

計畫編號: NCC-Y109-006

109 年委託研究報告

109 年度通訊傳播事業導入隱私保護
管理機制與資料加值服務之
研析委託研究
期末報告
(匿名版一下冊)

計畫委託機關：國家通訊傳播委員會

中華民國 109 年 12 月

計畫編號: NCC-Y109-006

109 年委託研究報告

PG10904-0134

109 年度通訊傳播事業導入隱私保護
管理機制與資料增值服務之
研析委託研究
期末報告

受委託單位

財團法人資訊工業策進會

計畫主持人

顧振豪

共同主持人 協同主持人

葉奇鑫 陳志宇

研究人員

宋佩珊、李沛宸、孫鈺婷、張腕純、劉純妤、

范晏儒、劉芷宜、許嘉芳、周芷瑄

本報告不必然代表國家通訊傳播委員會意見

中華民國 109 年 12 月

目次

目次	I
附錄（下冊）	379
附錄 1：通傳會處理通傳事業個資案例參考手冊	379
附錄 2：通傳產業個人資料保護與管理實作指引手冊	459
附錄 3：通傳產業個人資料保護與管理實作指引手冊領取名 單（略）	542
附錄 4：研討會會議手冊	542
參考書目	612
中文參考資源	612
外文參考資源	612



通傳事業個資案例參考手冊

國家通訊傳播委員會
109 年 12 月



目錄

第 1 篇.....	1
個人資料定義	1
A. 相關法規	2
B. 案例解析	3
1. 各電信業者將使用 VoLTE 服務之客戶電信號碼，提供予第三方設 置之資料庫，於《個資法》之相關規定為何？	3
2. 電信業者所有之用戶 IMEI 或 IMSI 是否為個人資料？	5
3. 電信業者寄發電信帳單時，是否應將客戶個人資料去識別化？	7
4. 在防疫期間，電信門市是否可量測來客之體溫？	9
第 2 篇.....	11
必要範圍	11
A. 相關法規	12
B. 案例解析	13
1. 為了防疫目的，傳播事業是否可調查員工之旅遊史、接觸史？ ..	13
2. 中央流行疫情指揮中心以「類細胞簡訊」技術發送簡訊至特定手機 （例如磐石艦確診案例足跡提醒簡訊），是否符合《個資法》規 範？	15
3. 消費者於申辦電信門號前，想要知道未來提前解約時應返還之補貼 款數額，電信業者便要求消費者先提供姓名、生日、身分證字號及 雙證件影本等個人資料才能查詢，是否符合《個資法》規範？ ..	17
4. 電信業者主張「○六七信用卡、現金卡、轉帳卡或電子票證業 務」、「一〇七採購與供應管理」、「○八五旅外國人急難救 助」、「一二七募款」為特定目的而蒐集電信服務客戶之個人資 料，是否符合《個資法》規範？	19
第 3 篇.....	21
特定目的外利用	21

A. 相關法規	22
B. 案例解析	23
1. 電信業者可否將國防部提供之應受教育召集人員身分證字號，與客戶的個人資料進行比對後代為發送教召之相關簡訊？	23
2. 電信公司能否為協助自殺個案處置（安心專案）提供衛生福利部來電自動顯示號碼呢？	25
3. 財政部為辦理電子發票中獎事宜，函請電信業者查詢並提供使用者資料，是否符合《個資法》？	27
4. 客服人員因與來電客戶發生爭執，竟將客戶的行動電話號碼於比價優惠網站上公開，請問該客服人員之行為有無違反《個資法》？雇主於《個資法》上有何責任？	29
5. 電信公司受保險公司委託，發送生日優惠權益簡訊予行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，請問電信公司有無違反《個資法》？	32
6. 電信業者接獲客戶對某通訊行之申訴後，將載有客戶個資之申訴單轉傳給與執行申訴業務無關之通訊行人員，是否違反《個資法》？	34
第 4 篇	36
委外監督	36
A. 相關法規	37
B. 案例解析	38
1. 有線電視業者將其申裝契約置於通路商門市供訂戶簽約，並蒐集個人資料，於《個資法》上之適用為何？	38
2. 傳播事業可否將客戶個人資料提供給印刷廠印製帳單？如何辦理委外監督？	40
3. 電信業者將客戶個人資料提供予資產管理公司催收欠費，是否違反《個資法》？	42

第 5 篇.....	44
告知義務.....	44
A. 相關法規.....	45
B. 案例解析.....	46
1. 通傳業者於向當事人蒐集個人資料時應如何向其履行告知義務呢？	46
2. A 有線電視業者在官方網站提供「留言版」功能，並將「姓名」、「電話」、「地址」等欄位加註*號，為留言者必填欄位。A 業者應如何確保「蒐集」個資行為符合《個資法》規範？.....	47
3. 通傳業者員工於電話中蒐集首次申辦服務的客戶之個人資料，是否應踐行《個資法》規定的告知義務，向該客戶揭露業者蒐集個資的目的、利用個資的方式、當事人權利及其他法定應告知資訊？如何執行？.....	49
第 6 篇.....	51
當事人權利.....	51
A. 相關法規.....	52
B. 案例解析.....	53
1. 電信業者未經客戶同意將電話內容錄音，有無違反《個資法》？客戶得否請求刪除之？.....	53
2. 通傳業者將與當事人之對話錄音，當事人得否請求閱覽或複製該錄音？.....	55
第 7 篇.....	56
安全維護.....	56
A. 相關法規.....	57
B. 案例解析.....	58
1. 防疫期間，傳播事業如何確保遠距工作之資訊安全？.....	58

2. 電信業者員工違反公司資安規定，以未經公司核准之隨身碟存取公司電腦中的客戶個人資料，若因此發生個資侵害事故（例如使電腦中毒致客戶資料遭駭，或隨身碟遺失致客戶資料遭竊取），該電信業者是否違反《個資法》？	60
3. 電信業者員工違反公司規定，於公司電腦安裝即時通訊軟體，傳送客戶雙證件影本等個人資料，致個資侵害事故發生（如不慎誤傳予友人導致客戶個資外洩），該電信業者是否違反《個資法》？ ..	61
第 8 篇.....	62
事故通報.....	62
A. 相關法規	63
B. 案例解析	64
1. 傳播事業如遇個人資料外洩等個資事故，是否應通報個資當事人或主管機關？	64
第 9 篇.....	66
屆期刪除.....	66
A. 相關法規	67
B. 案例解析	68
1. 客戶於電信公司網路門市申請攜碼後又取消，電信公司應如何處理該客戶之個人資料始符合《個資法》規範？	68
2. 電信公司未將已離職員工之個人資料（聯絡方式）自工作群組移除，仍繼續寄送工作訊息給已離職員工，有無違反《個資法》？	69
3. 通傳業者若將已終止服務契約之客戶資料永久保存，是否違反《個資法》？	69



第 1 篇

個人資料定義



A. 相關法規

◆ 個人資料保護法

第 2 條第 1 項：「本法用詞，定義如下：

- 一、個人資料：指自然人之姓名、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、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、社會活動及其他得以直接或間接方式識別該個人之資料。
- 二、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。
- 三、蒐集：指以任何方式取得個人資料。
- 四、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。
- 五、利用：指將蒐集之個人資料為處理以外之使用。
- 六、國際傳輸：指將個人資料作跨國（境）之處理或利用。
- 七、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。
- 八、非公務機關：指前款以外之自然人、法人或其他團體。
- 九、當事人：指個人資料之本人。」

◆ 個人資料保護法施行細則

第 3 條：「本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」

B. 案例解析

— 案例 1 —

問題

各電信業者將使用 VoLTE 服務之客戶電信號碼，提供予第三方設置之資料庫，於《個資法》之相關規定為何？

解答

- 一、電信業者將使用 VoLTE 服務之手機號碼提供予第三方設置資料庫，依照《個資法》第 2 條第 1 款規定，雖然該手機號碼乍看之下只是一連串數字，但與其他資料互相比對後，仍然能連結識別出特定個人，因此手機號碼屬於個人資料。
- 二、設置第三方資料庫，是為了因應電信業者提供客戶 VoLTE 語音直連服務的需要，而由電信業者提供手機號碼給第三方成立資料庫，由此可知，電信業者提供前述資料之目的應該與當初蒐集個資之特定目的相符，不屬於特定目的外之利用，因此電信業者無需再另外取得當事人同意。
- 三、倘若未來主管機關直接明訂電信業者應設置集中式查詢資料庫之相關規定時，則電信業者可依據相關規定提供上述資料予第三方。

說明

- 一、電信業者將使用 VoLTE 服務之手機號碼提供予第三方設置資料庫，依照《個資法》第 2 條第 1 款規定，雖然該手機號碼乍看之下只是一連串的數字，但與電信業者所持有的其他資料互相勾稽比對後，即可連結識別出特定個人，此人自得藉由行動電話號碼由群體中予以區別，因此該資料在群體中顯然對於某特定人具有專屬性、獨特性，可以直接或間接識別特定人，應屬個人資料（參照臺灣高等法院臺南分院 105 年度上易字第 393 號刑事判決意旨，但也有法院採不同見解）。
- 二、前述第三方資料庫的設置，是為了因應電信業者提供 VoLTE 語音直連服務的需要，因此由電信業者提供手機號碼給第三方成立資料庫，由此可知，電信

業者提供前述資料之目的應與當初蒐集個人資料之特定目的（代號一三三，經營電信業務與電信增值網路業務）相符，不屬於特定目的外之利用，故無需再依照《個資法》第 20 條第 1 項但書第 6 款規定取得當事人同意。

三、如前所述，由電信業者提供手機號碼予第三方成立資料庫，符合蒐集個資之特定目的，倘若未來主管機關所掌法規，直接明訂電信業者應設置集中式查詢資料庫之相關規定時，電信業者便可依照相關規定提供前述資料予第三方。

個資法 §2

個資法 §20

— 案例 2 —

問題

電信業者所有之用戶 IMEI 或 IMSI 是否為個人資料？

解答

我國《個資法》就 IMEI 或 IMSI 等資料是否屬於個人資料，至今尚無明確規範，實務上亦無相關函釋或法院判決就此表達明確見解，如參考英國 ICO 的意見（詳如說明），因 IMEI 及 IMSI 等網路上識別碼再結合其他資料，即有可能可識別出特定人，故 IMEI、IMSI 等資料可能被認定為個資，不過，IMEI 及 IMSI 等資料於我國是否屬個人資料而適用《個資法》，仍應該以我國主管機關意見為準。

說明

- 一、按《個資法》第 2 條第 1 款規定：「個人資料指自然人之姓名、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、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、社會活動及其他得以直接或間接方式識別該個人之資料」。另外，《個資法施行細則》第 3 條規定：「本法第 2 條第 1 款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」。
- 二、由此可知，《個資法》所稱個人資料，包括得以直接或間接方式識別該特定個人之資料。至於所保有之資料，是否可以直接或間接方式識別特定個人，須從蒐集者本身綜合各種情況與事證判斷，沒有一致的標準，因此應依不同個案分別審查、認定，不能僅依單一資料的類型判斷是否為《個資法》所稱之個人資料（參照法務部 103 年 6 月 17 日法律決字第 10303506500 號函釋意旨）。
- 三、如所保有之資料與其他資料對照、組合、連結而得以識別特定個人，仍屬《個資法》所稱得以間接方式識別個人資料；而該資料經如加工處理後，已

無從直接或間接識別此人，自然不屬於《個資法》適用範圍（參照法務部 107 年 04 月 26 日法律字第 10703505830 號函釋意旨）。

- 四、電信業者所有之用戶 IMEI (International Mobile Equipment Identity) 及 IMSI (International Mobile Subscriber Identity) 等資料，依前述法律規定及函釋見解，如與電信業者所保有之其他資料對照、組合、連結，而進一步得以識別特定個人，即屬《個資法》所稱得以間接方式識別之個人資料；但該等資料若經加工處理，已經無從直接或間接識別此人，則不屬於個人資料，不適用《個資法》。不過，因為我國《個資法》目前針對 IMEI 或 IMSI 等資料是否屬個人資料一事，尚未有明確規範，實務上主管機關也沒有發布相關函釋，法院亦未就此議題表達見解，因此本議題須參考國外相關見解。
- 五、英國資訊委員會辦公室 (ICO) 曾於「給應用程式開發者的行動裝置應用程式指引」 (Privacy in mobile apps Guidance for app developers) 第 3 頁中指出，個資的定義並不僅侷限於傳統的識別方式 (例如：人名或人臉照片等)，最好的例子就是獨特的裝置識別碼 (如 IMEI)，即便 IMEI 並未顯示出個人名稱，但以此序號仍然可比對出不同的個人資料，因此當事人使用之行動裝置資訊 (如 IMEI) 等網路上識別碼，應屬於個人資料的範圍，故 IMEI 及 IMIS 於歐盟應已被認定屬於個人資料¹。
- 六、綜合以上所述，雖然我國《個資法》、法院判決、函釋等目前沒有就 IMEI 及 IMSI 等資料是否屬於個人資料一事表示明確見解，但參照前述 ICO 之意見，因 IMEI 及 IMSI 等網路上識別碼再結合其他資料，即有可能可識別出特定人，故 IMEI、IMSI 等資料可能被認定為個資。不過，IMEI 及 IMSI 等資料在我國是否屬個人資料而適用《個資法》，仍應該以我國主管機關之意見為準。

個資法 §2

個資法施行細則 §3

¹參考網址：<https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf>。

— 案例 3 —

問題

電信業者寄發電信帳單時，是否應將客戶個人資料去識別化？

解答

- 一、電信帳單包含用戶之姓名、地址、號碼、費用（可供評估財務狀況），如含通話明細時，亦包含受話號碼（可能識別受話對象）、通話時間等，與用戶的社會活動相關。按《個資法》第 2 條定義如下：「自然人之姓名、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、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務狀況、社會活動及其他得以直接或間接方式識別該個人之資料」，可見姓名及聯絡方式皆屬個資之範圍。
- 二、主管機關目前尚未要求電信業者應將電信帳單內的用戶個人資料去識別化，不過，雖然將用戶自己的個人資料提供給用戶本人並無違反《個資法》，但若電信帳單遺失或不慎寄錯時，對用戶（當事人）仍然存有個資外洩甚至遭濫用的風險。如屬電信業者過失，即可能需依《個資法》第 29 條規定負損害賠償責任。因此，為確保客戶個人資料安全並降低業者自身風險，電信業者可參考金融業的作法，若電信帳單由系統自動帶入客戶個人資料時，可考慮將個人資料顯示欄位以去識別化處理。

說明

- 一、電信帳單包含用戶之姓名、地址、號碼、費用（可供評估財務狀況），如含通話明細，則亦包含受話號碼（可能識別受話對象）、通話時間等，與用戶的社會活動相關。按《個資法》第 2 條規定：「自然人之姓名、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、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務狀況、社會活動及其他得以直接或間接方式識別該個人之資料」，可見姓名及聯絡方式皆屬個資之範圍。

- 二、又《個資法施行細則》第 17 條，就「無從識別特定當事人」的作法，提出進一步說明：「個人資料以代碼、匿名、隱藏部分資料或以其他方式，無從辨識該特定個人」。
- 三、至於電信業者是否應該將電信帳單中將客戶個資去識別化，主管機關目前尚無明確規範，實務上也沒有相關函釋或法院判決就此表達明確見解。但若電信帳單遺失或不慎錯寄時，對用戶（當事人）仍存有個資外洩甚至遭濫用的風險。依照《個資法》第 29 條規定，若電信公司違反《個資法》規定，導致他人個資外洩，須負損害賠償責任。
- 四、實務上，金融業者提供客戶線上服務時，如果是系統自動帶入既有客戶個人資料時，則規定其個資顯示欄位應以隱碼處理（參考金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第 10 條第 1 項第 2 款、金融監督管理委員會 104 年 7 月 22 日金管銀合字第 10400156260 號書函）。因此，電信業者於寄發帳單時未將用戶個資去識別化，不會違反《個資法》，但是，為了降低業者自身法律風險及用戶個資外洩風險，仍建議電信業者可以參考金融業的實務做法，當電信帳單是由系統自動帶入客戶個人資料時，可考慮將其個人資料顯示欄位以去識別化處理。

個資法 §2

個資法 §29

個資法施行細則 §17

金融監督管理委員會指定非公務機關個人資料檔案
安全維護辦法 §10

— 案例 4 —

問題

在防疫期間，電信門市是否可量測來客之體溫？

解答

電信門市在防疫期間量測體溫為蒐集一般個人資料之行為，為維護員工及其他來客之健康安全，符合《個資法》第 19 條第 1 項第 5 款「經當事人同意」或第 6 款「為增進公共利益所必要」等要件，故電信門市可量測來客體溫。

說明

一、體溫是一般個人資料，非特種個資

電信門市量測來客體溫所蒐集的資料，並非依照《個資法施行細則》第 4 條第 5 項規定由醫事人員「以醫療行為施以檢查所產生之資料」，由此可知體溫不屬於《個資法》第 6 條規定之「特種個資」，而是一般個人資料。

二、量測體溫屬蒐集個人資料之行為

量測體溫但不做成紀錄，是否屬於《個資法》第 2 條第 3 款規定「以任何方式取得個人資料」之「蒐集」行為，或有爭議。其他國家之個資保護主管機關如英國 ICO、瑞士 FDPIC、法國 CNIL、比利時 DPA 等，於討論防疫措施之個資保護事宜時，均認定「量測體溫或詢問身體症狀」是蒐集個人資料，故本文亦認為量測體溫是屬於蒐集個人資料之行為。

三、量測來客體溫可能「經當事人同意」或屬「為增進公共利益所必要」，符合《個資法》規範

在防疫的迫切需求下，由於發燒為罹患新冠肺炎的症狀之一，而新冠病毒又具有極強大的傳染力，因此，為維護員工或是其他來客的健康安全，電信門市可能會先詢問來客意願再測量體溫，此為《個資法》第 19 條第 1 項第 5 款規定「經當事人同意」；若電信門市採用紅外線自動體溫量測儀，雖未經當事人同意，但可認為電信門市是以《個資法》第 19 條第 1 項第 6 款規定「為增進公共利益所必要」作為蒐集體溫資料的法律依據。

四、此外，中央流行疫情指揮中心於 109 年 5 月發布「實聯制措施指引」，為兼顧個資保護與疫調需求，電信門市如基於防疫目的蒐集民眾個人資料，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，並應指定專人辦理、善盡資料保護責任，資料最多存放 28 天，之後必須刪除或銷毀等。詳情請參閱衛生福利部疾病管制署網址：<https://www.cdc.gov.tw/Bulletin/Detail/h4JHDHTxkceidB1NzV9EKA?typeid=9>。

個資法 §2

個資法 §6

個資法施行細則 §4

第 2 篇

必要範圍



A. 相關法規

◆ 個人資料保護法

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 15 條：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」

B. 案例解析

— 案例 1 —

問題

為了防疫目的，傳播事業是否可調查員工之旅遊史、接觸史？

解答

為了防疫目的，傳播事業調查員工之旅遊史、接觸史等個人資料，符合《個資法》第 19 條第 1 項第 1 款或第 6 款之要件，且該調查仍應受《個資法》第 5 條必要範圍原則之限制。

說明

一、旅遊史或接觸史是個人資料

依照《個資法》第 2 條第 1 項規定，旅遊史或接觸史涉及員工的社會活動與家庭、社會關係，屬於員工的個人資料。傳播事業調查員工的旅遊史、接觸史，即是蒐集、處理個人資料的行為。

二、調查員工之旅遊史、接觸史，符合《個資法》第 19 條第 1 項第 1 款或第 6 款之要件

- (一) 傳播事業調查員工之旅遊史、接觸史，其法律依據為勞動部職業安全衛生署按《職業安全衛生法》第 6 條第 3 項授權之《職業安全衛生設施規則》所發布的「因應嚴重特殊傳染性肺炎（武漢肺炎）職場安全衛生防護措施指引」第四點規定：「二、勞工應做好自我管理，保持手部清潔消毒，落實使用肥皂勤洗手、呼吸道衛生與咳嗽禮節、遵守社交禮節及保持社交距離，避免前往列為國際旅遊疫情建議等級第三級之地區旅遊、避免接觸野生動物。」
- (二) 若出現發燒、咳嗽等身體不適，請速就醫，告知醫師旅遊史、職業史、接觸史及是否群聚，並主動告知雇主及配合各項防疫管制措施。」由此可知，傳播事業調查員工的旅遊史或接觸史，可能符合《個資法》第 19 條第 1 項第 1 款「法律明文規定」之要件。

(三) 不過，有論者認為，勞動部職業安全衛生署所發布的「因應嚴重特殊傳染性肺炎（武漢肺炎）職場安全衛生防護措施指引」是行政指導，不是法律授權之法規命令，並不符合《個資法》第 19 條第 1 項第 1 款「法律明文規定」之要件，但調查員工的旅遊史或接觸史，可幫助傳播事業掌握工作場所的潛在病毒傳染風險，亦可據以判斷該員工是否違反居家隔離或居家檢疫的規定，對所有員工甚至是訪客的健康安全均有所助益，亦符合《個資法》第 19 條第 1 項第 6 款「為增進公共利益所必要」之要件。

三、調查員工之旅遊史、接觸史應受《個資法》第 5 條「必要範圍」的限制

此外，傳播事業調查員工的旅遊史或接觸史，仍應受《個資法》第 5 條「必要範圍」的限制，例如：中央流行疫情指揮中心曾於 4 月時公告建議「清明連假期間曾前往特定 11 處人潮擁擠景點旅遊之民眾」應進行 14 天的自主健康管理，傳播事業欲調查員工旅遊史時，僅需確認員工「有無」前往經指揮中心公告之特定景點旅遊，即可安排員工遠距工作，而無須再進一步詢問其同行旅客的年籍等個人資料，如此便能符合《個資法》第 5 條「必要範圍」之規定。

