淡江大學110年度

個資管理教育訓練

資訊處專案發展組
徐翔龍組長

2021/11/26

大綱

- 面對個資事件
- 認識個資法
- BS10012:2017差異重點
- 淡江大學個資管理制度
- 個資盤點
- 稽核注意事項

面對
個資事件

個資事件

- 2021/04/06
  Facebook超過5億用戶的個人數據外洩，包括電話號碼、電子郵件等資料
- 2020/06/01
  大學入學考試中心在6月1日證實，報名系統遭到入侵，約有2千筆學生報名的資料遭不當存取

個資事件

- 2020/09/30

  Neiman Marcus百貨業者系統遭入侵，造成超過430萬客戶資訊外洩

個資事件

解除分期詐騙5大高風險賣場

2021年第一季	2021年第二季
HITO本舖（121件）	誠品網路書店（310件）
GOMAJI（107件）	金石堂網路書店（175件）
Booking.com（102件）	萬年東海模型（147件）
DR情趣（95件）	婕洛妮絲計（144件）
Check2Check（94件）	Booking.com（119件）

資料來源：刑事警察局，iThome整理，2021年8月

個資事件

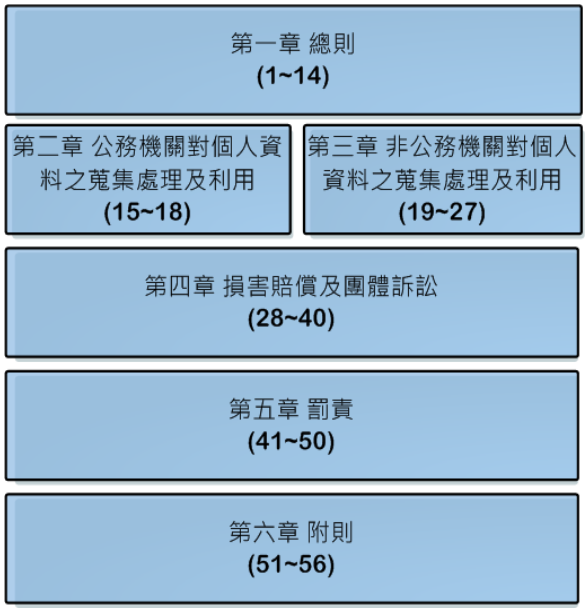
個資外洩原因

1.網路釣魚詐騙
2.帳號被駭、系統入侵
3.遭惡意軟體及不法應用程式的惡意操縱
4.設備遭竊取、遺失
5.在社群網站上過度公開資訊
6.將個資檔案夾帶寄出
7.紙本個資文件未妥善保管

認識
個人資料保護法

個資法(56)　104/12/30
施行細則(33) 105/03/02
105/3/15施行

個資法架構



用詞定義(第2條)

自然人

- 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

特種個資

- **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
- 其他得以**直接**或**間接方式識別**該個人之資料)

用詞定義(第2條)

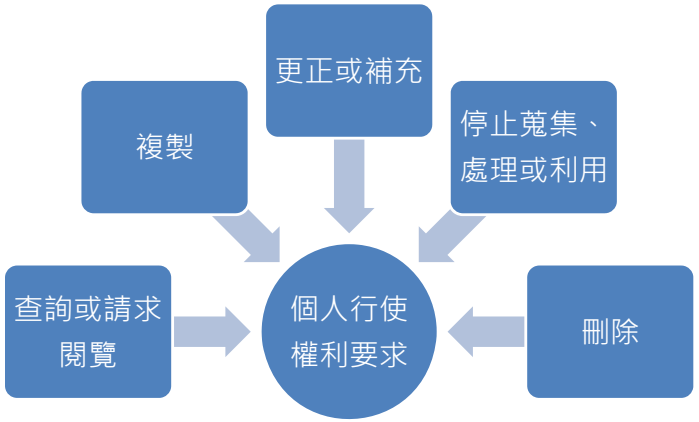
- **蒐集：**
  指以任何方式取得個人資料。
- **處理：**
  指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
- **利用：**
  指將蒐集之個人資料為處理以外之使用。

用詞定義(第2條)

- **國際傳輸：**
  指將個人資料作跨國（境）之處理或利用。
- **公務機關：**
  指依法行使公權力之中央或地方機關或行政法人。
- **非公務機關：**
  指前款以外之自然人、法人或其他團體。
- **當事人：**
  指個人資料之本人。

當事人權利(第3條)

不得預先拋棄或以特約限制之



第13條 ...為准駁之決定

查詢、閱覽或複製 15日

更正或補充、停止處理或利用、刪除 30日

第5條

- 個人資料之蒐集、處理或利用，
  應尊重當事人之權益，
  依誠實及信用方法為之，
  不得逾越**特定目的**之必要範圍，
  並應與蒐集之目的具有正當合理之關聯。

