個資保護政策執行與經驗分享

104學年校務資訊系統及資訊服務交流研討會

東吳大學電子計算機中心

余啟民

2015.11.27

報告大綱

1. 教育部訪視表單
2. 東吳專案規劃
3. 個資適法性查檢暨管理制度導入
4. 個資教育訓練分享

教育部大專校院統合視導訪視表

- 視導項目：校園保護智慧財產權與資訊安全（含個資保護）
- 視導對象：公私立大專校院
- 【訪視內容說明】
- 一、訪視項目共分3大項，為校園保護智慧財產權（40%）、資訊安全（30%）、**個資保護（30%）**，整體總分共100分。
- 二、依據校園保護智慧財產權行動方案、教育體系資通安全管理規範、教育部所屬機關及各級公私立學校資通安全工作事項、**個人資料保護法及其施行細則、教育體系個人資料安全保護基本措施及作法辦理**。
- 三、本訪視項目內容及指標為教育部資訊及科技教育司、高等教育司與技術及職業教育司共同訂定。

訪視細項	訪視指標	評分標準
(一)個資法遵循性(10%)	1.已**建立個人資料保護組織？並指定機關高層為個資業務之機關召集人**？(2分)	已建立個人資料保護組織並指定機關高層為個資業務之機關召集人：2分。 (檢附機關個人資料保護組織相關規範)
	2.已**定期界定並清查機關內「個人資料檔案」**？(2分)	已定期界定並清查機關內「個人資料檔案」：2分。 (提供歷年及最新「個人資料檔案」清冊)
	3.已**指定具備適當資格或經驗之專人依法令規定辦理個資安全維護及保管事項**？(2分)	已指定具備適當資格或經驗之專人依法令規定辦理個資安全維護及保管事項：2分。 **(檢附受指定專人相關經驗或資格文件(如具BS 10012 LA或相關個資證照等))**
	4.已**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分)	已設置「個資保護聯絡窗口」並將聯繫方式置於單位網站：2分。 (提供個資聯繫之網頁資料)
	5.已**訂定個人權力行使的流程，並於法律允許之範圍內提供資料當事人下列權益**：(2分) (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	已訂定個人權力行使的流程且包含提供5種資料當事人權益：2分。 (提供已訂定個人權力行使的流程規範)

訪視細項	訪視指標	評分標準
(二)教育部頒訂「教育體系個人資料安全保護基本措施及作法」配合度(12%)	1.已依據「教育體系個人資料安全保護基本措施及作法」，辦理「人員管理措施」？(2分)	提供佐證資料：2分。 (提供「人員管理措施」相關說明文件)
	2.已依據「教育體系個人資料安全保護基本措施及作法」，辦理「作業管理措施」？(2分)	提供佐證資料：2分。 (提供「作業管理措施」相關說明文件)
	3.已依據「教育體系個人資料安全保護基本措施及作法」，辦理「物理環境管理措施」？(2分)	提供佐證資料：2分。 (提供「物理環境管理措施」相關說明文件)
	4.已依據「教育體系個人資料安全保護基本措施及作法」，辦理「技術管理措施」？(2分)	提供佐證資料：2分。 (提供「技術管理措施」相關說明文件)
	5.已依據「教育體系個人資料安全保護基本措施及作法」，辦理「認知宣導及教育訓練」？(2分)	提供佐證資料：2分。 (提供當年度辦理「個資認知宣導及教育訓練」相關佐證資料)
	6.已依據「教育體系個人資料安全保護基本措施及作法」，辦理「紀錄機制」？(2分)	提供佐證資料：2分。 (提供「紀錄機制」相關說明文件)

訪視細項	訪視指標	評分標準
(三)個人資料保護持續改善管理流程(8%)	1.已進行**個資風險評鑑**，設定資料保護要求？(2分)	提供佐證資料：2分。 (提供風險評鑑報告書)
	2.已**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？(2分)	提供佐證資料：2分。 (提供稽核結果報告書)
	3.已**將個資業務委外監督管理機制納入合約條款，並進行適當之稽核**？(4分)	(1)已將個資業務委外監督管理機制納入合約條款且有進行相關監督稽核紀錄：4分。 (2)僅有委外監督管理機制之合約條款，仍未進行相關監督稽核作業：2分。 (a.提供個資委外契約範本；b.提供委外監督相關稽核紀錄)