個資法 §2

個資法 §5

個資法 §19

職業安全衛生設施規則 §4

— 案例 2 —

問題

中央流行疫情指揮中心以「類細胞簡訊」技術發送簡訊至特定手機（例如磐石艦確診案例足跡提醒簡訊），是否符合《個資法》規範？

解答

衛福部成立的中央流行疫情指揮中心以「類細胞簡訊」技術發送確診案例足跡提醒簡訊，是以「確診者停留點的周遭基地台」為基礎，請電信業者提供曾在同一時間和該基地台交換過訊號的手機號碼，以一般簡訊方式傳送警示訊息，此為執行衛福部的法定職務「預防或控制傳染病疫情的發生或蔓延」所須，沒有逾越必要範圍。因此，中央流行疫情指揮中心蒐集、處理個資的行為符合《個資法》第 15 條第 1 款「執行法定職務必要範圍內」規定，利用個資的行為亦符合同法第 16 條本文「於執行法定職務必要範圍內為之並與蒐集之特定目的相符」規定。

說明

一、行動電話號碼及位置資訊為個人資料。

- (一) 行動電話號碼本身雖僅是一串數字組合，並無特定識別性，但與其他個人資料如姓名、國民身分證統一編號、特徵及其他社會活動資料相互比對、組合、連結及勾稽，即得以間接方式識別特定個人（臺灣臺北地方法院 103 年度北小字第 1360 號民事判決意旨參照），因此依照《個資法》第 2 條及《個資法之特定目的及個人資料之類別》規定，行動電話號碼為 C001 識別類之個人資料²。
- (二) 雖然「位置資訊」未明列於我國《個資法》第 2 條或法務部公告的《個資法之特定目的及個人資料之類別》之類別內，法院在實務上亦尚未對此表示意見，但若藉由「位置資訊」（足跡）與其他資料進行連結、交叉、對比，而可能得以間接識別特定人，再參照歐盟 GDPR 第 4 條第 1 款規定，亦明訂位

² 詳可參照國家發展委員會網站：https://www.ndc.gov.tw/Content_List.aspx?n=F98A8C27A0F54C30。

置資訊 (location data) 是個人資料，故本文認為位置資訊屬於《個資法》第 2 條規定之個人資料。

二、中央流行疫情指揮中心蒐集、處理及利用民眾行動電話號碼及位置資訊為執行法定職務之必要行為。

(一) 中央流行疫情指揮中心由衛生福利部成立，無論依《傳染病防治法》或為本次新冠肺炎制定的《嚴重特殊傳染性肺炎防治及紓困振興特別條例》規定，「預防或控制傳染病疫情的發生或蔓延」都當然屬於衛福部的法定職務³。

(二) 在題示情形中，衛福部中央流行疫情指揮中心取得民眾的行動電話號碼及位置資訊以發送足跡通知簡訊，提醒民眾留意自身健康狀況，此手段有助於達成防疫目的（適當性）；而發送簡訊是目前最快速、有效的提醒方式，僅取得行動電話號碼（不包含民眾其他個資如姓名、通訊地址等）與位置資訊（辨別需否發送提醒簡訊），是對民眾侵害程度最小之手段（必要性），且所追求防疫控制的重要性與發送簡訊之手段間也符合比例原則（衡平性）。

(三) 因此，衛福部中央流行疫情指揮中心採用「類細胞簡訊」技術，向特定時間經過特定區域的民眾發送足跡提醒簡訊，其蒐集、處理個資的行為符合《個資法》第 15 條第 1 款「執行法定職務必要範圍內」，利用個資的行為符合同法第 16 條本文「於執行法定職務必要範圍內為之，並與蒐集之特定目的相符」等規定。

個資法 §5

個資法 §15

個資法 §16

個資法 §19

³ 例如《傳染病防治法》第 7 條「主管機關應實施各項調查及有效預防措施，以防止傳染病發生；傳染病已發生或流行時，應儘速控制，防止其蔓延」，或《嚴重特殊傳染性肺炎防治及紓困振興特別條例》第 7 條「中央流行疫情指揮中心指揮官為防治控制疫情需要，得實施必要之應變處置或措施」。

— 案例 3 —

問題

消費者於申辦電信門號前，想要知道未來提前解約時應返還之補貼款數額，電信業者便要求消費者先提供姓名、生日、身分證字號及雙證件影本等個人資料才能查詢，是否符合《個資法》規範？

解答

消費者於申辦電信門號前，想要知道未來提前解約時應返還業者之補貼款金額，但電信業者要求先提供姓名、生日、身分證字號及雙證件影本等個人資料才能查詢，顯然已逾越提供查詢所需之必要範圍，與《個資法》第 5 條規定之比例原則不符。

說明

- 一、《個資法》第 19 條第 1 項規定，非公務機關對個人資料之蒐集或處理應有特定目的，應符合「與當事人有契約或類似契約之關係，且已採取適當之安全措施」等情形⁴。
- 二、消費者與電信業者間申辦電信門號程序尚未完成時，雙方顯然未成立契約關係，但兩者間是否成立前述「類似契約關係」，應依照《個資法施行細則》第 27 條規定來判斷是否符合「契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為」或「契約因無效、撤銷、解除、終止而消滅或履行完成時，為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為」等情形⁵，而使業者得以蒐集、處理消費者之個資。

⁴ 《個資法》第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、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。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

⁵ 《個資法施行細則》第 27 條：「本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。本法第十九條第一項第

- 三、另依照《個資法》第 5 條規定，個資之蒐集、處理或利用，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⁶。故電信業者蒐集、處理或利用個資之行為，即使符合《個資法》規定，仍應留意「比例原則」之要求，不得逾越特定目的之必要範圍。
- 四、題示情形中，如消費者想要知道未來提前解約時應返還業者之補貼款金額，電信業者即要求消費者先提供姓名、生日、身分證字號及雙證件影本等詳細個資，才協助查詢，而未提供前述個人資料，就無從得知應返還之金額，此時業者蒐集消費者個資之範圍，顯然已逾越提供查詢所需之必要範圍，與《個資法》第 5 條規定之比例原則不符⁷。

個資法 §5

個資法 §19

個資法施行細則 §27

二款所稱類似契約之關係，指下列情形之一者：一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。」

⁶ 《個資法》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。」

⁷ 法務部 106 年 08 月 24 日法律字第 10603511520 號函釋參照。

— 案例 4 —

問題

電信業者主張「○六七信用卡、現金卡、轉帳卡或電子票證業務」、「一〇七採購與供應管理」、「○八五旅外國人急難救助」、「一二七募款」為特定目的而蒐集電信服務客戶之個人資料，是否符合《個資法》規範？

解答

題旨所示「○六七信用卡、現金卡、轉帳卡或電子票證業務」、「一〇七採購與供應管理」、「○八五旅外國人急難救助」、「一二七募款」等目的似與電信業者提供客戶電信服務之契約無關，可能構成過度蒐集個人資料違反《個資法》第 5 條規定。

說明

- 一、依《個資法》第 5 條規定：「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。」
- 二、電信業者為了提供客戶電信服務，與客戶成立電信服務契約，以《個資法》第 19 條第 1 項第 2 款的「與當事人有契約或類似契約之關係，且已採取適當之安全措施」作為蒐集個資的法律依據，依此契約關係作為蒐集客戶個人資料之特定目的，所蒐集之個資即不應逾越電信業者履行電信服務契約之範圍。
- 三、但題旨所述的「○六七信用卡、現金卡、轉帳卡或電子票證業務」、「一〇七採購與供應管理」、「○八五旅外國人急難救助」、「一二七募款」等，雖然屬於法務部訂定《個資法之特定目的及個人資料之類別》之特定目的，實務上常見記載於電信業者的隱私權政策中，但這些特定目的均與電信業者履行電信服務契約無正當合理之關聯。

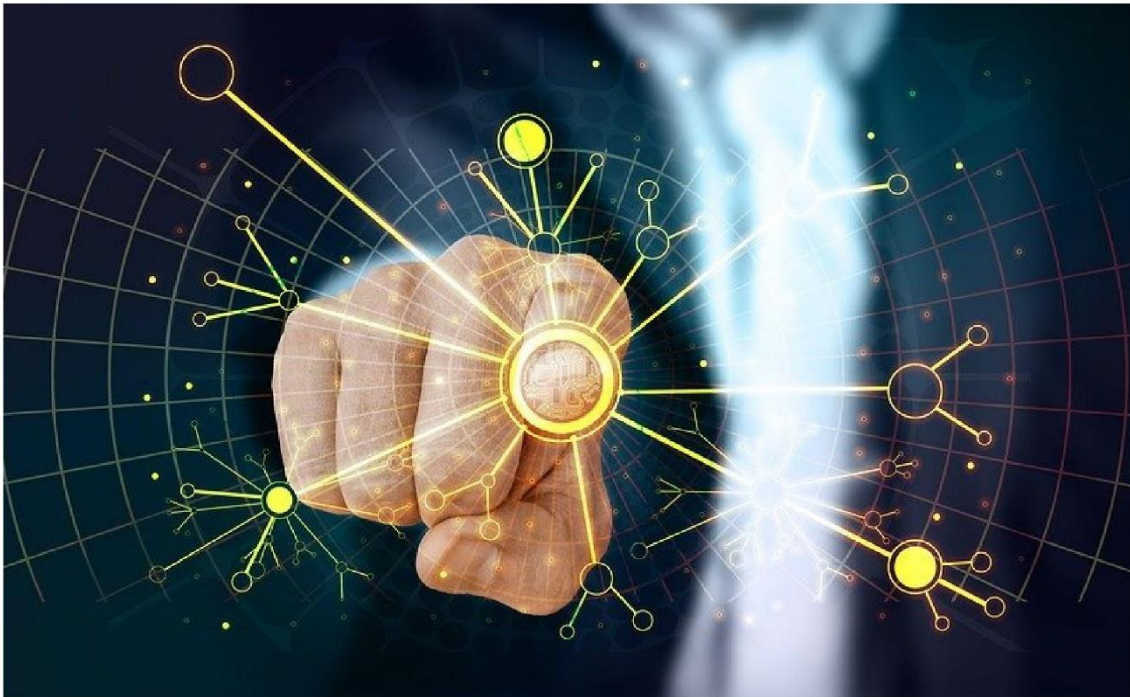
四、因此，電信業者主張上述特定目的而蒐集客戶之個人資料，因與履行電信服務契約無關，電信業者可能會因此過度蒐集個資，不符合比例原則，違反《個資法》第 5 條規定。

個資法 §5

個資法 §19

第 3 篇

特定目的外利用



A. 相關法規

◆ 個人資料保護法

第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，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是別特定之當事人。
- 六、經當事人同意。
- 七、有利於當事人權益。」

B. 案例解析

— 案例 1 —

問題

電信業者可否將國防部提供之應受教育召集人員身分證字號，與客戶的個人資料進行比對後代為發送教召之相關簡訊？

解答

- 一、教育召集是國防部所職掌的法定職務之一，因此國防部利用應受教召人員的身分證字號之行為是屬於特定目的內的利用，並沒有違反《個資法》。
- 二、各電信業者為了輔助國防部快速傳遞教育召集報到訊息，符合《個資法》第 20 條第 1 項第 2 款「為增進公共利益所必要」，因此，電信業者利用應受召集人個資之行為並無違法。
- 三、雖國防部及各電信業者之行為皆無違法，但國防部在提供個資予各電信業者時仍應特別注意比例原則之規定。

說明

- 一、本件參照法務部 106 年 7 月 24 日法律字第 10603510040 號函釋。
- 二、教育召集是國防部所職掌的法定職務之一，因此，依照《個資法》第 15 條規定第 1 款規定，基於「兵役行政」之特定目的，國防部為了通知應受教召人員教召訊息，可以將合法蒐集而來的應受召集人員之身分證字號，委由各電信業者與用戶資料比對，確認應受召集人員是否為自家用戶後（委外監督參考《個資法》第 4 條、《個資法施行細則》第 8 條規定），再請各電信業者協助利用用戶的行動電話號碼，發送教召簡訊通知應受召集人員；因此國防部將合法蒐集的身分證字號提供給各電信業者，屬於特定目的內利用。
- 三、各電信業者確認應受召集人員是自家電信公司的用戶後，利用用戶的電話號碼發送教召簡訊，是為了輔助國防部快速傳遞教育召集報到訊息，提醒應受召集人員教召事項，因此應符合《個資法》第 20 條第 1 項第 2 款「為增進公共利益所必要」。

四、雖國防部及各電信業者之行為皆無違法，但國防部應考量其提供應受教召人員的身分證字號提供給電信業者比對、利用，是否已經是為達成前述目的，對人民採取侵害程度最小的手段，或有其他對人民之權利侵害程度更小之替代方式，以符合比例原則。

個資法 §4

個資法 §8

個資法 §15

個資法 §20

個資法施行細則 §8

— 案例 2 —

問題

電信公司能否為協助自殺個案處置（安心專案）提供衛生福利部來電自動顯示號碼呢？

解答

- 一、依《精神衛生法》第 33 條第 1 項及第 2 項規定，衛生福利部得要求電信公司提供來電自動顯示號碼及其所在地，以協助自殺個案處置，電信公司不得拒絕。
- 二、依《個資法》第 15 條規定第 1 款規定，衛生福利部為了執行《精神衛生法》所定的法定職務，在執行法定職務之必要範圍內蒐集來電者的顯示號碼屬於合法行為。
- 三、電信公司提供上述資料，符合《個資法》第 20 條第 1 項但書第 1 款「法律明文規定」、第 2 款「為增進公共利益所必要」、第 3 款「為免除當事人之生命、身體、自由或財產上之危險」或第 4 款「為防止他人權益之重大危害」，故屬特定目的外合法利用個資之行為。

說明

- 一、本件參照法務部 100 年 6 月 15 日法律字第 1000012630 號函釋。
- 二、按照《精神衛生法》第 33 條第 1 項的規定，為利於提供緊急處置，以維護民眾生命、財產安全，相關機關所設置特定的對外服務專線（例如：110、119 等），可以要求各電信業者配合提供來電自動顯示號碼及來電所在地；同條第 2 項規定，電信業者就此類情形，不可以拒絕提供來電顯示號碼、所在地址及相關救護資料給衛生福利部。
- 三、因此，依《個資法》第 15 條規定第 1 款規定，衛生福利部是為了執行《精神衛生法》所定的法定職務所必要，而合法蒐集來電者的顯示號碼，以維護

可能受有傷害之民眾（自己或他人）之生命、財產安全，故衛生福利部蒐集來電者的顯示號碼屬於合法行為。

四、而電信業者提供來電顯示號碼，雖然與當初蒐集客戶個資的特定目的不同，但是為了協助自殺個案的危機處置，因此符合《個資法》第 20 條第 1 項但書規定的下列情形，可以為特定目的外之利用：

- (一) 法律明文規定（《精神衛生法》第 33 條）
- (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

個資法 §15

個資法 §20

精神衛生法 §33

— 案例 3 —

問題

財政部為辦理電子發票中獎事宜，函請電信業者查詢並提供使用者資料，是否符合《個資法》？

解答

- 一、財政部在民眾使用電子發票相關系統前（蒐集民眾手機號碼時），技術上應可依《個資法》有關目的外利用個人資料之規定，先徵詢當事人是否同意於中獎時，由電信業者提供必要之個人資料予財政部，並由民眾自行評估選擇是否使用該項服務功能。
- 二、若民眾已同意於中獎時由電信業者提供相關個資，即等同於電信事業已經過當事人之同意而得在目的外利用當事人個資。
- 三、綜合以上所述，如以此方式為之，電信業者提供使用者之個資予財政部做為辦理電子發票中獎等事宜之使用，並無違反《個資法》。

說明

- 一、本件參照法務部民國 106 年 06 月 12 日法律字第 10603504480 號函釋。
- 二、財政部為發給統一發票中獎獎金，於必要範圍內蒐集中獎人之個資，屬於執行統一發票給獎辦法所定法定職務，並基於稅務行政（代號 120）之特定目的的蒐集行為，應可認定符合《個資法》第 15 條第 1 款規定「執行法定職務必要範圍內」。
- 三、依《所得稅法》第 88 條、第 92 條及其施行細則第 85 條之 1 等相關規定，統一發票中獎人須詳填姓名、住址等個資，以完成扣繳稅款及核銷作業，因此財政部為提供民眾更便利之領獎方式，規劃以手機號碼作為電子票證載具歸戶之方式，並由電信事業提供手機號碼用戶（中獎人）之個資。而電信業者雖然是為協助財政部執行其法定職務，並便利中獎人領取獎金而提供用戶個資，但此是否為《個資法》第 20 條第 1 項但書第 2 款「增進公共利益」，仍應符合比例原則；另外是否符合《個資法》第 20 條第 1 項但書第 7 款「有

利於當事人權益」，也不宜過於寬鬆解釋，故本件是否能符合前述二款規定而為特定目的外之利用，必須仔細討論。

- 四、民眾既然須先提供手機號碼作為電子票證載具歸戶，則可以於蒐集民眾手機號碼時，一併徵詢其是否同意於中獎時，由電信事業提供其必要之個資予財政部，並明確告知利用該個資之目的、範圍、及同意與否對其權益之影響（參考《個資法》第 7 條第 2 項規定），由民眾自行評估、選擇是否使用該項服務功能，使電信事業得依《個資法》第 20 條第 1 項但書第 6 款「經當事人同意」而在目的外利用個資，確保民眾（中獎人）之「隱私合理期待」，因此，如電信業者以此方式將前述個資提供予財政部使用，並無違反《個資法》。

個資法 §7

個資法 §15

個資法 §20

所得稅法 §88、92 細則 §85

— 案例 4 —

問題

客服人員因與來電客戶發生爭執，竟將客戶的行動電話號碼於比價優惠網站上公開，請問該客服人員之行為有無違反《個資法》？雇主於《個資法》上有何責任？

解答

客服人員將來電客戶的行動電話號碼於網路上公開，可能違反《個資法》第 20 條第 1 項規定之目的外利用個人資料的違法行為。該客服人員的雇主為客戶個人資料的蒐集者，依《個資法》第 29 條第 1 項規定，將承擔損害賠償責任。

說明

一、行動電話號碼為個人資料。

- (一) 有論者主張，行動電話號碼本身僅係一串數字組合，並無特定識別性，不是個人資料。
- (二) 但曾有法院實務認為，行動電話號碼雖然乍看之下僅為一連串之數字，但該號碼之持有人於當時僅有 1 人，對某特定人具有專屬性、獨特性，以其為憑據，即可與該人連結而識別出特定個人⁸。
- (三) 另外也有法院見解認為，如將行動電話號碼與其他個人資料（例如：姓名、國民身分證統一編號、特徵及其他社會活動資料）相互比對、組合、連結及勾稽結果，即可以間接方式識別特定自然人。⁹
- (四) 此外，我國《個資法》主要是參考歐盟 1995 年《個人資料保護指令》（下稱《95 指令》）制定的，其中個人資料之定義，也和《95 指令》相似。歐盟法院（CJEU）2016 年判決（Case C-582/14）亦明確指出，所有足以使特定資料主體被識別之資料不一定都必須全部由同一人掌握，此資料才屬於

⁸ 參照臺灣高等法院臺南分院 105 年上易字第 393 號刑事判決意旨。

⁹ 參照臺灣臺北地方法院 103 年度北小字第 1360 號民事判決意旨。

「個人資料」，例如保有動態 IP 位址 (dynamic IP address) 資料之服務提供者得以可能、合理之方式，透過其他網路服務提供者取得對照、組合之資料識別特定資料主體，即可認定動態 IP 位址屬於個人資料¹⁰。

(五) 因此，行動電話號碼應得以直接或間接方式識別該號碼使用人，符合《個資法》第 2 條第 1 款對於個人資料之定義。(法務部公告之《個資法之特定目的及個人資料之類別》也將行動電話列為 C001 識別類之個人資料)

二、客服人員因與來電客戶發生爭執，將客戶的行動電話號碼於網路上公開，違反《個資法》第 20 條第 1 項「目的內利用個資」之規定。

(一) 客服人員蒐集來電客戶之行動電話號碼的特定目的，應為「消費者、客戶管理與服務」，依《個資法》第 20 條第 1 項規定，除非符合該項但書的例外情形¹¹，客服人員只能在該特定目的之必要範圍內利用個人資料。

(二) 但若客服人員因與來電客戶發生爭執，將客戶的行動電話號碼於網路上公開，此利用個資之行為顯然已逾越上述蒐集客戶行動電話號碼的特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個資之行為，且應不符合任一項前述之例外情形。

三、客服人員的雇主為客戶個人資料的蒐集者，須承擔受雇人違法的民事損害賠償責任。

(一) 於題示情形中，客服人員的雇主為客戶個人資料的蒐集者，依《個資法》第 29 條第 1 項規定¹²，應由雇主對客戶承擔損害賠償責任。

(二) 但如雇主能證明無故意或過失，例如雇主已按《個資法》第 27 條規定採行「適當安全措施」，即同法施行細則第 12 條規定中，配置管理之人員及相

¹⁰ 參照國家發展委員會 109 年 7 月 24 日發法字第 1090015912 號函釋。

¹¹ 《個資法》第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，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。」

¹² 《個資法》第 29 條第 1 項：「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者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

當資源、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、資料安全稽核機制等，則或許可依《個資法》第 29 條第 1 項但書之規定而免責。

四、實務上曾發生類似題示情形之案例，電信業者客服人員受理民眾申訴電話，將民眾行動電話號碼洩漏至其他網站，曾被國家通訊傳播委員會認定違反《個資法》第 27 條第 1 項規定，並依同法第 48 條第 4 款規定要求限期改正¹³。

個資法 §20

個資法 §29

統計法 §2

個資法 §27

個資法 §48

個資法施行細則 §12

¹³ 國家通訊傳播委員會 109 年 8 月 26 日第 924 次會議紀錄。

— 案例 5 —

問題

電信公司受保險公司委託，發送生日優惠權益簡訊予行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，請問電信公司有無違反《個資法》？

