談個資法修法對教育體系的影響與行政檢查

徐國鈞

國立台北商業大學
資訊與網中心主任

大綱

1. 個資法修法對教育體系的影響
2. 教育部對教育體系個資行政檢查的規劃
3. 結語

大綱

1. 個資法修法對教育體系的影響
2. 教育部對教育體系個資行政檢查的規劃
3. 結語

防止非公務機關個資外洩精進措施

112 年03 月02 日行政院第3845次會議

◆強化業者防護能力、完備法制、落實執法，提升個資保護

策略一：強化聯繫會議功能(1/3)

事前

事中

事後

強化執法能量，提升防護能力

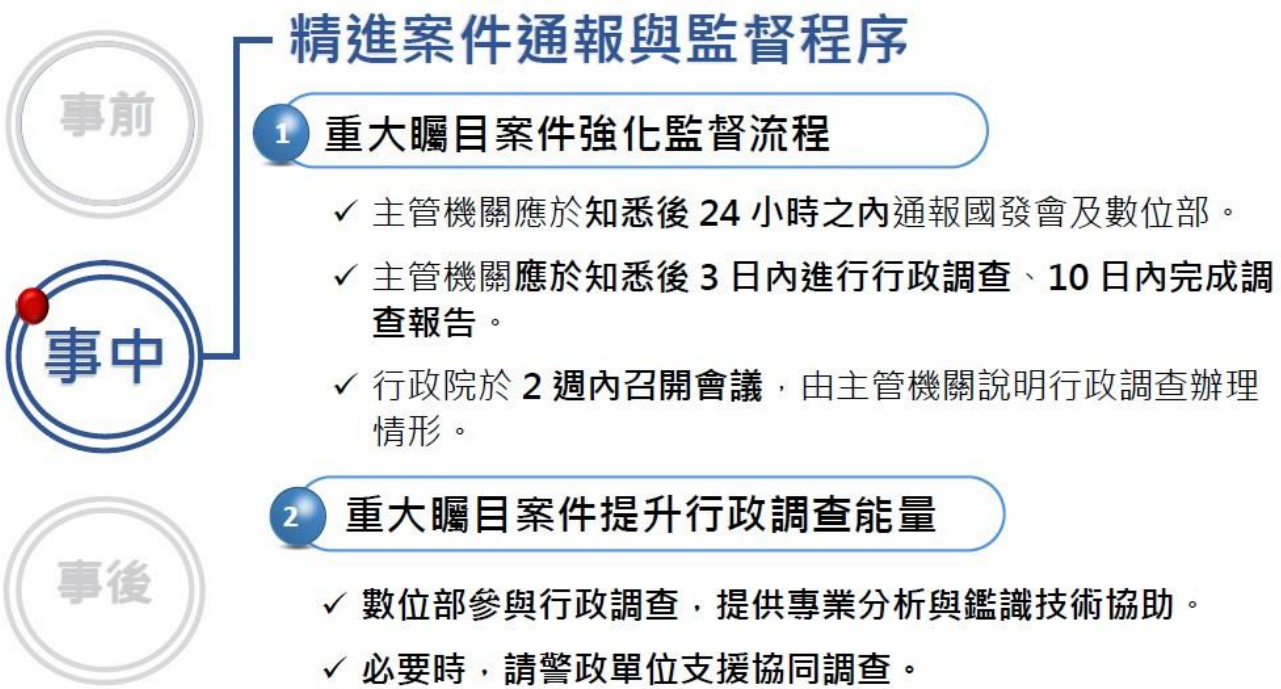
1 行政機關強化執法能量

- ✓ 各主管機關應成立**常設之「個資行政檢查小組」**，並由**數位部**適時行政協助。
- ✓ 各主管機關**每年擬定行政檢查計畫，並對高風險業者，強化例行性行政檢查。**

