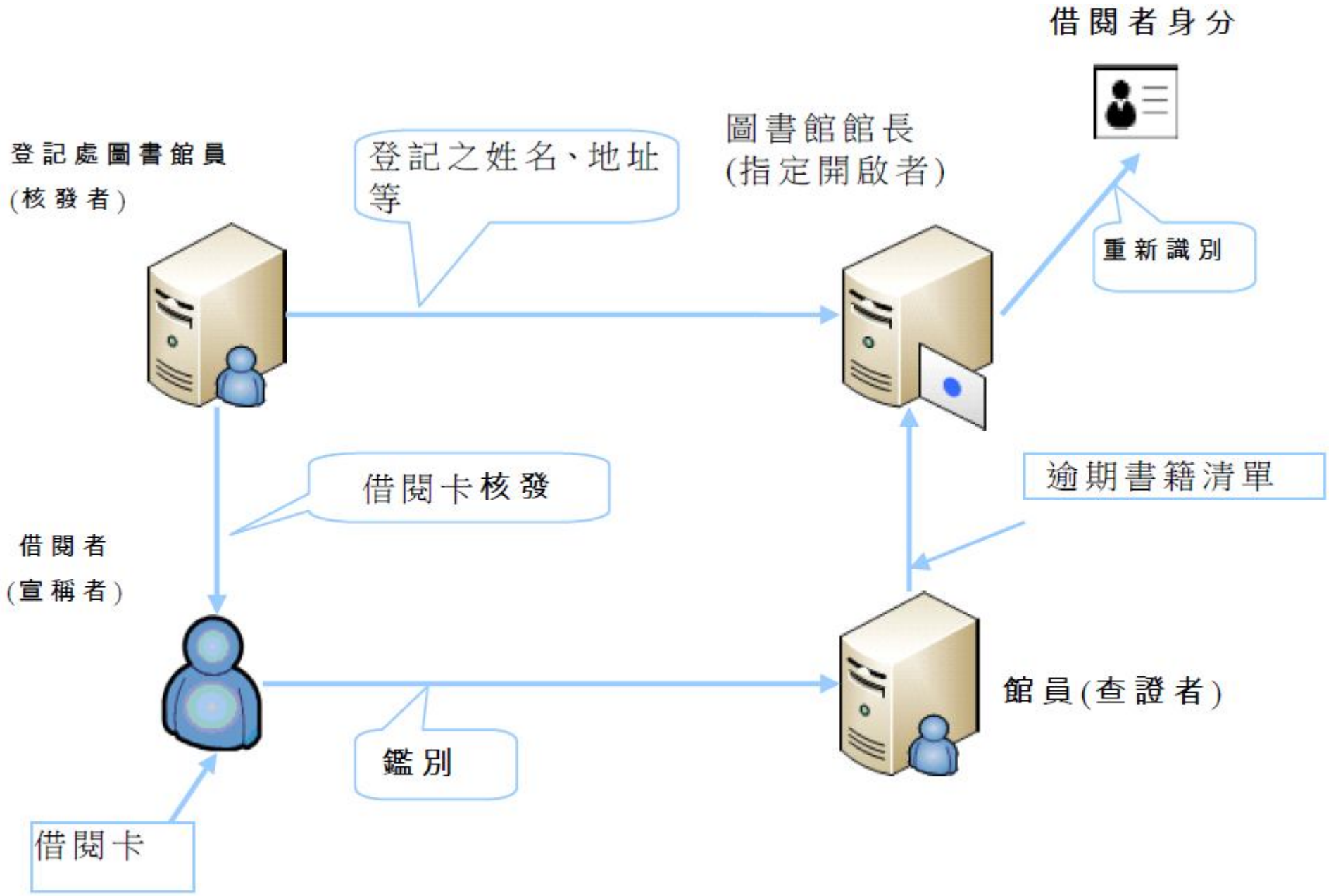

借閱者身分
登記處圖書館員
(核發者)
登記之姓名、地址等
圖書館館長
(指定開啟者)
重新識別
借閱卡核發
逾期書籍清單
借閱者
(宣稱者)
館員(查證者)
鑑別
借閱卡