第6條(特種個資)

有關**病歷、醫療、基因、性生活、健康檢查及犯罪前科**之個人資料，**不得蒐集、處理或利用**。

但有下列情形之一者，不在此限：

一、法律明文規定。

二、公務機關執行法定職務或**非公務機關履行法定義務**必要範圍內，且事前或事後有適當安全維護措施。

三、當事人**自行公開**或其他**已合法公開**之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為**統計或學術研究而有必要**，且資料經過提供者處理後或經蒐集者依其揭露 方式**無從識別特定之當事人**。

五、為協助公務機關執行法定職務或**非公務機關履行法定義務**必要範圍內 ，且事前或事後有適當安全維護措施。

六、經**當事人書面同意**。但逾越特定目的之必要範圍或其他法律另有限制 不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者 ，不在此限。

明確告知(第8條第1項)

向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

免為告知(第8條第2項)

有下列情形之一者，得免為前項之告知：

一、依法律規定得免告知。

二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害公共利益。

五、當事人明知應告知之內容。

六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

間接蒐集免為告知(第9條)

有下列情形之一者，得免為前項之告知：

一、有前條第二項所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

資料保留(第11條)

- 個人資料蒐集之**特定目的消失**或**期限屆滿**時，應**主動**或依**當事人之請求**，刪除、停止處理或利用該個人資料。
- 但因**執行職務**或**業務所必須**或經當事人**書面同意**者，不在此限。

目的消失或期限屆期保留
(細則第21條)

- 有下列各款情形之一者，
  屬於本法第十一條第三項但書所定因執行職務或業務所必須：
  一、有**法令規定**或**契約約定**之保存期限。
  二、有理由足認**刪除將侵害當事人值得保護之利益**。
  三、其他不能刪除之**正當事由**。

特定目的消失
(細則第20條)

- 本法第十一條第三項所稱特定目的消失，
  指下列各款情形之一：
  一、公務機關經裁撤或改組而無承受業務機關。
  二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與 原蒐集目的不符。
  三、**特定目的已達成而無繼續處理或利用之必要**。
  四、其他事由**足認該特定目的已無法達成或不存在**。

個人資料安全
(細則第12條)

- **安全維護措施、安全維護事項、適當之安全措施：**
  指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，**採取技術上及組織上之措施**。
- 前項措施，得包括下列事項，**以與所欲達成之個人資料保護目的間，具有適當比例為原則**

技術上及組織上之措施
(細則第12條)

- 一、配置管理之人員及相當資源。
- 二、界定個人資料之範圍。
- 三、個人資料之風險評估及管理機制。
- 四、事故之預防、通報及應變機制。
- 五、個人資料蒐集、處理及利用之內部管理程序。
- 六、資料安全管理及人員管理。
- 七、認知宣導及教育訓練。
- 八、設備安全管理。
- 九、資料安全稽核機制。
- 十、使用紀錄、軌跡資料及**證據保存**。
- 十一、個人資料安全維護之整體持續改善。

賠償、罰責

第28、29條

- $500~$20,000 (每人每一事件)
- 最高總額以**新臺幣二億元**為限
- **因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。**

損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行 使而消滅；自損害發生時起，逾五年者，亦同。(30條)

第29條

- 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵 害當事人權利者，負損害賠償責任。但能**證明其無故意或過失者，不在此限**。

第41、42條

- **意圖為自己或第三人不法之利益或損害他人之利益，.....，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。**

第47條

- 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：

一、違反第六條第一項規定。
二、違反第十九條規定。
三、違反第二十條第一項規定。
四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。

第48條

- 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：

一、違反第八條或第九條規定。
二、違反第十條、第十一條、第十二條或第十三條規定。
三、違反第二十條第二項或第三項規定。
四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

第50條

- 非公務機關之**代表人**、**管理人**或其他有**代表權人**，因該非公務機關依前三條規定受罰鍰處罰時，**除能證明已盡防止義務者外**，應並受同一額度罰鍰之處罰。
- 第47條 5萬-50萬元
- 第48條 2萬-20萬元
- 第49條 2萬-20萬元

教育部

- 教育部臺教資(四)字第10200179090號
- 學校為達成教育或訓練行政目的，於其必要範圍內所為獎勵學生行為，如張貼榮譽榜揭示姓名，符合個資法第16條、第20條利用規定，無需過度遮掩姓名，否則有違個資法第1條規定所稱「促進個人資料之合理利用」意旨。

PIMS
BS10012:2017
新版重點

差異重點

3.1.14 自然人/資料主體

- 現存個人的識別符可被直接或間接識別，例如：姓名、身分證字號、位置資料、網路識別符碼，或生理、心理、遺傳、精神上、經濟、文化或是社會身分等。

3.1.20 個人資料

- 與自然人相關之已識別或可識別的資訊，包含擬匿名化，但不包含完全匿名化的資料。

差異重點

3.1.27 剖析 (profiling)

