如何將『個人資料保護法』準備到位

NII產業發展協進會　王俊凱協理

All Rights Reserved by NII產業發展協進會

報告人簡介 (王俊凱)

資訊風險管理組協理

1. 現任NII產業發展協進會資訊風險管理組協理
2. TUV NORD漢德技術監督服務(亞太)有限公司 技術協理
3. 安侯(KPMG)企業管理股份有限公司 協理
4. 東森華榮傳播事業股份有限公司 資訊副理
5. 勤業眾信(Deloitte)管理顧問公司 經理

1. 合作金庫、ICBC (中國國際商業銀行) SCSB(上海商業儲蓄銀行)、台灣工業銀行、美國ING 安泰壽險台灣分公司
2. ISO27001 LAC、BS25999 LAC、上海訊息化中心 ISOAC公開班課程講師
3. 數位證據保全特殊專案
4. 行政院研究發展考核委員會政府機關公開金鑰基礎建設所屬憑證機構外部稽核委外服務案

1. 高雄市國稅局、中區國稅局、台灣大哥大、中央健康保險局、台灣固網電信技術中心、台灣電力公司電力調度處ISO27001機制導入專案
2. 行政院主計處稽核團【稽核委員】
3. 金融研訓院、電腦稽核協會、中正大學、大同大學、成大醫學院、恩主公醫院、虎尾諾瑟醫院(講師)
4. Oracle ERP統之軟硬體設備導入及維護

大綱

1. 個人資料保護法施行細則草案
2. 因應的國際標準
3. 學校機關應遵循原則
4. 律師回覆問題分享
5. 問題與討論

All Rights Reserved by NII產業發展協進會

大綱

1. 個人資料保護法施行細則草案
2. 因應的國際標準
3. 學校機關應遵循原則
4. 律師回覆問題分享
5. 問題與討論

All Rights Reserved by NII產業發展協進會

個資法施行細則草案

- 法務部2011年10月27日在官方網站公布個資法施行細則草案。法務部法律事務司副司長鍾瑞蘭表示，草案將進行14天的法案預告，來蒐集各界對草案的建議。

All Rights Reserved by NII產業發展協進會

個人資料檔案(細則預告草案)

- 間接識別
  - 僅以該資料不能識別，須與其他資料對造、組合、連結等，始能辨別該特定個人
  - 但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限
  - 何謂『查詢困難、需耗費過鉅或耗時過久』？

All Rights Reserved by NII產業發展協進會

間接識別案例說明

- Q：何謂以間接方式識別該個人之資料？何謂不能識別？例如學校職員A從校務行政資料庫，將學生資料中之一個欄位「聯絡方式」賣給補教業者B，則是否屬個人資料保護法所規範之可識別個人資料。
- A：(1)就A 而言，雖然A 只挑選學生資料中一個欄位「聯絡方式」，單純就連絡方式之資料內容來看，無法得知該資料之特定個人為何人，但是A 或A 所代表的機關本身，仍有該校務行政資料庫之其他資料欄位可供對照、組合、連結等間接方式，而能識別該特定個人，故就A 或A 所代表的機關該單筆資料欄位仍屬可間接識別之個人資料。A 以意圖營利之方式販賣可識別之個人資料，該當個人資料保護法第41條第2項之刑事構成要件而應負刑事責任。

  (2)就B而言，該「聯絡方式」之個人資料如無法透過資料庫之對照、組合、連結等間接方式而加以識別該特定之學生，則屬查詢有困難之情形（究屬查詢困難、耗費過鉅或耗時過久始能特定之情形需個案認定），故為無法識別之個人資料，無個人資料保護法之適用，惟如屬其他法令規範之範圍，則仍有其他法令之適用，例如民法第18條及第195條之侵害隱私權等規定。

All Rights Reserved by NII產業發展協進會

個人資料檔案(細則預告草案)

- 敏感性資料定義
  - 病歷
    - 醫師依醫師法製作之病歷
    - 各項檢查、檢驗報告資料
    - 其他各類醫事人員執行業務所製作之記錄
    - 基於治療、矯正或預防人體疾病、傷害、殘缺為目的所為之診察、診斷及治療
    - 基於診察、診斷結果，以治療為目的，所為之處方、用藥、施術或處置等行為全部或一部所產生之個人資料
  - 犯罪前科
    - 緩起訴、職權不起訴或經法院判決有罪確定之記錄

All Rights Reserved by NII產業發展協進會

個人資料檔案(細則預告草案)

個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

- 備份資料
- 軌跡資料(Log Files)
  - 蒐集、處理或利用過程中所產生非屬於原搜集個資本體之衍生資料，包括但不限於資料存取人之代號、存取時間、使用設備代號、網路位址(IP)、經過祇網路路徑...等，可用於比對、查證資料存取之適當性
- 學校如何因應維護軌跡資料？資訊監控之必要性?

All Rights Reserved by NII產業發展協進會

專人(細則預告草案)

- 公務機關指定『專人』辦理安全維護措施
  - 指具有管理及維護個人資料檔案之專業能力，且足以擔任機關檔案資料安全維護經常性工作之人員
  - 公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練
  - 公務機關是否均有符合專業能力之經常性人員？包括資訊安全、隱私保護、推論控制之控制措施等課程在內

All Rights Reserved by NII產業發展協進會

刪除

- 本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。
- 前項規定，如為事後查核、比對或證明之需要而留存軌跡資料者，得不予刪除。
- 刪除既指使已儲存之個人資料自個人資料檔案中消失，然如使個人資料自個人資料檔案中全部消失，將不利於電腦系統追查過往作業紀錄，為考量資訊安全與數位鑑識等證明作業之需要，乃增列由系統留存之必要軌跡資料，不在刪除之範圍內，爰規定如第二項。