圖 A.1　圖書館使用案例

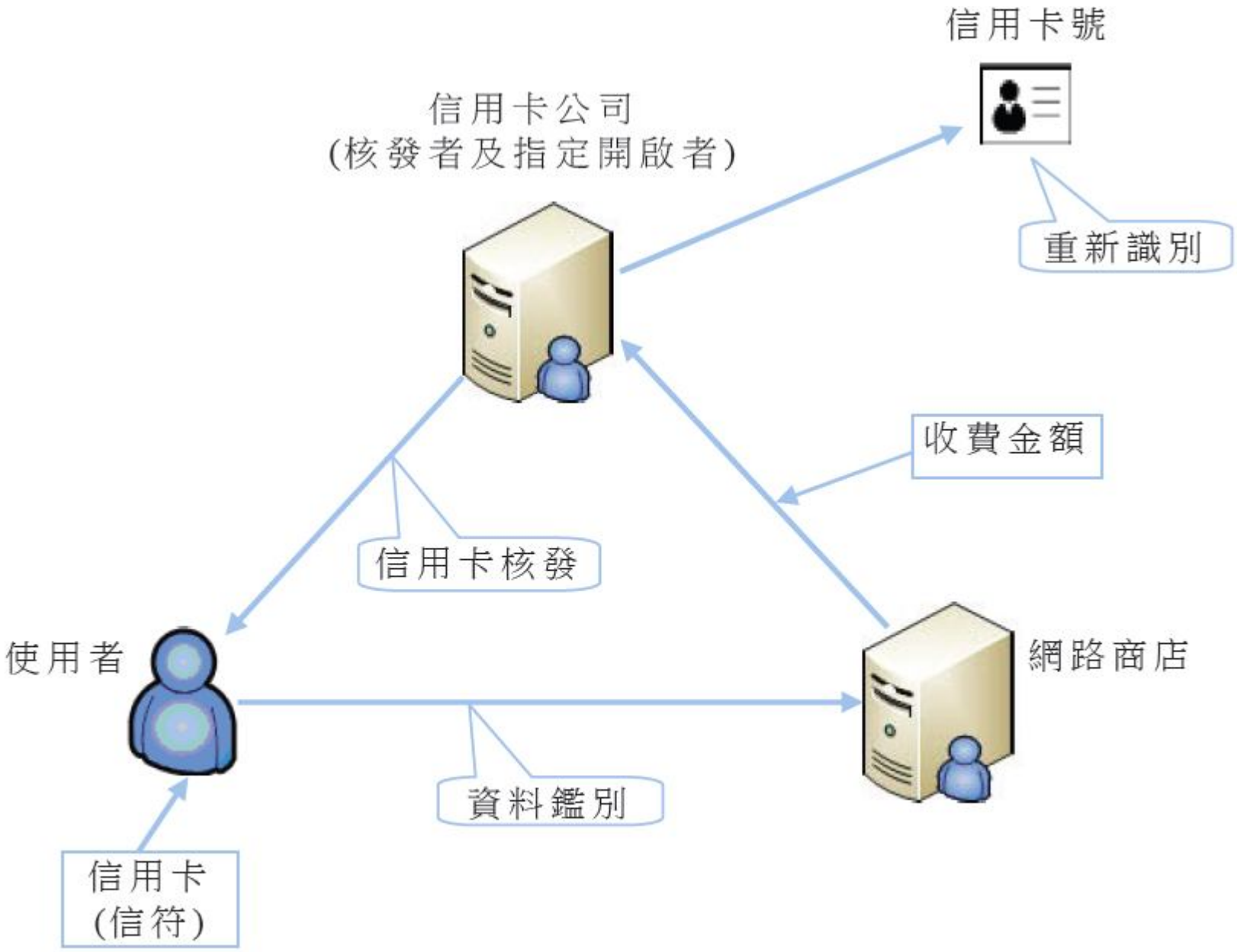


圖 B.1　隱藏付款帳戶

個人資料去識別化過程驗證要求及控制措施

去識別化之定義

- 依個資法第2條第1款有關個人資料之定義反面解釋可知，所謂「去識別化」，即指透過一定程序的處理，使個人資料不再具有直接或間接識別性
- 換言之，如將公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自無個資法之適用

