

經濟部個資保護要點暨個資管理作業說明

廖淑君 研究員
資訊工業策進會 科技法律研究所
jolieliao@iii.org.tw

前言

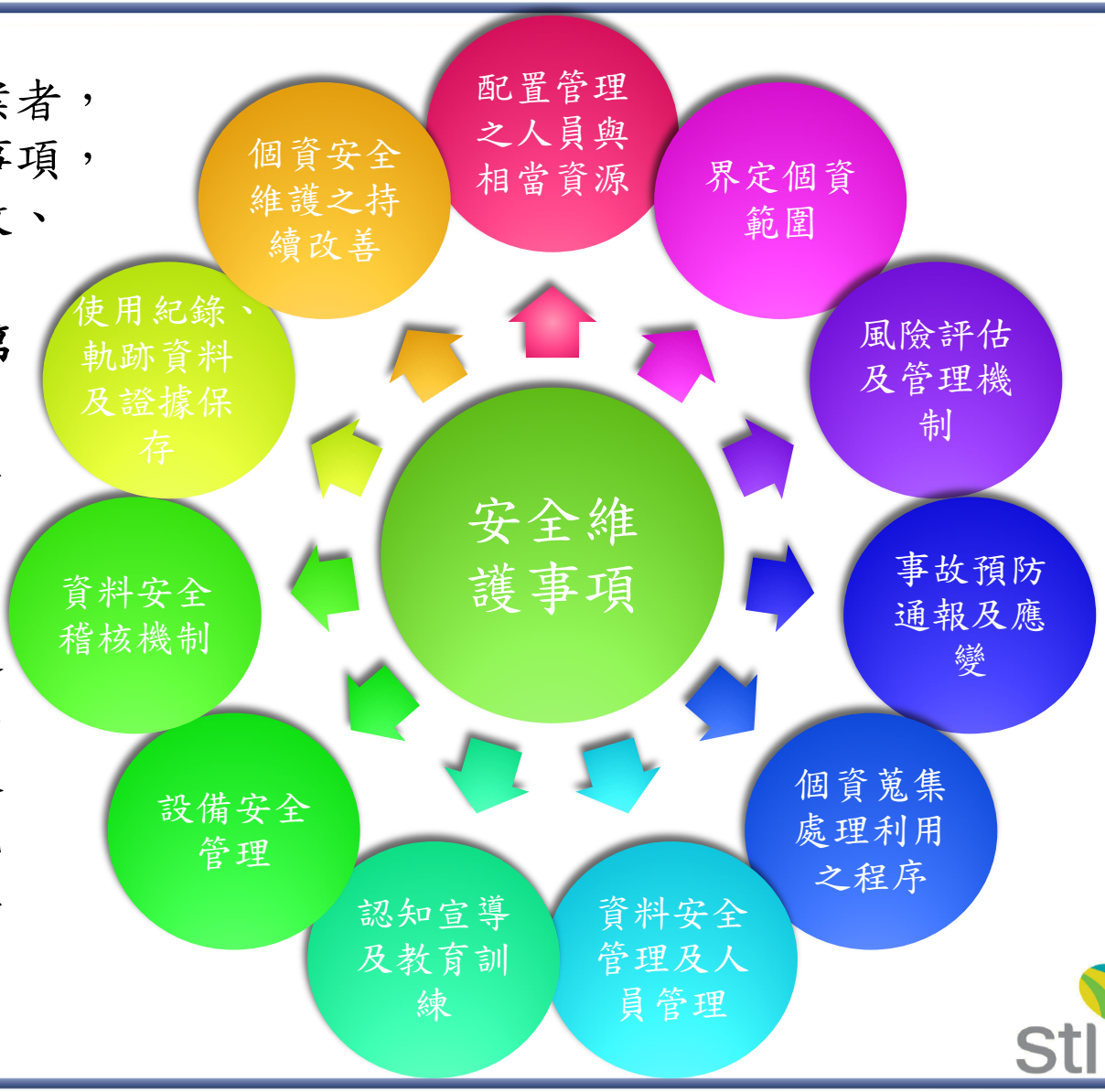
個人資料安全維護事項

個人資料保護法第18條

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

個人資料保護法施行細則 第12條

本法第六條第一項第二款所稱適當安全維護措施、第十八條所稱安全維護事項、第二十七條第一項所稱適當之安全措施，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。.....