- 透過自動化的處理、利用的方式，作為評估與自然人相關的個人資料。

3.1.30 特種個資

- 與自然人相關的個人資料，包含：種族或族群背景、政治理念、宗教或其他信仰、職業工會會員、基因資料、基於識別唯一自然人為目的的生物特徵資料、與健康或自然人性生活或性傾向的資訊。

差異重點

6.1.7 從設計著手保護隱私

- 當設計作出重大變更時應：
  1) 使用於組織內或資料處理者的系統；
  2) 使用於當事人或其他組織的產品與服務。
- 系統、產品或服務處理個人資料時，組織應：
  1) 預設最小化；
  2) 盡可能使用去識別化資訊；
  3) 功能與處理個人資料的透明化考量。
- 以組織化與技術程序適當實現：
  1) 相稱於風險識別結果；
  2) 確認隱私風險處置被適當實施為個人資料保護；
  3) 以文件化方式將從設計著手保護隱私活動及結果予以記錄

差異重點

8.2.1.2 資料保護官(DPO)

- 當組織依照法規、主管機關要求或營運需要，被要求指派資料保護官時，應指派符合資格之人員擔任此角色。資料保護官的聯絡方式應向相關主管機關報備。
- 資料保護官或符合資格之人員應確保個人資訊管理系統符合適用的法律、法規與營運需要。
- 資料保護官或符合資格之人員應確保適當的隱私衝評估與風險評鑑於必要時確實完成。
- 資料保護官或符合資格之人員應確保當需要向主管機關回報時都有完成。
- 組織應適時涉入資料保護官或符合資格之人員與個人資料處理相關之議題。

差異重點

8.2.7.3 處理兒童的個人資料

- 在處理與兒童有關的個人資料時，尤其是為了建立個人資料剖析和/ 或行銷上，個人資訊管理系統應將父母或監護人同意納入機制中，但有關於提供專業諮詢與預防性服務的情況除外。

8.2.7.5 開放資料

- 當個人資料被發佈為「開放資料」的一部分時，個人資料應去識別化使該自然人無從識別，除非有公開個人資料的基礎。
- 當採取去識別化方式，應考慮可能用於重新識別自然人的所有合理手段。

差異重點

8.2.12.1 回應其權利 -1

- 個人資訊管理系統應包括確保自然人與其個人資料有關的權利受到尊重的程序，並且在收到自然人的請求後一個月內，無不當延遲地滿足執行該權利的請求。
- 個人資訊管理系統應確保遵守要求，如有需延長該一個月期限，自然人應被告知，並依自然人請求的電子或紙本副本格式提供資訊。個人資訊管理系統應確保符合遵守自然人請求延長該一個月期限，任何延期不超過額外的兩個月。

差異重點

8.2.12.1 回應其權利 -2

- 備註：權利包括個人資料近用權、反對處理權、補正不正確資訊權利、刪除和/ 或限制使用個人資料、個人資料可攜權，以及當處理涉及剖析或重大影響自然人時，不進行自動處理的權利。
- 個人資訊管理系統應確保程序包括考慮是否適用任何減損或豁免。

差異重點

8.2.12.6 資料可攜權

- 個人資訊管理系統應確保自然人擁有個人資料可攜權，當資訊以自動化方式處理時，自然人能夠將這些資訊免費和以結構化、通用和機器可讀格式傳輸給他們，或者給其指名的另一個組織。

8.2.12.8 自動化決策，含剖析

- 個人資訊管理系統應確認辨別包括剖析的自動化決策對自然人可能造成重大影響的處理個人資料的程序。
- 個人資訊管理系統應至少應確認當自然人請求時，任何自動化決策會涉及人為介入。

去識別化資料(法務部)

透過一定程序的加工處理，使個人資料不再具有直接或間接識別性。依其去識別化之加工程度不同，有以下列類型：

- **匿名化資料**（anonymised data）：對任何人而言，均無法採取任何合理 可能之方法識別特定個人，亦即資料經加工後，毫無保留連結之可能性。
- **擬匿名化資料**（pseudonymised data）：擬匿名化資料乃是以編碼或別名取代識別符號（例如姓名、國民身分證統一編號等），使研究或統計人 員得以針對個體資訊進行分析而無須識別個體身分，可再分為2種態樣：
  1. **不可逆**（non-retraceable/irreversible）
  2. **可逆**（retraceable/reversible）：多用於特定依法允許重新識別之領域， 例如：進行醫療實驗研究時，為能適時回溯追蹤調整對受試病患之醫療處置。

去識別化資料

法務部103年11月17日法律字第10303513040號函：「如將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，自非個資法之適用範圍 。」