架構

壹、目的

貳、用語及定義

參、隱私權政策

肆、PII隱私風險管理過程

伍、個人可識別資訊(PII)之隱私權原則 (暫不實施)

陸、PII去識別化過程

柒、重新識別PII之要求 (此部分為選項)

壹、目的

- 因應「政府資料開放」及「大數據」之推動，為驗證個人資料去識別化的過程，特訂定本驗證要求及控制措施

貳、用語及定義(1/3)

- CNS 29100 + CNS 29191之用語及定義
- 去識別化(de-identification)：採取一組合理之步驟，移除識別資料與資料主體間之關聯的過程
- 直接識別資料(direct identifying data)：直接識別PII當事人之資料。直接識別資料係不需額外資訊或經由交互連結公開資訊中之其他資訊即可用以識別PII當事人之資料。例：身分證號碼、指紋等
- 間接識別資料(indirect identifying data)：僅於與其他間接識別資料一起使用時方足以識別PII當事人之資料。例：郵遞區號、生日、年齡等
- 不可逆性(irreversibility)：由可識別至擬匿名之任何轉換的狀況，其由擬匿名追踪回原始識別符於計算上是不可行的

貳、用語及定義(2/3)

- 去連結資料(unlinkable data) ：僅包含難以由熟練的分析師以合理工作量連結至PII資料
- 重新識別(re-identification)：將已去識別化資料與原PII當事人重新建立關聯的過程
- K-匿名性(K-Anonymity)：若發布之資料中所包含之PII當事人的資訊與至少K-1個人的資訊，無法區別
- PII處理生命週期(PII processing life cycle)：包含PII之蒐集、移轉、使用、儲存、移除等階段
- 推論控制(inference control)：控制僅揭露無法據以推論出原PII當事人之資料

貳、用語及定義(3/3)

- CNS 29191用語對應於本要求及控制措施之用語如下：

CNS 29191用語	本要求及控制措施對應用語
宣稱者	PII當事人
核發者	PII控制者
指定開啟者	PII控制者
查證者	(擬)匿名資料接受者

參、隱私權政策(1/5)

- **要求事項(3.1.1)**：涉及PII處理之組織的高階管理階層，應依營運要求及相關法律與法規，建立隱私權政策，提供隱私權保護之管理指導方針及支持
- **控制措施(3.1.1.1)**：隱私權政策應如下
  - 合於組織目的
  - 提供設定目標之框架
  - 包括滿足適用之隱私保全要求事項的承諾
  - 包括持續改善之承諾
  - 於組織內傳達
  - 公眾(或相關各方)可適時且容易取得
- **控制措施(3.1.1.2)**：組織應以書面載明其隱私權政策
- **控制措施(3.1.1.3)**：隱私權政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性

參、隱私權政策(2/5)

- **控制措施(3.1.1.4)**：隱私權政策應依不同隱私權利害相關者，補充更詳細之PII處理規則及義務(例：特定部門或員工之程序)。此外，應載明於特殊設置下(例：存取控制、告知條款、稽核等)，用以增強隱私權政策之控制措施。
- **控制措施(3.1.1.5)**：內部隱私權政策應載明組織採用之目標、規則、義務、懲處規定、限制及/或控制措施，以滿足與其PII處理生命週期各階段有關之隱私保全要求事項。
- **控制措施(3.1.1.6)**：組織應傳達予隱私權相關者下列資訊
  - – PII控制者及所有相關之PII處理者的身分。
  - –關於移轉PII至PII處理者之政策。
  - –蒐集PII之目的。
  - –識別將蒐集之PII。
  - –加強隱私權保護之作為及其目的。
  - –PII當事人對其被蒐集之PII的法律權利。

參、隱私權政策(3/5)