個人資料安全維護規定

個人資料保護法施行細則 第24條

公務機關保有個人資料檔案者，應訂定個人資料安全維護規定

經濟部及所屬機關個人資料保護管理要點

101.10.26 經法字第 10104681660 號函下達

壹、總則

一、經濟部(以下簡稱本部)及所屬機關為執行個人資料保護法(以下簡稱本法)，以落實個人資料之保護及管理，特訂定本要點。

二、本部一級單位及所屬機關辦理下列事項，應設置個人資料保護聯絡窗口：

(一)公務機關間個人資料保護業務之協調聯繫及緊急應變通報。

(二)非資訊面個人資料安全事件之通報。

(三)重大個人資料外洩事件之民眾聯繫單一窗口。

(四)本部一級單位及所屬機關個人資料專人名冊之製作及更新。

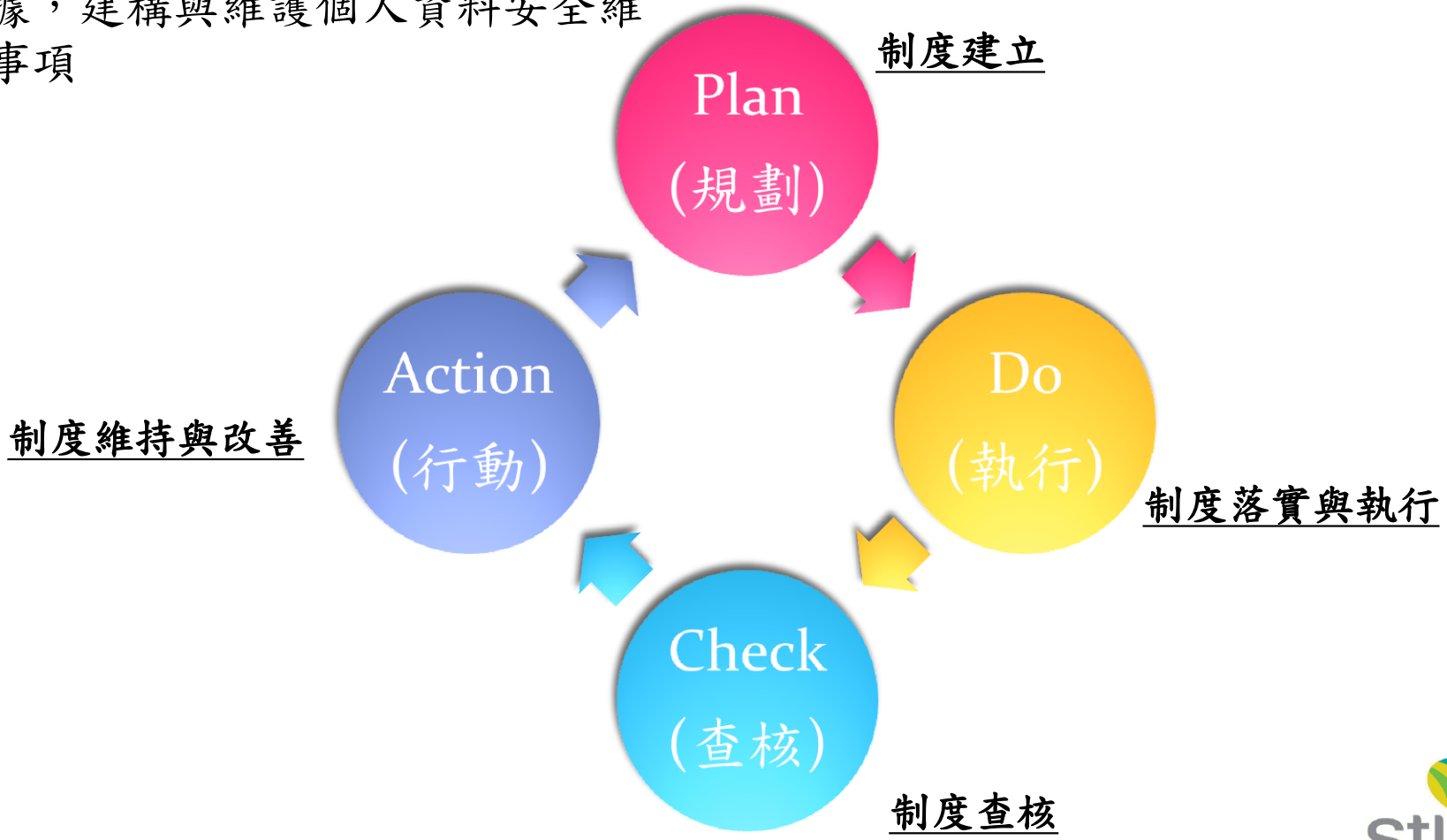
(五)本部一級單位及所屬機關個人資料專人與職員工教育訓練名單及紀錄之彙整。

個人資料安全維護事項建立

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

方法論

- 以PDCA（Plan-Do-Check-Act）方法論為基礎，個人資料保護法令為依據，建構與維護個人資料安全維護事項



個人資料安全維護事項建立流程

設置專人

界定個人資料範圍(個人資料檔案盤點)