All Rights Reserved by NII產業發展協進會

內部傳送

- 本法第二條第四款所稱內部傳送，係指公務機關或非公務機關本身內部之資料傳送。
- 第三項新增，明定內部傳送係指公務機關或非公務機關內部之資料傳送，例如公務機關內部各單位間之資料傳送，不包括上級機關傳送個人資料予下級機關，或者法人或團體或自然人之內部資料傳送。又內部傳送，包括機關內部跨國（境）之資料傳送。

All Rights Reserved by NII產業發展協進會

書面意思表示

- 本法第七條所定書面意思表示之方式，如其內容可完整呈現，並可於日後取出供查驗者，經蒐集者及當事人同意，得以電子文件為之。為明確本法書面意思表示之方式，包括無實體存在介面之意思表示方式，乃參考電子簽章法第四條之規定，如其內容可完整呈現，並可於日後取出供查驗者，經蒐集者及當事人同意，得以電子文件為之，爰為本條規定。

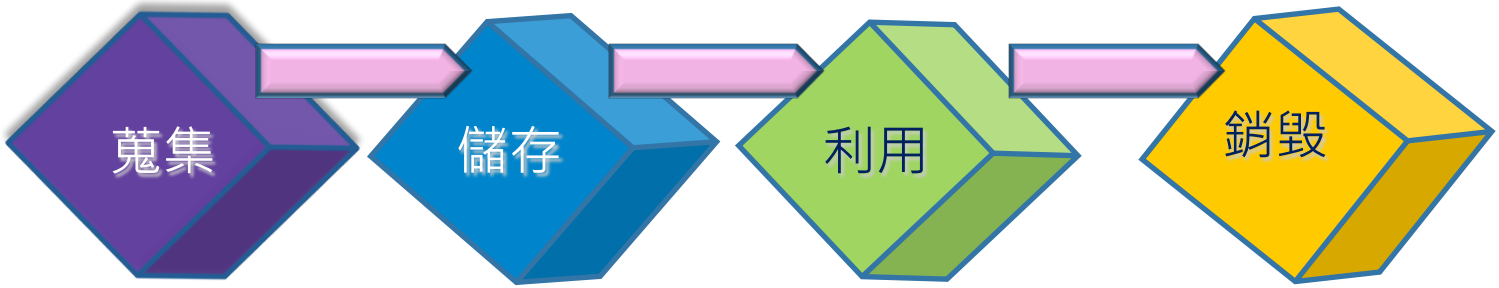
All Rights Reserved by NII產業發展協進會

單獨所為之書面意思表示

- 本法第七條第二項所定單獨所為之書面意思表示，如係與其他意思表示於同一書面為之者，應於適當位置使當事人得以知悉其內容後並確認同意。
- 故明文規範須為單獨所為之書面意思表示，惟該意思表示如與其他意思表示於同一書面為之者，應於適當位置使當事人得以知悉其內容後並確認將其個人資料作與蒐集目的不同之其他目的使用之同意，以避免當事人疏忽而為概括同意，爰為本條規定。

All Rights Reserved by NII產業發展協進會

施行細則預告草案內容



蒐集	儲存	利用	銷毀
依法進行告知義務 取得書面同意	採取適當保護措施，避免個人資料被竊取、竄改或毀損	應於蒐集之特定目的內 使用 特定目的外之使用應另 外取得書面 同意	特定目的消失 期限屆滿 當事人要求

All Rights Reserved by NII產業發展協進會

必要措施包括(細則預告草案)

- 成立管理組織，配置相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓練
- 設備安全管理
- 資料安全稽核機制
- 必要之使用紀錄、軌跡資料及證據之保存

個人資料安全維護之整體持續改善

All Rights Reserved by NII產業發展協進會

必要措施包括(細則預告草案)

- 必要措施，以所須支出之費用與所欲達成之個人資料保護目地符合適當比例者為限
- 國際標準要項明確規定於必要措施內容，學校如何因應？
- 委託機關如何監督受託機關符合必要措施之規定？

All Rights Reserved by NII產業發展協進會

大綱

1. 個人資料保護法施行細則草案
2. 因應的國際標準
3. 學校機關應遵循原則
4. 律師回覆問題分享
5. 問題與討論

All Rights Reserved by NII產業發展協進會

國際間個人資料保護法律比較

比較項目	日本	韓國	德國	英國	台灣
個人資料保護主要法規	個人情報保護法	資通訊網路利用及資訊保護法	聯邦個人資料保護法 聯邦個人資料保護審驗法	個人資料保護法	個人資料保護法 台灣個人資料保護與管理制度（TPIPAS）
法律規範內容	企業負有個人資料保護義務	網站經營者及線上企業負有個人資料保護義務	企業個人資料保護義務及審驗權責機關、審驗客體及程序等	當事人之權利、持有者之義務、除外規定及主管機關監督規定	當事人之權利、持有者之義務、除外規定及主管機關監督規定
標章發放	P-Mark	ePrivacy-Mark	個人資料保護標章	無	無 電子商務業者 「個人資料隱私保護標章（Data Privacy Protection Mark；DP Mark）」
適用範圍	企業個人資料	透過網際網路所蒐集的個人資料	資通訊產品、服務	以自動化設備處理之資料或已建檔之資料	指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合
管理制度/標章發放組織	日本情報處理開發協會 (JIPDEC)	韓國資訊通信協會(KAIT)	個人資料保護審驗機構	英國標準協會(BSI) 設計制度	個人資料保護法-法務部 台灣個人資料保護與管理制度（TPIPAS）」-經濟部商業司
機構維運	初期：政府資金 穩定後：自行維運	依法設立， 享有政府預算	個人資料保護審驗機構自行維運	機構自行維運	依法設立 機構自行維運