解答

電信公司受保險公司委託，發送生日優惠權益簡訊給行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，已逾越當初簽訂電信服務契約所載明之特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個人資料之行為。

說明

- 一、電信公司與行動電話用戶簽訂電信服務契約時，其蒐集、處理個人資料之特定目的為「經營電信業務與電信加值網路業務」，依《個資法》第 20 條第 1 項規定，除非符合該項但書的例外情形¹⁴，電信公司僅可在該特定目的之必要範圍內利用行動電話用戶之個人資料。
- 二、若電信公司受保險公司委託，發送生日優惠權益簡訊予行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，此利用個人資料之行為顯然已經逾越上述特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個資之行為，且應不符合該項規定但書的任一例外情形。
- 三、實務上，曾發生電信公司於電信服務契約所載之特定目的外，利用行動電話用戶之個人資料，且未經當事人同意，發送某保險公司之行銷簡訊，並將回傳簡訊之行動電話號碼提供給保險公司，此舉被國家通訊傳播委員會認定違

¹⁴ 《個資法》第 20 條第 1 項但書情形：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。

反《個資法》第 20 條第 1 項規定，並依同法第 47 條第 3 款及行政罰法第 25 條規定，分別核處罰鍰新臺幣 30 萬元、5 萬元，合計新臺幣 35 萬元¹⁵。

個資法 §20

個資法 §47

行政罰法 §25

¹⁵ 詳參 104 年 9 月 23 日國家通訊傳播委員會第 662 次委員會議紀錄。

— 案例 6 —

問題

電信業者接獲客戶對某通訊行之申訴後，將載有客戶個資之申訴單轉傳給與執行申訴業務無關之通訊行人員，是否違反《個資法》？

解答

電信業者將載有客戶個資之申訴單，傳送給與執行申訴業務無關之通訊行人員，違反《個資法》第 20 條第 1 項規定，構成目的外利用個人資料的違法行為。

說明

- 一、依《個資法》第 20 條第 1 項規定，電信業者於客訴流程中蒐集、處理客戶個人資料之特定目的為「消費者、客戶管理與服務」，除非有符合該條項但書之例外情形¹⁶，否則電信業者只可以在特定目的之必要範圍內利用客戶之個人資料。
- 二、題示情形中，電信業者收到客戶對某通訊行之客訴資料，應交由其負責客訴之承辦人員處理，相關個人資料不應提供給非負責處理申訴業務之人員。電信業者卻將客訴資料（包含客戶個人資料）轉傳給與執行申訴業務無關之通訊行人員，即已逾越上述特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個資之行為，且不符合該項但書任一例外情形。
- 三、實務上，類似題示情形之案例，電信業者將載有客戶個資之申訴單，未經去識別化即傳送予被申訴之通訊行人員，因該通訊行人員並非該電信業者負責

¹⁶ 《個資法》第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，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。」

處理申訴業務之人員，曾被國家通訊傳播委員會認定違反《個資法》第 20 條第 1 項規定，並依同法第 47 條第 3 款核處罰鍰新臺幣 10 萬元¹⁷。

個資法 §20

個資法 §47

¹⁷ 詳參 106 年 1 月 4 日國家通訊傳播委員會第 730 次委員會議紀錄。

第 4 篇

委外監督



A. 相關法規

◆ 個人資料保護法

第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

◆ 個人資料保護法施行細則

第 8 條：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。前項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。第一項之監督，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。」

B. 案例解析

— 案例 1 —

問題

有線電視業者將其中裝契約置於通路商門市供訂戶簽約，並蒐集個人資料，於《個資法》上之適用為何？

解答

- 一、若通路商僅是受有線電視業者委託，並以有線電視業者名義進行用戶個資之蒐集、處理或利用，應適用《個資法》第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」之規定蒐集訂戶之個人資料。有線電視業者應依照《個資法施行細則》第 8 條規定，對受託者（通路商）進行適當之監督。
- 二、若有線電視業者及通路商是各自（或共同）蒐集訂戶之個資時，則雙方應各自適用《個資法》規定，承擔法律義務，即有線電視業者與通路商均需有蒐集個資的法律依據（《個資法》第 19 條），且均需踐行告知義務（《個資法》第 8 條），並對保有之個人資料採取適當安全維護（《個資法》第 27 條）。

說明

- 一、若通路商僅是受有線電視業者委託，並以有線電視業者名義進行個資之蒐集、處理或利用，則此時有線電視業者即具有決定個資蒐集目的的權力，而應適用《個資法》第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」之規定。
- 二、有線電視業者將蒐集個資之業務委託通路商，應依照《個資法施行細則》第 8 條規定，對受託者（通路商）進行適當之監督。
- 三、個資委外監督內容應包含：「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。」此外，依照《個資法施行細則》第 8 條第 3 項規定，委託機關（有線電視業者）應定期確認受託者（通路商）執行之狀況，並將確認結果留下紀錄。

四、故若受託者（通路商）於受託範圍內違反《個資法》之規定時，有線電視業者應按《個資法》第 29 條規定，負損害賠償責任。

五、另若有線電視業者與通路商各自（或共同）蒐集、處理、利用客戶之個資時，則有線電視業者與通路商於此情形下，皆應符合《個資法》第 8 條踐行告知聲明義務，及同法第 19 條非公務機關對個資應於特定目的內蒐集或處理之規定，並應採取《個資法》第 27 條規定之安全維護措施：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關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。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」。

六、依照《個資法》第 29 條規定，若非公務機關違反《個資法》規定，致他人之個資外洩者，須負損害賠償責任，故於此情形下，有線電視業者及通路商若違反此規定，即應分別負損害賠償責任。

個資法 §4

個資法 §8

個資法 §19

個資法 §27

個資法 §29

— 案例 2 —

問題

傳播事業可否將客戶個人資料提供給印刷廠印製帳單？如何辦理委外監督？

解答

傳播業者委託印刷廠印製客戶帳單此時印刷廠蒐集、處理及利用個資之行為，適用《個資法》第 4 條之規定，視同委託機關（即傳播業者）所為，傳播業者則應依《個資法施行細則》第 8 條規定，對印刷廠進行適當的委外監督。

說明

- 一、傳播業者委託印刷廠印製客戶帳單，將客戶個資提供予印刷廠，而印刷廠收受個人資料後加以處理、利用，依照《個資法》第 4 條規定¹⁸，視同委託機關（傳播業者）所為。
- 二、傳播業者應依《個資法施行細則》第 8 條第 1 項及第 2 項規定，對受託者（即印刷廠）進行適當之委外監督，監督內容應至少包含下列事項：
 - (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) 受託者就第十二條第二項採取之措施（亦即適當安全維護措施）。
 - (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。
- 三、個資保護實務上的「委外監督」，分為事前、事中及事後監督作業，分述如下：

¹⁸ 《個資法》第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

-
- (一) 事前監督：傳播業者與印刷廠簽訂委託契約時，應於委託契約中將「個資保護及委外監督條款」寫入合約，以要求印刷廠配合辦理，此為委外監督之事前作業。
- (二) 事中監督：傳播業者應依照《個資法施行細則》第 8 條第 3 項規定，定期依照前述監督內容確認印刷廠的執行情形，並將確認結果留下紀錄，此為委外監督之事中（稽核）作業。
- (三) 事後監督：當委託關係中止或解除時，傳播業者應確認印刷廠已將相關個人資料刪除、銷毀，或是已全數返還給傳播業者，避免個資外洩風險，此為委外監督之事後作業。
- 四、另依《個資法施行細則》第 8 條第 4 項規定，印刷廠僅得於傳播業者指示之範圍內，蒐集、處理或利用個人資料，印刷廠若認傳播業者之指示有違反《個資法》等相關規定，應立即通知傳播業者。
- 五、此外，倘印刷廠於受託範圍內違反《個資法》規定，導致個資當事人權益受損，若個資當事人向傳播業者求償，此時依照《個資法》第 4 條規定，受委託機關（印刷廠）之權利義務視同委託機關（傳播業者），故傳播業者須按《個資法》第 29 條第 1 項規定對個資當事人負損害賠償責任¹⁹。

個資法 §4

個資法 §29

個資法施行細則 §8

¹⁹ 《個資法》第 29 條第 1 項：「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。」

— 案例 3 —

問題

電信業者將客戶個人資料提供予資產管理公司催收欠費，是否違反《個資法》？

解答

電信業者委託資產管理公司對客戶催收欠費，將客戶個人資料（姓名、電話、欠費金額等）提供予資產管理公司進行催收，依《個資法》第 4 條規定，資產管理公司處理、利用個人資料之行為，均視同電信業者所為；且電信業者仍然是基於客戶管理、催繳欠費等特定目的之必要範圍內，將客戶個人資料提供給資產管理公司，符合《個資法》規範；電信業者亦應依《個資法施行細則》第 8 條規定對資產管理公司進行適當的委外監督及稽核。

說明

- 一、按《個資法》第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」因此，電信業者委託資產管理公司辦理催繳費用等，該資產管理公司即適用《個資法》規定，並視同委託機關（即電信業者）。
- 二、電信業者委託資產管理公司之行為，仍然是基於客戶管理、催繳費用之特定目的而提供欠費客戶個人資料予資產管理公司，由資產管理公司向客戶催繳欠費，應仍屬特定目的內利用個資行為，符合《個資法》第 20 條第 1 項本文規定。
- 三、電信業者亦應依照《個資法施行細則》第 8 條規定，對資產管理公司進行適當的委外監督，至少應於事前約定下列事項：
 - (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。
- 四、此外，依《個資法施行細則》第 8 條第 3 項規定，電信業者應於委託期間定期確認資產管理公司執行之狀況，並將確認結果留下記錄，以此落實委外監督責任。

個資法 §4

個資法 §20

個資法施行細則 §8

第 5 篇

告知義務



A. 相關法規

◆ 個人資料保護法

第 8 條（直接蒐集）：「Ⅰ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。Ⅱ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。」

第 9 條（間接蒐集）：「Ⅰ公務機關或非公務機關依第十五條或第十九條規定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條第一項第一款至第五款所列事項。Ⅱ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。第一項之告知，得於首次對當事人為利用時併同為之。」

B. 案例解析

— 案例 1 —

問題

通傳業者於向當事人蒐集個人資料時應如何向其履行告知義務呢？

解答

- 一、《個資法》為了要保障當事人知的權利，以供其決定是否要提供個資，明確要求企業於蒐集個人資料時，除非有法定的免告知事由，否則都應該要依照《個資法》第 8 條（直接蒐集）或第 9 條（間接蒐集）之規定進行告知。
- 二、一般而言，目前最常見的告知方式為通傳業者提供書面或電子文件以供當事人詳閱後提供個資，但其實告知的方式，只要足以使當事人知悉或可得知悉即可，並不以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件等方式為限。
- 三、至於告知的時間點，如是直接蒐集，應於向當事人蒐集個資時，明確告知依法應告知之項目，方可取得個資，例如：某電信公司於世貿辦理促銷活動，便應先以適當之方式告知當事人《個資法》第 8 條規定之應告知內容，當事人如同意提供個資，方為適當之作法；至於間接蒐集，因個資並非直接向當事人取得，故難以在蒐集前履行告知義務，故依法應於處理、利用前，或首次利用當事人個資時一併告知，例：某 A 公司透過與其他公司合作之行銷方案，取得一批消費者的個資作為行銷之用，A 公司便應於第一次寄發行銷訊息時，向當事人踐行告知義務，方為合法。

— 案例 2 —

問題

A 有線電視業者在官方網站提供「留言版」功能，並將「姓名」、「電話」、「地址」等欄位加註*號，為留言者必填欄位。A 業者應如何確保「蒐集」個資行為符合《個資法》規範？

解答

- 一、A 業者應在網站留言版區塊的醒目位置揭露法定的必要資訊（《個資法》第 8 條的應告知事項），或記載要旨並提供完整內容的網頁連結，以盡到業者的告知義務，並取得留言者的知情同意。
- 二、此外，業者也應檢視其所要求提供的資料，有無超過蒐集目的之必要範圍，若業者列為必填欄位的資料對達成蒐集目的沒有幫助，即可能構成逾越必要範圍的違法蒐集行為。

說明

- 一、業者蒐集留言者個資的法律依據應為「經當事人同意」
 - (一) 業者在官方網站留言版蒐集留言者的個人資料，首先須依《個資法》第 19 條第 1 項檢視蒐集個資的法律依據。
 - (二) 由於「單純留言」與「線上申辦」不同，如是後者，申辦人與業者間是「在契約成立前，為商議訂立契約之目的，所進行之接觸行為」，依照《個資法施行細則》第 27 條第 2 項第 1 款規定，雙方存有「類似契約之關係」，因此符合《個資法》第 19 條第 1 項第 2 款的要求，業者可主張「與當事人有類似契約之關係，且已採取適當之安全維護」作為蒐集個資的法律依據。
 - (三) 然而「單純留言」的留言者，因不是客戶，與業者間可能不存在這樣的契約或類似契約關係。因此，業者較保險的作法應是在網站留言版區塊，利用適當的文字揭露設計「知情同意」機制，以《個資法》第 19 條第 1 項第 5 款「經當事人同意」作為合法蒐集個資的依據。
- 二、合法的同意以揭露法定資訊為前提

- (一) 依《個資法》第 7 條第 1 項規定，合法的同意是指「當事人經蒐集者告知個資法所定應告知事項後，所為允許的意思表示」。因此，業者要以「經當事人同意」作為蒐集留言者個資的法律依據，就必須在網站留言版區塊的醒目位置，以適當方式揭露《個資法》第 8 條第 1 項規定的「應告知事項」，包含：A 業者名稱；蒐集之目的；個人資料之類別；個人資料利用之期間、地區、對象及方式；當事人依第三條規定得行使之權利及方式；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。
- (二) 雖然應告知事項項目繁多，但在「留言版」的背景之下，由於蒐集目的理論上僅為「答覆留言事項」，利用個資的方式亦不複雜，因此以文字撰寫應不至於冗長而干擾使用者體驗。
- (三) 如果業者以一份涵蓋所有業務（包含網站留言版）的「隱私權政策（或類似名稱文件）」記載應告知事項，內容較為繁複，不便將其全文與留言板置於同一頁面，則依照《個資法施行細則》第 16 條規定，「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」都是合法的告知方式，業者亦可選擇在留言板醒目位置記載應告知事項的要旨，並附上完整隱私權政策（或類似名稱文件）的連結，供留言者點選閱讀。

三、若業者蒐集的資料超過必要範圍，仍然違法

- (一) 依《個資法》第 5 條規定，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。
- (二) 因此，縱使業者經留言者同意而可合法蒐集個人資料，但若所蒐集的資料超過留言者同意目的之必要範圍，仍然是違法蒐集個資的行為。
- (三) 如果 A 業者蒐集留言者資料的目的是為「答覆留言事項」時，似乎只要蒐集留言者的姓名及電話即可達到目的，此時 A 業者將「地址」欄位加上*號列為必填欄位，恐怕已經超過必要範圍。

個資法 §5

個資法 §7

個資法 §8

個資法 §19

個資法施行細則 §16、27

— 案例 3 —

問題

通傳業者員工於電話中蒐集首次申辦服務的客戶之個人資料，是否應踐行《個資法》規定的告知義務，向該客戶揭露業者蒐集個資的目的、利用個資的方式、當事人權利及其他法定應告知資訊？如何執行？

解答

通傳業者員工於電話中蒐集客戶的個人資料，應依《個資法》第 8 條規定，向客戶揭露法定應告知資訊。實務上可考量以播放錄音搭配分層告知的方式執行。

說明

- 一、依照《個資法》第 8 條規定，原則上通傳業者向客戶蒐集個人資料時，應明確告知下列資訊：「1.機關名稱。2.蒐集之目的。3.個人資料之類別。4.個人資料利用之期間、地區、對象及方式。5.當事人得行使之權利及方式。6.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」。此為《個資法》課予蒐集個資機關的法定告知義務。
- 二、又依照《個資法施行細則》第 16 條規定，上述資訊的「告知方式」包含「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」。
- 三、由上述規定可知，通傳業者履行告知義務的方式，只要足以使客戶知悉或可得而知應告知的內容即可，並沒有其他限制。
- 四、通傳業者透過電話蒐集個人資料時，實務上可由接線員工以口語敘述方式，向客戶說明應告知資訊。不過，完整的應告知資訊內容恐較繁複，通傳業者可考慮採用播放錄音搭配分層告知的方式履行告知義務，即以預先錄音提供應告知資訊的簡要內容，並向客戶說明可以何種方式取得完整資訊，例如官網上的特定網頁、以簡訊將官網上載有完整應告知資訊的網址發送給客戶，

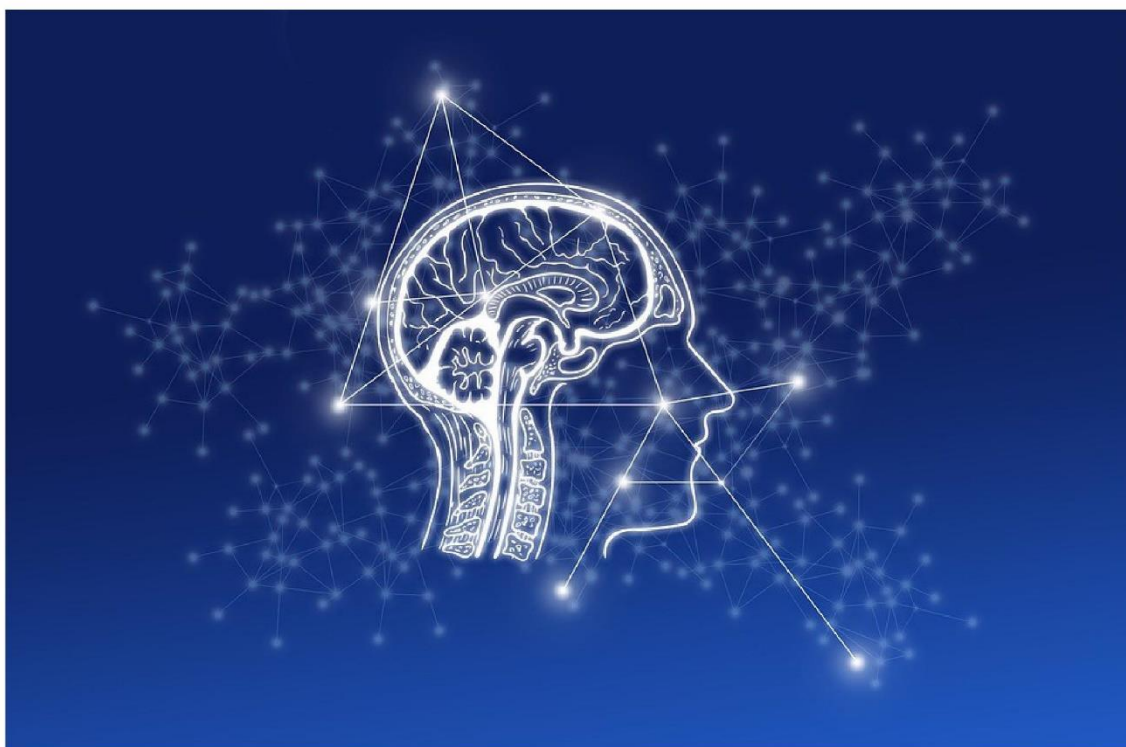
或以電子郵件方式寄予客戶詳閱等，應均符合《個資法施行細則》第 16 條規定。

個資法 §8

個資法施行細則 §16

第 6 篇

當事人權利



A. 相關法規

◆ 個人資料保護法

第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

- 一、查詢或請求閱覽。
- 二、請求製給複製本。
- 三、請求補充或更正。
- 四、請求停止蒐集、處理或利用。
- 五、請求刪除。」

B. 案例解析

— 案例 1 —

問題

電信業者未經客戶同意將電話內容錄音，有無違反《個資法》？客戶得否請求刪除之？

解答

- 一、電信業者若是於履行契約必要範圍內，將與客戶間之通話內容錄音，且當時雙方仍存在契約關係，則此為「依契約關係」而合法蒐集，應無須經客戶同意。
- 二、但電信業者於錄音時未告知客戶，有違反《個資法》第 8 條之虞，行政機關得命業者限期改正之；法院另有見解認為：業務錄音，通常僅是留存供自保之用，而並非基於營利之目的，且電信業者對客戶也無其他不利之影響，應符合免為告知之情形。

說明

- 一、個資當事人之聲音或影像，如經蒐集建檔且足以直接或間接識別特定人，即屬《個資法》第 2 條第 1 款所定義之個人資料。
- 二、電信業者若是於履行契約的必要範圍內，將與客戶間之通話內容錄音，且當時雙方仍存在契約關係，符合《個資法》第 19 條第 1 項第 2 款，應無須取得當事人之同意。
- 三、電信業者於錄音時未告知客戶，有違反《個資法》第 8 條之虞，故得由中央目的事業主管機關或直轄市、縣（市）政府依《個資法》第 48 條命業者限期改正；但法院似有不同見解，臺灣士林地方法院 107 年度訴字第 1824 號判決認為，業務電話進行錄音僅是為避免另生糾紛、留存供自保之用，而非基於營利之目的；電信業者就業務電話之錄音檔若於通話後沒有其他處理、散布或利用之行為，則該錄音行為對客戶顯無不利之影響，故應認定為符合《個資法》第 8 條第 2 項第 6 款「免為告知之情形」。

四、前述業務錄音內容，是為解決契約相關之紛爭，故合法蒐集客戶個資之特定目的尚未消失，若客戶依《個資法》第 11 條第 3 項要求業者予以刪除，並不合理。

個資法 §2

個資法 §5

個資法 §11

個資法 §19

— 案例 2 —

問題

通傳業者將與當事人之對話錄音，當事人得否請求閱覽或複製該錄音？

解答

通傳業者依《個資法》之規定所蒐集、留存之錄音錄影資料檔，客戶既為資料之當事人，自然可請求業者答覆查詢、提供閱覽或製作、提供複本，除非有下列情形，業者不得拒絕當事人之請求：