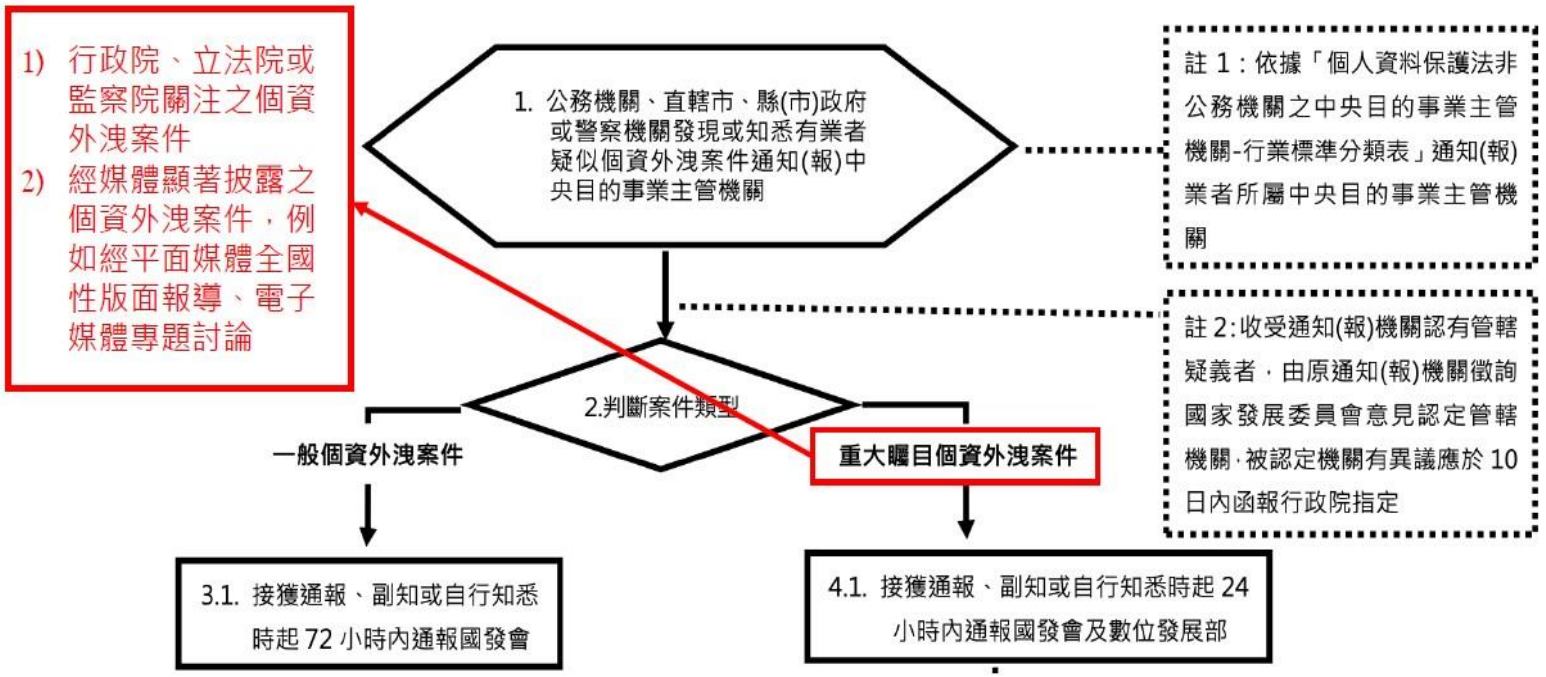
2 業者提升個資防護能力

- ✓ **數位部協助各主管機關建立適當分級規範及技術規格。**
- ✓ **各主管機關**輔導所轄業者提升個資保護意識及防護措施，分階段輔導業者取得個資保護管理或資訊安全驗證。
- ✓ **金管會**強化對上市櫃公司內稽內控要求，促請業者取得適當之個資保護管理或資訊安全驗證。