部份資料參考來源：經濟部

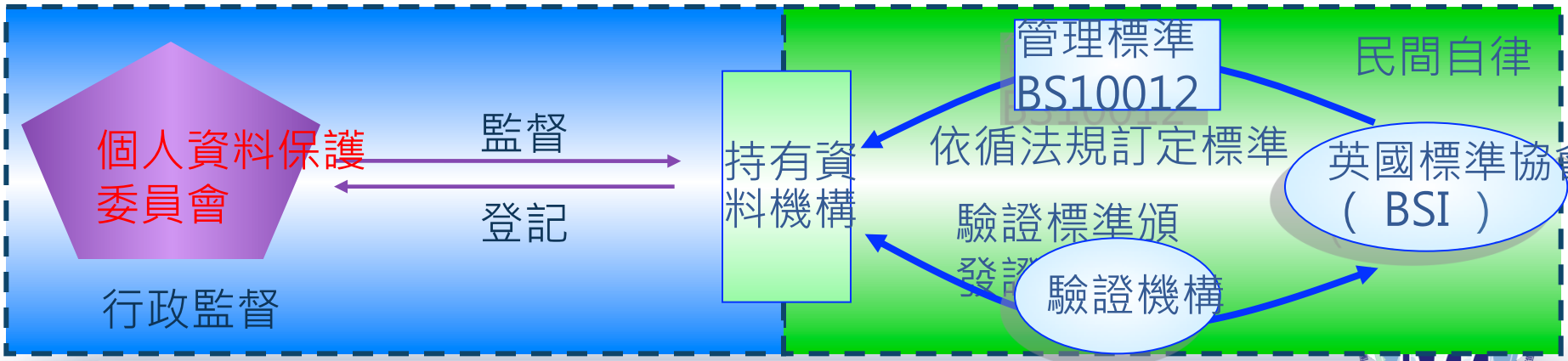
個人資料保護法涵蓋範圍

All Rights Reserved by NII產業發展協進會
20

個人資訊管理標準 BS 10012

- 英國於1998年將歐盟之「個人資料保護指令」與「電子通訊隱私指令」內國法化為「個人資料保護法」（The Data Protection Act 1998）。並由個資保護委員（Information commissioner ）監督法令執行。
- 2001、2007修正擴大個人資料適用範圍，引發適用困擾。
- 英國標準協會（BSI）於2009年5月順應企業需要正式推出一套個人資料管理之標準（BS10012 ），協助企業遵循英國個人資料保護法。

英國個人資料保護法(The Data Protection Act)