- 一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
- 二、妨害公務機關執行法定職務。
- 三、妨害該蒐集機關或第三人之重大利益。

說明

- 一、個資當事人之聲音或影像，如經蒐集建檔且足以直接或間接識別特定人，即屬《個資法》第 2 條第 1 款所定義之個人資料。
- 二、另依《個資法》第 3 條及第 10 條等規定，請求查詢、閱覽及製給複製本為個資當事人之法定權利，不得要求當事人預先拋棄；除非有妨害重大公共利益等例外情形，亦不得以特約限制當事人請求複製、刪除等權利。
- 三、綜合以上所述，業者依《個資法》規定所蒐集、留存之錄音錄影資料，客戶既為該等資料之當事人，自然可請求業者製作及提供複製本，除非有《個資法》第 10 條但書所定情形，業者不得拒絕（參考金融監督管理委員會保險局保局（綜）字第 10410912710 號書函意旨）。

個資法 §2

個資法 §3

個資法 §10

第 7 篇

安全維護



A. 相關法規

◆ 個人資料保護法

第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

◆ 個人資料保護法施行細則

第 8 條：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。前項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。第一項之監督，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。」

B. 案例解析

— 案例 1 —

問題

防疫期間，傳播事業如何確保遠距工作之資訊安全？

解答

建議傳播事業檢視現有資訊安全政策有無包含「遠距工作」項目，並可參照《個資法施行細則》第 12 條第 2 項規定及下述說明調整或訂定之。

說明

- 一、依照《個資法》第 27 條規定，維護個人資料的安全，是傳播事業的法定義務。進行遠距工作時的個資或資安保護，對大部分傳播事業來說可能都是一項新挑戰，建議傳播事業可先檢視既有的資訊安全政策有無包含「遠距工作」項目，再視情形調整或訂定。
- 二、依《個資法施行細則》第 12 條第 2 項規定，傳播事業可採取 11 項適當安全維護措施，本文參考澳洲資訊委員辦公室（Office of the Australian Information Commissioner, OAIC）「評估已改變的工作環境下的隱私風險：隱私衝擊評估（Assessing privacy risk in changed working environments: Privacy Impact Assessments）」之意見，提供數點關於遠距工作的評估（完整建議內容請詳參網址<https://www.davinci.idv.tw/news/769>），建議如下：
 - (一) 組織治理：組織有無建立包含員工遠距工作的資安政策？（細則§12Ⅱ（6）資安管理及人員管理）
 - (二) 資通訊安全：員工能夠使用私人裝置遠端存取系統嗎？組織針對這些私人裝置採取哪些技術上與程序上控管措施，以降低安全風險？（細則§12Ⅱ（6）資安管理及人員管理）
 - (三) 存取安全：組織有無考量在員工的終端裝置內安裝遠端刪除程式，以便在裝置遺失或遭竊時刪除個人資料？（細則§12Ⅱ（8）設備事故管理）

-
- (四) 安全管理：因應遠距工作的安排，現有計畫中有關通知事故或可疑事故的方式需要調整嗎？（細則§12Ⅱ（11）個人資料安全維護之整體持續改善）
- (五) 實體安全：組織是否考慮主動採取措施以確保員工家中有適當的實體安全維護（例如考慮以現場或遠端方式持續抽查員工家中環境，檢視員工的遠距工作環境安全）？（細則§12Ⅱ（9）資料安全稽核機制）

個資法 §27

個資法施行細則 §12

— 案例 2 —

問題

電信業者員工違反公司資安規定，以未經公司核准之隨身碟存取公司電腦中的客戶個人資料，若因此發生個資侵害事故（例如使電腦中毒致客戶資料遭駭，或隨身碟遺失致客戶資料遭竊取），該電信業者是否違反《個資法》？

解答

電信業者員工以非公司核准之隨身碟存取公司電腦中之客戶個人資料，導致個資侵害事故發生，即便業者已制定資安規範禁止該行為，但未採取其他實務上合理可行的措施避免該行為的發生，則仍有遭認定違反《個資法》第 27 條第 1 項規定，未對客戶個人資料採行適當之安全措施。

說明

- 一、依《個資法》第 27 條第 1 項規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」因此，電信業者對其員工存取客戶個資之行為，應採行適當之安全措施，例如參考《個資法施行細則》第 12 條第 6 款「資料安全管理及人員管理」之措施，訂定使用公司之電腦設備所應遵循的資安相關規定。
- 二、然而，即便電信業者已制定資安規範，倘員工仍違反規定，使用未經核准之隨身碟儲存客戶個人資料，並因此造成個資侵害事故，此時無法直接認定業者是否已採行適當之安全措施。
- 三、如實務上存有其他合理可行措施，可在實作上避免此事故發生（例如業者封鎖員工電腦使用 USB、系統設定無法匯出客戶之個人資料、或在員工匯出客戶個資時，在系統出現提醒文字，告知員工務必循公司程序申請使用經核准的無惡意程式、加密隨身碟等），則業者不一定能以「已制定資安規範」來證明其已善盡適當安全維護的責任。

個資法 §27

個資法施行細則 §12

— 案例 3 —

問題

電信業者員工違反公司規定，於公司電腦安裝即時通訊軟體，傳送客戶雙證件影本等個人資料，導致個資侵害事故發生（如不慎誤傳予友人導致客戶個資外洩），該電信業者是否違反《個資法》？

解答

電信業者員工未經許可，於公司電腦自行安裝即時通訊軟體，並用以傳送客戶雙證件影本等個人資料，導致個資侵害事故發生，即使業者已制定資安規範禁止該等行為，但未採取其他實務上合理可行之措施避免該等行為發生，則仍可能違反《個資法》第 27 條第 1 項規定，未對客戶資料採行適當安全措施。

說明

- 一、依照《個資法》第 27 條第 1 項規定，電信業者保有個人資料檔案，「應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」。
《個資法施行細則》第 12 條第 2 項並提出 11 項安全措施，供業者參照執行。
- 二、因此，電信業者蒐集客戶雙證件影本等個人資料，即應採行適當之安全措施，例如參考《個資法施行細則》第 12 條第 2 項第 5 款規定，訂定個人資料蒐集、處理及利用的內部管理制度，或是依照第 6 款規定，訂定資料安全管理及人員管理程序，甚至依照第 8 款規定，訂定設備安全管理政策。
- 三、然而，即便電信業者已制定相關規範，若其員工仍違反規定，自行於電腦安裝即時通訊軟體，用以傳送客戶證件資料，並因此造成個資侵害，此時無法直接認定業者是否已採行適當之安全措施。如果實務上有其他合理可行措施可避免此事故發生（例如以系統設定限制電腦裝置使用者安裝軟體時，要求管理員權限，而一般員工無法自行安裝通訊軟體等），則業者不一定能以「已制定相關規範」主證明其已善盡適當安全維護之責。

個資法 §27

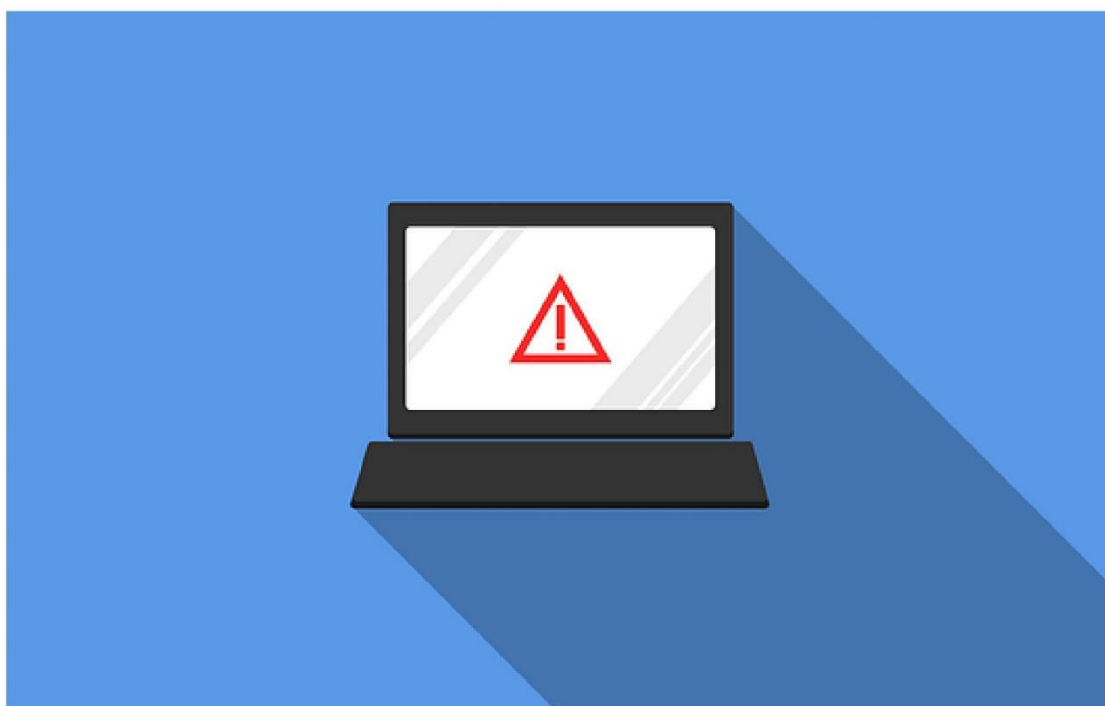
個資法施行細則 §6

個資法施行細則 §8

個資法施行細則 §12

第 8 篇

事故通報



A. 相關法規

◆ 個人資料保護法

第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

◆ 個人資料保護法施行細則

第 22 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

◆ 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法

第 4 條：「非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制：一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。二、事故發生後應受通報之對象及其通報方式。三、事故發生後，其改善措施之研議機制。非公務機關遇有重大個人資料事故者，應即通報國家通訊傳播委員會（以下簡稱本會）。前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。」

B. 案例解析

— 案例 1 —

問題

傳播事業如遇個人資料外洩等個資事故，是否應通報個資當事人或主管機關？

解答

傳播事業如遭遇個人資料外洩等個資事故，應依照《個資法》第 12 條、《個資法施行細則》第 22 條及《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 4 條等規定，以適當方式即時通知個資當事人，通知之內容應包括「個人資料被侵害之事實」及「已採取之因應措施」；如個資事故情節重大，將危及傳播事業正常營運或大量當事人權益，應立即通報國家通訊傳播委員會。

說明

- 一、傳播事業如遭遇個人資料外洩等個資事故，應依照《個資法》第 12 條、《個資法施行細則》第 22 條及《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 4 條等規定履行法定義務。
- 二、依《個資法》第 12 條及《個資法施行細則》第 22 條規定，當傳播事業違法導致個人資料外洩等事故發生時，應在查明後以適當方式即時通知個資當事人，所謂「適當方式」包含以言詞、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。通知的「內容」則應包含「個人資料被侵害之事實」及「已採取之因應措施」。
- 三、原則上，傳播事業應該「主動」、「個別」通知個資受侵害的當事人，避免個資當事人的損害發生或擴大（例如即時變更密碼、留意詐騙電話等）。但若主動個別通知將花費過鉅（例如個資被侵害者的人數甚多），傳播事業才可考量技術上的可行性及對當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式進行通知。

四、此外，如個資事故情節重大，將危及傳播事業正常營運或大量當事人權益之時，依照《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 4 條第 2 項及第 3 項規定，傳播事業應立即通報國家通訊傳播委員會。

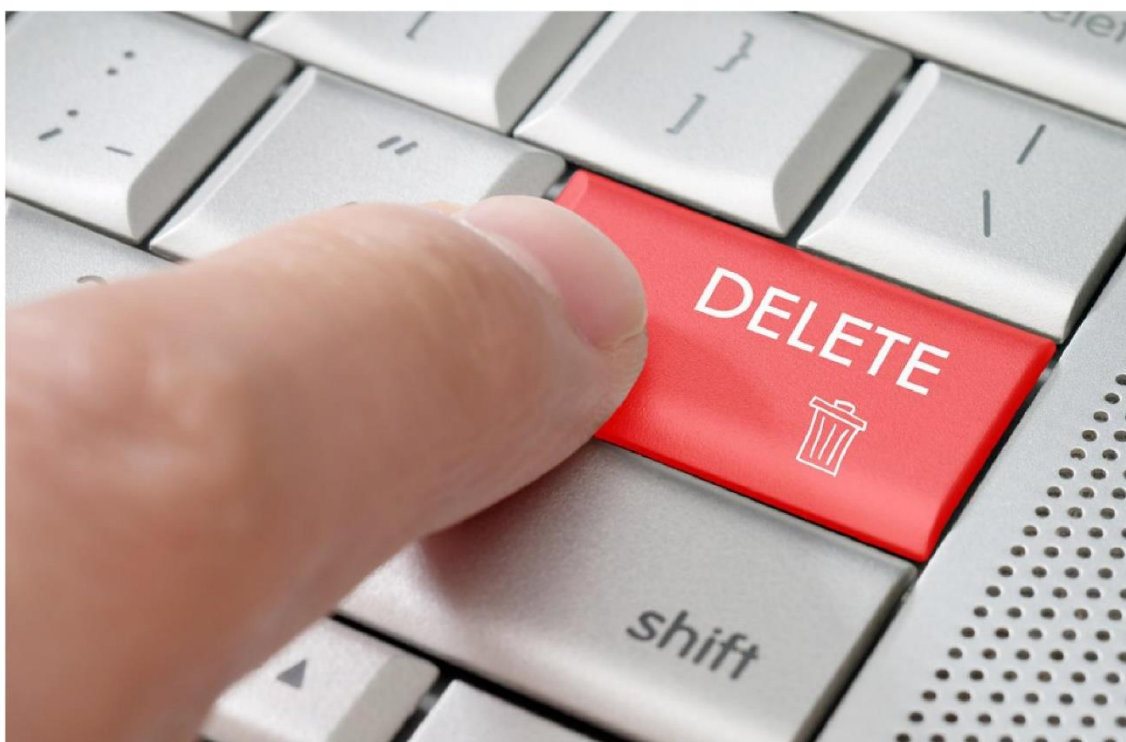
個資法 §12

個資法施行細則 §22

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法 §4

第 9 篇

屆期刪除



A. 相關法規

- ◆ 個人資料保護法

- ◆ 第 11 條第 3 項：「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。」

B. 案例解析

— 案例 1 —

問題

客戶於電信公司網路門市申請攜碼後又取消，電信公司應如何處理該客戶之個人資料始符合《個資法》規範？

解答

客戶於電信公司網路門市辦理攜碼後又申請取消，此時電信公司未能與客戶成立電信服務契約，該客戶所留存之個人資料除非有《個資法》第 11 條第 3 項但書規定之情形，電信公司應主動或依當事人之請求刪除、停止處理或利用該等個人資料。

說明

- 一、依《個資法》第 11 條第 3 項規定：「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。」當客戶於網路門市辦理攜碼（NP）時，電信公司原依「經營電信業務與電信增值網路業務」等特定目的，基於「與當事人有契約或類似契約之關係」，向客戶蒐集、處理其個人資料（參考《個資法》第 19 條第 1 項第 2 款規定）。
- 二、但若客戶又因故向電信公司取消辦理攜碼，導致該電信服務契約未成立，此時，電信公司因履行契約而蒐集個人資料之特定目的已不存在。
- 三、雖然過去沒有函釋直接說明電信公司應如何處理未成立契約之客戶個人資料，但仍可參考法務部 104 年 9 月 7 日法律字第 10403509510 號及金融監督管理委員會 105 年 2 月 2 日金管保壽字第 10410938020 號等函釋意旨：「有關保險業因保險契約未成立或有其他未完成保險交易之因素，其所留存未承保保戶之個人資料，除有《個資法》第 11 條第 3 項但書規定之情形外，應主動或依當事人之請求刪除、停止處理或利用該等個人資料。」

四、由前述函釋意旨可知，若客戶因故取消辦理攜碼，導致該契約未成立，電信公司因履行契約而蒐集個人資料之特定目的已不存在，因此除非有《個資法》第11條第3項但書規定（因執行職務或業務所必須或經當事人書面同意者）之情形，電信公司應主動或依當事人之請求，刪除、停止處理或利用該等個人資料。

個資法 §11

個資法 §19

— 案例 2 —

問題

電信公司未將已離職員工之個人資料（聯絡方式）自工作群組移除，仍繼續寄送工作訊息給已離職員工，有無違反《個資法》？

解答

電信公司於員工離職後應主動刪除或停止處理或利用其個人資料，如電信公司繼續利用其個人資料寄送工作訊息，將違反《個資法》第 11 條第 3 項有關停止利用個資之規定，構成違法利用個人資料之行為。

說明

- 一、依《個資法》第 11 條第 3 項規定：「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」²⁰。
- 二、因此，當員工離職時，電信公司除非有《個資法》第 11 條第 3 項但書規定之情形外，應主動或依當事人之請求刪除、停止處理或利用其個人資料。
- 三、若電信公司於員工離職後，未將已離職員工之個人資料（例如：電話、E-mail 等）自工作群組移除，仍繼續寄送工作訊息給已離職員工，此時電信公司並不符合任何《個資法》第 11 條第 3 項但書所列之情形，顯已違反該規定。

²⁰ 並參《個資法施行細則》第 20 條：「本法第 11 條第 3 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」；第 21 條：「有下列各款情形之一者，屬於本法第 11 條第 3 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」。

四、實務上曾發生電信公司不慎利用已離職員工個人資料分派工作之事件，國家通訊傳播委員會即認定違反《個資法》第 11 條第 3 項規定，並依照同法第 48 條第 2 項限期於 1 個月內改正並提報改善計畫²¹。

個資法 §11

個資法施行細則 §20

個資法施行細則 §21

²¹ 詳參 107 年 8 月 15 日國家通訊傳播委員會第 817 次委員會議紀錄。

— 案例 3 —

問題

通傳業者若將已終止服務契約之客戶資料永久保存，是否違反《個資法》？

解答

客戶終止服務契約，依照《個資法》第 11 條第 3 項規定，如通傳業者蒐集該客戶個人資料之特定目的已消失，即應主動或依客戶之請求，刪除、停止處理或利用該客戶的個人資料。

說明

- 一、《個資法》第 11 條第 3 項本文規定：「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」。所謂「特定目的消失」，依照《個資法施行細則》第 20 條規定，是指下列情形之一：「1.公務機關經裁撤或改組而無承受業務機關。2.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。3.特定目的已達成而無繼續處理或利用之必要。4.其他事由足認該特定目的已無法達成或不存在」。
- 二、通傳業者為「履行服務契約」或「履行法定義務」等特定目的蒐集客戶的個人資料，當客戶終止服務契約後，該特定目的可能已達成或已不存在（但若因客戶尚欠費未繳，應視為履行服務契約之特定目的仍存在），此時除非有《個資法》第 11 條第 3 項但書「因執行職務或業務所必需或經當事人書面同意」的情形，否則通傳業者即必須履行前述刪除個資的義務。此處所謂「因執行職務或業務所必須」，依照《個資法施行細則》第 21 條規定是指下列情形之一：「1.有法令規定或契約約定之保存期限。2.有理由足認刪除將侵害當事人值得保護之利益。3.其他不能刪除之正當事由」。
- 三、實務上，通傳業者可能依照適用的法規不同，而對不同的個人資料負有保存一定期限的義務（例如依照《電信事業用戶查詢通信紀錄及帳務紀錄作業辦法》第 4 條規定，電信事業應將通信紀錄及帳務紀錄自紀錄發生時起保存至

少一年，供用戶查詢），不過，法規通常僅要求業者保存資料的最低期限，並未明定最長期限，以保留一定彈性。

四、因此，通傳業者在客戶終止服務契約後，若要繼續甚至永久保存客戶的個人資料，必須嚴格檢視是否有上述《個資法》第 11 條第 3 項但書和《個資法施行細則》第 21 條規定的例外情形。

五、然而，如果通傳業者考量系統內資料無法單筆刪除，或是需要分析客戶曾經留下的資料（紀錄）也可考慮以適當匿名技術對個人資料加工，讓保存的資料無法再用以識別特定客戶身分（包含業者自己也無法還原、識別），以此達到去識別化的效果，該資料即不受《個資法》規範。