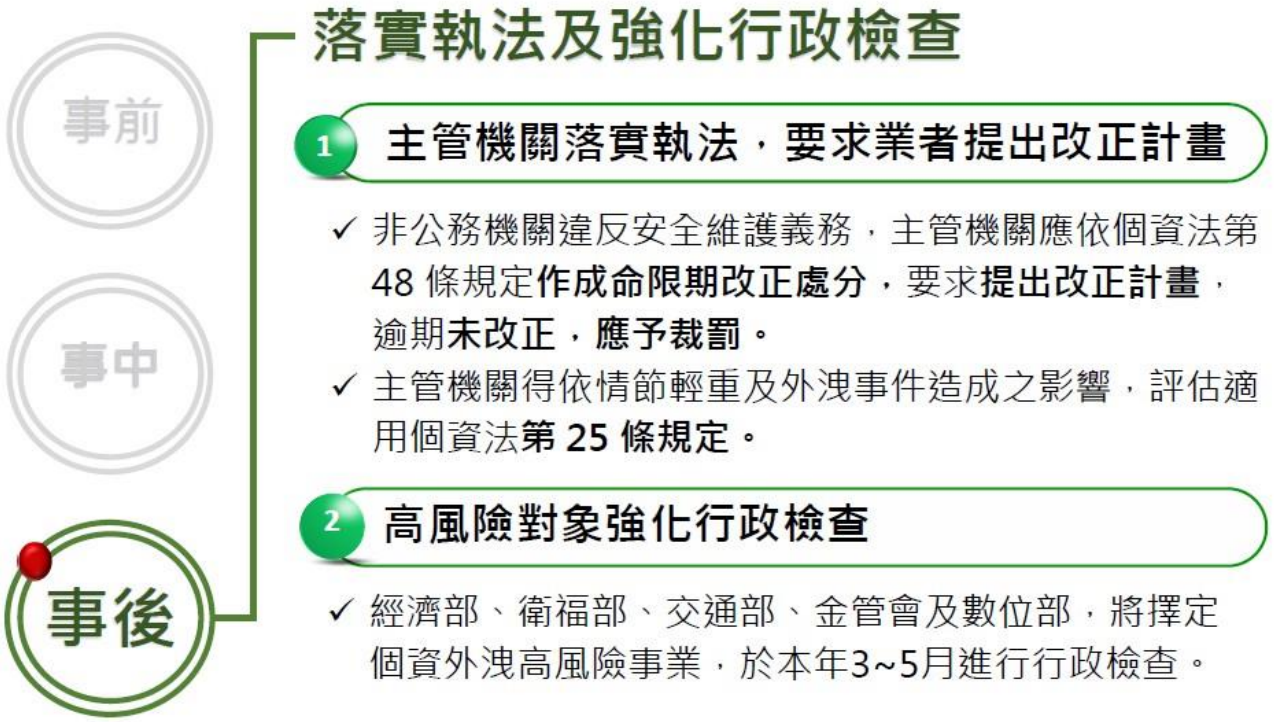
策略一：強化聯繫會議功能(2/3)



行政院及所屬各機關落實個人資料保護聯繫作業要點(112.05.29)



策略一：強化聯繫會議功能(3/3)



策略二：提高個資法相關罰則

- 研議提高個人資料保護法相關罰則，並同步檢視其他相關法規罰則之合理性。

現況問題

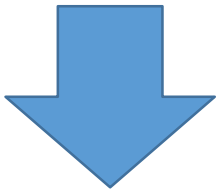
- 非公務機關未採行適當安全措施防止個資外洩，應依個資法第48條，先命限期改正，屆期未改正，按次處罰新臺幣2萬元以上20萬元以下罰鍰。
  - ✓ 最高罰鍰金額上限僅為20萬
  - ✓ 須先命改正，未為改正方能處罰

後續推動

- 研議修正個資法第48條，參考相關國際立法例提高罰則。
- 各部會盤點所主管個資保護相關法規，並評估罰則之合理性。

修法重點(1)

- 個資法第四十八條，非公務機關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之裁罰方式及額度。



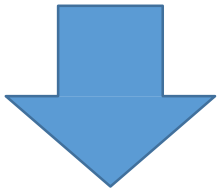
- 逕行處罰同時命改正，提高罰鍰上限，新臺幣2萬元以上200萬元以下。
- 情節重大者，新臺幣15萬元以上1500萬元以下。
- 屆期未改正者，按次處新臺幣15萬元以上1500萬元以下。

個資保護法修正案

- 112年5月16日 立法院三讀通過個資法修正案。
- 促使非公務機關投入人力、技術及成本，落實保護民眾個人 資料之責任，並有助於政府打擊詐欺相關政策推動。
- 另針對公務機關個資保護之強化，除落實現行資通安全管理法對於公務機關的管理規範外，未來個人資料保護委員會將以獨立專責機關的定位，整體規劃對於公務機關及非公務機 關個資保護之監督機制。

修法重點(2)