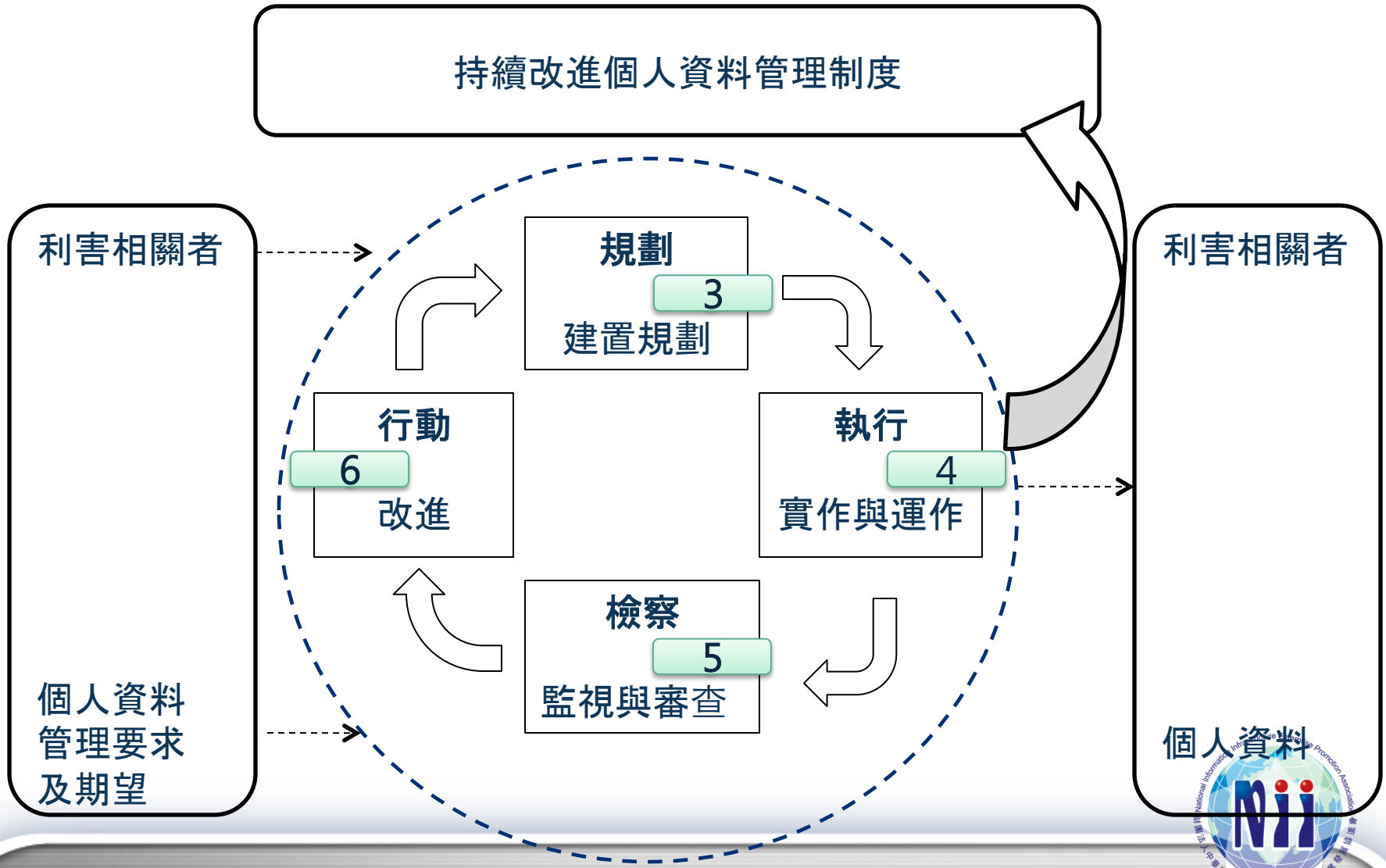
資料參考來源：經濟部

All Rights Reserved by NII產業發展協進會

BS10012要求

All Rights Reserved by NII產業發展協進會

Plan-Do-Check-Act (PDCA) 循環



All Rights Reserved by NII產業發展協進會

英國標準BS 10012(PIMS) V.S 國內個人資料保護法

BS 10012相關管理規範摘要	國內個人資料保護法相關管理規範摘要	
1.善盡告知義務	1.善盡告知義務	11.個資定義不同(未包含種族、政黨等)
2.依特定目的蒐集個資	2.依特定目的蒐集個資	12.提供閱覽或製給複製本
3.公正且合法使用個資	3.公正且合法使用個資	13.規範特種資料不得蒐集
4.保護個人隱私相關項目	4.保護個人隱私相關項目	14.區分公務機關與非公務機關之處理方式
5.確保存取控制之安全	5.確保存取控制之安全	15.具團體訴訟機制
6.確保資料之正確性	6.確保資料之正確性	
7.確保資料傳輸之安全	7.確保資料傳輸之安全	
8.確保個人修改之權利	8.確保個人修改之權利	
9.妥善處理抱怨與申訴	9.妥善處理抱怨與申訴	
10.落實委外安全管理	10.落實委外安全管理	

All Rights Reserved by NII產業發展協進會

BS 10012、ISO 27001與個資法要求

BS 10012 (管理要求)

蒐集 → 處理 → 利用 → 傳輸 → 銷毀

ISO 27001(管理要求及技術支援)

All Rights Reserved by NII產業發展協進會

BS 10012與ISO 27001之關聯

BS 10012 (管理要求)

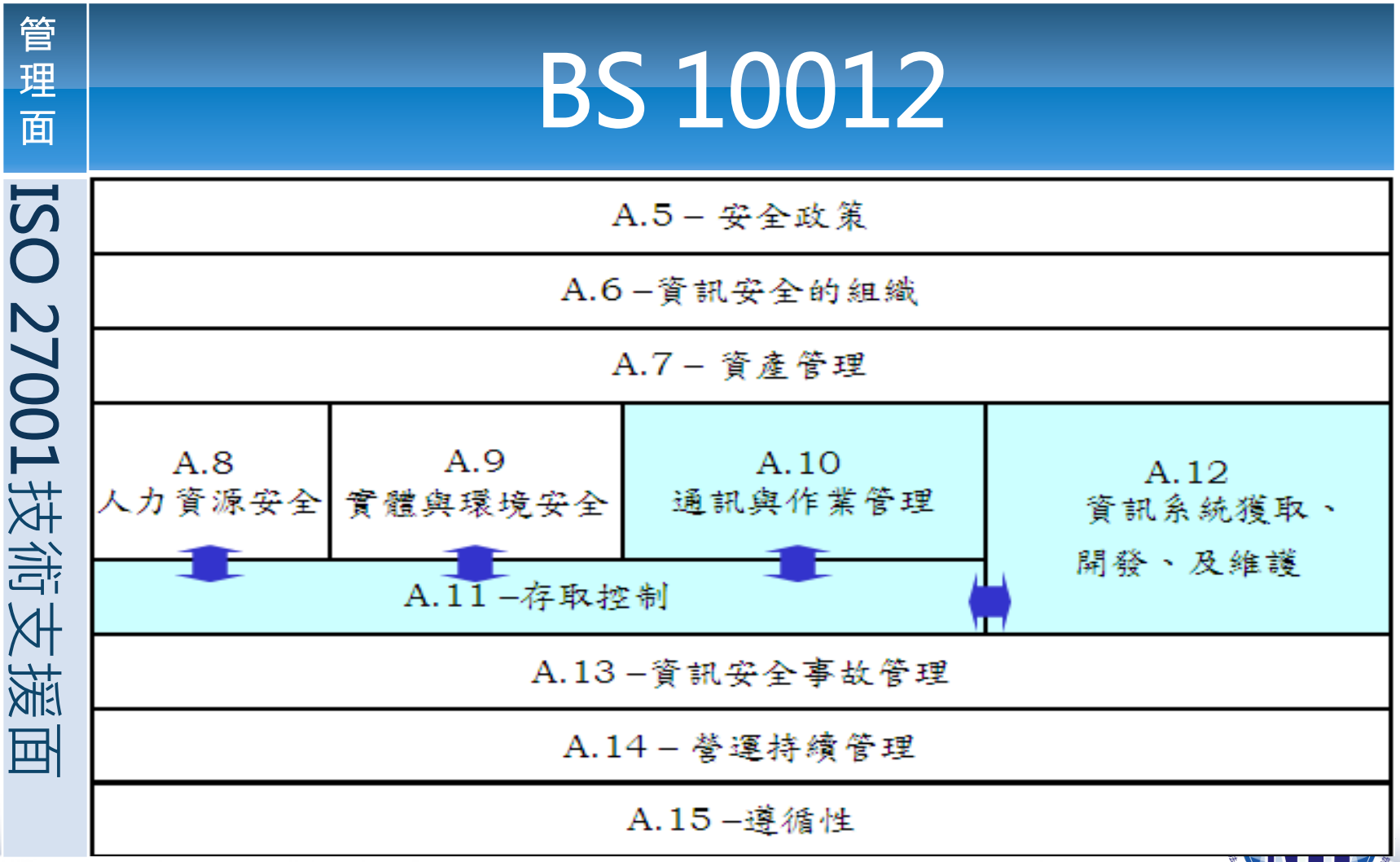
蒐集 → 處理 → 利用 → 傳輸 → 銷毀

BS 10012 (4.13)(安全議題--安全控管、儲存與處理、傳輸、存取控制、安全評估、資安事故管理)