個資法 §11

個資法施行細則 §20

個資法施行細則 §21

附錄2：通傳產業個人資料保護與管理實作指引手冊



通傳產業 個人資料保護 與管理

實作指引手冊



通傳產業 個人資料保護 與管理

實作指引手冊

目錄 CONTENTS

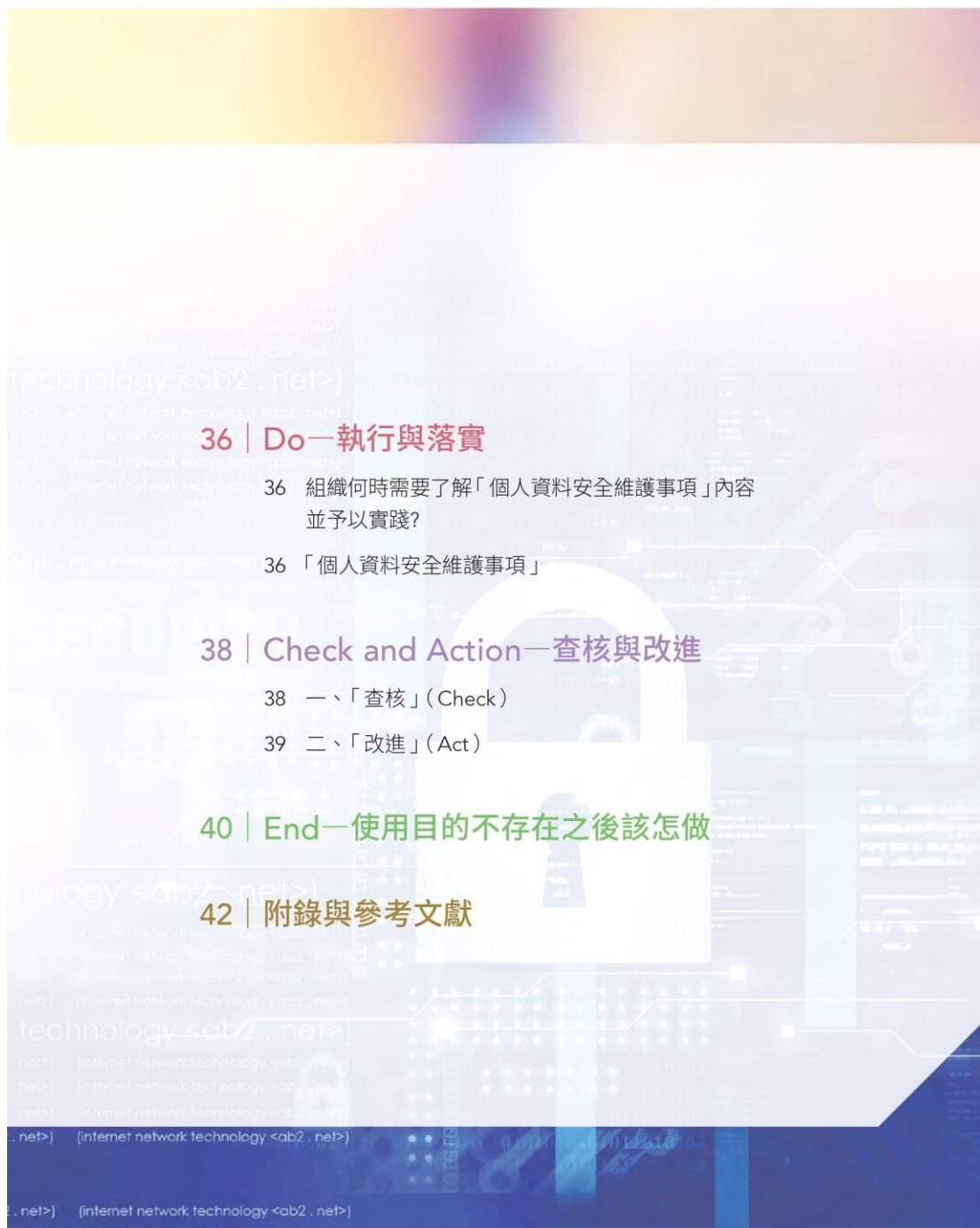
04 | 前言

06 | 個資安全維護系統建置

- 06 一、個資安全維護措施
- 07 二、個資安全維護系統設計概念

09 | Plan—規劃與建置

- 09 一、個人資料安全維護系統建置第一步驟：
配置適當的管理人員及資源
- 13 二、個人資料安全維護系統建置第二步驟：
界定個人資料檔案盤點的範圍
- 19 三、個人資料安全維護系統建置第三步驟：
建立個人資料風險評估及管理機制
- 21 四、個人資料安全維護系統建置第四步驟：
訂定個人資料安全維護規定



36 | Do—執行與落實

36 組織何時需要了解「個人資料安全維護事項」內容並予以實踐？

36 「個人資料安全維護事項」

38 | Check and Action—查核與改進

38 一、「查核」(Check)

39 二、「改進」(Act)

40 | End—使用目的不存在之後該怎做

42 | 附錄與參考文獻



數位時代來臨，全球產業經營型態產生新興科技模式，透過巨量資料之利用與剖析，成為數位經濟不可或缺的成功要素，更為現代新興商業模式營運之重要基礎。是以，近年來個資隱私保護與合法利用加值資料等議題備受關注。

由於通傳產業通常會掌握大量用戶的個人資料，而且個人資料保護法（簡稱個資法）與個人資料保護法施行細則（簡稱個資法施行細則）都明確規定，非公務機關單位如果保有個人資料檔案，應該要採取適當的安全維護措施。因此，國家通訊傳播委員於2016年11月發布「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」（簡稱安全維護辦法），讓通訊傳播事業單位在落實個人資料之保護及管理上有所依循，以促進企業組織內部落實個資法遵。



為了落實個人資料的安全維護，傳通業者應該建置公司內部的個人資料檔案安全維護程序及業務終止後個人資料處理機制。但是，實際上應該要怎麼做呢？所謂的管理計畫，應該包含哪些項目？個人資料安全維護事項有哪些？如何配置人力與資源？如何盤點個資？如何進行風險評估？公司內部資料安全維護規定的訂定、個資保護認知宣導及教育訓練、稽核與持續改善又都應該要如何進行？而個資的蒐集使用目的消失後或期限屆滿時，個人資料檔案該如何處理？

本手冊旨在針對通傳產業實務操作者提供個資管理的實務指引。將從個資保護與管理制度整體建置方法著手，納入執行個人資料保護管理時應注意的事項，並透過實際個資輔導訪查案例說明分析，使讀者更能清楚掌握個資保護管理實務之要點。



2 個資安全維護系統建置

一、個資安全維護措施

通傳產業根據產業特性從實務上來看，往往會因為特定目的而需要蒐集使用並保存個資，而我國個人資料保護法針對一般企業組織保存個資的情況，要求企業組織執行「適當安全維護措施」，防止個人資料被竊取、竄改、毀損、滅失或洩漏的情況發生。

什麼是「適當安全維護措施」呢？適當安全維護措施應該包含以下事項：

- 配置管理之人員及相當資源。
- 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。
- 使用紀錄、軌跡資料及證據保存。
- 個人資料安全維護之整體持續改善。

為了協助通傳產業業者有效建立「適當安全維護措施」，通訊傳播委員會公佈的安全維護辦法提供業者相當的指示及依循。然而，要更進一步的在企業體制內落實個人資料安全維護系統的建置及運作，應該要先明白個人資料安全維護之運作方法。



個資法小法典 個資法施行細則第12條

二、個資安全維護系統設計概念

我國個人資料保護相關法令與國內外個人資料管理系統¹，皆以PDCA品質管理循環方法論作為管理系統設計基礎。所謂PDCA，是以Plan計畫→Do執行→Check檢查→Act行動為循環基礎之方法論。

- 1.計畫：制定規劃個人資料保護管理政策、目標及相關程序。
- 2.執行：落實個人資料管理制度。
- 3.檢查：依據個人資料保護管理政策、目標及要求，評估監督流程並檢視執行成果，將結果回報給最高管理階層加以審查。
- 4.行動：根據檢查結果採取措施，持續改善個人資料管理制度。

隨著計劃制定、計畫執行、執行檢查、採取改善措施等步驟持續循環，個人資料安全維護系統將會越趨完善整密。

► 實務操作提醒 ◀

個資保護缺一不可 PDCA循環精進

個人資料安全維護運作需透過PDCA不斷循環，除了計畫與執行個人資料保護與管理制度之建置，更需要透過組織內部稽核或外部審查，進而發現個資管理制度之缺失，加以矯正改善。

實務上許多組織只依個資法形式上建置管理制度，並未根本落實、實踐個人資料保護相關措施，亦未定期稽核個人資料保護制度，更遑論矯正改善。這樣的形式操作狀況下，導致組織潛在管理弱點未能被發現，個人資料保護與管理制度視同虛設，可能造成外部侵害破口與重大損害。

► 個資法遵建議 ◀

一年一循環 安全自然來

個人資料保護與管理制度至少應於每年循環檢視一次，進而確保組織內部個資保護管理機制為有效且符合組織現況。除此之外，當組織架構有重大變更或組織業務拓展時，應同步檢視個資保護管理制度或相關程序有無需要調整之處。

1 時下常見個人資料管理系統 (Personal Information Management System, PIMS) 例如臺灣個人資料保護與管理制度 (TPIPAS)、BS10012、CNS29100等。



建立個人資料安全維護系統及落實個人資料安全維護措施會涉及：組織投入的資源人力、個人資料蒐集處理利用的流程、個人資料檔案盤點及風險評估方法、事故應變處理程序、通報及改善機制、個人資料安全管理方法、當事人權利行使處理程序、委外監督、認知宣導及教育訓練、資訊安全稽核、使用紀錄及相關證據保存，以及持續改善措施等事項。

接下來將針對建置個人資料安全維護系統所涉及的各個事項逐一說明。

一、個人資料安全維護系統建置第一步驟：配置適當的管理人員及資源

組織必須要有一定的人力和資源投入，才能夠進行內部個資盤點與風險分析，也才有能力進一步規劃並執行事故應變、通報及改善機制、個人資料安全管理、當事人權利行使、委外監督等事項。

「配置管理人力」意思是，組織內部應透過專任或兼任方式指派專責人員承擔內部個人資料保護的責任，且所負責的個人資料安全維護工作屬於經常性業務。

需特別注意的是，我國與歐盟一般資料保護規則（General Data Protection Regulation, GDPR）對於專責人員的要求規範不同。我國的個資相關規範並沒有要求組織必須成立專職個人資料保護與管理的資料保護專員或個資長，只需要有專責人員負責組織內部個人資料保護即可。

配置「相當資源」的意思，是指組織提供維護及管理個人資料檔案所需要的資源，包括經費、技術支持等。以落實資料保護角度來說，組織若要確實做好個人資料安全維護，所投入的資源與人力應和組織規模成相當比例，否則可能會成效不彰。

►實務操作提醒◀

- 實務上在規模較大的組織，若只有指派少數人進行個資安全維護工作，勢必會有所不足。因此，若能以建立「個資檔案安全維護管理小組」方式進行，並配合適當的認知宣導與教育訓練，才能有效落實適當安全維護措施。
- 建立個資管理小組，應該同時要考慮層級、功能、及業務性質等因素。管理小組的領導者，最好在單位內具有相當高度或管理權限，才能避免發生管理小組政策難以推動之窘況。
- 一定規模的組織，應該建立具備管理代表、執行人員與內評人員（詳見下圖）的個資管理小組。
 1. 管理代表：組織個資管理制度之主要負責人，作為統籌整個管理組織並分配相關工作的角色。管理代表需定期向企業組織負責人報告，組織內部個資管理小組運作之相關事項。通常由企業最高管理階層指派一位總

經理或副總經理的管理階層，擔當組織內部個人資料保護之責任，並視推行情況提供執行監督人員必要的資源與協助。

2. 管理人員：相較於管理代表負責統籌組織，決定政策，給予相關資源，管理人員為實際第一線執行之人員。為了有效推動企業組織個資管理制度，需因應企業規模與組織架構，各個部門應至少推派一名個資管理負責人員，負責辦理業務範圍內個資安全維護事項的經常性工作，例如該部門個資盤點、確認個人資料安全維護事項遵循狀況、個人資料安全維護事項落實等。
3. 內評人員：為有效督導與評核個資保護管理程序運作及安全措施執行之成效，除個人資料管理代表外，管理組織亦應安排內部監督或評量計畫是否確實執行之監督人員。

這樣的管理結構有助於實質並有效地落實個資保護。如果遇到組織規模較小或組織人力與資源有限的情形，則管理與維護個人資料檔案的專責人員，可以由組織內部具有相關權責權限的管理高層擔任。



圖1 | 管理小組例示圖

資料來源：本研究自製

► 實務案例 ◀

A為有線電視經營業者，擁有用戶資料高達上萬筆，因意識到近年來個資外洩事件頻繁與消費者意識抬頭，為了使公司用戶個資有完善之保障，避免產生個資外洩事故，破壞公司聲譽，決定導入個人資料保護與管理制度來改善公司現況，同時又能符合主管機關之要求，正所謂一兼二顧。於是次日即叫來公司唯一之法務人員B，請B於一個月內建立個人資料安全維護事項，並要完成全公司之個資盤點與風險評估。B原本於公司就身兼數職，任何與法律相關之案件皆會落到他頭上，現在又多了個資管理制度導入，讓其困擾不已，找其他單位來開會，大家都用公務忙碌推拖。最後，B因為無法承受過多業務量而選擇離職。

► 個資法遵建議 ◀

個資保護 人人有責

- 個資管理制度之建置不能僅靠單一部門，實務上執行應該由各部門共同推動建置比較適合。組織應配置管理人員與相當資源，才有能力執行個資管理制度，並且辦理個資安全維護事項。細部分工與職責規劃可依據公司實際狀況組成，基本上建議各部門主管與業務人員，以具備管理代表、管理人員及內評人員三種功能成員為個資管理小組編制概念核心，進行任務編組。
- 前面的案例中，雖然公司經營者A有意識個資制度建立之重要性，但是除了指派專人負責個資保護相關事宜外，應該還要授命由各相關部門同仁組成之個資保護小組一同進行，才能使個資保護制度有效推動，否則僅靠法務單位一人建置不僅人力不足，往往無法有實質權力協調各單位配合推動，且法務單位通常專精於法律事務，對於各單位實際執行業務蒐

集處理及利用個資狀況並不一定明瞭，於相關業務個資盤點時易有疏漏之處，故應該由公司各部門推派代表進行較為適當。

二、個人資料安全維護系統建置第二步驟：界定個人資料檔案盤點的範圍

雖然大家都知道要保護個人資料，但組織內部有什麼資料是需要保護的呢？有哪些資料是不需要特別保護的呢？

如果不知道有什麼資料要保護，將會不知該從何做起。因此，必須先瞭解個人資料的定義，並且將屬於個資法所保護的資料，透過一定的盤點方法，確認組織內部目前掌握及保存個資的情況，以確保個資保護沒有疏漏。

（一）個資盤點範圍

個人資料的保護範圍，包含自然人之姓名、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、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、社會活動及其他得以直接或間接方式識別該個人之資料。

值得注意的是，可以「直接識別」的個人資料，是指資料本身具有高度的識別性，可以直接透過資料指涉特定個人。而「間接識別」是指，沒有辦法藉由資料本身來辨別指涉對象，須與透過其他資料對照、組合、連結等方式，才能識別資料所指涉的對象。



個資法小法典 個人資料保護法第2條第1款、個人資料保護法第3條

► 實務操作提醒 ◀

個資排排坐 未盤容易錯

實務上組織所掌握的個人資料是非常多元的，除了基本的員工個人資料與消費者個人資料以外，時常被忽略的部分，包括訪客登記表、領據、臉書私訊小編報名活動及委外廠商滿意度調查表等，只要是個資法所保護的個人資料，都應該納入個人資料盤點清冊，以防疏漏。

► 實務案例 ◀

某C電視購物頻道，在消費者進線時沒有提供個資蒐集使用及處理的告知聲明，只有在消費者訂單成立之後才提供告知聲明給消費者，並表示訂單成立之前不會儲存任何消費者個資，所以不需要事先提供告知聲明。雖然電視購物頻道業者認為，單純的以錄音方式紀錄與消費者間的對話，應該不需要先行告知聲明，但在電話的對話內容中，往往已經包含了個資。

► 個資法遵建議 ◀

- 前面的案例中，首先應該確認電視購物消費者錄音是否為個人資料。而確認消費者錄音是否屬於個人資料，需要透過錄音內容是否能直接或間接識別當事人進行判斷。從案例中之情形來看，消費者於進線時的錄音內容包括：購物台客服人員與消費者確認姓氏與稱謂等基本資料。而電視購物電話進線時客服人員端也會顯示消費者的電話號碼。電視購物業者可以透過結合相關消費者的綜合資訊，以間接識別的方式識別當事人。
- 以個資管理法遵實務角度來看，針對案例的情況，會建議在電話進線開始錄音前先進個資告知聲明。

(二)釐清蒐集、處理及利用個人資料之目的

蒐集個人資料必須基於特定目的，組織因業務需求而蒐集、處理或利

用消費者個人資料時，除了必須基於特定目的外，同時必須符合個資法的要求，在該特定目的必要範圍內，為相關個資蒐集、處理及利用行為。

「目的外利用」應符合法定情況，若組織將原特定目的蒐集、處理及利用之個人資料，作於目的外的使用時，就會落入個資法上所稱「目的外利用」的情況。

以一般網站會員申請個資聲明為例，如果取得會員之個人資料，原本的目的只是為了會員管理，而個資聲明中也聲明「個人資料僅用於會員管理」，但後續卻想將這些個人資料用來進行消費喜好研究分析或行銷，這種超出原本個資蒐集目的使用，即屬於「目的外利用」。

若要對個人資料進行目的外利用，必須至少符合下列任一種情況，方得使用：

- 1.法律明文規定。
- 2.為增進公共利益所必要。
- 3.為免除當事人之生命、身體、自由或財產上之危險。
- 4.為防止他人權益之重大危害。
- 5.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。
- 6.經當事人同意。
- 7.有利於當事人權益。



個資法小法典 個人資料保護法第19條、個人資料保護法第20條

► 實務操作提醒 ◀

組織在建立「個資盤點清冊」時應該呈現的內容包含：

- 資料是在什麼作業過程中進行蒐集、處理、利用；
- 這筆資料包含哪些資料種類；
- 資料的蒐集來源為何，可用以判斷資料為直接或間接蒐集；
- 蒐集之特定目的為何，機關內部目前保管的部門以及場所；
- 資料的保存期限；
- 該資料是否會委託他人進行蒐集、處理或利用。

實務上組織在執行個人資料檔案盤點時，常常無法輕易的區別蒐集個人資料的特定目的，若能在盤點清冊上標明其代號，常見特定目的例如：○九○為消費者、客戶管理與服務；一三六為資(通)訊與資料庫管理；類別C○○一為辨識個人等，將有助於確認個人資料蒐集種類、特定目的及程序的關聯性與合法性。

► 實務案例 ◀

D 電信公司企業文化相當重視個人資料保護，法務人員為了避免掛一漏萬，便在撰寫公司隱私權政策說明特定目的的地方，直接將法務部公告的「個人資料保護法之特定目的及個人資料之類別」中與公司營運有關係的所有目的，最大限度的都先放入特定目的之內容，例如○四○行銷、○六九契約、類似契約或其他法律關係事務、○七二政令宣導、○八一個人資料之合法交易業務、○八五旅外國人急難救助、○九○消費者、客戶管理與服務等。

由於電信公司實際業務目的應該是契約、類似契約關係、行銷及一般

消費者客戶管理。因此，D公司可能不適合以外國人急難救助作為蒐集個人資料的特定目的。

► 個資法遵建議 ◀

- 特定目的應以實際業務目的虛列即可。若於法務部所公布的「個人資料保護法之特定目的及個人資料之類別」找不到適合之項目，建議應該要將蒐集、處理及利用個人資料的特定目的清楚地合理闡述。
- 實務上很常見的情形是許多組織將大部分可能用到之特定目的匡列進去，但過於寬鬆的特定目的，難以使當事人了解蒐集的真正目的，因此個資法遵上建議特定目的應該扣合業務執行範圍，也不要使用「…」或「包含但不限於」等不明確之用語。總而言之，特定目的的匡列應該以當事人能夠清楚且明白瞭解蒐集個人資料之目的為準。

(三) 個資盤點方法與範例

實務上個資盤點之作法很多，沒有保證完全無疏漏的方法，但組織進行個資盤點時，大多建議以分析個資蒐集使用流程著手，盤點出公司所蒐集、處理以及利用的個人資料。這種方式可以比較精準的掌握組織蒐集使用個資的狀態，比較不容易有疏漏，也可以降低漏盤風險。

盤點其內容包括下列項目：

1. 整理組織各作業流程中所保有的各類文件、檔案、簿冊，清查確認其是否含有個人資料。
2. 清查所有涉及個人資料的文件，歸納整理成個人資料檔案，並建立個資盤點清冊。
3. 使用個資盤點清冊檢視組織保存的個人資料種類、確認個人資料檔案名稱、保存的特定目的及依據，以及保存現況。

- 4.使用個資盤點清冊檢視並確認，在平常業務的蒐集、處理及利用個人資料的過程當中，是否有違法的可能。
- 5.組織建立個資盤點清冊將個人資料檔案盤點檢視之成果。
- 6.製作個資盤點清冊並妥善保管且定期維護。

※個資盤點清冊範例參照附錄四

► 實務操作提醒 ◀

除了一開始建置個人資料管理制度時，需要進行個資盤點，更應該每年定期進行個人資料盤點。除此之外，若公司有新增業務或有業務變更終止時也應進行更新，並維護先前所建立的個資盤點清冊，藉以確實呈現組織當前個資管理現況。

► 實務案例 ◀

某 E 電信業者將客戶網路申裝與滿意度調查統一委外給 F 廠商進行一併作業，F 廠商針對客戶需求裝機完成後，將會請客戶簽名確認申裝服務已順利完成，並且同步給客戶填寫滿意度調查表。滿意度調查表上有該客戶申裝案號、姓名、年齡及產品訊息。惟 E 電信業者於年度個資盤點時卻忽略委外申裝與滿意度調查作業，未於個資盤點清冊中呈現，直至外部單位來查核時才發現缺失。

► 個資法遵建議 ◀

- 個資漏盤是實務上常見的缺失，尤其常發生於新拓展或委外處理的業務。
- 我國個資法規定，在個資法適用範圍內，受委託蒐集、處理或利用個人資料的單位，執行蒐集、處理或利用個人資料的行為，視同委託機關的行為。

- 一般公司常認為委外處理就不用將該業務納入個資盤點是錯誤的觀念。委外的個資相關業務仍要納入盤點範圍，尤其近年來常見發生委外廠商個人資料外洩事故，應更加注意。
- 個人資料管理制度上，建議於各部門個資盤點後，應該再由主要推動個資管理制度之單位或公司內部的稽核單位進行複查，避免有漏盤之狀況發生。

**個資法小法典 個人資料保護法第4條**

三、個人資料安全維護系統建置第三步驟：建立個人資料風險評估及管理機制

組織完成個資盤點後，可以比較清楚的掌握企業內部所擁有的個人資料範圍。為了正確評估並有效管理個人資料檔案可能面臨的風險，應建立個人資料的風險評估與管理機制，並執行個人資料風險評估與管理作業。