個人資料檔案風險評估與擬定管控措施

建立個人資料保護與管理內部程序

實際運作(含預防演練)並實施教育訓練

制度檢視

持續改善

設置專人

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

經濟部及所屬機關個人資料保護管理要點

壹、總則

一、經濟部(以下簡稱本部)及所屬機關為執行個人資料保護法(以下簡稱本法)，以落實個人資料之保護及管理，特訂定本要點。

二、本部一級單位及所屬機關辦理下列事項，應設置個人資料保護聯絡窗口：

(一)公務機關間個人資料保護業務之協調聯繫及緊急應變通報。

(二)非資訊面個人資料安全事件之通報。

(三)重大個人資料外洩事件之民眾聯繫單一窗口。

(四)本部一級單位及所屬機關個人資料專人名冊之製作及更新。

(五)本部一級單位及所屬機關個人資料專人與職員工教育訓練名單及紀錄之彙整。

(六) 個人資料保護法令之諮詢。

經濟部及所屬機關個人資料保護管理要點

三、本部及所屬機關之一級單位辦理下列事項，應指定專人處理：

(一)執行當事人依本法第十條及第十一條第一項至第四項所定請求之督導。

(二)執行本法第十一條第五項及第十二條所定通知之督導。

(三)本法第十七條所定公開或供公眾查閱。

(四)本法第十八條及個人資料保護法施行細則(以下簡稱本法施行細則)第十二條所定個人資料檔案安全維護。

(五)職員工之個人資料保護意識提升及教育訓練計畫之執行。

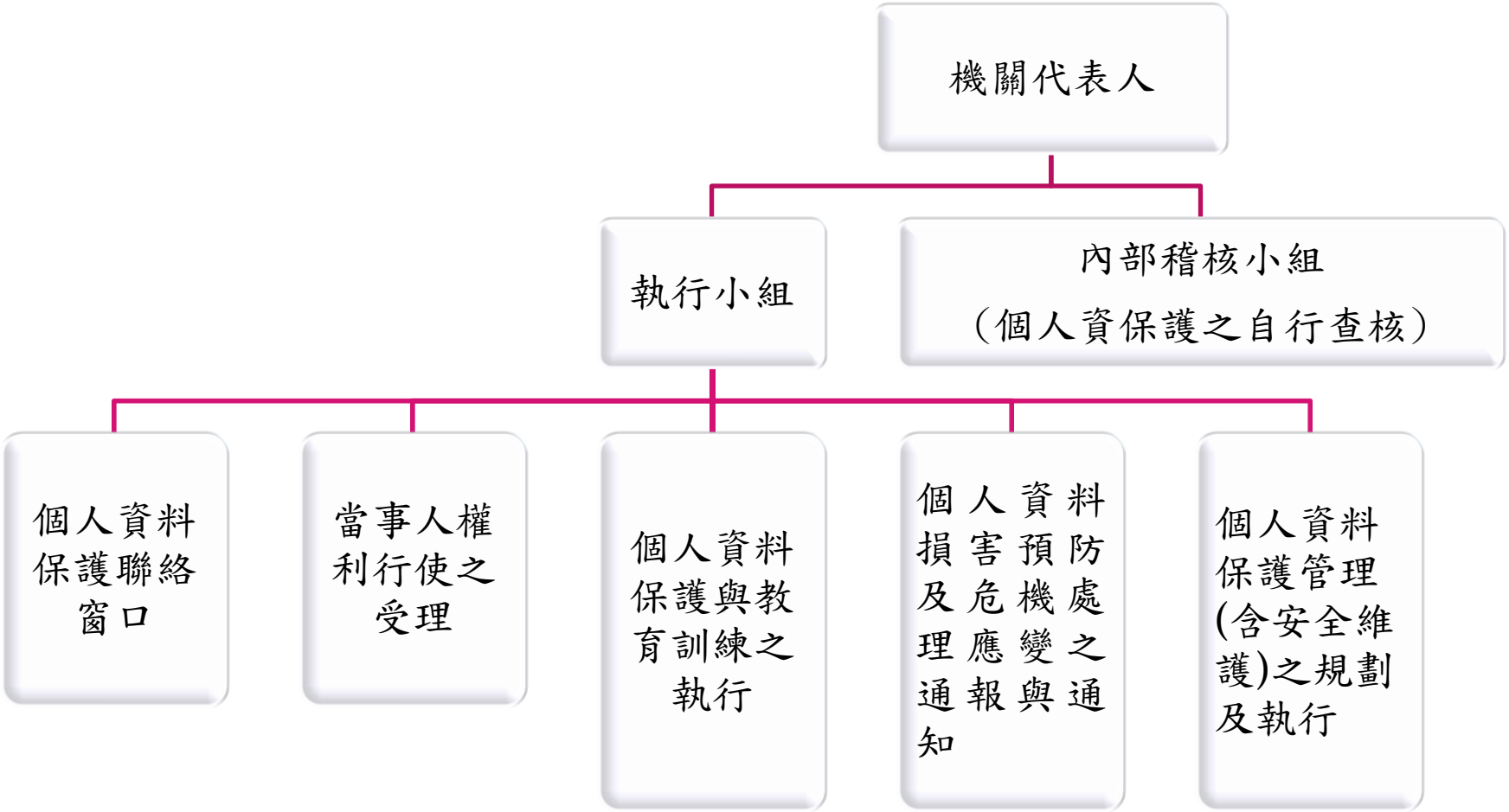
(六)個人資料保護事項之協調聯繫。

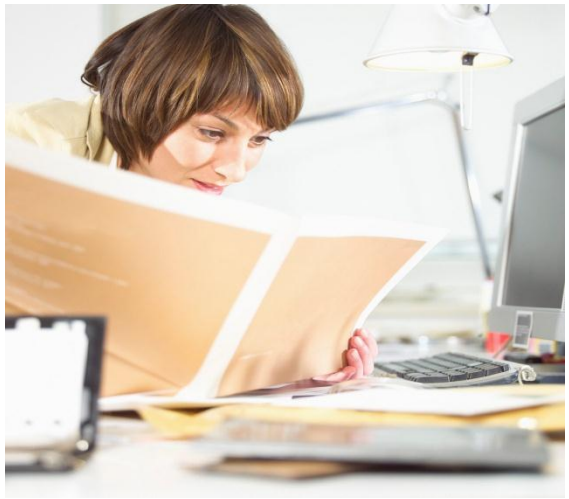
(七)單位內個人資料損害預防及危機處理應變之通報。

(八)本部及所屬機關個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。

(九)其他有關單位內個人資料保護管理之規劃及執行。

範例：個人資料保護與管理組織





界定個人資料範圍(個人資料檔案盤點)

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

個人資料保護法第17條所定公開或供公眾查閱

國立臺灣大學教職員生資料檔案清冊

編號	個人檔案資料名稱	法律依據	個人資料類別[*1]	保有單位
1	國立臺灣大學公務通訊錄	行政院及所屬機關人事資料統一管理要點	C001,C054,C061,C011,C003	本校各一、二級單位
2	專案助理聘任報帳資料	國立臺灣大學約用工作人員工作規則、會計法	C001,C002,C003,C011,C051	本校各一、二級單位
3	單位同仁通訊錄	行政院及所屬機關人事資料統一管理要點,國立臺灣大學組織規程 第21條, 第24條；國立臺灣大學行政單位組織運作要點 第5點		各一、二級
4	電腦暨財產物用品增加、移轉及減損報銷單與財產盤點紀錄表	國立臺灣大學財產管理		、二級
5	廠商暨業務相關人士連絡資料			本校各一、二級單位
6	IP使用者對應表			本校各系所
7	各系所暨相關課程成績單		C011,C057	本校各系所
8	系所研討會報名系統		C001,C003	本校各系所

第 17 條

公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

一、個人資料檔案名稱。

二、保有機關名稱及聯絡方式。

三、個人資料檔案保有之依據及特定目的。

四、個人資料之類別。

資料來源：台灣大學 www.ntu.edu.tw/service/ntulist20111223.pdf

掌握動態，策略不失焦

○○○單位執行○○○部之計畫，不尊重民眾隱私，未當事人同意將個人資料提供○○○公司使用，○○○單位未做好保護民眾權益之工作，公然帶頭違法!!

個人資料檔案盤點之目標

1. 確認有無間接蒐集之個人資料。
2. 確認已蒐集之個人資料有特定目的與法定職務
3. 確認個人資料之流程
4. 後續運用時，確認個人資料特定目的消失(特定目的達成無繼續處理或利用之必要)與期限屆滿，以判斷是否違停止處理、利用、刪除之行為
5. 確認是否有委外。
6. 確認風險處理之標的。

個人資料檔案盤點

- 盤點目的

由機關所處理的資料中盤點出應受保護的個人資料（個資盤點）

從個人資料作業的識別各個情境、評估風險，並訂定風險對策（風險評估）

實施所訂定的風險對策，合法適當地處理個人資料，以達到保護當事人的權益

合法適當地使用個人資料，並得到民眾的信賴，以提高機關行政服務品質

- 盤點程序
  - 作業流程普查
  - 個人資料檔案普查
- 盤點時機
  - 定期
  - 不定期
- 盤點方法：
  - 人工盤點
  - 自動化盤點(利用資訊軟體進行盤點)

範例：個人資料檔案盤點之程序

臺大個資盤點經驗分享

主導單位	資訊部門
盤點方式	人工（自行開發盤點系統）
盤點表的欄位	(1) 保管者：單位名稱、資料保管人的姓名 / 聯絡電話 / 電子郵件。 (2) 個人資料檔案：個人資料檔案名稱、法源依據、特定目的、個人資料類別、個人資料範圍、有沒有特種資料及類別、有沒有監督管理之非公務機關、資料保管地點、資料保存期限。
盤點對象	教職員工
盤點心得	龐大員工人數多的組織，最好階段性盤點個資，先做普查再逐一深入調查，避免引起反彈。 個資盤點工作需動員全體員工，最好由組織中層人士帶頭，比較有成效。

製表：[redacted]，2011/9

資料來源：資安人，2011年10月

範例：個人資料檔案盤點工具

個資盤點表(參考範例)