- **控制措施(3.1.1.7)**：外部隱私權政策應提供外部人員對組織隱私權實務作法聲明，以及其他相關資訊，如PII控制者之身分及辦公室地址、PII當事人可能取得額外資訊之連絡窗口等。
- **控制措施(3.1.1.8)**：組織應具備正式懲處過程，並傳達予員工及約用人員，以對違反隱私權者採取行動。
- **控制措施(3.1.1.9)**：(告知之透明性)若PII處理者非PII控制者，則PII處理者之隱私權政策應依循PII控制者之隱私權訂定。

參、隱私權政策(4/5)

- **控制措施(3.1.1.10)**：組織若進行PII去識別化過程，則隱私權政策應包含下列項目，並應對外公布適宜之內容。
  - 敘明組織之去識別化作法，並以一般用語描述將使用何種去識別化技術
  - 敘明備妥何種保護措施，以盡量減少可能之相關風險。尤其是，應敘明去識別化資訊是否會對外公開或僅有限揭露，及其公開原則(例：離群值之處理、K-匿名性之使用時機)
  - 敘明對公眾開放關於進行之去識別化過程的任何風險。
  - 公開敘明關於公布已去識別化資訊之推理過程，說明如何衡量及取捨、考量或未考量哪些因素、原因為何

參、隱私權政策(5/5)

- **實作指引**：對公眾之資訊透通性可增加信任度，然基於資訊安全之考量，為不助長重新識別風險，組織應衡量是否需移除所公布之風險評鑑報告等文件中之某些資訊，或僅公布其彙總報告

肆、PII隱私風險管理過程

- **要求事項(4.1.1)**：組織應定期執行廣泛之PII風險管理活動並發展與其隱私保護有關的風險剖繪。
- **控制措施(4.1.1.1)**：組織應建立PII處理生命週期各階段之風險管理過程。各階段應包含下列子過程
  - 建立全景過程：藉瞭解組織(例：PII處理、職責)、技術環境及影響隱私風險管理之因素(亦即法規因素、契約因素、營運因素與其他因素)達成
  - 風險評鑑過程：藉識別、分析及評估PII隱私權原則之風險(可能有負面影響之風險)達成
  - 風險處理過程：藉定義隱私保全要求事項、識別及實作隱私控制措施以避免或減少PII隱私權原則之風險達成
  - 溝通及諮詢過程：藉從利益相關者得到資訊、對每一風險管理過程獲得共識，以及通知PII當事人與溝通風險及控制措施達成
  - 監視及審查過程：藉追查風險及控制措施，以及改善過程達成

肆、PII隱私風險管理過程

- **實作指引**：隱私權衝擊評鑑為一項產出，其為風險管理之一部分，隱私權衝擊評鑑乃專注於確保遵循隱私權及資料保護法規之要求，以及評鑑於新的或大幅修改計畫或活動中的隱私權含意
- **實作指引**：隱私權衝擊評鑑宜框限於更大範圍之組織風險管理框架內

陸、PII去識別化過程

- **要求事項(6.1)**：組織應建立有效且周延之PII去識別化過程的治理結構
- **控制措施(6.1.1)**：組織應指定足夠數量具技術與法律知識之員工或約用人員進行PII去識別化
- 並應指定資深員工，負責授權及監督PII去識別化過程。此負責人員應有能力負責PII去識別化主要決策、宣達及協調組織之PII去識別化作法、召集組織內部及外部相關專家，並應能協助高階管理階層決定已去識別化資料之適當揭露形式(亦即公開或有限存取)
- **控制措施(6.1.2)**：應經由人員訓練，使PII去識別化工作人員清楚認識PII去識別化技術、所涉及之所有風險及減輕此等風險之措施。尤其是，各工作人員應了解其於確保安全進行去識別化之特定角色

陸、PII去識別化過程

- **控制措施(6.1.3)**：應提供獨立及隔離(無法連線)空間(及系統)進行PII去識別化工作，並管制及記錄人員與資料之進出(及存取)，且人員不得攜帶任何具照像及記錄功能之設備進入工作區域
- **控制措施(6.1.4)**：應備妥以文件記錄之程序，識別決定是否對資料進行PII去識別化、其實施方法，以及產生之資料是否需揭露、揭露原則及揭露方式
- **控制措施(6.1.5)**：組織應備妥以文件記錄之程序，用以識別於實務上去識別化可能是有問題或難以達成之情況。例：難以評估重新識別之風險，或是對某些個人之風險太高