個人資料之風險評估與管理機制，可以分為風險評估與風險管理兩部分。

（一）風險評估

「風險評估」的目的在於識別可能導致風險發生的原因（包含本身的弱點與可能的威脅來源）。風險的發生可能來自四面八方，無論來自內部或外部、天然的或人為，惡意或非惡意，都可能形成風險。風險通常會利用組織或資產的弱點，對組織造成潛在損害或實質上的損失。

目前實務上最常發生的情形，像是來自組織外部、人為的且惡意的駭客入侵。另外，還包含利用組織或資產本身所存在的弱點，間接導致損害的產生，例如紙本文件具有易燃、方便攜帶的特性，而毀損、滅失或竊取含有個人資料的紙本文件。

關於風險評估之具體標準及實務作法，可參考經濟部標準檢驗局公布的CNS 27005「資訊技術—安全技術—資訊安全風險管理」與CNS 31000「風險管理—原則與指導綱要」等國家標準。

（二）風險管理

「風險管理」是針對個人資料所面臨的可能風險，提出相對應的管理策略。組織針對其保有之個人資料風險評估出來後，即可找到自身弱點所在，進而研擬風險對策進行管控。

參照經濟部標準檢驗局所公布的國家標準，內容包含下列4項處理原則：

1.風險修改

在符合風險評鑑及風險處理要求下，選擇適切及經過衡量的控制措施，以管理風險。控制措施內容可以是矯正、消弭、預防、偵測及監視等方式。藉由施行、移除或改變控制措施可管理風險等級，進而使殘餘風險被控制在可接受範圍。

2.風險保留

風險經評估過後，若特定的風險明顯符合組織內部個人資料管理政策的風險接受準則，則該風險可以保留，但建議組織可以預先提撥風險準備金，用以確保風險結果實現時，能支應相關費用與損害賠償。

3.風險避免

當特定風險持續增加或持續發生，而且接受或保留風險可能會為組織帶來損失或不利影響時，應該規劃避免風險的措施（包括避免產生風險的情形繼續發生，或變更目前產生風險的運作情形）。例如將實體檔案或

儲存媒體存放於上鎖空間中；設置防火牆等機制；加強員工個資保護相關教育訓練等。

4.風險分擔

經過風險評估後，可以將特定風險結果請求第三方進行有效管理。例如透過分包方式將監視資料系統的風險，轉交由資訊安全機構協助相關業務。值得注意的是，組織所管理風險的賠償責任，無法透過分包方式轉由第三方承擔。



個資法小法典

CNS 27005「資訊技術—安全技術—資訊安全風險管理」
CNS 31000「風險管理—原則與指導綱要」

四、個人資料安全維護系統建置第四步驟：訂定個人資料安全維護規定

(一)個人資料侵害事故預防、通報及應變作業程序

依照個資法施行細則與安全維護辦法，非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（下稱事故），應訂定下列應變、通報及改善機制：

- 事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。
- 事故發生後應受通報之對象及其通報方式。
- 事故發生後，其改善措施之研議機制。

另外應注意的是，當非公務機關遇到「重大個人資料事故」時，應即通報國家通訊傳播委員會。所謂「重大個人資料事故」是指個人資料遭竊取、

竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益的情形。

縱然有再周延的個資保護措施，個資事故發生的風險始終存在，因此依照上述規定制定並落實事故發生後的應變與通報等措施，才能夠在事故發生時，讓組織內部人員迅速應對，確保讓損害降到最小。



個資法小法典

個人資料保護法施行細則第12條第2項第4款
安全維護辦法第4條

► 實務操作提醒 ◀

個資事故通知

當組織發生個資事故時，組織應查明後以適當方式通知個資當事人，通知的內容至少應包含個人資料被侵害的事實及組織已採取的因應措施。

通知個資當事人的方式可以透過言詞、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。當前述通知方式需要的花費過鉅的時候，組織在斟酌技術的可行性與當事人隱私的保護情況下，可以透過網際網路、新聞媒體或其他適當公開方式為之。

※個資事故通知範本參照附錄五

有備無患 迅速防堵

除了避免個資事故發生之相關安全措施，組織應於事前訂定個資事故緊急應變措施，以防個資事故發生時可緊急應變處理，於短時間將損害降至最低。實務上常見組織訂有個資事故緊急應變之程序，但實際內容卻

無明確通報窗口與運作機制，這樣會導致事故發生時組織內部無法有效應變。

個資事故緊急應變措施應該有明確的流程，如此一來才能於事故發生的第一時間緊急處理。另外，組織所訂定之個資事故緊急應變措施，關於通報部分，往往僅有規定內部通報，而疏忽個資法通知當事人部分。

其實多數企業組織原本就有相關緊急應變程序，例如工安通報機制或資安通報事故，個資事故通報亦可直接適用類似之架構與方法為之，不用再建立新的通報制度。

► 實務案例 ◀

G為H電信業者的個資管理人員，負責公司個資管理制度程序書之撰寫與維護更新。鑑於近來同業發生重大個資外洩，造成當事人損害，造成該公司商譽嚴重受影響。所以G打算針對個資事故緊急應變程序多加著重，特別是個資事故發生當事人通知之部分。但卻發現公司相關程序規範為「對於個人資料遭竊取之當事人，以書面通知……」，將通知當事人之事故限縮於「個人資料遭竊取」，涵蓋範圍與個資法規定之事故類型不符合。

► 個資法遵建議 ◀

- 我國個資法規範個資事故之態樣，並非侷限於竊取而已，其明定公務機關或非公務機關違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。
- 針對個資事故當事人通知部分不能僅規範竊取而已，應該要符合個資法規範，包含竊取、洩漏、竄改等其他侵害才是。況且近年來亦常發生竄改當事人資料使其受損害之案例，若組織對此未有事故緊急應變措施，可能使當事人損害加重。

- 通知個資事故當事人的方式並不只限於「書面」，組織於通知時，可以靈活運用言詞、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的方式。如果組織將相關程序規範限定為「以書面通知……」，則可能大幅提高組織通知個資事故當事人所需支出的費用。
- 對於事故通知當事人之內容應該要明確，並以書函、簡訊等方式通知當事人個人資料被侵害之事實、事故經過、個人資料處理情形及事後所採取之因應措施等。若遇有重大個人資料事故者，應即通報主管機關。相關人員事後需檢討事故發生之原因並研擬預防措施，對於因個資事故可能發生之訴訟或損害，也應該加以分析評估。



個資法小法典 個人資料保護法第12條

(二) 符合個資法相關法令規定之內部管理程序

依照我國個資法與安全維護辦法，通傳產業者應就下列事項，訂定個人資料之管理程序：

- 蒐集、處理或利用之個人資料包含個資法第6條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。
- 檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。
- 檢視個人資料之蒐集、處理，是否符合個資法第19條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合個資法第7條第1項規定。

- 檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的之外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合個資法第7條第2項規定。
- 利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。
- 委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依個資法施行細則第8條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。
- 進行個人資料國際傳輸前，檢視是否受國家通訊傳播委員會相關法令限制並遵循之。
- 當事人行使個資法第3條所定權利之相關事項：
 - ◇ 當事人身分之確認。
 - ◇ 提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。
 - ◇ 對當事人請求之審查方式，並遵守個資法有關處理期限之規定。
 - ◇ 有個資法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。
 - ◇ 檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依個資法第11條第1項、第2項及第5項規定辦理。
 - ◇ 檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依個資法第11條第3項規定辦理。
 - ◇ 設置聯絡窗口供當事人申訴與諮詢。

► 實務操作提醒 ◀

- 組織除了訂定個資法相關法令規定之內部管理程序，最重要的是要遵守程序規範。個資管理制度上著重「說、寫、做」三者需一致，也就是程序書、人員認知與實際執行方式要同一。實務上常見空有內部管理程序，卻無落實、程序書規範和組織內部執行不一，或是程序書與內部業務根本無法扣合，這在個資管理制度上都不是有效管理，也容易造成管理上風險。
- 委外管理也是實務上常被忽略的部分，組織於程序書上往往制定相當嚴謹之管理規範，例如每半年對委外廠商進行查核、委外廠商合作終止後會進行個資刪除銷毀，但實際上卻無執行，造成個資管理上之漏洞，需加以注意。
- 實務運作上，組織之隱私權政策、隱私權聲明或是公告，都必須納入上述有關個資法之管理事項。並且建立文件化之程序。隱私權公告與個資告知聲明，應確保在蒐集個人資料之前，提供給當事人或讓其能顯而易見。例如業者為了受理民眾申辦電信相關業務，可於業者門市現場明顯處，以立牌方式公告說明其隱私權聲明，以達到告知隱私權政策的目的。
- 個資告知聲明要清楚說明，明確包含以下內容，如：機關名稱、蒐集目的、個資類別、個資使用方式及個資當事人權益等。須特別注意的是，對於蒐集目的的說明不應該模糊，或以概括方式表述。如果告知的內容並不符合實際個資蒐集使用情形，可能就不符合「明確告知」規定。因此，業者提供給個資當事人的個資聲明，必須因應不同業務內容，調整使用目的說明。

※告知函範本參照附錄六



個資法小法典 個人資料保護法第8條

► 實務案例 ◀

I 電視購物業者為了增加公司營收，讓業績達新高峰，開發一款新APP讓消費者能快速於手機完成單手下單消費，不用再一直等待進線，增加多元消費管道。但同樣為加入會員之流程，公司官網與APP所蒐集之個人資料目的與種類並無不同，且最終皆匯入同一資料庫做會員管理，官網與APP隱私權聲明卻有出入不一致之情況。實際加入會員流程中有蒐集消費者生日，卻沒有在APP版隱私聲明中提及。個資蒐集目的的說明也有差異，明明有行銷事實，公司APP上也沒有告知消費者。

► 個資法遵建議 ◀

- 如前述案例，實務上常見到明明是同一的公司的相同業務，網站入口的隱私權政策與APP入口的隱私權政策卻不同。這時候需進一步確認是因為具體蒐集、處理或利用個人資料之行為有所差異，還是僅為疏漏。通常同一業務的個資流程應為相同，隱私權政策應該要一致。
- 為了避免網站入口的隱私權政策與APP入口的隱私權政策出入或版次不一之情形發生，建議組織於管理制度流程中增加隱私權政策與個資告知聲明定期檢視，以及相關的變更之機制。

(三) 個人資料安全管理程序

個人資料安全管理的程序，包含資料安全管理、人員管理與設備安全管理。組織可從這三個面向著手個人資料安全的管理，確保個人資料檔案的安全，避免個人資料遭有心人士竊取、竄改、毀損、滅失或洩漏。

以下將就這三個面向說明組織應注意的事項：

1. 資料安全管理

- 訂定個人資料儲存媒體使用規範並確實執行。

- 個人資料儲存媒體於廢棄或轉作其他用途前，應以適當方式銷毀或確實刪除該媒體中所儲存之個人資料，確保個人資料完全移除，避免洩漏。委託他人執行上開行為時，也應依個資法施行細則第8條為適當監督。
- 蒐集、處理或利用個人資料時，如有加密或遮蔽之必要，應採取適當之加密或遮蔽機制。
- 傳輸個人資料時，針對不同的傳輸方式，組織應有相對應的適當安全防护機制。
- 依據所保有個人資料之重要性，採取適當之備份機制，同時對備份資料也必須予以適當保護。
- 採取適當之安全機制，避免用以蒐集、處理或利用個人資料之電腦、相關設備或系統遭無權限之存取或發生個資事故，例如：
 - ◇ 就個人資料之存取權限，設定必要之控管機制，並定期確認控管機制之有效性與適當性。
 - ◇ 安裝與建置防毒軟體、防火牆、入侵偵測系統 (Intrusion Detection System, IDS) 與入侵預防系統 (Intrusion Prevention System, IPS)。
 - ◇ 使用多因素認證機制 (Multi-Factor authentication, MFA)，同時帳號密碼應符合一定複雜度並定期更換。
 - ◇ 涉及個人資料的系統變更時，應確保其系統的安全性並未降低。
- 定期確認蒐集、處理或利用個人資料之電腦、相關設備或系統具備必要之安全性，包括但不限採取適當之安全機制，因應惡意程式及系統漏洞所造成之威脅。例如：
 - ◇ 定期更新病毒碼與執行掃毒作業。
 - ◇ 定期針對系統與程式漏洞安裝修補程式，倘遇有重大更新時，應即時安裝修補程式。

- 進行軟硬體測試時，應避免使用實際個人資料。如確有使用實際個人資料之必要時，應明確規定其使用之程序及安全管理方式。
- 定期檢查使用於蒐集、處理或利用個人資料之電腦、相關設備或系統之使用狀況及個人資料存取之情形。同時也必須設定異常存取個人資料行為的監控機制。

2.人員安全管理

- 確認蒐集、處理及利用個人資料的相關業務流程的負責人員。
- 依據執行業務的必要，建立管理機制，設定組織所屬人員關於個人資料蒐集、處理或利用，及接觸個人資料儲存媒體之相關權限，定期檢視權限設定內容之必要性與適當性，並控管接觸個人資料之情形。
- 要求所屬人員妥善保管個人資料的儲存媒介物，並與所屬人員約定保密義務（包含在職時與離職後的保密義務）。
- 當所屬人員離職時應確保取消其存取權限，並要求將執行業務所持有保管的文件與資料辦理交接，不得攜離使用。

3.設備安全管理

- 依據作業內容及環境之不同，實施必要之安全環境管制。
- 妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備。
- 針對不同作業環境，建置必要之保護設備或技術（例如設置監視器與門禁）。



個資法小法典

個人資料保護法施行細則第12條第1項
個人資料保護法施行細則第12條第2項第6款、第8款

► 實務操作提醒 ◀

- 個資法中所謂的適當安全措施，並非要求組織應一律以最高保護規格保護組織所保有的個人資料，而是組織應判斷其內部所保有的個人資料風險，依據風險評鑑的結果，同時考量組織內部運作的效率，選擇相對應的適當安全措施，並與所欲達成之個資保護目的間具有適當比例為原則。
- 實務上常見組織未經評估衡量，直接將個人資料安全管理程序用高規管理，但卻沒有資源或人力可以確實執行，如此僅為空泛程序無法有效管理，不是個資管理制度所要求的個人資料安全管理程序，有效的管理程序應要視組織風險評估採取適切管理模式。
- 法院實務上也會考量組織規模，判斷組織是否已採行適當安全措施，曾有組織於個資事故的民事損害賠償案件中主張其已採取防火牆、電子加密系統、封包加密處理與員工個人電腦防毒軟體等安全保護措施，也定有電腦使用管理辦法與舉辦資訊安全教育訓練，然而法院認為考量該組織規模與蒐集處理的個人資料數量，組織前述的安全防護措施只是基本配備（臺灣臺北地方法院107年度北小字第266號民事判決參照），因此組織仍應依循個資法及其施行細則與安全維護辦法規定，定期辦理個資盤點與風險評鑑，如此才能識別風險，並進而對症下藥。



個資法小法典 個人資料保護法施行細則第12條第2項

► 實務案例 ◀

J 電信公司為了方便用戶續約，直接將特惠續約方案以簡訊方式發送給用戶，簡訊內容含有網頁連結，網址為該公司網頁與消費者手機號碼組

成，點進連結則可直接看到該用戶之會員資料並可選擇直接續約，但由於該公司發送之簡訊網址連結為公司網頁與用戶手機號碼明碼組成，網址末端即為用戶之手機號碼，點進去即可看到其個人資料，造成有心人士只要變更網址手機號碼連結，即可清楚獲得他人個資，造成重大資安漏洞，該公司用戶個資亦因此被他人不當存取。

► 個資法遵建議 ◀

- 組織除了訂定個人資料安全管理程序，更應有相關管控與檢核程序，以避免前述案例發生。該案並不是遭受重大惡意攻擊，僅是廠商於相關業務服務功能設計時未將個資隱私考量進去，造成個資與資安上之問題。
- 近幾年隨著科技日益進步，大多商業模式往往為結合個人資料與新興科技運用而生，故相關業務服務功能設計是否有涵蓋個人資料之隱私保護亦格外重要，應該從業務服務功能設計時就將隱私報護納入考量。
- 組織於開發產品時，應一併考量隱私保護設計，如此一來則能避免個資隱私保護之疑慮。另外，新產品或新服務提供前，內部應要訂定檢核機制，避免有疏漏之處。如上述J公司之案例，只要於事前有設立相關檢核人員進行確認，即可避免問題發生。

(四) 國際傳輸

我國個資法針對個人資料的國際傳輸，是採取「原則開放，例外禁止」的規定。原則上，非公務機關可以進行國際傳輸個人資料，但是涉及下列情形時，中央目的事業主管機關（例如國家通訊傳播委員會），可以限制非公務機關進行個人資料國際傳輸：

1. 涉及國家重大利益。

- 2.國際條約或協定有特別規定。
- 3.接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
- 4.以迂迴方法向第三國（地區）傳輸個人資料規避個資法。

國家通訊傳播委員會曾於101年9月25日發布通傳通訊字第10141050780號令，表示「衡酌大陸地區之個人資料保護法令尚未完備，因此限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。」業者在進行個人資料國際傳輸應特別注意前述命令。此外，依照安全維護辦法，在進行個人資料國際傳輸前，也應該檢視該項傳輸是否受到國家通訊傳播委員會相關法令限制。



個資法小法典 安全維護辦法第5條第1項第7款

► 實務操作提醒 ◀

- 基於大陸地區個人資料保護法令尚未完備，國家通訊傳播委員會禁止通傳業者跨境傳輸至中國大陸，通傳業者在進行個人資料之國際傳輸時應該特別注意。
- 由於將個人資料進行國際傳輸，性質上依個案情節可能分別屬於個人資料的處理或利用，因此進行個人資料傳輸前，也必須依照個資法規定將相關事項告知個資當事人，例如個人資料所欲進行國際傳輸的區域、期間與對象。
- 若執行個人資料傳輸的是受委託的單位，委託機關也必須針對受委託單位執行個人資料國際傳輸情況進行適當監督。監督事項應該包含：
 - ◇ 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。

- ◇受託者就安全維護措施所採取之措施。
- ◇有複委託者，其約定之受託者。
- ◇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。
- ◇委託機關如對受託者有保留指示者，其保留指示之事項。
- ◇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。



個資法小法典

個人資料保護法施行細則第8條
個人資料法護法施行細則第12條第2項

(五)使用記錄、軌跡資料及證據保存

非公務機關對於個人資料的使用紀錄、軌跡資料及證據保存，應訂定相關機制並予以落實。這邊所指的機制應包含，為了執行個人資料檔案安全維護計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄的個人資料使用情況、軌跡資料及相關證據。

針對依個資法規定刪除、停止處理或利用所保有之個人資料後留存的紀錄，如刪除、停止處理或利用之方法、時間，或將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據等資料，也必須訂定相關紀錄、證據保存機制，並加以落實。



個資法小法典

個人資料法護法第11條第3項
個人資料保護法施行細則第12條第2項第10款
安全維護辦法第6條

► 實務操作提醒 ◀

- 個人資料保存應該有一定之期限，組織應依照該個人資料性質訂定。若有法定保存期間的規定，需依照法定保存期間保存以符合法規要求。
- 國家通訊傳播委員會針對通傳產業資料保存有許多規定，例如：
 - ◇ 有線廣播電視法第50條規定系統經營者對訂戶申訴案件應即妥適處理，並建檔保存六個月。
 - ◇ 電信管理法第9條電信事業對於用戶或使用電信人使用電信服務所生通信紀錄及帳務紀錄，應確保紀錄正確，保存一定期間及應予保密；用戶查詢其通信紀錄及帳務紀錄時，應予提供。
 - ◇ 行動寬頻業務管理規則第83條之2機房告警與錄影紀錄至少應保存六個月。



◇固定通訊業務管理規則第74條之6與行動寬頻業務管理規則第83條之5規定委外維運作業時應由電信設備機房員工全程監控，並將系統連線之操作指令完整記錄之，該紀錄檔應至少保存六個月。

這些國家通訊傳播委員會對資料保存期間之法定要求相關業者皆應遵守。

- 組織可依照個資保存之必要性，訂定相關保存期限，實務上許多業者會將會員資料定為永久保存，但基於個人資料保存必要性考量，不建議永久保存，應依法評估保存期限與後續利用行為是否妥當定之，否則在特定目的消逝後，皆應刪除銷毀。





組織何時需要了解「個人資料安全維護事項」內容並予以實踐？

組織執行業務時蒐集、處理或利用個人資料需合法，在掌握個人資料期間，組織有義務避免其所蒐集、處理或利用之個人資料被竊取、竄改、毀損、滅失或洩漏。此時，組織需了解並執行「個人資料安全維護事項」。

「個人資料安全維護事項」

「個人資料安全維護事項」是為了防止個人資料被竊取、竄改、毀損、滅失或洩漏，所採取的技術上及組織上之措施。「技術上措施」的實踐，可包括針對組織內之設備採取安全管理措施，以於技術上避免個人資料受到侵害。「組織上措施」的實踐，可包括組織對其成員提供個人資料保護相關之認知宣導及教育訓練。實踐上，組織需要：

(一) 依照內部成員對應的職務內容、執行計畫，成員於組織內之角色、職

務權限，分別辦理相對應之個人資料保護專業教育訓練，以確保組織內負責各項職務之成員，確切掌握職務內個人資料保護相關知識，以及避免個人資料侵害的應對措施。

- (二) 針對所有成員提供個人資料保護之教育訓練，訓練內容應要包括個人資料保護相關法令之規定，以及說明各成員對個人資料保護之責任範圍與各項個人資料保護之管理程序、機制及措施等要求。