ISO 27001(技術支援)

All Rights Reserved by NII產業發展協進會

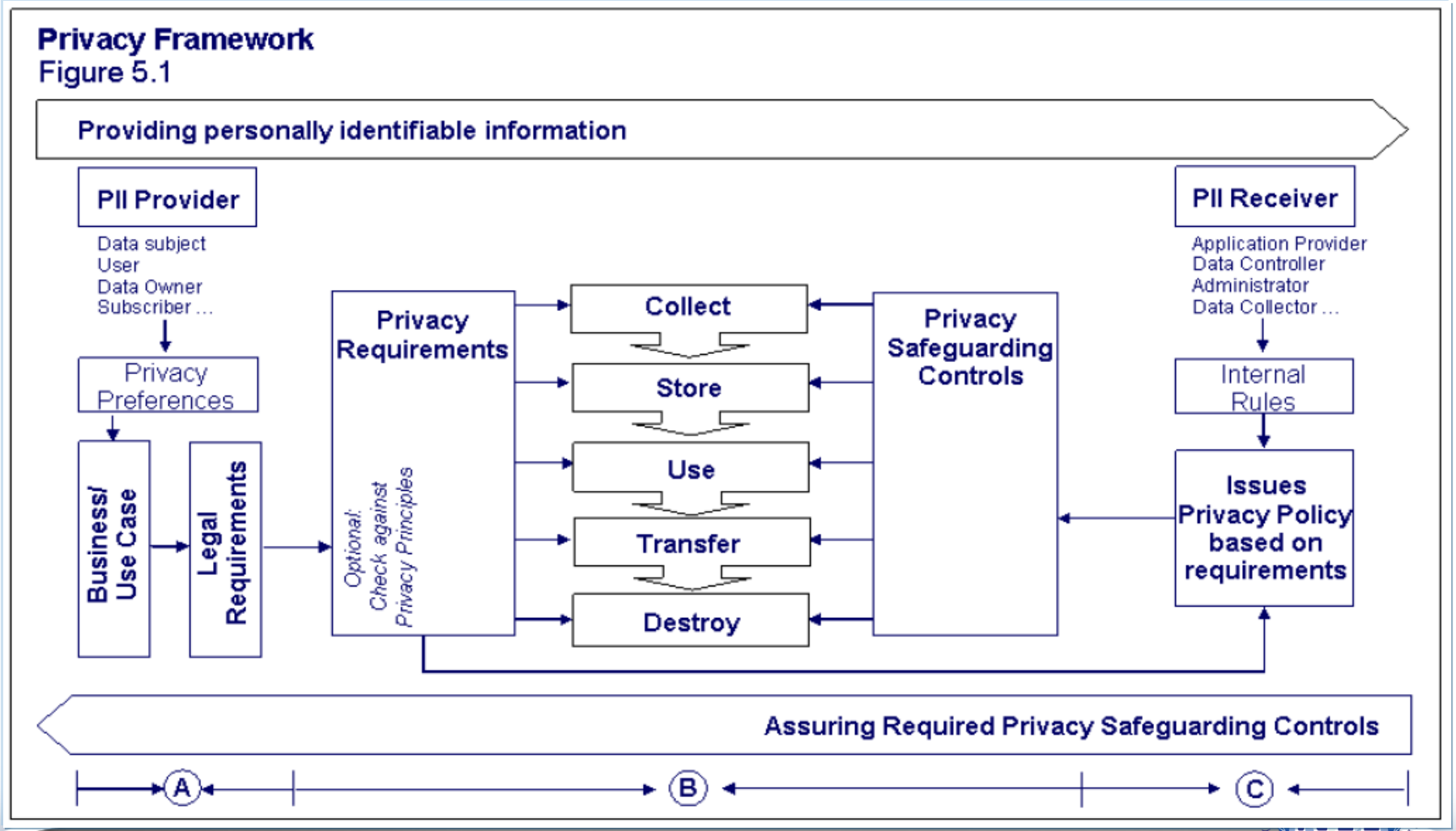
BS 10012與ISO 27001之關聯



All Rights Reserved by NII產業發展協進會

國際標準—ISO29100

- Information technology -- Security techniques -- Privacy framework
- Target publication date: 2011/12/5 ISO 29100 Privacy Framework for Graphical



All Rights Reserved by NII產業發展協進會

提醒

1. 個資法與“PIMS”：不只是建立制度，取得驗證而已，而是如何將機制與個資法作必要的連結（過去ISO27001建制，在台灣只集中於資訊部門）
2. 個資盤點不能只集中於資訊部門，因為個資法客體包含「各種形式含有個資的檔案」（如紙張等），而且必須全面。
3. 盤點個資時應涵蓋其生命週期（蒐集、處理、利用、傳輸、儲存、銷毀），階段合法性必須回到蒐集時的特定目的或法律的基礎。「蒐集合法」，不保證其他階段合法，否則將造成疏忽而觸法。