陸、PII去識別化過程

- **控制措施(6.1.6)**：組織應依據法律規定、組織任務、營運要求、資料使用對象及目的、所持有包含PII之資料內容、型式及數量、資料揭露範圍、處理成本及風險評鑑結果等因素，選擇適宜之去識別化方法，並經管理階層核准，且以文件記錄
- **控制措施(6.1.7)**：資料去識別化過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改，並定期稽核
- **控制措施(6.1.8)**：委外處理PII去識別化時，組織應監督及監視委外處理活動。原始資料以不攜出組織場域為原則。含有PII之資料應經組織之高階管理階層核准方可攜出場域外，而受委託單位須依組織之隱私權政策及隱私權原則妥善並安全保存原始資料，並於完成PII去識別化後，立即歸還組織或安全銷毀

陸、PII去識別化過程

- **要求事項(6. 2)**：組織之高階管理階層應監督及審查PII去識別化過程之治理的安排
- **控制措施(6.2.1)**：組織應管理，關於PII去識別化之任何新指引、法規、法律、裁判、行政解釋、可用技術或威脅之相關知識，並據以評估風險
- **控制措施(6.2.2)**：組織應與同行業或從事類似工作之其他組織分享並交流關於PII去識別化之知識
- **控制措施(6.2.3)**：組織應定期進行隱私衝擊評鑑(privacy impact assessment, PIA），並應公布其PIA報告，顯示如何處理風險評鑑過程。PIA應包含所採用去識別化技術之有效性，以及評估重新識別風險，以制定風險緩解措施

陸、PII去識別化過程

- **實作指引**：專家用以協助決定資料可識別性風險之原則如下，可使用此等原則，判定資料集之中的PII資料之風險值

原則	解釋	風險值範例
重現性 (Replicability)	根據資料將持續連結至PII主體之機率，將資料屬性定出風險等級之優先序	**低**：病患之口腔疾病，會改變 **高**：病患之牙齒照片相對穩定
資源可用性 (Resource Availability)	判定哪些外部資源含有特定個人之識別資料及資訊中之重覆特性，以及何人被允許存取該資源	**低**：實驗室報告中之個人身份通常不會對實驗室外披露。 **高**：個人身份及人口資料往往出現於公共資源中，例：出生、死亡及婚姻狀態。
區別性 (Distinguish)	判定某PII資料可於資料集之中區別的程度	**低**：據估計在美國使用出生年、性別及郵遞區號前3碼之組合約有0.04%機率可唯一識別某居民。此意指僅經由此等資料之組合可識別特定居民 **高**：據估計在美國使用出生日期、性別及5碼郵遞區號可唯一識別某居民之機率超過50%。此意指經由此3個資料之組合可識別一半以上的美國人
評鑑風險 (Assess Risk)	重現性風險、資源可用性風險及區別性風險越高，被識別之風險越高	**低**：資料不具區別性，但其可能並未獨立重現，且很少於許多人可存取之多個資源中揭露 **高**：人口資料具高度區別性、高度重現性並揭露於公共資源中

陸、PII去識別化過程

- **控制措施(6.2.4)**：組織之高階管理階層應決定已移除PII之資料之可接受剩餘風險
- **控制措施(6.2.5)**：管理階層應依規劃之期間或發生重大變更時審查去識別化過程
- **控制措施(6.2.6)**：告知之透通性，同控制措施(3.1.1.9)
- **控制措施(6.2.7)**：組織應依據對所收到回饋之分析，持續且及時審查PII去識別化過程。審查時應使用〝重新識別測試〞技術評鑑重新識別風險及減緩風險之措施
- **控制措施(6.2.8)**：應對已移除PII之所有資料進行系統化(自動或人工)檢查，確保其中未包含直接識別資訊，以及非必要保留之間接識別資訊。並確保必要保留之間接識別資訊皆已(經由匿名化、擬匿名化或其他方法)合理去除與PII當事人之連結