單位名稱	
單位主管	
盤點人員	

編號	資料檔案名稱	保有機關名稱及聯絡方式	保有依據(法定職務)	特定目的	個人資料之類別	特種個人資料		數量	資料型態	資料蒐集/處理				資料處理/利用			
										(原始+蒐集方法)or(加工+加工方法)二選一填寫				內部傳送		保管	
						特種個資種類	法定要件	(僅需填寫一年大約件數)		原始資料	蒐集方法	加工資料	加工方法	資料流向	傳送方式	保管方式	保存期限
1	民眾(廠商)抱怨處理單	服務科	經濟部工業局組織條例第2條第15項：其他有關工業發展、國際工業合作及工業行政事項	006公共關係 101 其他顧問諮詢服務	C001辨識個人者	■無 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	X	0-10	□電子 ■紙本	■直接向當事人蒐集 □間接蒐集(來源：____)	現場口頭陳述	原始檔案/系統名稱：_____	X	各組室	■人員親送 □Email □系統 □其他 _____	□儲存個人電腦(電子) □儲存於資料庫/主機(電子) ■存放個人櫃/抽屜(紙本) □存放檔案室(紙本) □其他___	□法定保存期限____ □自訂保存期限____ ■無保存期限	X
2	電子信箱處理單	服務科	經濟部工業局組織條例第2條第15項：其他有關工業發	101 其他顧問諮詢服務	C001辨識個人者	■無 □醫療 □基因 □性生活	X	1500	□電子 ■紙本	□直接向當事人蒐集 □間接蒐集(來源：____)	X	原始檔案/系統名稱：民眾抱怨信件	■輸入/編輯 ■輸出/列印 □影印 □掃描	各組室	■人員親送 □Email □系統 □其他	□儲存個人電腦(電子) □儲存於資料庫/主機(電子) ■存放個人櫃/抽屜(紙本)	□法定保存期限 □自訂保存期限	X

個人資料檔案風險評估與擬定管控措施

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

個人資料檔案風險評鑑(1)

萬芳醫院爆洩病歷、隱私

太離譜 服務台志工給的便條紙，背面竟是另名病患就醫資料，姓名、年齡、身高體重、就醫科別...資訊全都露。

【記者林進修、李樹人／台北報導】

一位病患日前到台北市立萬芳醫院就醫，到某科服務台詢問相關就醫資訊時，志工給他的便條紙，背面竟然有另一名病患的就醫資料，姓名、年齡、體重、就醫科別等資訊都清清楚楚，病患隱私全曝光。

萬芳院長震驚 下令追查

衛生署醫事處長石崇良仔細檢視這張便條紙，連說了好幾次：「不行！這真的是不行的！」「這是不對的」、「這是不可以的」；因爲上面記載的就醫資料包括患者病歷號碼、身高體重、出生年月日、看診日期、看診醫師、科別、醫師診斷資料，甚至連要做哪些檢查、健保特有的處置代碼都一清二楚。得...萬芳醫院院長李飛鵬相當震驚，立即下令追查到底哪個環節出了問題。爲了亡羊補...主任蔡文玲加強在職人員的繼續教育，務必確保病患隱私並防範個人...

...違反醫療法72條「醫療機構及其人員因業務而知悉或持有病人病情或健康資...洩疏失；衛生署將行文給台北市衛生局開罰，依規定該院必須面對5萬...

...涉收補習班金錢 10萬筆學...個資外洩

【字號】大 中 小

...北縣20日電〉彰化地檢署今天表示，...、高中校長涉嫌收取補習班金錢，...、彰化縣10萬筆學生個資外洩，其中...

...資料給補習班，作...

...高中...

...到學生個人資料名...

...說，吳姓業者坦承支付楊姓校長新台幣76萬元、顏姓校長35萬及吳姓校長39萬...涉嫌投資補習班，每個月收取1萬...到22萬5000元不等的紅利。

...表示，吳姓校長還涉嫌讓補習班業者進入學校招生，並讓補習班老師進入學校...上輔導課，不過3名校長否認不法，當中有...

風險是指在一定時間內、一定條件下可能發生的結果的不確定性，包括作業風險與資安風險

範例：作業風險與資安風險

個資盤點清冊

	資料蒐集/處理			資料處理/利用							
	(原始+蒐集方法)or(加工+加工方法)二選一填寫			內部傳送		保管		外部傳送		委託	廢棄方法
原始資料	蒐集方法	加工資料	加工方法	資料流向	傳送方式	保管方式	保存期限	資料流向	傳送方式		

加工

- 輸入/編輯
- 輸出/列印
- 影印
- 掃描

內部傳送

- 人員親送
- Email
- 系統
- 其他

保管

- 儲存個人電腦（電子）
- 儲存於資料庫/主機（電子）
- 存放個人櫃/抽屜（紙本）
- 存放檔案室（紙本）
- 其他

外部傳送

- 人員親送
- 郵寄
- 傳真
- Email
- 其他

刪除

- 刪除
- 碎紙銷毀
- 其他

個人資料檔案風險評鑑(2)

風險識別

- 個人資料檔案識別
- 威脅與弱點性識別
- 現有控制措施識別
- 後果識別

風險估計

- 鑑別個人資料檔案價值
- 評鑑事故發生的可能性
- 評估風險等級

風險評鑑

- 訂定風險等級
- 決定「可接受之風險等級」

參考資料：研考會，資訊系統風險評鑑參考指引，2011年12月

風險處置計畫與追蹤

避免風險

保有風險(剩餘風險)

減低發生的機率

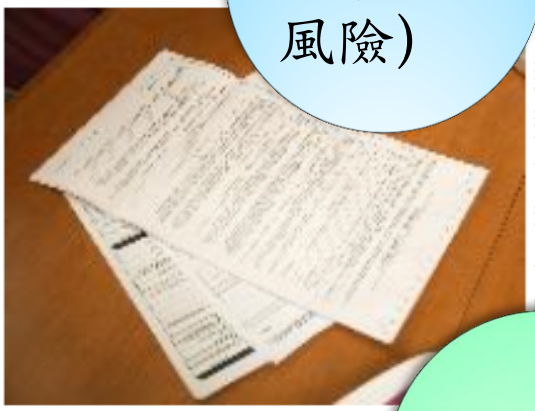
風險對策

風險轉嫁

減低影響與衝擊

轉移中 外洩風險 保護個 保險

作者：吳依恂 -10



過去十 企業為了 誠實保證保險」，避免員 的行為導致企業損失，發生像是竊盜或詐欺、 為。但是該法保護範疇只限台灣，是一種比較 。美亞產險金融保險部主任王俐欣說，一旦 發展至跨國 規模，可能就會需要「商業犯罪防護 ，但其條件較為嚴苛，自付款稍高，甚至可能高達美金 百萬美金，多 會考慮承保。