- 由「個人資料保護委員會」擔任個資法主管機關。
- 現行個資法並未設置單一專責機關。
- 落實憲法法庭判決，有關建立個資保護獨立監督機制之要求。

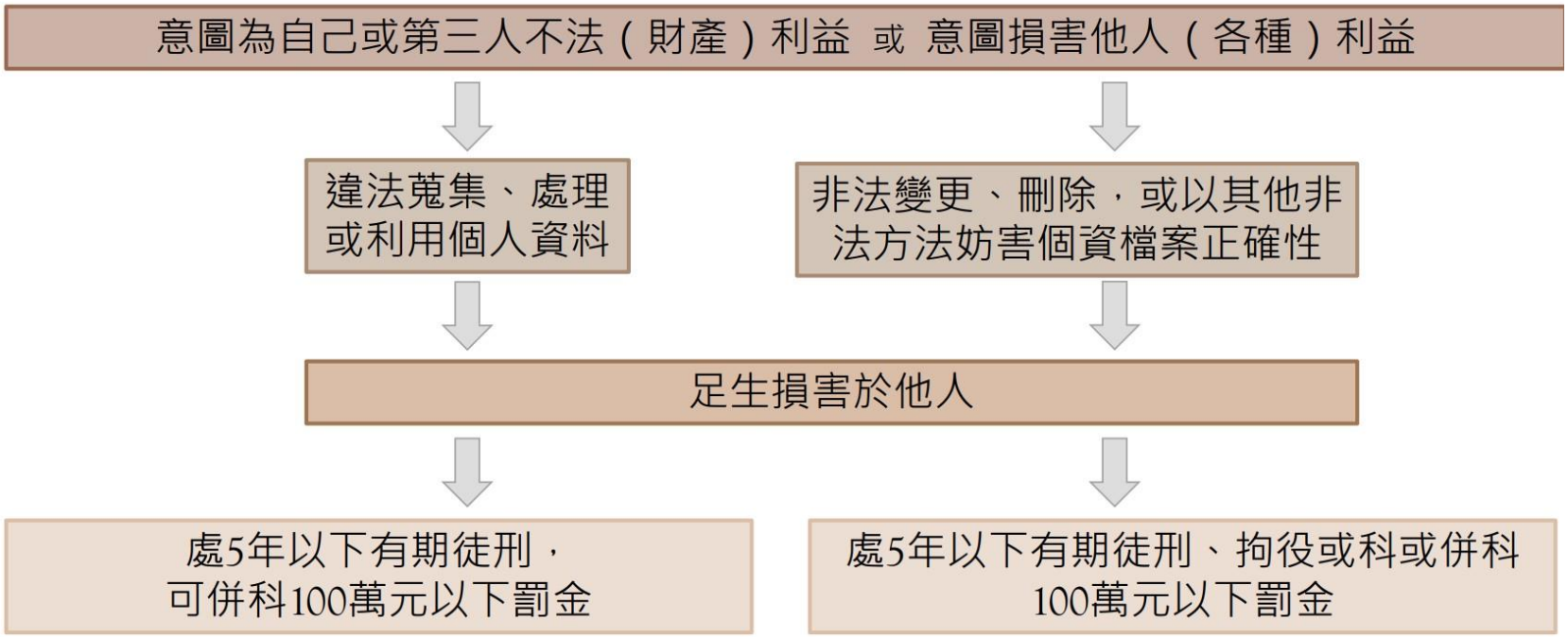


整合目前分屬於中央目的事業主管機關、地方政府及國發會的權責

修法前後比較

條文	修法前	修法後
增訂第1條之1規定	中央目的事業主管機關及地方　政府分散管理，並由國家發展　委員會擔任個資法解釋機關	將由個資委員會擔任個資法的主管機關，整合目前分屬的權責
增修第48　條第2項及 第3項規定	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 料處理方法者，中央目的事業 主管機關或地方政府須先限期 命其改正，屆期未改正者，方 得按次處新臺幣2萬元至20萬元 罰鍰	✓ 直接裁處新臺幣2萬元至200萬元 罰鍰，毋須先限期命其改正； ✓ 情節重大者，罰鍰則可提高至新臺幣15萬元至1,500萬元； ✓ 屆期未改正者，按次處新臺幣15 萬元以上1,500萬元以下罰鍰

違反個資法－刑事責任


意圖為自己或第三人不法（財產）利益 或 意圖損害他人（各種）利益
違法蒐集、處理或利用個人資料
非法變更、刪除，或以其他非法方法妨害個資檔案正確性
足生損害於他人
處5年以下有期徒刑，可併科100萬元以下罰金
處5年以下有期徒刑、拘役或科或併科100萬元以下罰金