要求事項(6. 3)：組織應訂定如下之PII去識別化步驟，並依此進行去識別化

步驟1：由領域專家(或有經驗人員)判定資料集之中的直接識別資料

步驟2：將直接識別資料遮罩(或變換)。即移除直接識別資料或將其(擬)匿名化

步驟3：建立威脅模型。組織分析可能使用額外資訊或間接識別資料進行重新識別攻擊之各種情境，判定各種“可能威脅”

步驟4：判定最小可接受使用之資料。於此步驟中，組織確定PII去識別化資料之用途，並據以判定可能需去識別化之資料的最大數量

步驟5：使用步驟3所建立之模型，確定重新識別攻擊之風險的檻值。組織判定使用所有已去識別化資料之可接受風險，以及可能降低風險之各項控制措施

要求事項(6. 3)：組織應訂定如下之PII去識別化步驟，並依此進行去識別化

步驟6：由來源資料庫中取得(樣本)資料。因資料庫可能很巨大，故取樣測試，以協助規劃

步驟7：評估實際之重新識別攻擊風險。即計算實際被重新識別之風險

步驟8：比較實際之被重新識別的風險與檻值。即比較步驟7與步驟5之結果

步驟9：設定參數並套用至所有需去識別資料。若實際風險小於最小可接受風險，則套用去識別參數，並變換資料。若風險過高，則需考慮新的參數或變換

步驟10：對解決方案進行診斷。測試已去識別資料，以確保其具有足夠效用，並確認於允許之參數範圍內，重新識別攻擊是合理的不可能的

步驟11：輸出已去識別資料至外部資料集。最後，輸出已去識別資料，並將所使用之去識別技術、參數、威脅模型、風險值及各項相關資料，記錄於書面報告中

陸、PII去識別化過程

- **控制措施(6.3.1)**：應對待移除PII之資料集，先行備份，必要時應依隱私權原則進行前置處理，抽出最少需處理之資料、欄位或其部分
- **控制措施(6.3.2)**：應依待移除PII之資料型式(例：書面文字資料、書面圖片、文字檔、資料庫、圖片檔等)，選擇適當去識別作法及工具
- **控制措施(6.3.3)**：組織應依資料揭露(公布)對象及資料敏感性，設定推論控制之檻值(例：K-匿名性之最小K值、揭露筆數占整體筆數之最小百分比)。不得揭露超過檻值之資料

陸、PII去識別化過程

- **實作指引**：個人資料保護法第2條第1款定義個人資料：指自然人之之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料
- **實作指引**：推論控制通常使用之「N回應k%支配」規則，指若超過k%以上之揭露(或公布)資料係來自少於N筆資料，則不得揭露(或公布)該等資料
  - 例：不應公布比爾蓋茲所住社區之家庭平均年收入，因其年收入占整個社區之年收入比例太高，若公布此資料，易被用以推估出比爾蓋茲之年收入

實作指引：PII資料去識別化技術範例

- 修訂或移除PII資料：使PII資料成為(人類或電腦)不可視。
  例：用黑筆將書面資料塗黑、將人臉打馬賽克、移除檔案中PII資料、將資料加密、移除整筆資料等
- 模糊化PII資料：於資料中加入隨機〝雜訊〞
  例：將某筆個人資料之年齡加5歲，而下1筆資料之年齡加8歲、只提供對部分資料之統計數字
- 概化PII資料：降低資料之精確度，使其較不特定
  例：將年齡25歲，變成年齡20~29歲
- 合併PII資料：將數個PII資料項合併成一資料項，使其較不具敏感性
  例：2014年及格人數為2人，2015年及格人數為3人，合併為2014~2015年及格人數為 5人
- 以平均值置換PII資料
  例：將某筆個人資料之年齡以所有資料之平均年齡置換
- 一致性置換PII資料：將所有PII資料位移相同量，以保持資料間之關係。
  例：將所有個人資料之年薪均加10萬元
- 交換PII資料：將2筆資料之PII資料欄位內容交換
  例：將2筆資料之年齡交換

陸、PII去識別化過程

- **實作指引**：K-匿名性為去識別化後判定是否揭露資料之限制條件，組織應僅揭露具相同值筆數大於等於K之資料
- 增加K值可降低資料遭重新識別之風險
- K-匿名性可與各種去識別化技術一起使用