上述兩者之間，並且 國資法新出現 保護保險」，條件則介於 資法的特 灣中小企業一個轉移個資風險的解決方式。主 制，提供 處理的經驗分享，以及針對調查、和解、訴 含有大量個資風險的三 信、百貨零售通路 物，是目前最主要的詢問族群，其核保原則主要是看其風險控管機制，包括是否通過國際安全驗證如ISO 27001、

範例：個人資料檔案風險評鑑工具

	單位主管						
	填表人員						
個人資料檔案	有無特種個資	個資類別數	檔案數量(一年大約件數)	作業情境	作業內容	具體風險類型	風險處理對策
民眾(廠商)抱怨處理單	■無 □有	1	10	加工	X	X	X
				內部傳送	人員親送	收發記載不確實以致遺失	確認收受記錄媒體內容、件數，雙方留存收受記錄
						紙本資料遭竊或遺失	使用傳遞專用公事包及隨身保管公事包、傳遞途中不作停留
						傳遞交付對象錯誤致遺失	確認移交對象，並雙方留存收發記錄
				保管	存放個人櫃/抽屜	不當存取(資料沒有依規定放入個人櫃或抽屜，直接放置於桌上遭外部人員窺視)	保持桌面淨空、紙本文件作業場所遠離外部人員、離席時要將資料收於抽屜中。
						保管資料的文件櫃忘記上鎖遭外部人員竊取致外洩。	文件櫃外部不標示保管文件種類內容、下班後確認文件櫃確實上鎖。
				外部傳送	X	X	X
				刪除	X	X	X
				加工	輸入/編輯	輸入錯誤資料或重複輸入資料	明確輸入/編輯程序，人員訓練、輸入/編輯後再次檢查內容、將輸入/編輯結果列印與電腦輸入/編輯資料對照、按輸入個資的重要性採取重複輸入、交互檢查
						輸入時遭外部人員窺視	個人電腦設置區域遠離外部人員、離席時啟動登出功能、鎖定電腦的螢幕保護程式、按個資重要性限制輸入專用處所、終端機及人員
							限制輸入/編輯作業人員權限，於必要時實施交互檢

建立個人資料保護與管理內部程序

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

按部就班，井然有序，不出錯

個資蒐集處理利用之程序

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

經濟部及所屬機關個人資料保護管理要點

貳、個人資料之蒐集、處理及利用

四、本部及所屬機關蒐集、處理或利用個人資料之特定目的，依個人資料保護法之特定目的及個人資料之類別規定者為限。

五、本部及所屬機關蒐集當事人個人資料時，應明確告知當事人下列事項。但符合本法第八條第二項規定情形之一者，不在此限：

(一)機關或單位名稱。

(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)當事人依本法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，不提供對其權益之影響。

經濟部及所屬機關個人資料保護管理要點

六、本部及所屬機關蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前點第一款至第五款所列事項。但符合本法第九條第二項規定情形之一者，不在此限。

前項之告知，得於首次對當事人為利用時併同為之。

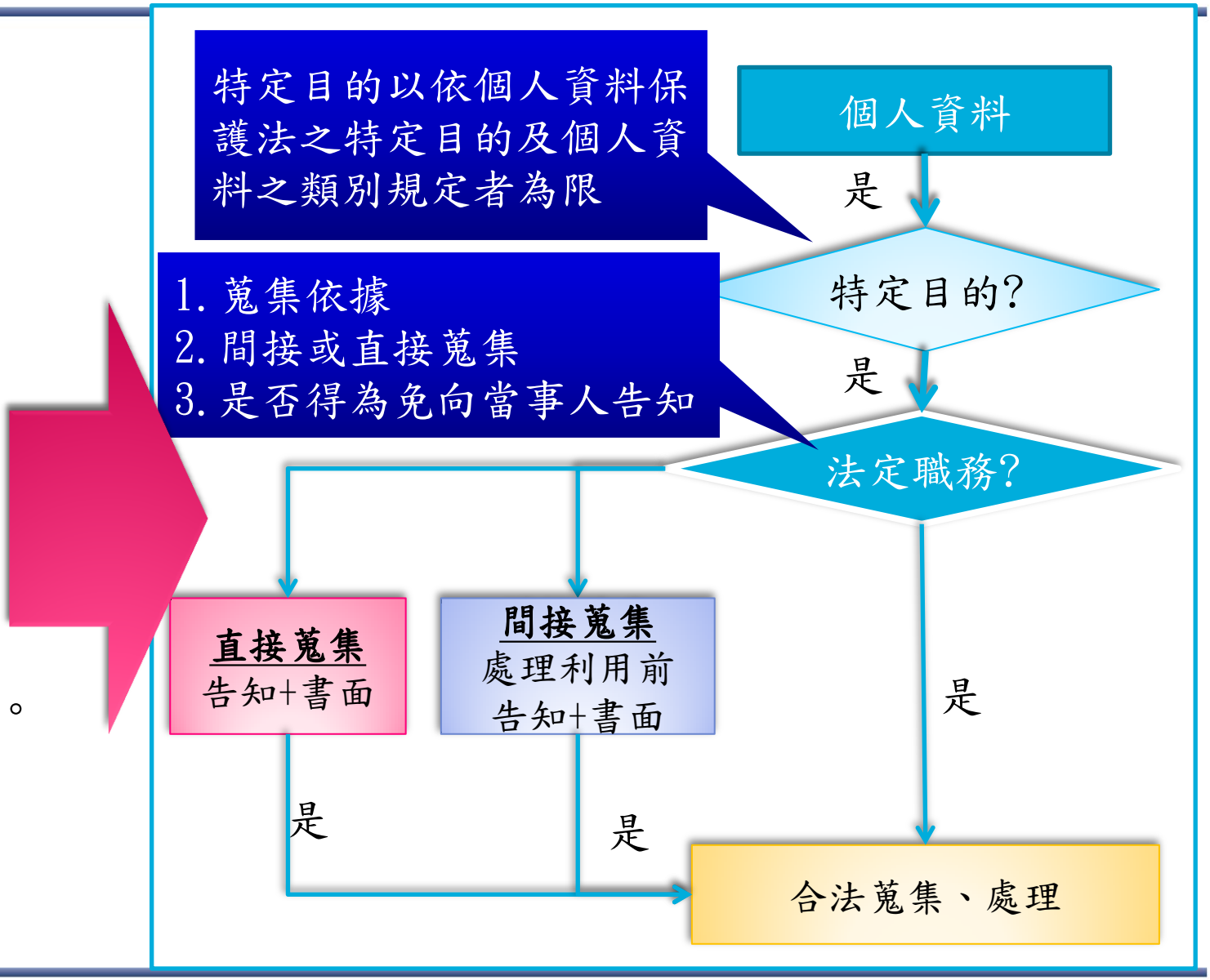
七、本部及所屬機關依本法第十五條第二款及第十六條但書第七款規定經當事人書面同意者，應取得當事人同意書；該同意書作成之方式，依電子簽章法之規定，得以電子文件為之。