東吳專案規畫目標

因應「個人資料保護法」施行與主管機關要求，本專案規劃同時進行個資適法性查檢及個資管理制度建置。重點目標包括：

(1) 透過教育訓練讓各單位人員瞭解個資法與個資保護相關認知。

(2) 完成業務個資清查，瞭解單位擁有哪些個資，及識別個資的屬性、蒐集、利用等作業。

(3) 藉由風險評鑑識別資料安全風險、違法使用情況。

(4) 承續業務個資清查、風險評鑑結果，協助改善資料安全管控與管理；並以法律專業能力協助進行適法性矯正。

(5) 承續資料安全與適法性鑑別結果，建置可遵循以合法作業之全校性個人資料管理制度通用規範。

(6) 於個人資料管理制度建置完成後進行本年度之個人資料管理制度內部稽核。

(7) 協助滿足「104年度教育部大專校院統合視導」規範之個資管理要求事項。

東吳專案執行範圍

施行範圍原則為東吳大學相關一、二級單位，共計86各單位，說明如下：

- (1)　獨立業務之一、二級行政單位
- (2)　院級、系級之教學單位辦公室
- (3)　經手個人資料的研究單位

- 適法性查檢
- 適法性顧問
- 個資委外稽核
- 管理制度導入

聯經數位

(一)
個資
保護政策

(二)
個資清查與
風險評鑑

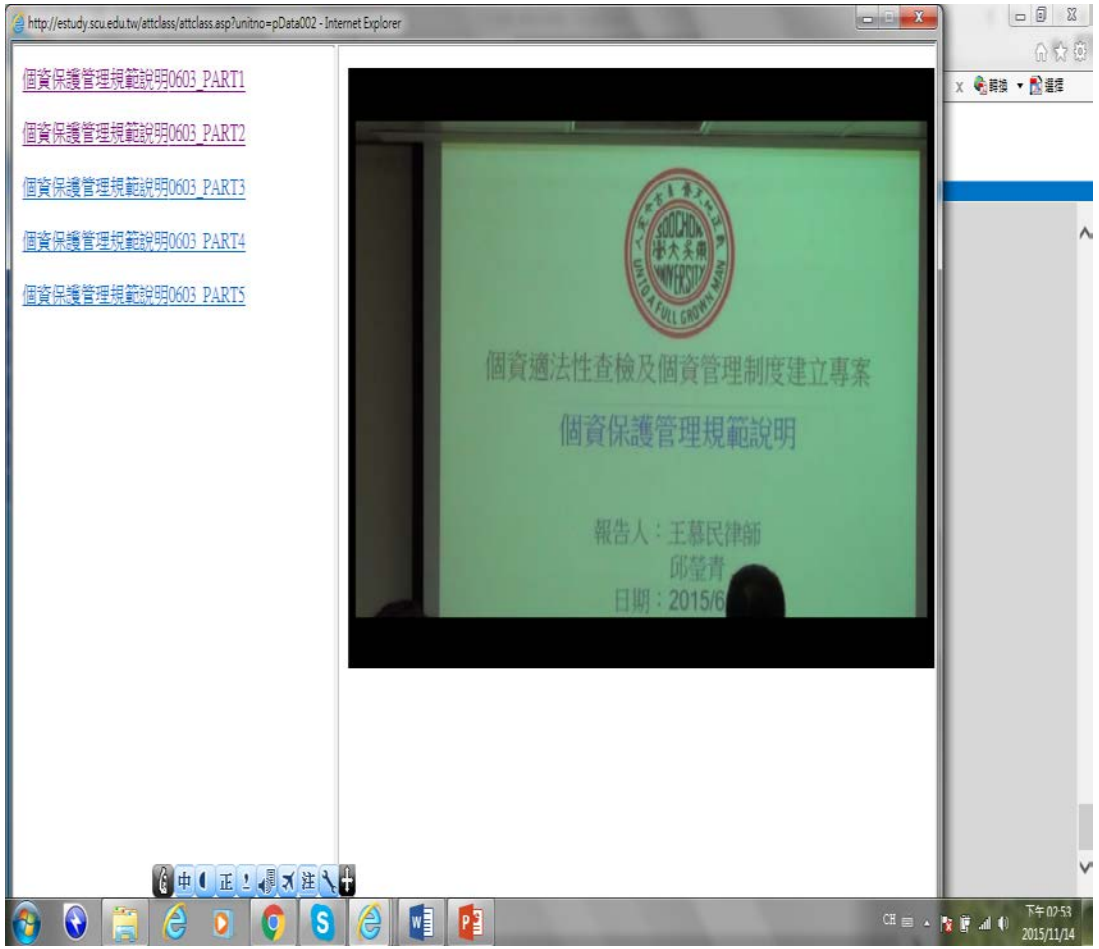
(三)
風險改善
方案

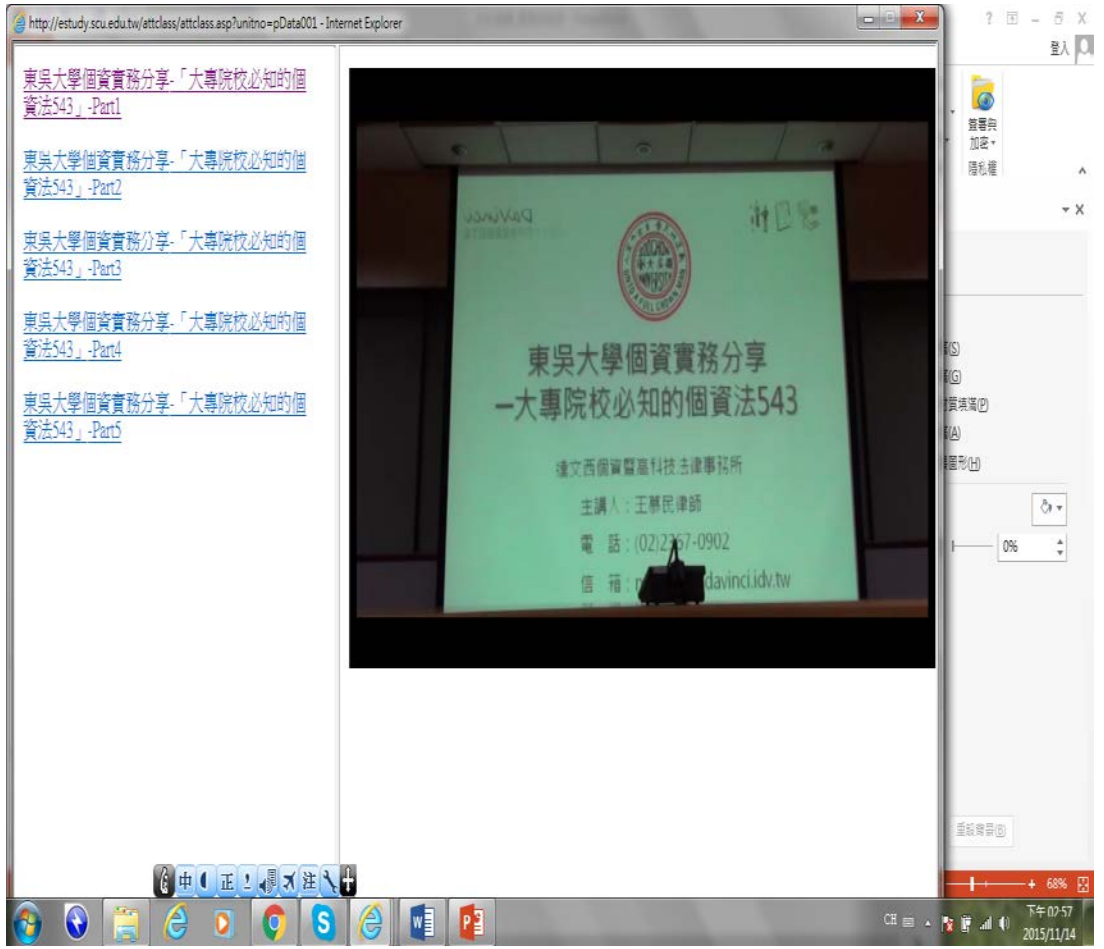
(四)
個資管理
制度

(五)
監控與稽核

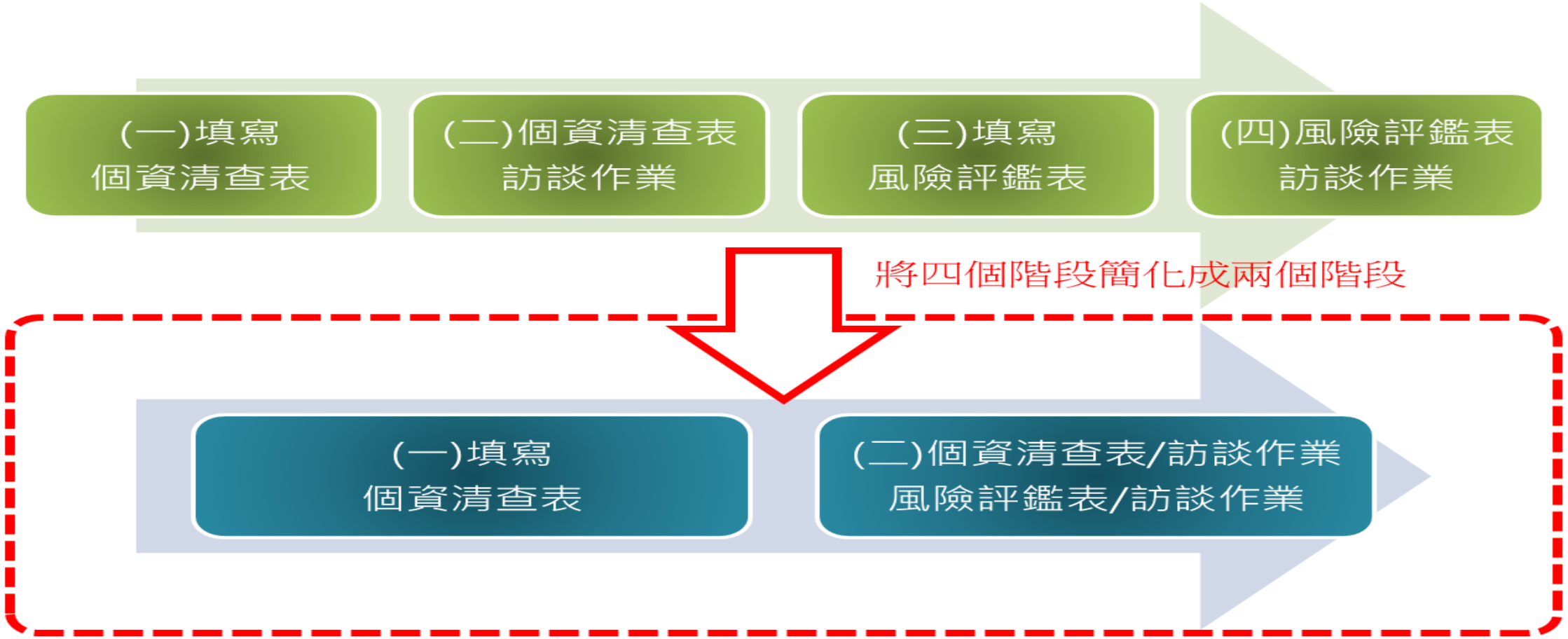
東吳專案作業規劃階段圖

教育訓練


http://estudy.scu.edu.tw/attclass/attclass.asp?unitno=pData002 - Internet Explorer
個資保護管理規範說明0603_PART1
個資保護管理規範說明0603_PART2
個資保護管理規範說明0603_PART3
個資保護管理規範說明0603_PART4
個資保護管理規範說明0603_PART5
個資適法性查檢及個資管理制度建立專案
個資保護管理規範說明
報告人：王慕民律師
邱瑩青
日期：2015/6