違反個資法－民事責任

要件

- 違反個資法規定，致個資遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。
- **除非能證明無故意或過失**。

種類

- 財產損害
- 精神損害
- 回覆名譽

範圍

- 不容易或不能證明實際損害額時，可請求法院依照侵害情節，以每人每一事件500元以上2萬元以下計算。
- 同一事件＋多數受害人，賠償上限2億元

違反個資法－行政責任

2萬-20萬

- 先改再罰
- 蒐集個資沒有告知法定資訊
- 不讓當事人行使權利
- 違法行銷

5萬-50萬

- 先罰再改
- 違法蒐集、處理、利用個人資料
- 違法國際傳輸個人資料

2萬-1500萬

- 先罰再改
- 沒有做到適當安全維護
- 沒有訂定安全維護計畫
- 2萬 - 200萬
- 情節重大：15萬 -

代表人一起罰

- 企業受罰時
- 代表人、管理人、有代表權人
- 受同額罰鍰處罰
- **除非能證明盡到防止義務**

策略三：設立個資保護獨立監督機關

● 推動獨立監督機關必要性

1. 憲法判決：建立統籌性個資保護獨立監督機制 (以114年8月為期限)
2. 落實國家人權行動計畫：設置獨立隱私專責機關 (以113年5月為期限)
3. 國內實務監管課題解決、國際趨勢接軌急迫需求
4. 朝野立委、監察院與各界倡議期盼

● 國際以設置獨立監督機關為趨勢

1. 各國普遍設置獨立監督機關
   - ✓ 至少70個國家設置個資保護獨立監督機關
2. 隱私相關國際組織需獨立機關方能入會
   - ✓ 如：全球隱私大會(GPA)入會會員須為具獨立性之個資保護機關
3. 獨立機關為取得GDPR適足性認定條件
   - ✓ 日、韓皆已成立獨立機關並取得適足性認定

大綱

1. 個資法修法對教育體系的影響
2. **教育部對教育體系個資行政檢查的規劃**
3. 結語

個資行政檢查緣由

- **依據：行政院112年2月8日「個資外洩及資安事件處理機制討論會議」，**
- **指示：請各目的事業主管機關應就其業管非公務機關研提年度行政檢查計畫。**

[註] 教育部各事業別個人資料檔案安全維護計畫及處理辦法：
1.私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法
2.私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法
3.私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法
4.短期補習班個人資料檔案安全維護計畫實施辦法
5.運動彩券業個人資料檔案安全維護計畫實施辦法
6.海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法(113年度開始查核)

檢查對象(1/3)

- 私立大專校院事業分組：(由高教司及技職司主辦)
  1. 私立大專校院**(依私立學校法核准設立之私立專科以上學校)**
  2. **依學術研究機構設立辦法核准設立之私立學術研究機構**。
- 私立高中以下學校及學前事業分組：(由國教署主辦)
  1. 私立高中以下學校及學前教育
  2. 國教署轄管之其他非公務機關或事業。

檢查對象(2/3)

- 海外學校事業分組：(由國際司主辦)
  1. 海外學校
  2. 國際司轄管之其他非公務機關或事業。

- 終身學習事業分組：(由終身司主辦)
  1. **短期**補習
  2. 課後照顧**中心**

檢查對象(3/3)

- 體育事業分組：(由體育署主辦)
  - 體育署轄管之其他非公務機關或事業。

教育部主管「各事業別」相關辦法

單位	受查核對象	對應之安維辦法
高等教育司及技職司	私立專科以上學校	私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法
國民及學前教育署	私立高級中學、 私立國民中學、 私立國民小學、 私立幼兒園	私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法
終身司	私立兒童課後照顧服務中心	私立兒童課後照顧服務中心個人資料檔案安全維護計畫實施辦法
終身司	短期補習班	短期補習班個人資料檔案安全維護計畫實施辦法
國際司	海外臺校	海外臺灣學校及大陸地區臺商學校個人資料檔案安全維護計畫實施辦法
體育署	彩券	運動彩券業個人資料檔案安全維護計畫實施辦法