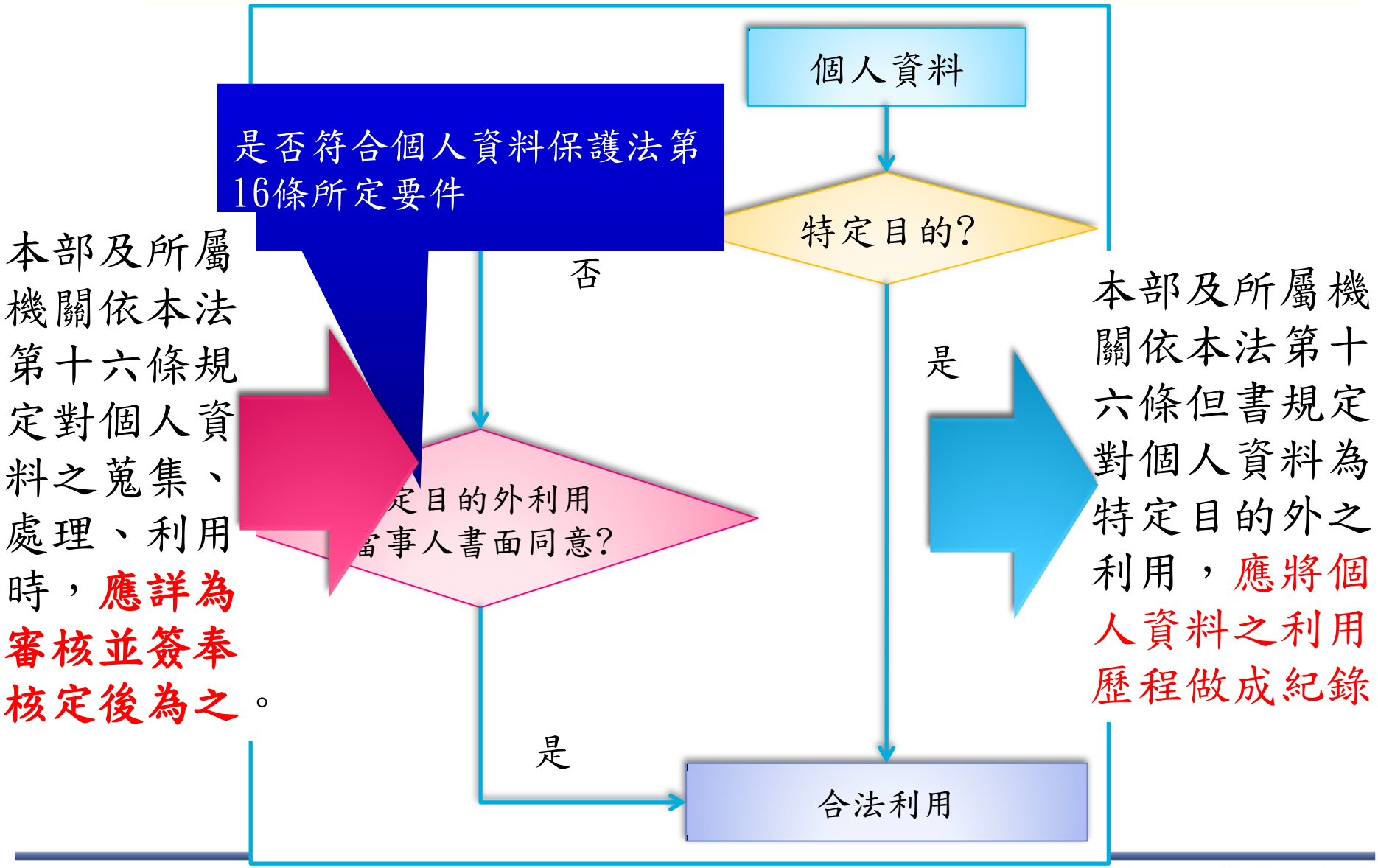
八、本部及所屬機關依本法第十五條或第十六條規定對個人資料之蒐集、處理、利用時，應詳為審核並簽奉核定後為之。

本部及所屬機關依本法第十六條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄。

本部及所屬機關對於個人資料不得為非法之利用，並不得為資料庫之恣意連結，且不得濫用。

本部及所屬機關依本法第十五條規定對個人資料之蒐集、處理、利用時，**應詳為審核並簽奉核定後為之**。





本部及所屬機關依本法第十六條規定對個人資料之蒐集、處理、利用時，**應詳為審核並簽奉核定後為之**。

本部及所屬機關依本法第十六條但書規定對個人資料為特定目的外之利用，應將個人資料之利用歷程做成紀錄

經濟部及所屬機關個人資料保護管理要點

十、本部及所屬機關保有之個人資料正確性有爭議者，應由資料蒐集單位簽奉核定後，移由資料保有單位停止處理或利用該個人資料。但符合本法第十一條第二項但書情形者，不在此限。

個人資料已停止處理或利用者，資料保有單位應確實記錄。

十一、本部及所屬機關保有個人資料蒐集之特定目的消失或期限屆滿時，應由資料蒐集單位簽奉核定後，移由資料保有單位刪除、停止處理或利用。但符合本法第十一條第三項但書情形者，不在此限。

個人資料已刪除、停止處理或利用者，各該單位應確實記錄。

十二、本部及所屬機關依本法第十一條第四項規定應主動或依當事人之請求刪除、停止蒐集、處理或利用個人資料者，應簽奉核定後移由資料保有單位為之。

個人資料已刪除、停止蒐集、處理或利用者，資料保有單位應確實記錄。

簽奉核定

個人資料蒐集單位

- 個人資料正確性有爭議
- 個人資料蒐集之特定目的消失或期限屆滿時
- 依本法第十一條第四項規定應主動或依當事人之請求刪除、停止蒐集、處理或利用個人資料

個人資料保有單位

- 刪除、停止蒐集、處理或利用個人資料

應確實記錄

事故預防通報及應變

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

經濟部及所屬機關個人資料保護管理要點

十三、本部及所屬機關遇有本法第十二條所定個人資料被竊取、洩漏、竄改或其他侵害情事者，經查明後，應由資料外洩單位依本法施行細則第二十二條所定之適當方式儘速通知當事人。