GDPR：若個人資料已**「去識別化」達到無從識別個人資料當事人**，而為「匿名（anonymous）」之狀態，歐盟認為此時**已非個人資料**，自無歐盟個人資料保護指令之適用，原則上應屬政府資訊開放公眾利用之範圍，惟去識別化的資料必須達到**「以一切可能合理之方法」無從再識別資料當事人**之程度，否則仍應受個人資料保護指令規範。

兒童定義

兒童及少年福利與權益保障法第 2 條：

本法所稱兒童及少年，指未滿十八歲之人；
所稱**兒童，指未滿十二歲之人**；
所稱少年，指十二歲以上未滿十八歲之人。

民法第12條：

滿**二十歲**為成年。

聯合國兒童權利公約：

兒童係指未滿十八歲之人。

高風險個人資料

BS 10012:2017高風險個人資料 (8.2.2.2)

a) 特種個人資料 (3.1.30)
- 種族或族群背景
- 政治理念
- 宗教或其他信仰
- 職業工會會員
- 基因資料的處理
- 基於識別唯一自然人為目的的生物特徵資料
- 與建康或自然人性生活或性傾向的資訊

b) 個人銀行帳戶及共他財務資訊

C) 國家身分，如：國家保險號碼

d) 與弱勢成人和兒童有關的個人資料

e) 對個人特徵的詳細描述 (包含兒童)

f) 可能對自然人造成不利影響的敏感協商

特種個人資料

個資法特種個人資料 (第6條)
- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

BS 10012:2017管理摘要

1.法源依據 (6.1.3)
2.合法、公平且透明的處理 (8.2.6)
3.善盡告知義務 (隱私權資訊 (8.2.6.1)
4.僅基於特定合法目的取得(8.2.7)
5.適當、相關及限於資料侷限原則(資料最小化 8.2.8)
6.正確並及時更新 (正確性 8.2.9)
7.資料的儲存不得超過許可的必要 (保管期限 8.2.10)
8.適當確保個人資料安全 (完整性及機密性 8.2.11)
9.確保資料傳輸之安全 (8.2.11.4)
10.落實委外安全管理 (8.2.11.10)
11.自然人權利 (8.2.12)
12.妥善處理訴怨程序 (8.2.12.9)

BS 10012:2017管理摘要

自然人權利 (8.2.12)
- 個人資料近用權
- 更正權
- 刪除權
- 限制處理權
- 個人資料可攜權
- 反對權
- 自動化決策 (含剖析)

個資法當事人權利
- 查詢或請求閱覽
- 請求製給複製本
- 請求補充或更正
- 請求停止蒐集、處理或利用
- 請求刪除

淡江大學
個資管理制度

認證標準：BS10012
認證範圍：淡江大學全校
通過認證：103年1月29日
校長核定
108學年起每年2次內稽

淡江 PIMS

適用範圍

一、本校**所有人員**均屬適用本政策之涵蓋對象。
二、個人資料管理制度之驗證範圍為本校**個人資料流程**之相關作業。

所有人員

涵蓋本校正式及約聘之教職員工、本校之委外廠商等。

PIMS實作

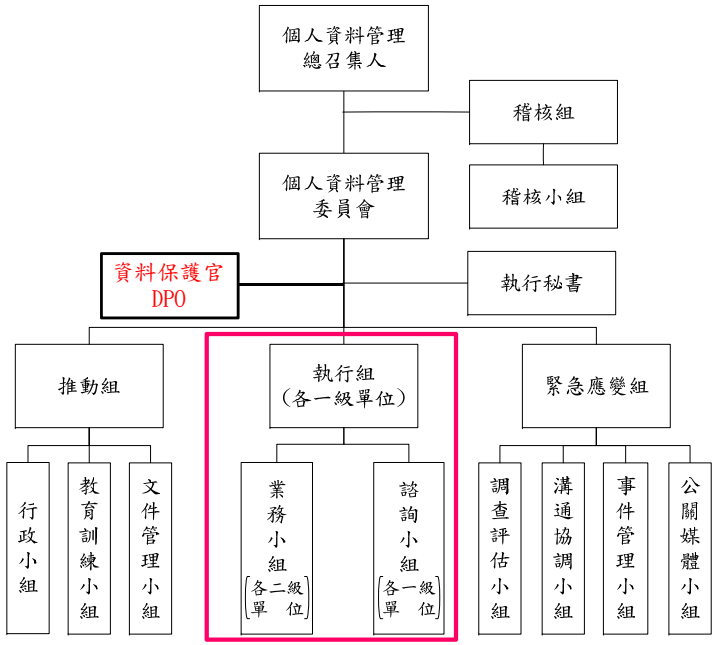
- **P 規劃**
  範圍及目標、管理政策、職責與當責性、資源提供、落實組織文化
- **D執行**
  管控機制、認知與教育訓練、辨識及記錄個資、風險評鑑；公正與合法、基於特定目的、適當且不過度處理個資、正確性、保存、個人權利；安全議題、揭露給第三方、委外處理
- **C稽核**
  內部稽核
- **A改善**
  預防措施、矯正措施