http://estudy.scu.edu.tw/attclass/attclass.asp?unitno=pData001 - Internet Explorer
東吳大學個資實務分享-「大專院校必知的個資法543」-Part1
東吳大學個資實務分享-「大專院校必知的個資法543」-Part2
東吳大學個資實務分享-「大專院校必知的個資法543」-Part3
東吳大學個資實務分享-「大專院校必知的個資法543」-Part4
東吳大學個資實務分享-「大專院校必知的個資法543」-Part5
東吳大學個資實務分享
-大專院校必知的個資法543
主講人：王慕民律師
davinci.idv.tw

個資清查與風險評鑑


(一)填寫
個資清查表
(二)個資清查表
訪談作業
(三)填寫
風險評鑑表
(四)風險評鑑表
訪談作業
將四個階段簡化成兩個階段
(一)填寫
個資清查表
(二)個資清查表/訪談作業
風險評鑑表/訪談作業

個資清查表

個人資料檔案清查																											適法性評估																									
編號	個人資料檔案名稱	(一)生命週期(二)資料形式(三)相關人員	作業流程	檔案儲存方式	是否為資料權責單位	經手個資檔案			一般個人資料													特種個人資料			間接識別資料(填寫)	資料重要性	蒐集(1)					處理		利用				委託事項(13)	
						蒐集	處理	利用	姓名	生日	身分證號	護照號碼	特徵	婚姻	家庭	教育	職業	聯絡方式	財務情況	社會活動	醫療	健康檢查	犯罪前科			蒐集目的(2)	蒐集要件(3)	直接蒐集(4)	間接蒐集(5)	有無告知法定事項(6)	處理態樣(7)	合於蒐集目的(8)	外部利用(9)	對當事人利用(10)	蒐集目的內利用(11)	蒐集目的外利用(12)	委託他人辦理(14)	委外監督(15)

風險評鑑表

編號	個人資料檔案名稱	資料重要性	風險量化與值化	資料安全不足程度				弱點風險值	資料安全風險
				存取管控嚴謹度不足	作業流程嚴謹度不足	實體/系統保護不足	未有稽核記錄或制度		
			風險評估					0	0
			問題敘述						
			風險評估					0	0
			問題敘述						