對個人資料本人之通知

二十二、本部及所屬機關遇有個人資料檔案發生遭人惡意破壞毀損、作業不慎等危安事件，或有駭客攻擊等非法入侵情事，導致個資外洩事件時，應進行緊急因應措施，並迅速通報至本部個人資料保護推動執行小組；如屬資訊面之個資外洩事件，應另依經濟部資通安全事件緊急應變計畫及作業處理程序迅速通報至本部資通安全處理小組之資安聯絡人員上網通報至行政院國家資通安全會報緊急應變中心。

內部通報機制

當事人行使權利之處理

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

經濟部及所屬機關個人資料保護管理要點

十四、當事人依本法第十條或第十一條第一項至第四項規定向本部及所屬機關為請求時，應填具申請書，並檢附相關證明文件。

前項書件內容，如有遺漏或欠缺，應通知限期補正。

申請案件有下列情形之一者，應以書面駁回其申請：

(一)申請書件內容有遺漏或欠缺，經通知限期補正，逾期仍未補正。

(二)有本法第十條但書各款情形之一。

(三)有本法第十一條第二項但書或第三項但書所定情形之一。

(四)與法令規定不符。

十五、當事人依本法第十條規定提出之請求，應於十五日內為准駁之決定。

前項之准駁決定，必要時得予延長，延長期間不得逾十五日，並應將其原因以書面通知請求人。

經濟部及所屬機關個人資料保護管理要點

十六、當事人請求查詢、閱覽或製給個人資料複製本者，準用經濟部及所屬機關提供政府資訊收費標準或本部所屬機關另行訂定之相關收費標準收取費用。

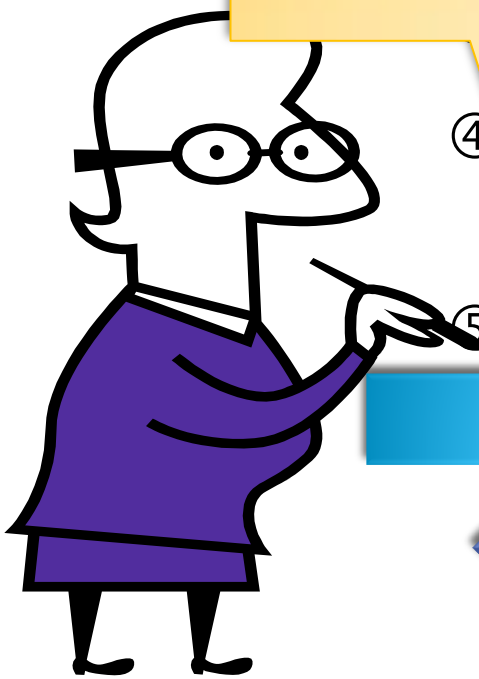
當事人閱覽其個人資料，應由承辦單位派員陪同為之，並依經濟部政府資訊及卷宗閱覽須知或本部所屬機關訂定之相關規定辦理。

十七、當事人依本法第十一條第一項至第四項規定提出之請求，應於三十日內為准駁之決定。

前項之准駁決定，必要時得予延長，延長期間不得逾三十日，並應將其原因以書面通知請求人。

十八、個人資料檔案，其性質特殊或法律另有規定不應公開其檔案名稱者，得依政府資訊公開法或其他法律規定，限制公開或不予提供。

當事人依本法第十條或第十一條第一項至第四項規定向本部及所屬機關為請求時，**應填具申請書，並檢附相關證明文件。**



個人資料本人

④ 止蒐
利用

⑤ 請求刪除

權利行使

准駁之

當事人閱覽其個人資料，應由承辦單位派員陪同為之，並依經濟部政府資訊及卷宗閱覽須知或本部所屬機關訂定之相關規定辦理。

- 查詢、**提供閱覽**、或製給複製本→15日內
- 更正或補充、停止蒐集、處理或利用、刪除→30日

個人資料檔案安全維護

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

經濟部及所屬機關個人資料保護管理要點

十九、為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本部及所屬機關指定之個人資料檔案安全維護專人，應依本要點及相關法令規定辦理個人資料檔案安全維護事項。

二十、個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。

二十一、為強化個人資料檔案之存取安全，防止非法授權存取，維護個人資料之隱私性，本部及所屬機關應將個人資料檔案安全稽核作業，納入公務機密檢查及資訊安全管理稽核機制中辦理之。

二十三、個人資料檔案安全維護工作，除本要點外，並應符合行政院與本部及所屬機關訂定之相關資訊作業安全與機密維護規範。

委外監督管理程序

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

經濟部及所屬機關個人資料保護管理要點

二十四、本部及所屬機關依本法第四條規定委託蒐集、處理或利用個人資料者，適用本要點。

前項委託應為適當之監督，其監督至少應包含下列事項：

(一)預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

(二)受託者就本法施行細則第十二條第二項採取之措施。

(三)有複委託者，其約定之受託者。

(四)受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。

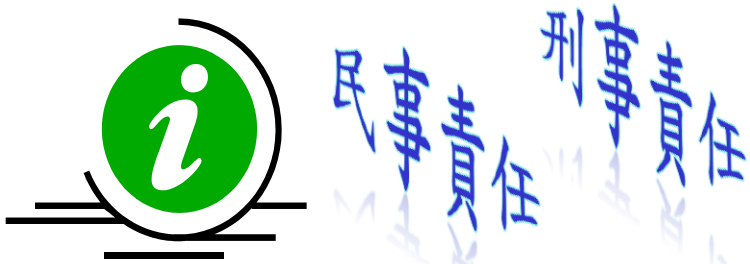
(五)委託機關如對受託者有保留指示者，其保留指示之事項。

(六)委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

前項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

受公務機關或非公務機關委託蒐集、處理、利用個人資料者，於本法適用範圍內視同委託機關。(個資法§4)



高公局委託遠通電收公司代收通行費，遠通電收蒐集當事人之車號及車主姓名資料等，遠通電收有違法蒐集、處理、利用，均由貴局依電腦處理個人資料保護法第27條、第30條規定（個資法第28 條、第31條）負國家賠償責任。