PIMS管理制度文件

- 一階文件 **政策**
- 二階文件 **規範**
- 三階文件 **程序**
- 四階文件 **表單**

http://pims.tku.edu.tw/

淡江大學個人資料管理組織架構



淡江個資制度執行摘要

- 法規遵循
- 蒐集最小化原則
- 清冊版本 V3.0　（盤點）
- 軌跡紀錄(傳遞)
- 保存方式(安全)
- 保存期限
- 銷毀紀錄 (Log)
- 權利 (行使窗口)
- 兒童資料
- 剖析資料

資料創建(蒐集)時
即知是否含個資，
而非完成時才知含個資

(6.1.7 從設計著手保護隱私)

尊重當事人之權益，
依誠實及信用方法為之，
且未逾越特定目的之必要範圍

善盡保護責任(儲存安全)

個資文件及清冊，
列入人員輪調移交重點項目

2018/1/9 外稽結束會議
稽核長、人資長

個資盤點

個資處理流程

蒐集→儲存→處理→利用

→傳輸→銷毀

個資盤點

全面清查 → 風險等級 → 控制措施

個資盤點

全面清查

業務流程分析(Phase Ⅰ)

ＢＩＦ流程圖(工作流程)

個資流程項目盤點分析(Phase ⅠⅠ)

個資盤點清冊

(版本 V3.0 2018.06.20)

Phase Ⅰ 業務流程分析

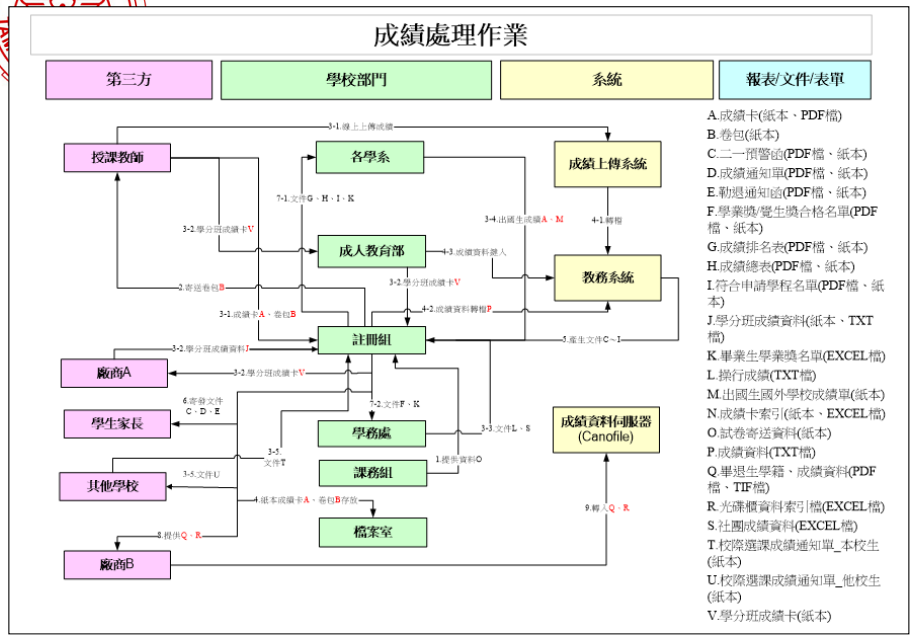
由**業務流程**為出發點進行盤點，

列出全數業務、作業流程。

Phase Ⅰ 欄位說明

項目		說明
1	盤點日期	實際盤點的日期
2	作業事項	內控流程已有規範，請填寫內控所屬作業事項。 未在內控中規範，請填寫目前作業名稱。
3	作業流程名稱/資訊系統模組	
4	作業負責單位名稱	
5	是否為個資流程(Yes/No) （Yes-繼續進行Phase Ⅱ）	
6	定期盤點是否異動（Yes/No）	業務流程或相關資訊異動即為 Yes (前4項及BIF變更)。
7	盤點單位	以二級單位或一級本部為盤點單位。
8	盤點人員	
9	覆核人員	單位主管簽章
10		

ＢＩＦ流程圖(範例)



個資盤點清冊

(版本 V3.0 2018.06.20)

Phase II 個資流程項目盤點分析

1	盤點日期	28~29	保管
2~19	基本資訊	30~33	揭露、委外、國際
20	蒐集	34~40	資訊環境
21~23	處理	41	是否異動
24~27	利用 (特定目的外)		