**個資法小法典**

個人資料保護法施行細則第12條第1項
個人資料保護法施行細則第12條第2項第7、8款

► 實務操作提醒 ◀

- 組織應定期舉辦宣導個人資料法遵管理相關之教育訓練，以使成員均得瞭解個人資料管理制度之內容，以及個人資料保護之重要性，使個人資料管理制度得以有效執行。
- 亦有組織會採取定期寄發電子報給成員，在組織例行會議中宣布個人資料管理政策，或在組織資訊系統中之公共資料夾設置「個人資料保護專區」等方式，實踐個人資料保護認知宣導。
- 個人資料保護相關之教育訓練，組織除得自行培訓講師外，也可以委託外部專家講習，或者是指派組織內之相關成員參與外部訓練等方式進行。
- 辦理個人資料保護相關之教育訓練或講習時，組織應記得留存如課程簽到表或測驗成績等相關文件，以利後續之稽核時能順利提出有辦理教育訓練之佐證。



依照PDCA之精神，組織內規劃並逐步實踐個人資料保護相關安全維護事項的同時，亦應針對其規劃及實踐之個人資料保護相關措施進行「查核」（Check），並力求持續「改進」（Act）。

一、「查核」（Check）

組織因執行業務而合法蒐集、處理或利用個人資料時，應採取「個人資料安全稽核機制」，以確認及防止個人資料遭受被竊取、竄改、毀損、滅失或洩漏等侵害。實踐上，組織得定期或不定期確認個人資料安全維護事項的實施情形。如有發現不符合組織個人資料保護政策之事項時，應記錄違反組織內個人資料保護政策之情況，並分析該缺失發生之原因，進而評估採取何種矯正或預防措施，以改善個人資料安全維護計畫之有效性和效率，達採取資料安全稽核機制之目的。

二、「改進」(Act)

組織內個人資料安全維護事項之實施情形確認後，組織應採取措施整體持續改善個人資料之安全維護，以達個人資料保護之目的。實踐上，組織透過個人資料安全稽核機制所發現之缺失，並評估採取何種矯正或預防措施後，除應確實執行外，也應持續追蹤矯正或預防措施之實行狀況。同時，組織也得以實行狀況，針對組織內成員及其所負責業務範圍，進行滾動式調整，以求動態地實踐個人資料保護之相關政策、機制，達個人資料安全維護之整體持續改善之成果。



個資法小法典

個人資料保護法施行細則第12條第2項第9款
個人資料保護法施行細則第12條第2項第11款

► 實務操作提醒 ◀

- 組織在制定內部之個人資料安全稽核機制時，得考量「組織內部政策要求」，「組織將如何建立及維持稽核制度運行」，「組織如何進行監督和審查內部個人資料安全維護措施，以確保其有效性與效率」等層面，進行相關規劃。
- 個人資料安全稽核機制之內容，可包括稽核計畫之擬訂方式、稽核執行之內容、稽核員之資格與選任、受稽核單位應配合事項、稽核結果之審核及追蹤等事項，以確保個人資料安全稽核作業順利進行。

※個人資料保護與管理稽核檢查表參照附錄七



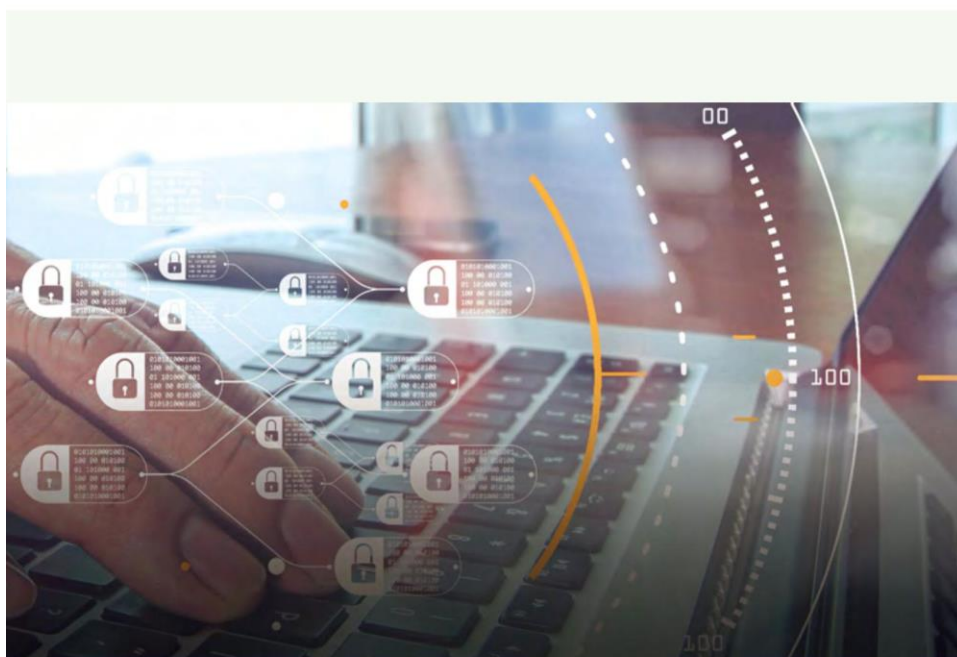
原則上，計畫中止後以下情形組織應主動或依個人資料當事人之請求，刪除、停止處理或利用該個人資料：

- (一) 組織如因業務規劃，導致先前合法蒐集、處理及利用個人資料之特定目的消失。
- (二) 組織個人資料保護政策規定的蒐集、處理及利用個人資料期限屆滿時。

但此原則例外情形如下：

- (一) 因組織執行職務或業務所必須。
- (二) 組織取得當事人書面同意得繼續處理或利用的狀況時。

實踐上，組織若因業務終止導致特定目的消失，進而著手刪除、停止處理或利用特定個人資料時，須記錄其刪除、停止處理或利用的方法、時間及地點。如果是因組織再造，而產生移轉特定個人資料的狀況時，除須



確認是否有移轉該個人資料之合法依據外，須確認接受該個人資料移轉之對象也具備相關合法依據。確認具備合法依據後，移轉個人資料時，應記錄移轉之原因，接受此個人資料移轉之對象、方法、時間、地點等資訊及接收者持有個資的合法依據。



個資法小法典 個人資料保護法第11條第3項

► 實務操作提醒 ◀

實務操作上最常發生的問題是，難以舉證資料是否已經確實刪除。為解決這個困境，建議組織得在刪除、銷毀個人資料與其相關載體（如公文夾、公用硬碟等）時，可採取全程錄影等有效紀錄銷毀軌跡的方式，保存完整刪除、銷毀的過程，以供未來查核時證明使用。

附錄一 | 個人資料保護法

第一章 總則

第1條（立法目的）

為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第2條（用詞定義）

本法用詞，定義如下：

- 一、個人資料：指自然人之姓名、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、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、社會活動及其他得以直接或間接方式識別該個人之資料。
- 二、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。
- 三、蒐集：指以任何方式取得個人資料。
- 四、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。
- 五、利用：指將蒐集之個人資料為處理以外之使用。
- 六、國際傳輸：指將個人資料作跨國（境）之處理或利用。
- 七、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。
- 八、非公務機關：指前款以外之自然人、法人或其他團體。
- 九、當事人：指個人資料之本人。

第3條（不得預先拋棄或以特約限制）

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

- 一、查詢或請求閱覽。

- 二、請求製給複製本。
- 三、請求補充或更正。
- 四、請求停止蒐集、處理或利用。
- 五、請求刪除。

第4條（視同委託機關）

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。

第5條（個人資料之處理行為）

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（特種個人資料之保護）

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。
- 依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

第7條（書面同意之內涵）

第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。

第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。

蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

第8條（直接蒐集個人資料應告知事項及免告知之情形）

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。

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。

第9條（間接蒐集個人資料之告知義務）

公務機關或非公務機關依第十五條或第十九條規定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條第一項第一款至第五款所列事項。

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。
- 第一項之告知，得於首次對當事人為利用時併同為之。

第10條（妨害重大利益要件之請求限制）

公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

- 一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
- 二、妨害公務機關執行法定職務。
- 三、妨害該蒐集機關或第三人之重大利益。

第11條（個人資料更正或補充及權責）

公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

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。

違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第12條（個人資料遭違法侵害之通知）

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

第13條（處理期限或延長）

公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

第14條（使用者付費）

查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

第二章 公務機關對個人資料之蒐集、處理及利用

第15條（公務機關蒐集或處理個人資料之要件）

公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

- 一、執行法定職務必要範圍內。
- 二、經當事人同意。
- 三、對當事人權益無侵害。

第16條（公務機關不得逾越執行法定職務之必要範圍）

公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

- 一、法律明文規定。
- 二、為維護國家安全或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、有利於當事人權益。
- 七、經當事人同意。

第17條（提供民眾查閱之公開事項）

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。

第18條（個人資料檔案之安全維護）

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。

第三章 非公務機關對個人資料之蒐集、處理及利用

第19條（非公務機關蒐集或處理個人資料之要件）

非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

- 一、法律明文規定。
- 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。
- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、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。
- 五、經當事人同意。
- 六、為增進公共利益所必要。
- 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
- 八、對當事人權益無侵害。

蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，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。

第20條（非公務機關利用個人資料之除外情形）

非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，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。

非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

第21條（非公務機關為國際傳輸個人資料之限制）

非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

- 一、涉及國家重大利益。
- 二、國際條約或協定有特別規定。
- 三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
- 四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。

第22條（行政監督之權責及保密義務）

中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認為必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

中央目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。

對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。

參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

第23條（扣留物或複製物之標示、保管及發還）

對於前條第二項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。

扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

第24條（不服聲明異議之權利及救濟）

非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。

前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。

第25條（違反規定之裁處）

非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分：

- 一、禁止蒐集、處理或利用個人資料。
- 二、命令刪除經處理之個人資料檔案。
- 三、沒入或命銷燬違法蒐集之個人資料。
- 四、公布非公務機關之違法情形，及其姓名或名稱與負責人。

中央目的事業主管機關或直轄市、縣（市）政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。

第26條（公布檢查結果）

中央目的事業主管機關或直轄市、縣（市）政府依第二十二條規定檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

第27條（個人資料檔案安全維護計畫及業務終止處理方法）

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

中央目的事業主管機關得指定非公務機關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。

前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

第四章 損害賠償及團體訴訟**第28條（公務機關違法之損害賠償）**

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。但損害因天災、事變或其他不可抗力所致者，不在此限。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。

對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。

同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。

第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第29條（非公務機關違法之損害賠償）

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。

依前項規定請求賠償者，適用前條第二項至第六項規定。

第30條（請求損害賠償之時效）

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。

第31條（公務、非公務機關損害賠償之適用法）

損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。

第32條（團體訴訟之符合要件）

依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：

- 一、財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。
- 二、保護個人資料事項於其章程所定目的範圍內。
- 三、許可設立三年以上。

第33條（損害賠償訴訟之管轄權）

依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。

前項非公務機關為自然人，而其在中華民國現無住所或住所不明者，以其在中華民國之居所，視為其住所；無居所或居所不明者，以其在中華民國最後之住所，視為其住所；無最後住所者，專屬中央政府所在地之地方法院管轄。

第一項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。

第34條（損害賠償團體訴訟裁判費減免）

對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。

前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。

其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。

其他因同一原因事實受有損害之當事人，亦得聲請法院為前項之公告。

前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認為必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。

依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。

第35條（撤回訴訟之當然停止）

當事人依前條第一項規定撤回訴訟實施權之授與者，該部分訴訟程序當然停止，該當事人應即聲明承受訴訟，法院亦得依職權命該當事人承受訴訟。

財團法人或公益社團法人依前條規定起訴後，因部分當事人撤回訴訟實施權之授與，致其餘部分不足二十人者，仍得就其餘部分繼續進行訴訟。

第36條（損害賠償請求權）

各當事人於第三十四條第一項及第二項之損害賠償請求權，其時效應分別計算。

第37條（訴訟行為之限制）

財團法人或公益社團法人就當事人授與訴訟實施權之事件，有為一切訴訟行為之權。但當事人得限制其為捨棄、撤回或和解。

前項當事人中一人所為之限制，其效力不及於其他當事人。

第一項之限制，應於第三十四條第一項之文書內表明，或以書狀提出於法院。

第38條（自行提起上訴之要件及時期）

當事人對於第三十四條訴訟之判決不服者，得於財團法人或公益社團法人上訴期間屆滿前，撤回訴訟實施權之授與，依法提起上訴。

財團法人或公益社團法人於收受判決書正本後，應即將其結果通知當事人，並應於七日內將是否提起上訴之意旨以書面通知當事人。

第39條（不得請求訴訟所得之報酬）

財團法人或公益社團法人應將第三十四條訴訟結果所得之賠償，扣除訴訟必要費用後，分別交付授與訴訟實施權之當事人。

提起第三十四條第一項訴訟之財團法人或公益社團法人，均不得請求報酬。

第40條（訴訟代理人）

依本章規定提起訴訟之財團法人或公益社團法人，應委任律師代理訴訟。

第五章 罰則

第41條（罰則）

意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，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42條（罰則）

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

第43條（罰則）

中華民國人民在中華民國領域外對中華民國人民犯前二條之罪者，亦適用之。

第44條（罰則）

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

第45條（告訴乃論）

本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。

第46條（從重處罰）

犯本章之罪，其他法律有較重處罰規定者，從其規定。

第47條（罰則）

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（罰則）

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49條（罰則）

非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。

第50條（罰則）

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。

第六章 附則

第51條（除外規定）

有下列情形之一者，不適用本法規定：

- 一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
- 二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

第52條（委託及保密義務）

第二十二條至第二十六條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理；其成員因執行委任或委託事務所知悉之資訊，負保密義務。

前項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

第53條（特定目的及個人資料類別之訂定）

法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。

第54條（告知義務及處罰）

本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。

前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。

未依前二項規定告知而利用者，以違反第九條規定論處。

第55條（施行細則）

本法施行細則，由法務部定之。

第56條（施行日）

本法施行日期，由行政院定之。

現行條文第十九條至第二十二條及第四十三條之刪除，自公布日施行。

前項公布日於現行條文第四十三條第二項指定之事業、團體或個人應於指定之日起六個月內辦理登記或許可之期間內者，該指定之事業、團體或個人得申請終止辦理，目的事業主管機關於終止辦理時，應退還已繳規費。已辦理完成者，亦得申請退費。

前項退費，應自繳費義務人繳納之日起，至目的事業主管機關終止辦理之日止，按退費額，依繳費之日郵政儲金之一年期定期存款利率，按日加計利息，一併退還。已辦理完成者，其退費，應自繳費義務人繳納之日起，至目的事業主管機關核准申請之日止，亦同。

｜附錄二｜個人資料保護法施行細則

第1條

本細則依個人資料保護法（以下簡稱本法）第五十五條規定訂定之。

第2條

本法所稱個人，指現生存之自然人。

第3條

本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

第4條

本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。

本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。

本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。

本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。

本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。

本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

第5條

本法第二條第二款所定個人資料檔案，包括備份檔案。

第6條

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。

本法第二條第四款所稱內部傳送，指公務機關或非公務機關本身內部之資料傳送。

第7條

受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

第8條

委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

前項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。

第一項之監督，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。

第9條

本法第六條第一項但書第一款、第八條第二項第一款、第十六條但書第一款、第十九條第一項第一款、第二十條第一項但書第一款所稱法律，指法律或法律具體明確授權之法規命令。

第10條

本法第六條第一項但書第二款及第五款、第八條第二項第二款及第三款、第十條但書第二款、第十五條第一款、第十六條所稱法定職務，指於下列法規中所定公務機關之職務：

- 一、法律、法律授權之命令。
- 二、自治條例。
- 三、法律或自治條例授權之自治規則。
- 四、法律或中央法規授權之委辦規則。

第11條

本法第六條第一項但書第二款及第五款、第八條第二項第二款所稱法定義務，指非公務機關依法律或法律具體明確授權之法規命令所定之義務。

第12條

本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及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。

前項措施，得包括下列事項，並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：

- 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。

第13條

本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱當事人自行公開之個人資料，指當事人自行對不特定人或特定多數人揭露其個人資料。

本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱已合法公開之個人資料，指依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

第14條

本法第六條第一項但書第六款、第十一條第二項及第三項但書所定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。

第15條

本法第七條第二項所定單獨所為之意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。

第16條

依本法第八條、第九條及第五十四條所定告知之方式，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。

第17條

本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

第18條

本法第十條但書第三款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

第19條

當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明。

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
- 三、原蒐集目的不符。
- 四、特定目的已達成而無繼續處理或利用之必要。
- 五、其他事由足認該特定目的已無法達成或不存在。

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。

第22條

本法第十二條所稱適當方式通知，指即時以言詞、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。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

第23條

公務機關依本法第十七條規定為公開，應於建立個人資料檔案後一個月內為之；變更時，亦同。公開方式應予以特定，並避免任意變更。

本法第十七條所稱其他適當方式，指利用政府公報、新聞紙、雜誌、電子報或其他可供公眾查閱之方式為公開。

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。

第25條

本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案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。

第26條

本法第十九條第一項第二款所定契約或類似契約之關係，不以本法修正施行後成立者為限。

第27條

本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。

本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者：

- 一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。
- 二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。

第28條

本法第十九條第一項第七款所稱一般可得之來源，指透過大眾傳播、網際網路、新聞、雜誌、政府公報及其他一般人可得知悉或接觸而取得個人資料之管道。

第29條

依本法第二十二條規定實施檢查時，應注意保守秘密及被檢查者之名譽。

第30條

依本法第二十二條第二項規定，扣留或複製得沒入或可為證據之個人資料或其檔案時，應掣給收據，載明其名稱、數量、所有人、地點及時間。

依本法第二十二條第一項及第二項規定實施檢查後，應作成紀錄。

前項紀錄當場作成者，應使被檢查者閱覽及簽名，並即將副本交付被檢查

者；其拒絕簽名者，應記明其事由。

紀錄於事後作成者，應送達被檢查者，並告知得於一定期限內陳述意見。

第31條

本法第五十二條第一項所稱之公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人、財團法人及行政法人。

第32條

本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。

第33條

本細則施行日期，由法務部定之。



附錄三 | 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法

第1條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第2條

本辦法所稱非公務機關包括下列各款：

- 一、第一類電信事業。
- 二、第二類電信事業。
- 三、有線廣播電視系統經營者及有線電視節目播送系統。
- 四、電視事業。
- 五、訂戶數達三千戶以上之直播衛星廣播電視服務事業。
- 六、經營國內新聞台頻道或購物頻道之衛星或其他類頻道節目供應事業。

第3條

非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）。

本計畫及處理方法之訂定或修正，應經非公務機關負責人或法定代理人簽署。

非公務機關蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫。

第4條

非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制：

- 一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。

二、事故發生後應受通報之對象及其通報方式。

三、事故發生後，其改善措施之研議機制。

非公務機關遇有重大個人資料事故者，應即通報國家通訊傳播委員會（以下簡稱本會）。

前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。

第5條

非公務機關應就下列事項，訂定個人資料之管理程序：

- 一、蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。
- 二、檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。
- 三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條第一項規定。
- 四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合本法第七條第二項規定。
- 五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。
- 六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。
- 七、進行個人資料國際傳輸前，檢視是否受本會相關法令限制並遵循之。
- 八、當事人行使本法第三條所定權利之相關事項：
 - （一）當事人身分之確認。
 - （二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。

(三)對當事人請求之審查方式，並遵守本法有關處理期限之規定。

(四)有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。

九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。

十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理。

十一、設置聯絡窗口供當事人申訴與諮詢。

第6條

非公務機關應就下列事項，訂定相關紀錄、證據保存機制：

一、因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之個人資料使用情況、軌跡資料及相關證據。

二、依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄：

(一)刪除、停止處理或利用之方法、時間。

(二)將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

第7條

本辦法自發布日施行。

附錄四 | 個資盤點清冊

盤點負責人：

[illegible]

資料來源：本手冊自行繪製

附錄五 | 個資事故通知範本

*以下僅供參考，實際內容應依安全維護辦法第3條規定，視實際事故情況及公司因應政策調整

個資事故通知範本（一）

親愛的使用者您好：

本公司近日接獲消費者告知有關詐騙集團以本公司網站名義及消費者相關個資進行詐騙。經本公司調查，該等疑似個資外洩事故可能來自於本公司系統的瑕疵，本公司在疑似個資外洩事故發生後，已先行修補，並確保系統已無相關瑕疵。此外，本公司也委託專業資訊廠商進行新版系統開發，確保個資保護機制能有效落實。

本公司致力於確保各位消費者使用本公司服務之良好體驗。若您有相關的建議與疑問，歡迎採以下聯絡管道與我們聯繫。

客服聯絡：0800-000-000

資料來源：本手冊自行繪製

個資事故通知範本（二）

親愛的會員您好

非常抱歉，由於您在今年的03月在本公司B網站購物消費，B網站近日因遭駭客入侵發生個人資料外洩事故，且已有消費者接獲詐騙集團電話。提醒您，如有接獲疑似詐騙電話，請不要聽從指示操作ATM或提供任何個人資料，請立即通報165警政署反詐騙專線，本公司已針對該個資事故進行系統升級與資訊安全加密保護，未來也會持續加強個人資料保護與資訊安全管理，以降低消費者個資被侵害的風險。如您有訂單問題或與本次事故之疑問，請於平日上班時間與本公司客服人員聯繫（02-0000-0000）。

資料來源：本手冊自行繪製

附錄六 | 告知函範本

*以下僅供參考，實際內容應依安全維護辦法第3條規定，視實際業務及公司個資政策調整

個資蒐集告知聲明範本（一）

個人資料蒐集告知聲明

○○電信股份有限公司基於「契約履行」、「消費者／客戶／會員管理與服務」、「經營電信業務／電信加值網路業務」、「電子商務服務」、「行銷」、「調查、統計與研究分析」、「資通訊服務」等目的，須蒐集您的個人資料。您可依法向我們行使「查詢／閱覽／補充／更正個人資料」、「提供個人資料複本」、「要求停止蒐集／處理／利用個人資料」、「要求刪除個人資料」等權利。更多關於我們如何蒐集／處理／利用您的個人資料，以及您的權利行使等資訊，請見○○電信股份有限公司個人資料蒐集告知聲明（註：此處置入網頁連結或另放置QR code；或依該消費者之特性，也可寄送電子郵件或直接交付紙本）。