大綱

1. 個人資料保護法施行細則草案
2. 因應的國際標準
3. **學校機關應遵循原則**
4. 律師回覆問題分享
5. 問題與討論

All Rights Reserved by NII產業發展協進會

學校機關個人資料的基本應用原則

- 學校機關應遵循以下個人資料保護原則
  - 限制蒐集原則
  - 資料內容原則
  - 目的明確化原則
  - 限制使用原則
  - 安全保護原則
  - 公開原則
  - 個人參與原則
  - 責任義務原則

All Rights Reserved by NII產業發展協進會

個人資料保護持續改善管理流程(1/2)

- 規劃(P)
  - 建立個人資料保護管理政策
  - 建立與維護個人資料檔案清冊並於網站上公布檔案大綱
  - 個人資料檔案應指定管理者
  - 確認個人資料之蒐集與利用符合法令規定
- 執行(D)
  - 機關學校應依「教育體系資通安全管理規範」或「國中、小學資通安全管理系統實施原則」以及本工作事項之安全原則及參考注意事項實施個人資料相關資訊安全控管措施

All Rights Reserved by NII產業發展協進會

個人資料保護持續改善管理流程(2/2)

- 檢查(C)
  - 機關學校應定期執行稽核作業，以確保相關管理措施之有效性
- 改善行動(A)
  - 機關學校應訂定個人資料資訊安全事件處理程序
  - 針對資訊安全事件及稽核缺失應訂定改善行動或預防措施，以減低事件再次發生機會

All Rights Reserved by NII產業發展協進會

個人資料保護及安全原則(1/4)

一. 機關學校應指定**單位副首長**為**機關召集人**，統籌決策與執行單位內資訊安全與個資隱私業務之資源整合運用。

二. 機關學校應指定**專人**依相關法令辦理安全維護及保管事項，作為**機關內部之個人資料管理代表**。機關組織編制較小者，則統一由該機關「**個資保護聯絡窗口**」兼辦專責人員業務。

三. 機關學校應設置並指定「**個資保護聯絡窗口**」，作為機關學校間個資業務協調聯繫之對口、機關學校本身個資安全事件通報之對口，以及重大個資外洩事件之民眾聯繫單一窗口。另單位應將「個資保護聯絡窗口」之聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟。

All Rights Reserved by NII產業發展協進會

個人資料保護及安全原則(2/4)

四. 個人資料檔案應定期備份，並防止個人資料被竊取、竄改、毀損、滅失或洩露。個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，宜釐定使用範圍及調閱或存取權限。個人資料檔案之處理行為應設置使用者代碼及通行碼，不得與他人共用並定期更新。另視需要考量採取權限區隔、資料加密機制，或相關核准程序加以控管，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。

五. 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身份之登入通行碼，並視業務及資料重要性，考量其他輔助安全措施。個人資料檔案使用完畢後，應即退出應用程式，不得留置於電腦終端機。

All Rights Reserved by NII產業發展協進會

個人資料保護及安全原則(2/4)

六. 含有個人資料之紙本報表的申請、讀取、列印、使用、存檔、轉交及銷毀等處理及利用行為，宜建立相關之授權、監督及行為記錄機制。

七. 內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向備查。

八. 對於個人資料之調閱宜經申請並核准，並加以記錄其調閱身分及行為。調閱紀錄可視機關實際需求存檔，以利後續人員查詢及追蹤。

All Rights Reserved by NII產業發展協進會

個人資料保護及安全原則(3/4)

九. 以電腦處理個人資料時，需核對個人資料之輸入、輸出、編輯或更正是否與原件相符。個人資料提供利用時，對資料相符與否如有疑義，應調閱原檔案查核。

十. 機關學校單位管理之網站或網頁內容，於確有必要公布個人資料時，需經所屬單位主管核准，且依相關法律及規範處理，始得公布。

十一.學校應於法律允許之範圍內提供資料當事人下列權利：

1. 查詢或請求閱覽。
2. 請求製給複製本。
3. 請求補充或更正。
4. 請求停止蒐集、處理或利用。
5. 請求刪除。

All Rights Reserved by NII產業發展協進會

教育機構個人資料保護檢核表

教育部 100 年度提升校園資訊安全服務計畫

教育機構個人資料保護檢核表

查檢單位：＿＿＿＿＿＿＿＿＿＿＿＿　　填表日期：＿＿年＿＿月＿＿日

查核項目（紅色為進階選項）	自我評審			稽核評量結果			
				完整性			
	是	否	不適用	非常	尚屬	不盡	不適用
1 個人資料保護持續改善管理流程							
1.1 是否建立個人資料保護管理政策？	☐	☐	☐	☐	☐	☐	☐
1.2 是否建立「個人資料檔案清冊」，並依個資法要求於網站公布個人資料檔案大綱？	☐	☐	☐	☐	☐	☐	☐
1.3 個人資料檔案是否指定管理者？	☐	☐	☐	☐	☐	☐	☐
1.4 管理者是否評估資料處理流程上的風險，設定資料保護要求？	☐	☐	☐	☐	☐	☐	☐
1.5 是否確認個人資料之蒐集與利用符合法令規定？包含： ● 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。 ● 蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。 ● 除符合法令規定外，有關醫療、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。	☐	☐	☐	☐	☐	☐	☐

All Rights Reserved by NII產業發展協進會

1.個人資料保護持續改善管理流程(1/2)(進階選項)

1.1 是否建立個人資料保護管理政策？

1.2 是否建立「個人資料檔案清冊」，並依個資法要求於網站公布個人資料檔案大綱？

1.3 個人資料檔案是否指定管理者？

1.4 管理者是否評估資料處理流程上的風險，設定資料保護要求？

1.5 是否確認個人資料之蒐集與利用符合法令規定？包含：

- 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。
- 蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。
- 除符合法令規定外，有關醫療、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。
- 當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。