Phase II 欄位說明

1	盤點日期	實際盤點的日期
2	盤點人員	實際負責盤點人員姓名。即為個資檔案資料控制者(蒐集者) 或資料處理者。 以**二級單位**或**一級本部**為盤點單位。
3	作業事項	內控大項（人事、財務、營運等）。若無請直接寫業務/作業名稱
4	作業流程名稱/資訊系統模組	子作業名稱，若有分更細項可一併填寫
5	單位名稱	Ex.資訊處、資訊處校務發展組
6	個資編碼	單位代碼/代號+**3碼流水編號**。刪除者保留編號。
7	個人資料檔案名稱（若無具體名稱請概述用途）	個人資料檔案名稱：可依據其目的、性質、名稱 Ex. 員工履歷表
8	個人資料範圍	蒐集之個人資料內容，例如資料表單欄位（此欄位需要詳盡填寫） Ex. 姓名、電話、身分證字號

Phase II 欄位說明

9	資料筆數	約略估計個資資料筆數，以**數字格式**填寫。保存期限內，個資筆數最高持有總數量估計。 紙本、電子資料請以單筆個資紀錄為 1 筆。 Ex1.工讀生勞保投保資料，若保存期限1周，但每周數量不一，則**以1年內**，某一周持有最高數量估計。**若1年內均為0時，則填寫之前某一周曾經持有最高數量。若有此項業務以來，均未有資料，則可填 0。** Ex2.工讀生報名表，保存期限3年，其個資數量為3年內累加估計。
10	資料格式（如：紙本、電子、系統）	請依照檔案格式寫 “紙本” 或 “電子檔” 或 “系統” ，電子檔請填寫資料格式，如 docx、xlsx、 pdf、 jpg、gif、odt、ods... 等； 若同時存在紙本、電子檔、系統，請分開表列（多列）。
11	特定目的之項目	請填寫代號 參考附錄一之特定目的項目資料範例，不一定只有一個。
12	個人資料類別	請填寫代號 參考附錄二之個人資料類別，依『個人資料範圍』之欄位內容，決定資料類別。

Phase II 欄位說明

13	資料保存期限	依據「相關文件」填寫資料保管期限； 依**法律、主管機關、校規、單位合理自訂** (可參考分層負責明細表)。 注意資料保存期限適當性。請據實填寫目前資料保存期限，若有法令規範依據，則依法規為主。 **資料在單位內存放的時間長度，** 如天、周、月、年、99年=永久，**最少1天**。
14	是否包含醫療基因、生物特徵...之個人資料（Y/N）	請填寫是否包含特種個資種類（醫療、基因、性生活、健康檢查及犯罪、病歷前科、基於識別唯一自然人為目的的生物特徵資料）。 若無請填寫"N"
15	蒐集對象	Ex. 學生、教職員、供應商、求職者、委外廠商
16	蒐集目的	處理個資之特定目的，請描述細節。如薪資發放、人員招募、績效考核等。
17	是否需依法告知（Y/N）	個資法第 8 條：公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知...。 若免告知須符合個資法第 8 條 第 2 項或第 9 條規定。

Phase II 欄位說明

18	是否經當事人同意（Y/N）	個資法#6-6：特種個資，經當事人**書面同意**。 個資法#19-5：依法告知當事人應告知事項後，經當事人同意。 細則#14：當事人**書面同意**之方式，依電子簽章法之規定得以電子文件為之。 細則#16：告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。 BS10012:2017：若為兒童個資，需經父母或監護人同意。
19	同意資料	確定目前仍存在該同意資料。 保留證據 告知方式之證明。Ex.同意書、契約、eMail紀錄、網站勾選留存、COOKIES等。
20	取得法規依據	依據什麼法律或是內部規定蒐集此項「個資檔案」，查詢後若無相關規定請註記 “NA” 。 Ex. 消防法、私校法、淡江大學OO管理辦法、招生簡章。
21	資料來源單位名稱	資料來源單位名稱通常為其他處組。 若蒐集與處理單位相同，請填寫"本單位"

Phase II 欄位說明

22	處理目的	請依據實際作業目的陳述處理目的。Ex. 申請獎學金、研究計畫。
23	處理方式（可複選）	記錄：書面資料記錄，log記錄 輸入：資料新增，如新建立表單。儲存：歸檔存查、複製 編輯：核准、彙整，分析。更正：資料核准後的修正。 檢索：資料搜尋。刪除：資料刪除。輸出：資料下載、報表檔案輸出。 內部傳送：資料轉入、轉出部門。
24	利用目的	是指「蒐集特定目的」以外的處理即為利用。 Ex. 取用學生資料，供辦理研討會活動、營隊使用。
25	是否已完成其他利用目的之告知（Y/N)	個資法第20條：有下列情形之一者，得為特定目的外之利用：一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。