個人資料檔案安全維護計畫

- 指定或設管理單位或指定專人，負責個人資料檔案安全維護

安全維護事項有哪些可做

個資管理PIMS	
組織資源配置	界定個資範圍
風險評估機制	通報應變機制
內部管理程序	資安人員管理
認知教育訓練	設備安全管理
安全稽核機制	資料紀錄保存
計畫持續改善	

資安管理ISMS	
資安管理政策	資訊資產管理
風險評鑑管理	實體安全管理
通信作業管理	存取控制管理
系統開發管理	委外業務管理
資安事件管理	業務持續管理
內部稽核管理	矯正改善管理
人員安全與教育訓練	

委外監督的法律要求

個資法委外監督
個資範圍、類別、目的、期間
受託者應採行的適當安全維護
複委託之受託者約定
受託者違法應通知事項及補救
委託者保留指示之事項
結束後個資之返還與刪除
定期確認執行狀況+記錄結果

資安管理法委外監督
完善資安管理措施或第三方驗證
配置專業人員
複委託與否、範圍、安全措施
涉及國安的適任性查核、管制出境
安全性檢測證明、授權證明
違法應通知及補救
結束後資料返還與刪除
其他資通安全相關措施
定期或知悉事件時執行稽核或確認

委外監督的要項

事前—明確約定

- 委託目的、類別、範圍、期間
- 權利&義務
- 安全措施
- 補救&通知事項
- 退場機制

事中—執行監督

- 低強度
  —廠商自評
- 中強度
  —機關提出項目，廠商提出符合性
- 高強度
  —機關執行稽核

事後—退場機制

- 資料返還
- 資料銷毀
- 資料遷移？
- 你被廠商「鎖定」了嗎？

113年查核目標

項次	業管單位	事業別	查核母數	預定查核
1	高等教育司	私立專科以上學校	106	20~25
2	技術及職業教育司	私立專科以上學校		
3	國民及學前教育署	私立高級中學	93	19
4	國民及學前教育署	私立高級中學 (直轄市、縣市政府主管)	117	10
5	國民及學前教育署	私立國民中學	12	2~3
6	國民及學前教育署	私立國民小學	31	6~7
7	國民及學前教育署	私立幼兒園	4500	7
8	體育署	體育團體、運動團體		4
9	終身教育司	私立兒童課後照顧服務中心	72	5
10	終身教育司	短期補習班	17411	30

檢核項目說明(1/2)

- (一)個人資料檔案安全維護計畫
- (二)組織及運作管理情形
- (三)專責人員或專責組織任務
- (四)個人資料盤點、管理與紀錄
- (五)保有個資達一百筆，或具對外電子商務服務系統，或具有特種個資之資通系統之安全管理

檢核項目說明(2/2)

- (六)環境管理措施。
- (七)業務終止之個資管理
- (八)事故通報與應變程序
- (九) 資安檢測
- (十)其他

113年查檢工作的精進

- 112年結案會議共識：
  - 應將查檢對象分級，來給予不同數量的檢查表
  - 應該儘量以填空題 代替 問答題，以引導答題者能明確表示。
  - 提供更詳細的填表說明。
  - 提供更具體的評審指引。

分級草案

評估構面	權重	1	2	3
個資數量 A	1	1000 筆以下	一般個資 1001~50,000筆 特種個資 1001~50,000筆	一般個資 50,001筆以上 特種個資 50,001筆以上
外部利用 B	0.6	無外部利用情形 1000筆內少量	一般個資 1001~50,000筆 特種個資 1001~50,000筆	一般個資 50,001筆以上 特種個資 50,001筆以上
國際傳輸 C	0.4	不涉及特殊類別敏感資訊 1000筆內少量	一般個資 1001~50,000筆 特種個資 1001~50,000筆	一般個資 50,001筆以上 特種個資 50,001筆以上

大綱

1. 個資法修法對教育體系的影響
2. 教育部對教育體系個資行政檢查的規劃
3. **結語**

務求法遵合規，善盡良善管理責任

- 個資法適用範圍涵蓋公私立學校，且分別負有行政、民事及刑事 等責任，教育體系應嚴加重視。

- 依個資法第27條及教育部個資安維計畫實施辦法第6條規定，私立 專科以上學校應訂定及執行安全維護計畫，包括業務終止後個人 資料處理方法。

結合資安推動個資保護，以收綜效

- 各校可評估結合現有資安管理(ISMS)及適度導入個資管理制度(PIMS)，避免重複資源投入以達到雙贏。