All Rights Reserved by NII產業發展協進會

1.個人資料保護持續改善管理流程(2/2)(進階選項)

1.6 是否依下列相關規定執行個人資料保護作業

- 教育體系資通安全管理規範
- 國中、小學資通安全管理系統實施原則

1.7 是否定期執行稽核作業，以確保相關個人資料保護管理措施之有效性？

1.8 是否訂定個人資料資訊安全事件處理程序？

1.9 針對資訊安全事件及稽核缺失是否訂定改善行動或預防措施，以減低事件再次發生機會？

All Rights Reserved by NII產業發展協進會

2.個人資料保護與安全(1/3)

2.1 是否指定機關副首長為個資隱私業務之機關召集人？

2.2 是否指定專人依法令規定辦理安全維護及保管事項？

2.3 是否設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式（如：電話、email）置於單位網站，以便利民眾提出申訴與救濟？

2.4 個人資料之處理行為是否經權責單位核准，釐定使用範圍及調閱、存取權限？

2.5 個人資料之處理行為是否留存使用者身分與其行為紀錄以供事後稽查？

2.6 含有個人資料之紙本報表，其處理及利用行為是否有適當之授權、監督，及記錄列印、轉交等行為？

2.7 交換紙本個人資料時，是否採取彌封或其他具備保密機制之傳遞方式？

2.8 交換個人資料時，是否記錄轉交或傳輸行為之流向？

2.9 對於個人資料之調閱，是否有申請及核准程序？

All Rights Reserved by NII產業發展協進會

2.個人資料保護與安全(2/3)

2.10 對於個人資料之調閱，是否記錄並保存調閱者身分及行為？
2.11 若需於單位管理之網站或網頁公布個人資料時，是否經所屬單位主管核准，並依相關法律及規範處理？
2.12 是否於法律允許之範圍內提供資料當事人下列權益：
- 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

2.13 處理個人資料檔案之個人電腦，是否設置使用者代碼及通行碼？
2.14 通行碼是否至少每六個月更換一次，長度應至少8碼，且包含文數字？
2.15 是否未與他人共用電腦系統帳號？
2.16 處理個人資料是否採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限？
2.17 個人資料檔案是否以安全的方式保護，例如：加密？

All Rights Reserved by NII產業發展協進會

2.個人資料保護與安全(3/3)

2.18 是否至少每月備份電腦內個人資料檔案？

2.19 個人資料檔案使用完畢後，是否立即退出應用程式？

2.20 電腦是否使用螢幕保護程式並設定密碼，並將螢幕保護啟動時間設定為15分鐘以內？

2.21 交換個人資料檔案時，是否對資料檔案加密，或是透過加密通道傳送？

2.22 是否禁止開啟網路芳鄰分享目錄與檔案？

2.23 是否停用作業系統Guest帳號？

2.24是否將存放敏感性個人檔案資料的電腦與外部網路隔絕（如：防火牆）？

2.25 存放個人資料之資訊設備是否安裝防毒軟體，並至少每日更新病毒碼，且每週執行排程掃瞄？

2.26 存放個人資料之資訊設備是否定期檢視、更新作業系統及應用程式漏洞？

All Rights Reserved by NII產業發展協進會

3.設備管理

3.1 是否指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息？

3.2 儲存個人資料之資訊設備是否置放於實體安全區域（如：門禁控管之辦公區域、機房）？

3.3 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，是否指定專人管理，並置於實體保護之環境？

3.4 儲存個人資料檔案之儲存媒體，是否建立備援機制？

3.5 儲存個人資料檔案之媒體是否有攜出、拷貝或複製的管控機制，並留存紀錄？

3.6 外部團體或個人更新或維修儲存個人資料檔案之電腦設備時，是否指派專人在場確保資料安全？

3.7 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其所儲存之個人資料檔案？

All Rights Reserved by NII產業發展協進會

4.人員管理

4.1 機關學校是否對處理個人資料檔案之人員施予資訊安全與個資隱私保護之教育訓練，並定期於單位內宣導個資隱私保護之重要性？

4.2 處理個人資料檔案之人員職務異動時，是否依規定列冊移交相關儲存媒體及資料？

4.3 處理個人資料檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？

4.4 處理個人資料檔案之人員，是否簽訂保密切結書？

4.5 處理個人資料檔案之人員離職或合約終止時，是否依規定取消或停用其使用者識別帳號並收繳通行證件？

4.6 是否禁止使用MSN或其他即時通訊軟體傳輸個人資料檔案？

4.7 是否禁止使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案？

4.8 是否禁止使用點對點(P2P)軟體及Tunnel相關工具下載或提供分享檔案？

4.9 是否禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料？

All Rights Reserved by NII產業發展協進會

5.系統開發及委外管理

5.1 處理個人資料檔案之資訊系統，是否在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入系統開發考量（如：邏輯測試）？

5.2 處理個人資料檔案的資訊系統之維護、更新、上線、及版本異動等作業，是否有安全管控措施？

5.3 維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作時，是否透過加密通道進行（如：HTTPS、SSH等）？

5.4 自行開發或委外處理個人資料檔案之資訊系統，是否將個人資料(包含測試用個人資料)施予妥善之保護與控管？

5.5 委外建檔的個人資料檔案，是否於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則？

All Rights Reserved by NII產業發展協進會

大綱

1. 個人資料保護法施行細則草案
2. 因應的國際標準
3. 學校機關應遵循原則
4. 律師回覆問題分享
5. 問題與討論

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 若當事人尚未成年，請問個人資料蒐集要取得當事人或監護人同意呢？