Phase II 欄位說明

26	告知方式	細則#16 **(請留佐證資料)** 告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。
27	同意資料名稱	Ex. 同意書、回復之電子郵件 。 若無取得同意之證明，請填寫"N"，但須符合個資法第20條規定。
28	儲存人 / 保管人	1.當個資資料經多個部門後，由最後一個部門負責保管 歸檔時，則保管人填寫最後一個部門， 其餘部門**有保留資料者亦需填**。 2.當電子表單有經由多個部門簽核時，則在盤點表中的保管人，每個部門皆應填寫。 OD系統簽核，未實際下載留存資料者除外。
29	儲存/保管單位、地點	存放個資資料的實際地點。 書面資料：如大樓、房間編號、系所資料櫃編號。 電子檔案：如大樓、房間編號、誰的電腦、備份磁碟。 Ex. 資訊處B207

Phase II 欄位說明

30	該個資是否有委外/分享/揭露作業	接受個資資料單位名稱或揭露方式，若無填寫"N"。 Ex.教育部、保險公司...、榜單等。 委外作業包括對外資料分享、揭露、作業委外等。
31	委外依據（委外合約名稱、主管機關函文）	1. 若有委外作業，請填寫委外合約名稱或公文文號 2. 若有委外作業無合約，請填寫"N"。 若無，請補保密承諾書。 **3.含接受委託計畫蒐集個資** 4. 若無委外作業，請填寫"NA"。
32	是否有國際傳輸情形	請填寫傳輸至的國家及城市名稱，若無填寫"N"。
33	國際傳輸至的單位/公司/組織	填寫對方組織名稱，若無填寫"N"。
34	個資處理系統（可能多個）	所有會處理到本項個資之系統名稱。 請與資訊處系統開發單位組長連絡， 單位自行委外開發者請自填。
35	系統資料保存年限	系統內個資保存年限，並描述目前實際作法。

Phase II 欄位說明

36	個資系統備份媒介（系統定期備份）	系統備份個資資料的媒體種類，Ex. 磁碟、磁帶USB、雲端磁碟。
37	備份資料存放地點	備份資料存放之實際位置 Ex. B208
38	是否拋轉外部（Y/N）	系統資料若有拋轉至學校外部時，填寫 "Y"。若無請寫"N"。
39	若有拋轉外部，請填寫拋轉之外部單位	系統資料若有拋轉至學校外部時，填寫外部單位名稱。Ex.教育部。 若無請寫"NA"。
40	若有拋轉外部，請填寫拋轉之外部之目的	資料拋轉目的簡述，若無請寫"NA"。
41	是否異動(Y/N)	盤點有異動 (2-40項) 時請填 "Y"。

盤點表保管欄位補充說明

項次	資料格式	情境	保管		備註
			儲存人/保管人	儲存/保管單位、地點	
1	紙本	保存在本單位	本單位保管人姓名	本單位名稱、存置地點	
2	紙本	經本單位業務處理後送出，且本單位不留存	本單位處理期間保管人姓名及 接收單位或最終單位名稱	本單位名稱、存置地點、及 接收單位或最終單位名稱	處理期間=資料保存期限
3	紙本	屬**公文流程**，閱後即送出，且本單位不留存副(影)本	無	無	無需盤點

盤點表保管欄位補充說明

項次	資料格式	情境	保管		備註
			儲存人/保管人	儲存/保管單位、地點	
4	電子檔	保存在本單位	本單位保管人姓名	本單位名稱、存置地點	
5	電子檔	本單位業務處理後送出，且本單位不留存	本單位處理期間保管人姓名及 接收單位或最終單位名稱	本單位名稱、存置地點、電腦、及接收單位或最終單位名稱	請留檔案銷毀紀錄 若有留存比照第4項
6	電子檔	屬OD、OA公文流程，閱後即送出，且本單位不留存副本	無	無	無需盤點、 有開過檔案者請刪除暫存區檔案
7	系統	資訊系統上的作業資料	本單位業務管理人或承辦人姓名(擁有系統權限者)	負責系統開發的單位名稱(組)	有開過檔案者請刪除暫存區檔案。 若有留存比照第4項

稽核注意事項

稽核注意事項

- **稽核準則**
  - ✓ 國際標準、政府相關法律、規定
  - ✓ 校規作業準則、合約或合理自訂(會議決議)
- **法源依據**
- **資料保存期限**
  - ✓ 主管機關法規
  - ✓ 機關共通性檔案保存年限基準 (20 大專校院類)

    106年5月17日國家發展委員會檔案管理局
    (檔徵字第1060009095號函訂頒)
  - ✓ 分層負責明細表
  - ✓ 業務主管部門公告 (OA)