陸、PII去識別化過程

- **要求事項(6. 4)**：組織應對PII遭非預期揭露備妥災難復原計畫
- **控制措施(6.4.1)**：應及時回應來自自認為個人資料遭揭露民眾之申述及查詢，並依已建立之程序採取因應措施
- **控制措施(6.4.2)**：應備妥程序，因應公開資料遭重新識別而揭露個人隱私之情況，包含：移除可能揭露個人隱私之資料，重新處理；停止或修改(採取更嚴格之)去識別化過程
- **控制措施(6.4.3)**：當公開資料遭重新識別而揭露個人隱私時，應告知隱私遭揭露之個人，並協助其採取必要之彌補措施

陸、PII去識別化過程

- **要求事項(6. 5)**：組織應備妥程序，對已移除PII之資料，依可接受風險，定期進行〝重新識別測試〞。
- **控制措施(6.5.1)**：應對已移除PII之資料進行〝重新識別測試〞，包含：
  - －搜尋網頁，嘗試連結PII當事人
  - －搜尋全國或地方新聞資料庫，嘗試連結PII當事人
  - －搜尋政府單位或其他組織之開放資料，嘗試連結PII當事人
  - －以社群網路嘗試連結PII當事人
- **控制措施(6.5.2)**：因公眾可用之資料庫，隨時會增長，故應定期重新對已移除PII之資料進行〝重新識別測試〞，以重新評鑑其風險

柒、重新識別PII之要求

- **說明**:重新識別係將已去識別化資料與PII當事人重新建立連結之過程。此將增加去識別化過程之複雜度。
- 組織需重新識別PII當事人之理由可能包括：
  - 對資料完整性之檢驗
  - 檢查是否有疑似重複之資料
  - 加入新資料
  - 連結至額外研究變量
  - 符合性稽核
  - 重大發現需通知PII主體或相關單位
  - 進行後續進一步研究
  - 法律要求
- 組織有重新識別需求時，應符合CNS 29191所有要求事項

柒、重新識別PII之要求

- **要求事項(7.1)**：經匿名(或擬匿名)處理後資料之接收者應僅能鑑別PII當事人之資料屬性，而無法識別出PII當事人
- **控制措施(7.1.1)**：經匿名(或擬匿名)處理後之資料不得提供任何可用以識別出資料之PII當事人，但必要時可允許資料接收者查證經匿名(或擬匿名)處理後之資料(或其屬性)是否真實
- **要求事項(7.2)**：同一PII當事人之經匿名(或擬匿名)處理後之不同資料，不得提供具有聚合後能連結至該PII當事人之資訊
- **控制措施(7.2.1)**：資料接收者取得之經匿名(或擬匿名)處理資料，不得包含可據以連結PII當事人之間接識別資料

柒、重新識別PII之要求

- **要求事項(7.3)**：資料經可逆之擬匿名處理後，應可由PII控制者重新識別PII當事人
- **控制措施(7.3.1)**：PII控制者應備有重新識別PII之程序，規定所使用方法、所需資訊、授權及啟動流程
- **控制措施(7.3.2)**：應定期審查重新識別PII之程序的有效性
- **控制措施(7.3.3)**：為使PII控制者之後能重新識別PII當事人，將資料經可逆之擬匿名處理後產生之紀錄單，應提供足以識別PII當事人之必要資訊
- **控制措施(7.3.4)**：PII控制者對將PII資料經可逆之擬匿名處理所產生之紀錄單及重新識別所需之必要資料，應妥善加密，持續保存
- **實作指引**：於適當情況下， PII控制者可使用其他資訊以重新識別PII當事人

柒、重新識別PII之要求

- **要求事項(7.4)**：PII控制者應提供能正確重新識別PII當事人之證據
- **控制措施(7.4.1)**：為避免PII控制者之不誠實宣稱，PII控制者應提供正確履行重新識別PII當事人之程序的證據
- **控制措施(7.4.2)**：重新識別PII當事人資料之過程應留下紀錄、全程受監督(例：全程錄影)，且其紀錄應無法竄改

謝謝
敬請指教