A. 民法規定，滿20歲為成年。未成年人包括：

(1) 未滿7歲者，為無行為能力人：應由法定代理人代為意思表示，並代受意思表示。
(2) 滿7歲以上者，為限制行為能力人：其為意思表示及受意思表示，原則上應得法定代理人之允許。

書面同意係以書面方式為意思表示。依據上述民法規定，未成年人為書面同意，確實應由法定代理人代為書面同意，或得到法定代理人之允許。
雖有上述限制，但民法規定，已經結婚之未成年人，有行為能力。換言之，已經結婚之未成年人，可以自行為書面同意，並無法定代理人代為書面同意或允許之問題。

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 學務處提供家長可以查詢學生的考試成績或學習紀錄，使用的方式是以「學生的身分證字號」登入為查詢依據，請問學務處可以提供家長查詢嗎？若可以，可以提供到什麼程度？另外針對已成年的學生或未成年的學生是否有不一樣的處理方式。

  A. 應區分成年和未成年，成年學生的家長應無法查詢，除非有學生授權。未成年的家長是學生的法定代理人，應該都能看才對。

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 某大學為獎勵學生畢業，將學生部分資料公開於網頁上，經學生提告後，將網頁資料撤銷，但在Google仍搜尋得到，請問是否可以要求學校向Goolge交涉，或需由學生自行要求Google撤銷其資料？

  A. 網頁由學校建立，學校應盡早自己去找 Google交涉，否則有可能仍然有責。

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 個資法中之特種個人資料規範中，若個資擁有者自行公開之個人資料，是可以收集的，但是請問這樣的資訊可以拿來傳播嗎？

  A. 雖然已經公開的特種個資是可以蒐集的，但蒐集以及利用時還是要依照個資法規定的範圍，也就是必須要有特定目的，並不是任意可以拿來傳播的。

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 學校可以為了保護學生，收集學生病史、健康、身分（低收入戶）資料等涉及特種個資嗎？

  A. 有關病史、健康檢查的部分，要看教育部的法規有沒有允許。低收入戶並非特種個資。

- Q. 在公告欄上公告曠課學生名單（學生姓名、學號）有違反個資嗎

  A. 有關獎懲之作法，應符合學校辦理教育行政之目的，公布應不違反個資。

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 學校是否可寄發認同卡相關資料給校友?

  A. 學校當初蒐集校友個人資料之特定目的為教育或訓練行政，或學生資料管理。學校寄發認同卡相關資料給校友，構成利用校友個人資料之行為，似已逾越上述特定目的，除非取得校友之書面同意，否則不得為之。

- Q. 導師是否可以知道班上同學的學習狀況，導師可以知道同學修課成績嗎?

  A. 如果導師取得學生的修課成績，是為了瞭解學生的學習狀況，應認係為執行法定職務必要範圍（公立學校）或因學校與學生間之契約關係（私立學校），為了特定目的（教育或訓練行政）所為，符合個資法的規定。

All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 學生成績預警制度，若有扣8分或扣16分的情形，是否可以寄給家長知道?

  A. 學校將學生預警制度的扣分情形告知家長，似為學校執行法定職務必要範圍，且與蒐集之特定目的（教育或訓練行政）相符。惟大學生收受成績預警制度之資料，依其年齡及身分，應為其日常生活所必需，且滿20歲之大學生已為成年人，不論其為意思表示或受意思表示，均無須法定代理人（家長）之允許，因此大專院校是否有必要將告知學生本人之成績預警資料，另行提供學生家長，始能達到教育或訓練行政之目的，恐有疑義，建議教育部對此作成統一解釋，以便學校知所遵循，避免學生質疑。

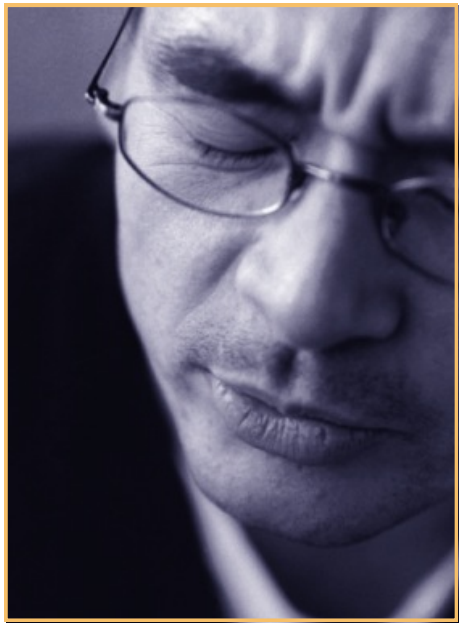
All Rights Reserved by NII產業發展協進會

學校常見個人資料保護議題

- Q. 網頁上的學生家長區，家長可以查詢學生的個人缺曠、操行嗎?

  A. 如上題所述，學校將學生的缺曠課資料及操行成績提供家長查詢，似為學校執行法定職務必要範圍，且與蒐集之特定目的（教育或訓練行政）相符。惟大學生瞭解自己的缺曠課資料及操行成績，依其年齡及身分，應為其日常生活所必需，且滿20歲之大學生已為成年人，不論其為意思表示或受意思表示，均無須法定代理人（家長）之允許，因此大專院校是否有必要將學生的缺曠課資料及操行成績提供家長查詢，始能達到教育或訓練行政之目的，恐有疑義，建議教育部對此作成統一解釋，以便學校知所遵循，避免學生質疑。

All Rights Reserved by NII產業發展協進會



Q&A

All Rights Reserved by NII產業發展協進會

Thank You !

NII產業發展協進會

All Rights Reserved by NII產業發展協進會