稽核注意事項

- 工讀生 勞動契約書、助學金出勤表、生活服務學習時數紀錄表 保存期限
- 勞工健康檢查表 保存期限
- **保存期 一致性**
- 表格版本控管 (**一致性**)
- 個資聲明 未列權利及不提供的影響、**訴怨程序與窗口**
- 表單 未列個資權利及不提供的影響
- 各系 繁星、推甄資料 要盤點
- 超過保存期限 **個資要銷毀 留紀錄**
- 銷毀清冊內容應列細節 要含**起迄期間、筆數**
- 只列電子檔卻有紙本、表列10年盤點僅1年

稽核注意事項

- 風險評鑑表公式不正確 **注意版本V3.0、風險值**
- **軟體安全更新** Windows、SEP、Acorbat Reader.....，
- 免費防毒軟體不要使用為原則
- **防毒軟體狀態須為啟用、病毒碼即時更新**
- 密碼長度及定期更新
- **外接式行動碟保管**
- 學生資料的使用目的不屬人事管理 (**盤點要正確**)
- 保存期限的計算 學年度與年度資料保留、紙本與電子檔要一致性
- 資料筆數的計算 保存期限的最大量 (約)

稽核注意事項

- **GDPR** 歐盟國家學生、考生資料
- 個資聲明 版次
- 個資表的**附屬文件含個資 應列入盤點範圍**
  (如醫生證明...)
- 電腦垃圾桶及實體垃圾桶要確認無個資文件
- 特定目的正確性 如學生用途不應002(人事管理)
- 系統使用 **SSL加密** (https://...../)、**資安弱點掃描**
- Email 個資檔案**要加密**
- **存在雲端硬碟 (如 google Drive) 的資料要加密**

稽核注意事項

- 各單向資料單位(如教、人)申請**師生資料**
  有無 **盤點、保管、銷毀紀錄**
- **工具軟體 (共享軟體)**
  是否即時更新
- **個人電腦垃圾桶、下載暫存區 清理**
- **備份硬碟、USB碟 儲存安全**
- **委外系統、資料存放雲端 要符合資安要求**
- **演練計畫**
- **新增業務**

工讀生資料保存期限

108學年度第1學期
各項工讀助學金分配時數及相關注意事項 (學務處)

108學年度起各項**助學金出勤表、生活服務學習時數紀錄表**，由**各單位自行管理及檢核**，需負責資料之正確性並留存備查，
依會計法各項會計憑證需**保留7年**(需列入移交)，不需送生輔組。

疫情期間蒐集個資

指揮中心：
為確保個資保護，各場域所蒐集的民眾個人資料，均要指定專人辦理並善盡資料保護責任，**最多存放28天**，之後必須**刪除或銷毀**。
這些資料只能在配合疫調時使用，不可用於其他目的，蒐集方式可採用紙本或電子，如使用電子方式蒐集，必須採行資安防護措施。
蒐集民眾個人資料時，**應明確告知**當事人包含蒐集機關、目的、個人資料項目、利用期間、利用對象及方式、當事人依個資法可請求的權益及不同意提供時的影響等7項資訊。

生物特徵

教育部：
108年12月23日 臺教資(四)字第1080181577號
校園使用生物特徵辨識技術個人資料保護指引

生物特徵：指具個人專屬性足以識別個別身分之個人生理特徵資料（如指紋、臉部特徵、虹膜、聲音、掌紋、靜脈等）

原始生物特徵資料： 個人生物特徵之原始資料

特徵值： 轉換成用於生物特徵比對之不可逆資料

生物特徵

學校為使用生物特徵辨識技術，並蒐集生物特徵個人資料前，應明確告知當事人個人資料保護法第八條第一項各款應告知事項及適當之申訴管道，應讓當事人充分了解所蒐集之目的及相關權利。

學校應取得當事人同意，未成年學生應同時取得其法定代理人同意後，始得蒐集。

當事人不同意提供生物特徵個人資料時，學校應提供替代方案，以**不影響教職員生之權益**為原則。

外部單位調用個資

- **個資法第8條**：(得免告知)
  個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- **刑事訴訟法第228、229、230條** (105/6/22)
  檢察官、司法警察官
  警政署署長、**警察局局長**或警察總隊總隊長、憲兵隊長官
  警察官長、憲兵隊官長、士官
- **調度司法警察條例第2、3條** (69/7/4)
  司法警察官
  市長、縣長
  警察廳長、警保處長、**警察局長**或警察大隊長以上長官、憲兵隊營長以上長官
  警察分局長、憲兵隊連長

外部單位調用個資

- 正式來文(函)
- 長官署名、理由、個人資料範圍
- 是否為合理事項
- 最小化提供
- 至少須經一級主管核准 (執行組)

個資保護、資訊安全

人人有責

將心比心

謝謝聆聽

Q&A