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

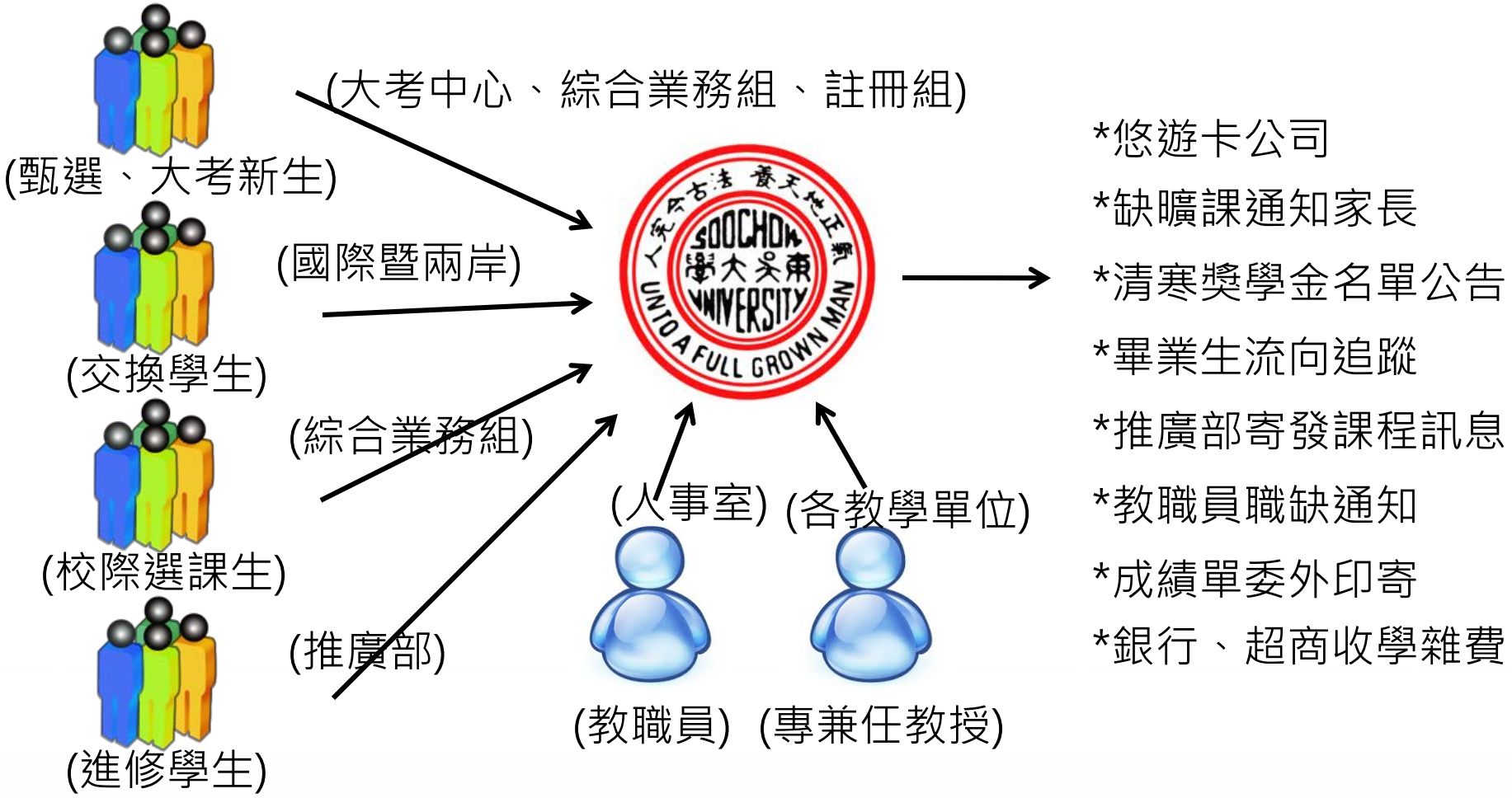
東吳大學
一個資適法性查檢暨管理制度
導入專案介紹

哪個較重要？

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

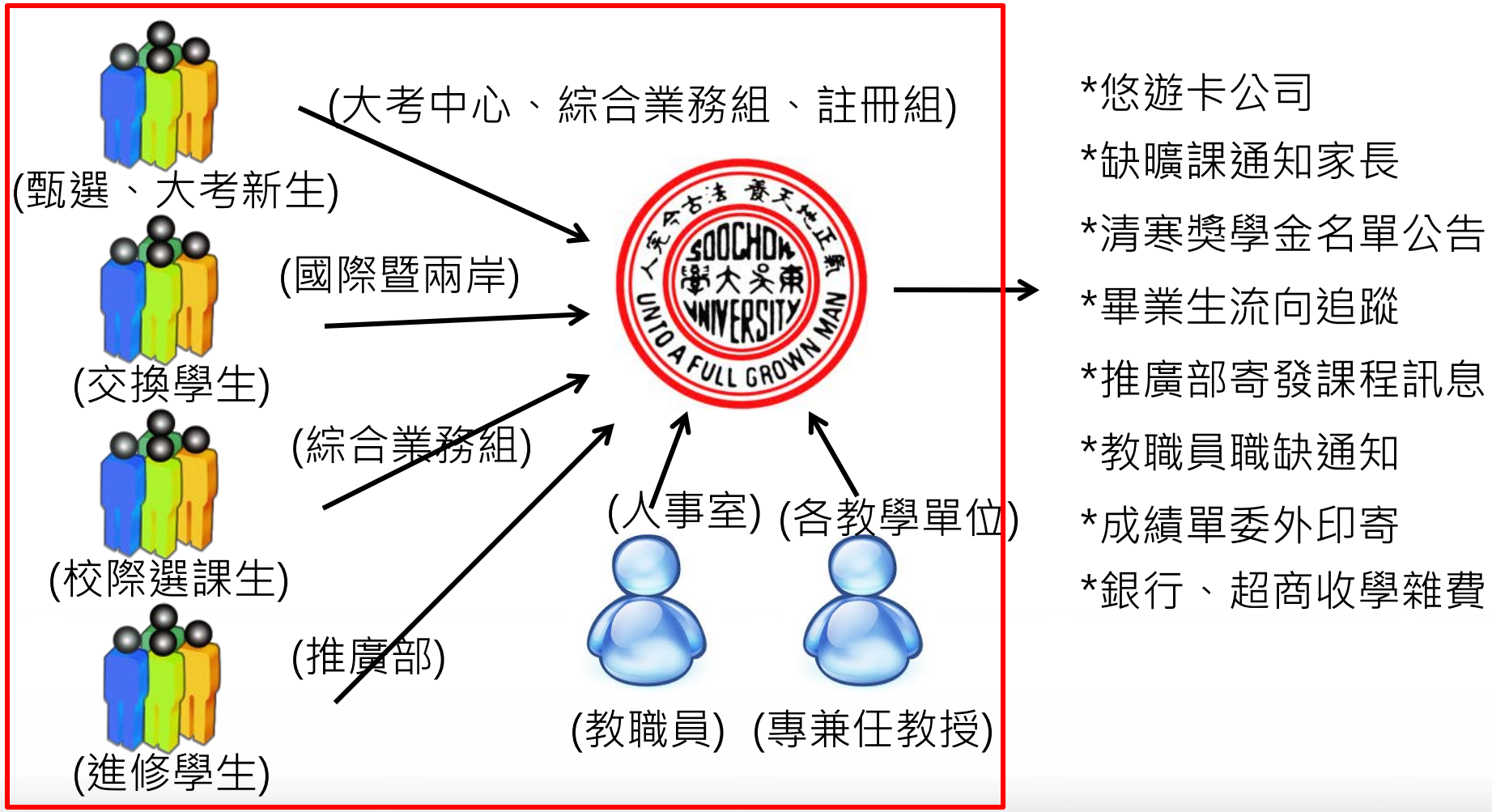