法務部99年8月19日法律決字0999028404號函

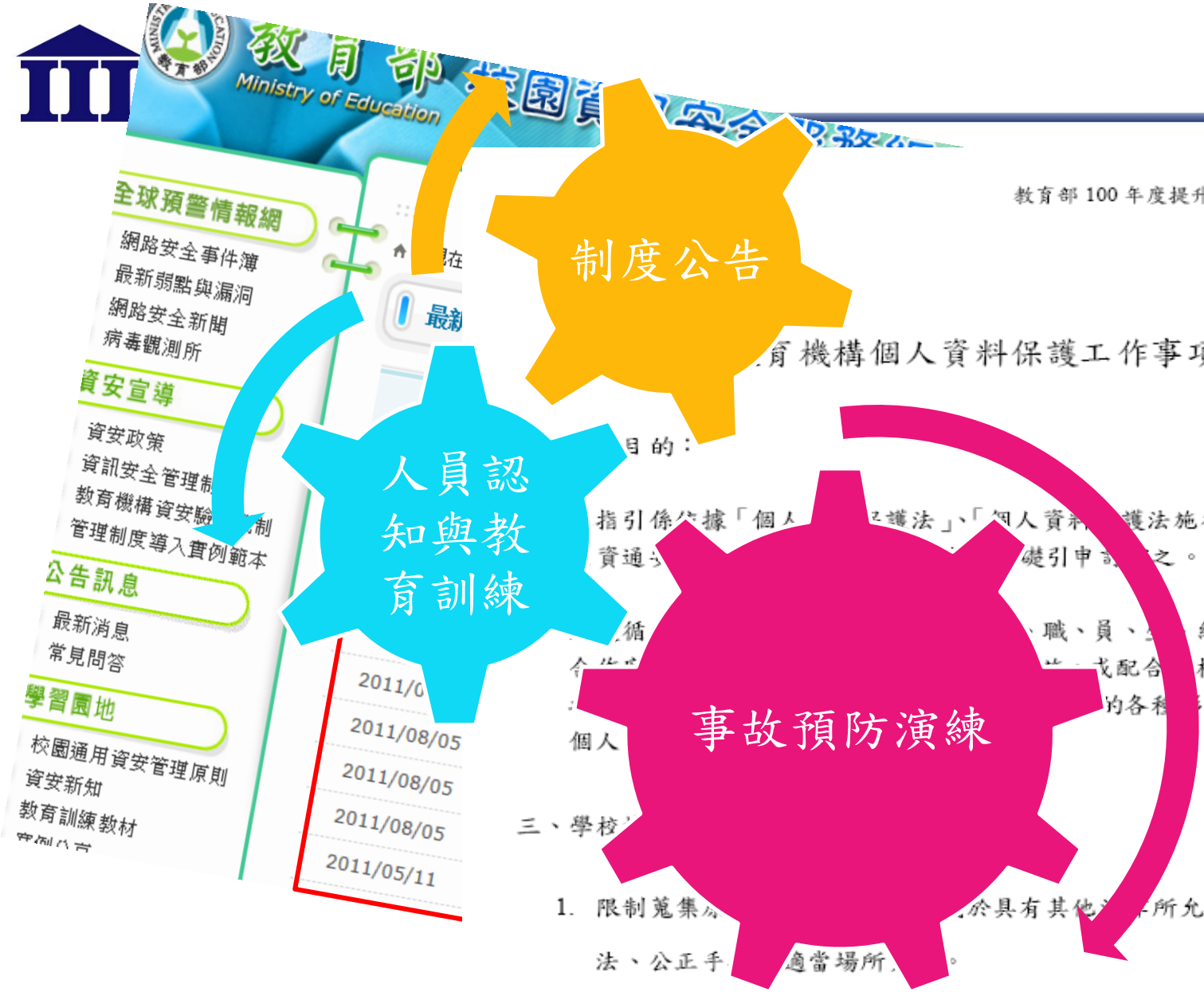
評選合格廠商

合約內容

定期確認

- 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
- 適當安全管理措施
- 有複委託者，其約定之受託人。
- 受託人或其受僱人違反個人資料保護法規或委託契約條款時，應向委託人通知之事項及採行之補救措施。
- 委託人對受託人保留指示之事項
- 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。

實際運作(含預防演練)並實施教育訓練



教育部 100 年度提升校園資訊安全服務計畫

育機構個人資料保護工作事項

目的：

指引係依據「個人 之護法」、「個人資料 護法施行細則」及「教育體 資通 礎引申訂 之。

循 、職、員、 約聘人員及相關委外 戈配合 校所修改或引用適當 的各種 式(含書面或電子)之 個人

三、學校

1. 限制蒐集 於具有其他 所允許之事由時，以合法、公正手 適當場所 。

2. 資料內容原則：符合蒐集個人資料特定目的，並確保資料之正確性、完整

制度檢視&持續改善

個人資料安全維護事項考核

- 考核目的
  - 有效性測量，以確認目標達成度
- 考核時間
  - 定期
  - 不定期
- 考核方式
  - 內部考核(機關內部自行執行考核)
  - 外部考核(由第三人執行考核)
- 考核作業
  - 機關內部考核監督作業
  - 委外作業考核監督作業

考核範圍	考核規劃	考核執行	改善措施與追蹤
考核目的	研擬考核計畫	書面審核	預防矯正措施
考核對象	研擬考核檢核表	實地審核	追蹤改善情況

案由：

某國中發現該校兩名學生一年多以 並利用晨間6:30到7:10空檔，使用辦公 校學生詳細個資，及全校教職員 系統，竄改學籍資料與成績

事件說明：

雖然電腦有設立帳 遭到有心人士破解；機密 竊而導 外洩。

稽核項目：

1. 是否定期備份→備份記錄
2. 電腦存取是否設定權限→權限設定表
3. 檔案是否加密？
4. 個人資料檔案是否由專人保管？
5. 是否有門禁出入管制機制？

：

政業務資料應養成備份習慣，避免造成資料永久遺失。

記型電腦、行動碟等儲存設備因攜帶方便、容易遺失，應設定密碼或資料加密，並儘可能避免存放機密公務資料，並妥善保管。

公處所應加強門禁管制，設備遭竊應立即向所轄派出所報案。

資料來源：教育部資訊安全資安事件案例宣導

- 本簡報之智慧財產權歸屬於資訊工業策進會或講師所有，未經授權不得翻印、轉載或以任何方式重製
- 本簡報之內容不構成任何實質法律意見，如您有任何法律諮詢服務需求，請不吝與敝單位聯絡 jolieliao@iii.org.tw