大學常見的個資違法問題

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm



大學常見的個資違法問題

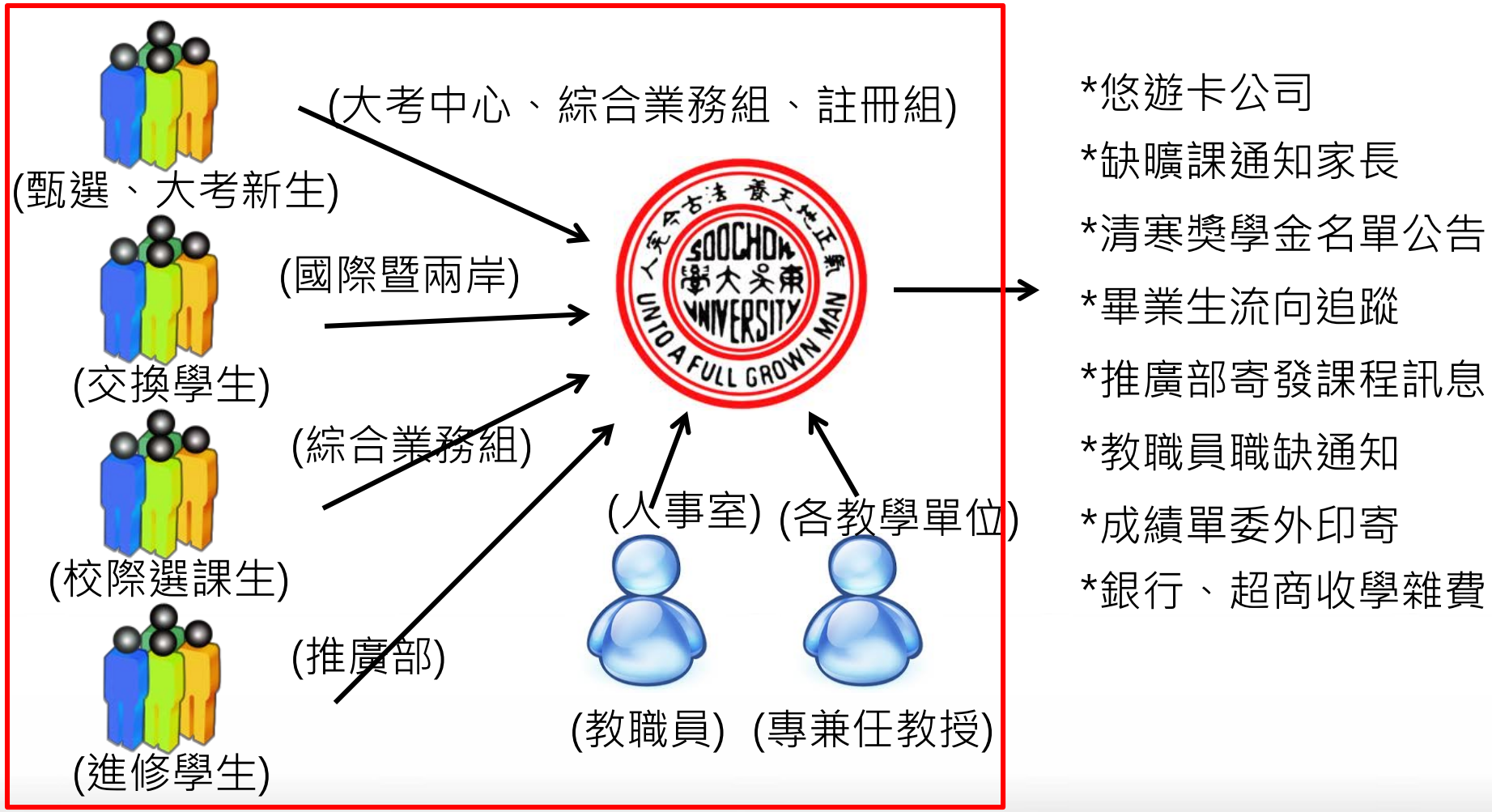
- 蒐集個資有無超過必要範圍？



大學常見的個資違法問題

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

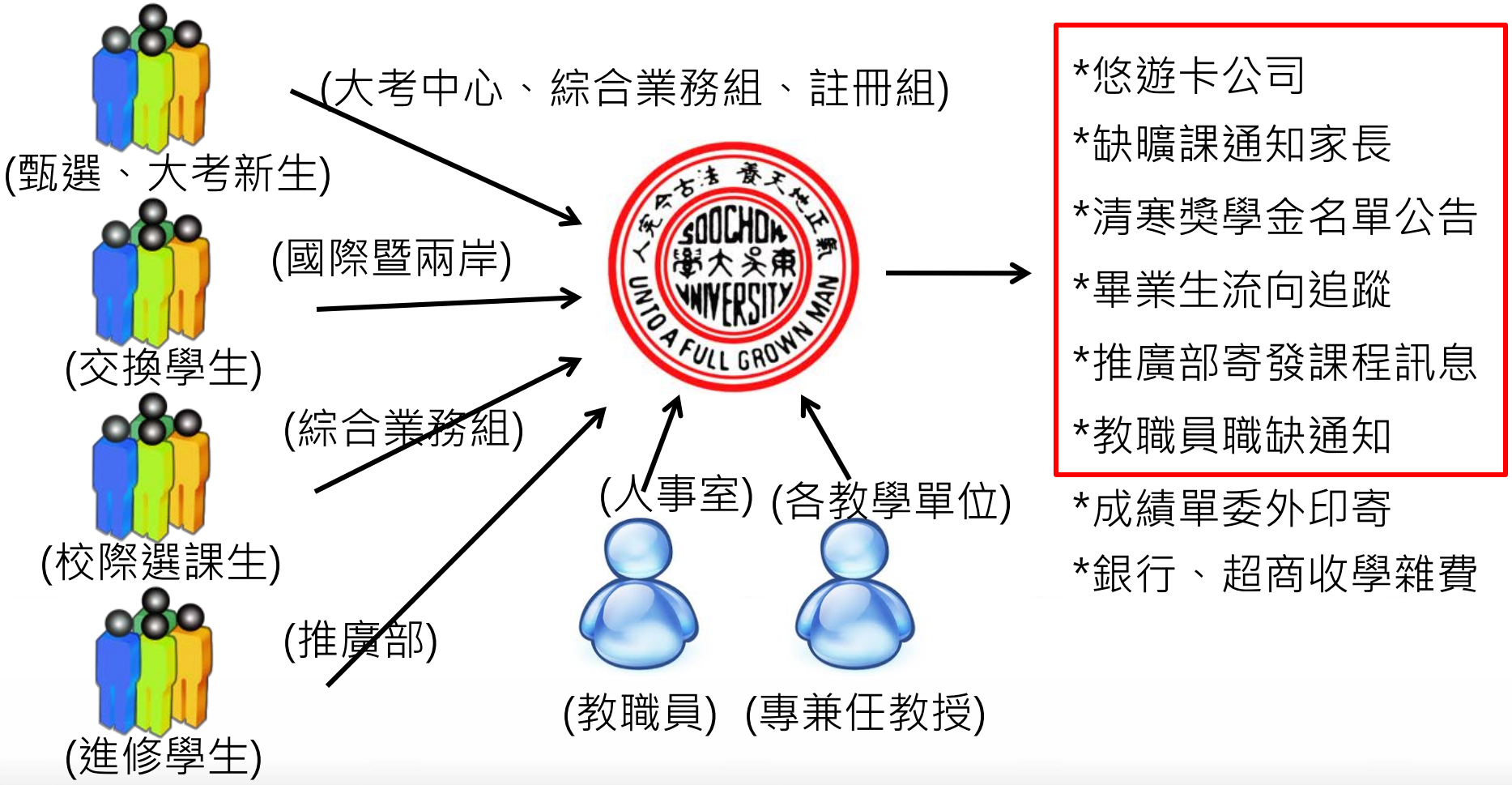
- 蒐集個資有無告知法定事項？(個資蒐集告知聲明)



大學常見的個資違法問題

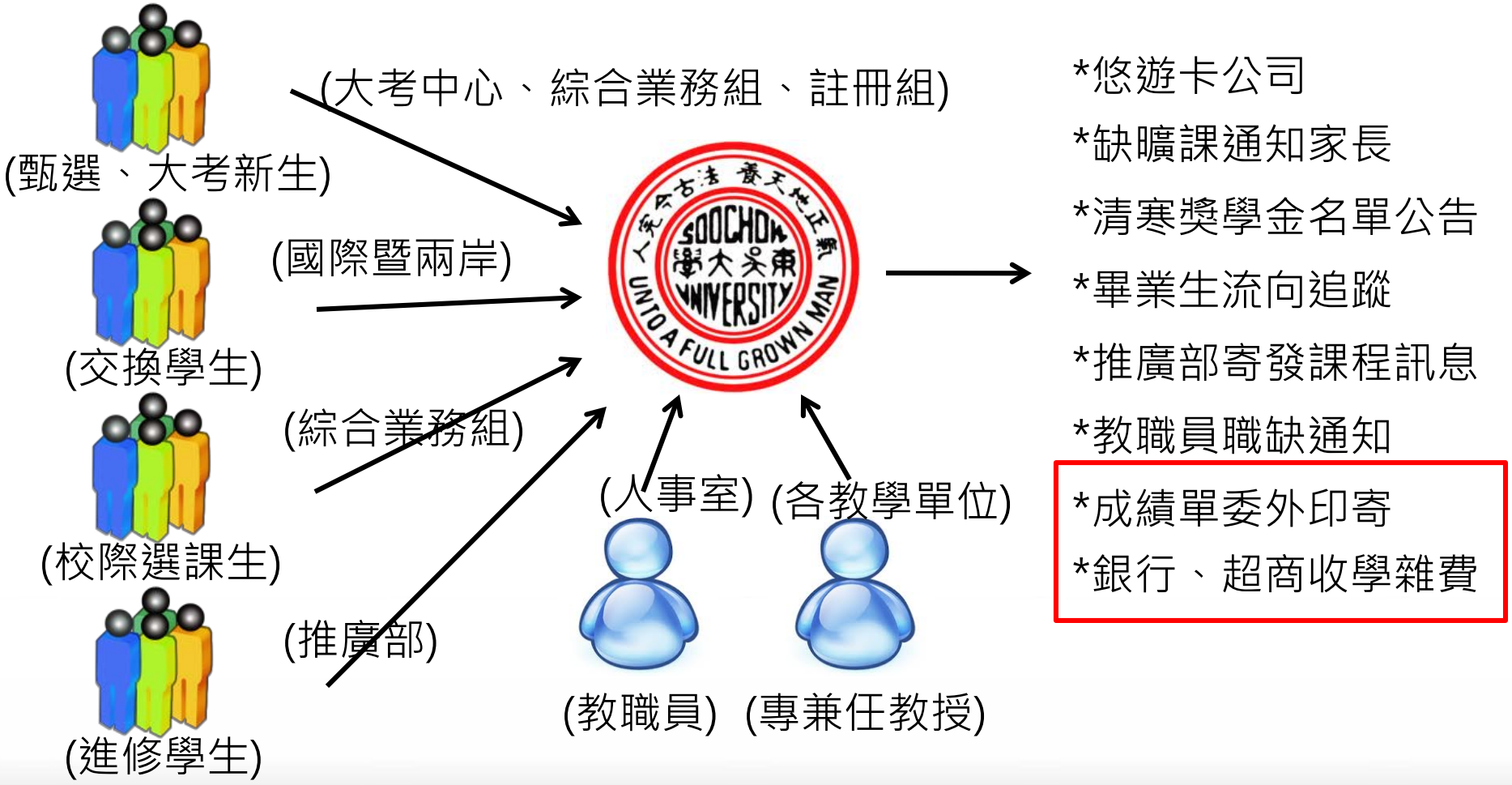
達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 利用個資有無超出蒐集目的？



大學常見的個資違法問題

- 委外處理、利用個資有無監督？



大學常見的個資違法問題

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 當事人權利行使管道未建置
- 個資保存期限不統一
- 院系研討會報名資料由老師負責，無法控管
- 學校與校友會非同一機關，但學校直接提供畢業學生個資給校友會

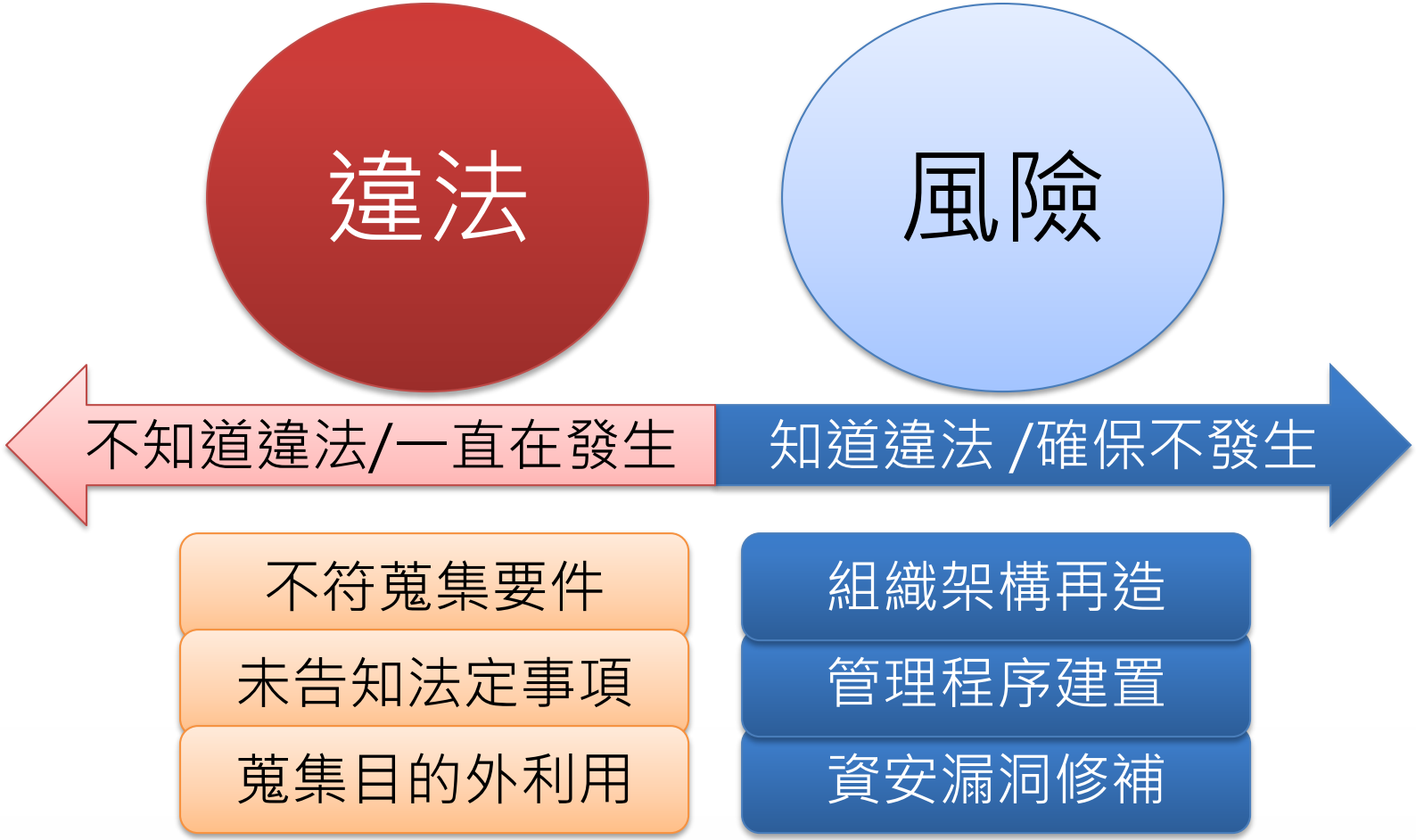
適法性查檢以矯正違法

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 個資盤點清查
- 個資蒐集、處理、利用適法性查檢
- 個資查檢缺失項目矯正
- 適法性複檢

該怎麼做才不觸法？

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm



管理制度建置以降低風險

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 個人資料管理制度建置
  - 依據個人資料保護法、個人資料保護法施行細則
  - 依據教育體系個人資料安全保護基本措施及作法
  - 依據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實施辦法

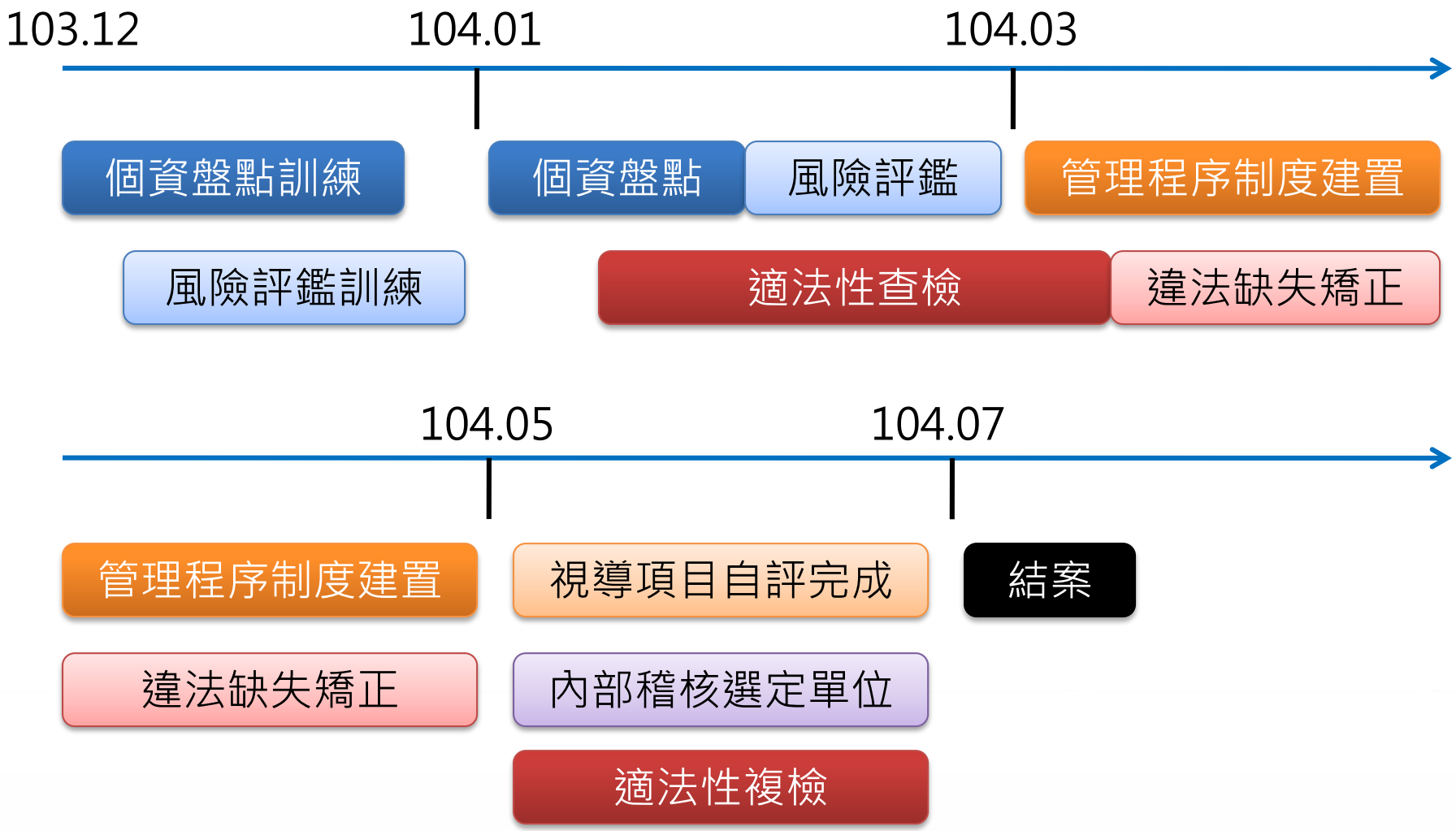
管理制度建置以降低風險

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 個人資料管理制度建置
  - 各單位(行政單位、教學單位)個資盤點清查(配合盤點教育訓練)
  - 個資暨資安風險評鑑(配合風險評鑑教育訓練)
  - 個資保護組織架構建置及專責人員配置
  - 個資事故通報、應變機制建置
  - 當事人權利行使程序建置
  - 個資委外監督程序建置
  - 個資內部稽核程序建置
  - 制訂人員管理措施規範
  - 制訂作業管理措施規範
  - 制訂物理環境管理措施規範
  - 制訂技術管理措施規範
  - 制訂使用紀錄保存機制規範

作業時程預估

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm



效益評估

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 具體辨別違法，矯正缺失，避免行政處罰及民事賠償責任
- 符合教育部「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實施辦法」規範
- 符合教育部104年下半年視導評核項目

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

東吳大學個資教育訓練
實務分享
─大專院校必知的個資法543

個資法543

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 5個方向
- 4大原則
- 3不3要

5個方向

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

1) 資訊自主
2) 違法蒐集
3) 違法利用
4) 黑箱作業
5) 個資意外

4大原則

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

1) 資料減量
    1) 個資欄位減量
    2) 個資數量減量
    3) 到期個資銷毀
2) 從一而終
    1) 在蒐集目的內利用個資
    2) 檢視有無符合例外
        1) 法律明文規定
        2) 增進公共利益
        3) 免除當事人危險
        4) 防止他人重大危害
        5) 為公共利益做統計+無從識別當事人
        6) 當事人書面同意-明確告知目的、範圍及同意與否的影響
3) 公開透明
    1) 該告知的告知　隱私權聲明、個資告知聲明
    2) 該通知的通知　個資侵害事故
4) 妥善保管

4大原則：4)妥善保管

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

適當安全維護

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
非公務機關保有個人資料檔案者，應採行適當之安全措施。

得採取下列措施

- 組織資源配置
- 通報應變機制
- 認知教育訓練
- 資料紀錄保存
- 個人資料範圍
- 內部管理程序
- 設備安全管理
- 安全維護計畫
- 風險評估機制
- 安全人員管理
- 安全稽核機制

3不3要

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

- 不蒐集、不保存用不到的個資
- 不在蒐集目的外利用個資
- 不掉以輕心
- 要攤在陽光下
- 要顧及當事人權利
- 要定期檢視個資法律遵循