資料來源：108年通傳事業導入隱私保護管理機制與資料加值服務之研析委託研究_期末報告-上冊_附件2

個資蒐集告知聲明範本（二）

○○電信股份有限公司個人資料蒐集告知聲明

感謝您成為本公司的客戶，本公司重視您的隱私與個人資料保護，並尊重您的個人資料控制權。以下將說明本公司如何蒐集、處理、利用您的個人資料，以及您有哪些權利可以行使。請留意，如您不是申辦本服務之人（非契約當事人）但使用本服務時（由他人申辦但供您使用），以下內容也對您適用。申辦本服務之人有義務讓實際使用本服務之人詳閱以下內容。

- 1.誰在蒐集您的個人資料
○○電信股份有限公司（以下稱為「我們」）。
- 2.我們為什麼蒐集您的個人資料（蒐集目的）
（註：請再依實際情形補充或調整）

- 履行契約義務及行使契約權利
- 履行法定義務
- 消費者／客戶／會員管理與服務
- 電子商務服務
- 電信業務／電信加值網路業務
- 行銷
- 調查、統計與研究分析
- 資(通)訊服務／資料庫管理／安全管理

3. 我們蒐集您的哪些個人資料(註：請再依實際情形補充或調整下列內容)

· 帳戶資訊

- 包含您的姓名、電話、地址、電子郵件信箱等在申請服務時提供的識別類及特徵類個人資料(須依法提供身分證明文件)。
- 其他與您申辦的服務有關，或您在使用過程產生的資訊，例如我們指配給您的號碼、通信紀錄、帳單紀錄、消費及繳費方式、服務歷程紀錄、服務或設備之識別代碼，以及其他與您的帳戶相關的個人資料。

· 服務使用與效能資訊

包含可揭露您如何使用我們的服務，以及我們的服務效能之資訊。

· 網路使用資訊

如果您使用我們的網路服務，我們將取得您的網路使用情形資訊，例如：

- 您的ip位址
- 您造訪的網頁之資訊(例如瀏覽網址、造訪及停留時間等)。
- 您的行動裝置應用程式使用資訊(例如應用程式名稱、使用情形等)。

· 位置資訊

如您使用我們的電話或網路服務，我們將取得您的地理位置資訊。

· 其他服務資料

如您已經或在將來成為我們其他服務的客戶／會員，我們可能會將您的個人資料與其他服務之資料串接整併。

4. 我們如何利用您的個人資料(註：請再依實際情形補充或調整下列內容)

4.1 期間及地區

我們會在您使用本服務(保有帳戶)的期間與地區內利用您的個人資料。
當本契約終止或解除(您不再使用本服務)後，我們會在法令要求或許可

的範圍與期限內保留及利用您的個人資料，並在該期限後，以無法識別您的身分之形式保存您使用本服務期間所提供或產生的資料。

4.2 利用個人資料之方式與對象

我們會以必要的方式利用您的個人資料以達成蒐集目的，例如：

- 為您建立客戶／會員檔案以便我們管理帳戶。
- 為提供客戶服務而以您的各項聯繫方式與您為業務聯繫（包含寄送商品）、向您通知與您申辦之服務有關的資訊，或回覆您的提問、申訴。
- 寄送帳單／催繳訊息至您的地址或電子郵件信箱；藉由電話聯繫或簡訊通知您有關繳費／催繳之資訊。
- 以您的各項聯繫方式向您提供行銷資訊，例如優惠方案、促銷活動、我們的其他服務，以及其他更適合您的服務方案等。
- 分析您的個人資料以維持、保護、開發及增進我們的服務。
- 分析您的個人資料以依分析結果向您推薦我們提供的其他您可能有興趣或適合您的商品／服務。
- 分析您的個人資料，並以統計數據、趨勢或其他無法識別您的身分之形式產出結果，對外提供給我們的企業客戶（例如讓企業客戶瞭解他們的門市熱點、消費者年齡／性別分布、消費者停駐時間等）。

將您的個人資料提供給受我們委託的第三人（例如行銷／分析／調查／廣告／公關業者、物流業者、金流業者、資訊服務業者等），在受委託的範圍內協助我們達成蒐集目的。我們會對受委託的第三人執行必要的監督，以確保您的個人資料安全

- 違約行為的預防、調查與權利行使。

4.3 蒐集目的以外的利用（註：非我國個資法要求應告知之內容，但適當揭露有助於提升透明度）

我們只會在蒐集目的之必要範圍內，依前述說明利用您的個人資料，除非：

- 法律明文規定。例如受司法機關或主管機關依法要求提供個人資料。
- 為增進公共利益所必要或為防止他人權益之重大危害。例如為維護網路完整性、確保網路與裝置安全、偵測／預防詐欺或網路犯罪等違法行為。

- 為免除您的生命、身體、自由或財產上之危險。例如當您行蹤不明時，將您的位置資訊提供給有權得知之第三人。
- 受公務機關或學術研究機構請託，基於公共利益為統計或學術研究而有必要，以無法識別您的身分之形式，提供資料給該公務機關或學術研究機構；或以可識別您的身分之形式提供資料，但該公務機關或學術研究機構保證所產出並對外揭露之結果無法識別您的身分。
- 依法得到您的同意。
- 有利於您的權益。

5. 您有哪些權利可以行使

- 您有權請求查詢、閱覽我們保有您的個人資料，或請求我們提供複製本。但我們依法得酌收必要的成本費用。
- 您有權向我們補充或更正您的個人資料
- 當本契約終止或解除後，或您認為我們不再需要您的個人資料時，您有權請求我們刪除、停止處理或利用您的個人資料。但我們因執行業務所必須（例如法令已規定保存期限），或另外取得您的書面同意時，仍得保存或繼續處理、利用您的個人資料。
- 如您認為我們違法蒐集、處理或利用您的個人資料時，您有權請求我們刪除、停止蒐集、處理或利用您的個人資料。但我們會檢視是否有違法情形，並回覆您結果。
- 如您不願再收到我們的行銷資訊，您有權通知我們拒絕接受行銷。
- 如您要行使上述各項權利，請洽……（註：請補充客戶行使權利之方式、管道）。

6. 您若不提供個人資料的影響

- 如您未正確、完整填寫或提供申辦服務所需資料，可能無法申辦本服務，或將無法即時收到與本服務相關的必要資訊。
- 其他個人資料是您在使用本服務的過程中（自動）產生並記錄，若您不願意我們處理或利用，請依上述權利行使方式辦理。

資料來源：108年通傳事業導入隱私保護管理機制與資料加值服務之研析委託研究_期末報告-上冊_附件2

附錄七 | 個人資料保護與管理稽核檢查表

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
1.法律責任	1.1 應清楚瞭解，違反個人資料保護法將有可能遭到民事損害賠償、刑事或行政處分的處罰。	☐ 符合 ☐ 不符合	
2.投入資源人力	2.1 應配置專責人員或組織及相當資源。	☐ 符合 ☐ 不符合	
	2.2 應確實訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法(以下簡稱本計畫及處理方法)，並由負責人或法定代理人簽署。	☐ 符合 ☐ 不符合	
	2.3 蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內(TPIPAS)或國際(BS等)個人資料安全稽核機制之規劃及執行計畫。	☐ 符合 ☐ 不符合 ☐ 不適用	
3.界定個人資料	3.1 應完整界定個人資料範圍。	☐ 符合 ☐ 不符合	
	3.2 應保留盤點紀錄，如盤點清冊。	☐ 符合 ☐ 不符合	
4.風險評鑑及管理機制	4.1 應針對含有個資之流程進行風險評鑑。	☐ 符合 ☐ 不符合	
	4.2 應保留相關紀錄，如風險評鑑表。	☐ 符合 ☐ 不符合	
	4.3 風險評鑑之方式應能有效評估流程中之高低風險。	☐ 符合 ☐ 不符合	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
4.風險評鑑及管理機制	4.4 針對組織所不能接受之風險，應進行有效之風險處理。	☐ 符合 ☐ 不符合	
5.事故之應變、通報及改善機制	5.1 針對個資事故應設有完善之通報、應變及改善機制。	☐ 符合 ☐ 不符合	
	5.2 應設計於適當期間內以適當方式及內容通知當事人之程序。	☐ 符合 ☐ 不符合	
	5.3 應設置遇有重大個人資料事故時，確實通報主管機關之機制。	☐ 符合 ☐ 不符合	
	5.4 機制中應含有防止損害擴大、補救措施及防止類似事件再次發生之要求。	☐ 符合 ☐ 不符合	
6.蒐集處理及利用之內部管理程序	6.1 資料蒐集、處理應具備確認符合法定要件之程序，並保留相關紀錄（如審核紀錄）。	☐ 符合 ☐ 不符合	
	6.2 蒐集當事人個資應履行告知義務（未履行告知義務時，應符合免告知之情形）。	☐ 符合 ☐ 不符合	
	6.3 個人資料之利用，應符合蒐集時特定目的之範圍。	☐ 符合 ☐ 不符合	
	6.4 如有原蒐集特定目的外之利用，應符合法定要件。	☐ 符合 ☐ 不符合	
	6.5 應符合個資法行銷相關規定（如提供拒絕行銷之方式或保留當事人拒絕行使行銷之處理紀錄）。	☐ 符合 ☐ 不符合 ☐ 不適用	
	6.6 特定目的消失或期限屆至時，應刪除、銷毀、停止蒐集處理利用個資。如未刪除、銷毀、停止蒐集處理利用個資，應有法定理由。	☐ 符合 ☐ 不符合	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
6.蒐集處理及利用之內部管理程序	6.7 應於蒐集、處理或利用過程中，確保個人資料之正確性，並就不正確或正確性有爭議之資料，有適當之處置方式。	☐ 符合 ☐ 不符合	
7.特種個人資料	7.1 應依個資法規定蒐集、處理或利用特種個人資料(病歷、醫療、健康檢查、基因、犯罪前科、性生活)。	☐ 符合 ☐ 不符合 ☐ 不適用	
8.當事人權利行使	8.1 應提供當事人權利行使之管道，並建立相關程序確保落實8.2到8.5之要求。	☐ 符合 ☐ 不符合	
	8.2 受理當事人權利行使時，應確認為當事人或其代理人身份之相關證明文件。	☐ 符合 ☐ 不符合	
	8.3 延長回覆期間時，應將原因以書面通知當事人。	☐ 符合 ☐ 不符合	
	8.4 駁回當事人申請時，應具備法定要件，並以書面將拒絕事由告知當事人。	☐ 符合 ☐ 不符合	
	8.5 應將當事人權利行使回覆情形做成紀錄供機關備查。	☐ 符合 ☐ 不符合	
9.個人資料業務委外	9.1 如有委託第三方蒐集、處理或利用個人資料，應對受託方為適當之監督，並保留必要之紀錄。	☐ 符合 ☐ 不符合	
	9.2 應於委託契約或相關文件中，約定個人資料委外監督之事項。	☐ 符合 ☐ 不符合 ☐ 不適用	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
10.國際傳輸	10.1 應符合個資法及主管機關關於國際傳輸相關法令之限制。	☐ 符合 ☐ 不符合 ☐ 不適用	
11.資訊安全 (如組織已通過資安相關驗證(如ISO27001)得提供驗證相關紀錄作為本問項之符合證明)	11.1 應針對含有個人資料之檔案設有存取控制措施，包括存取權限設定程序(含存取必要性與最小性之要求)、權限審核、權限清查、存取紀錄留存等。	☐ 符合 ☐ 不符合	
	11.2 應針對含有個人資料之檔案進行必要之加密，包括加密要求之規則、方式與強度。	☐ 符合 ☐ 不符合	
	11.3 應針對個人資料電子檔案之傳送進行管控，包括使用強度足夠之加密通訊協定、傳送必要性確認等。	☐ 符合 ☐ 不符合	
	11.4 應使用合法且無明顯漏洞之軟體，包括系統軟體licence確認、系統軟體即時更新確認等。	☐ 符合 ☐ 不符合	
	11.5 應確認必要防毒軟體之布建與更新狀況。	☐ 符合 ☐ 不符合	
	11.6 應要求處理個人資料之員工或供應商等簽署保密協定。	☐ 符合 ☐ 不符合	
	11.7 應針對重要之設備或場域進行必要之管控，包括建立必要安全網路架構、定期進行設備、系統元件、資料庫系統及軟體漏洞修補及可攜式儲存媒體使用安全管理作業規定等。	☐ 符合 ☐ 不符合	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
11.資訊安全 (如組織已通過資安相關驗證(如ISO27001)得提供驗證相關紀錄作為本問項之符合證明)	11.8 人員進出(管理)情形應具體掌控,包括人員存取權限與紀錄、門禁機制與紀錄等。	☐ 符合 ☐ 不符合	
	11.9 應保留稽核紀錄。	☐ 符合 ☐ 不符合	
12.認知宣導及教育訓練	12.1 應定期針對新進人員及內部員工進行個資保護與管理相關認知宣導與教育訓練,並保留相關紀錄。	☐ 符合 ☐ 不符合	
13.稽核機制	13.1 應定期實施稽核,並保留相關紀錄。	☐ 符合 ☐ 不符合	
14.紀錄保存	14.1 應保存個資管理紀錄、軌跡資料及相關紀錄。	☐ 符合 ☐ 不符合	
15.個人資料安全維護之整體持續改善	15.1 應針對稽核之結果、法規之變更、主管機關或業主之要求等情形定期檢視,並改善公司個人資料保護與管理制度之作法。	☐ 符合 ☐ 不符合	
備註	1. 建議事項		
	2. 觀察事項		
	3. 優良事項		

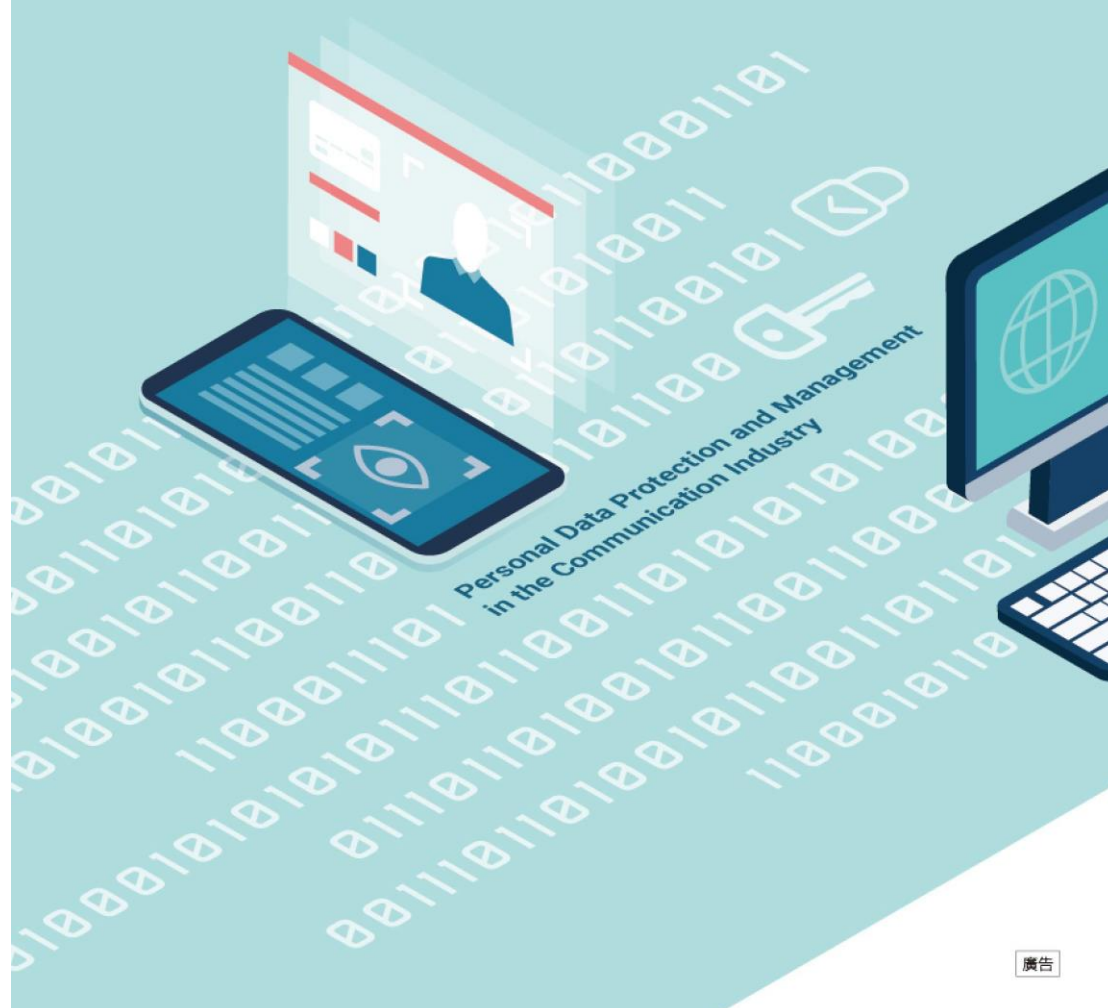
查核結果說明表

項目		定義
查核結果	符合	對本問項有完善落實，並能提具相關佐證證明或說明
	不符合 (高風險)	對本問項內容尚未執行、未確實落實以致有違法重大風險
	不適用	無執行與本問項有關之流程或業務，或未達法規適用門檻
備註	建議事項 (低風險)	針對查核項目之相關建議
	觀察事項 (中風險)	針對查核項目發現可能有負面影響，目前評為符合但未來若未改進則可能視為不符合
	優良事項	針對查核項目發現表現良好之具體事項

資料來源：本手冊自行繪製

主要參考資料

- 個人資料保護法
- 個人資料保護法施行細則
- 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法
- 台灣個人資料保護與管理制度 (TPIPAS)
- 國家標準 CNS 29100
- 財團法人資訊工業策進會科技法律研究所，《個資保護2.0》，書泉（2019）



廣告

附錄3：通傳產業個人資料保護與管理實作指引手冊領取名單（略）

附錄4：研討會會議手冊

通傳資料應用與法制整備研討會



通傳資料應用與法制整備研討會

時間	與會人員	
09:00-09:40	貴賓報到	
09:40-10:00	開幕致詞	國家通訊傳播委員會 陳耀祥 主任委員
		財團法人資訊工業策進會 科技法律研究所 王偉霖 所長
【場次一】通傳產業資料應用與法制研析		
10:00-12:00	主講人	財團法人資訊工業策進會 科技法律研究所 孫鈺婷 專案經理
	主持人	財團法人資訊工業策進會 科技法律研究所 顧振豪 副所長
	與談人	國家通訊傳播委員會 鄧惟中 委員
		國家發展委員會 李世德 參事
		東吳大學 法律系 余啟民 副教授
		景翊科技股份有限公司 陳奕廷 總經理
		意藍資訊股份有限公司 楊立偉 董事總經理
	財團法人工業技術研究院 產業科技國際策略發展所 趙祖佑 總監	
12:00-13:20	午餐時間	
【場次二】通傳產業資料應用與法遵運作		
13:20-15:10	主講人	達文西個資暨高科技法律事務所 王慕民 合夥律師
	主持人	達文西個資暨高科技法律事務所 葉奇鑫 所長暨主持律師
	與談人	國立臺北大學 經濟系 郭文忠 教授
		國立政治大學 法律系 劉定基 副教授
		凱擘股份有限公司 法務法規室 林雅惠 處長
		遠傳電信 法務法規暨採購群 李和音 資深副總經理
	財團法人資訊工業策進會 科技法律研究所 林冠宇 組長	
15:10-15:30	休息時間	
【場次三】通傳資料應用與疫情防制議題研析		
15:30-17:10	主講人	財團法人資訊工業策進會 科技法律研究所 王德瀛 專案經理
	主持人	財團法人電信技術中心 陳人傑 主任
	與談人	國家通訊傳播委員會 孫雅麗 委員
		中國文化大學 法律學系 李寧修 教授
		中原大學 財經法律學系 江耀國 教授
		中華電信股份有限公司 法律事務處 鍾國強 法務副總
		理律法律事務所 曾更瑩 合夥律師
	財團法人資訊工業策進會 科技法律研究所 宋佩珊 副主任	



場次一 主持人 顧振豪

財團法人資訊工業策進會 科技法律研究所 | 副所長

專長領域

通訊傳播匯流法制、新興媒體與視聽文化傳播、個人資料保護與資料開放運用、創新科技與法規調適

專業經歷

資策會科技法律研究所 | 副所長
國家通訊傳播委員會籌備處 | 法律研究員
台灣經濟研究院 | 助理研究員
網路內容防護機構 (iWIN) 多方利害關係人諮詢會議 | 委員
TWNIC 網域名稱委員會 | 委員
臺灣高等檢察署電腦犯罪防制中心諮詢協調委員會 | 委員
Open Data 聯盟制度法規組 | 副召集人
國家發展委員會資料開放諮詢小組 | 諮詢委員
臺北市政府 | 市政顧問
行政院政府資料開放諮詢小組 | 諮詢委員
國立故宮博物院政府資料開放諮詢小組 | 諮詢委員

相關著作

- ▶ 完備資料開放與自主管理機制，建構數位國家發展基礎，顧振豪，國土與公共治理季刊第 4 卷第 4 期，2016
- ▶ 資通安全規範下的關鍵資訊基礎設施保護，收錄於 104 年國家關鍵基礎設施防護法制架構及推動略研討會論文集，2015
- ▶ 建構資料開放之良善法制環境 (戴豪君、顧振豪)，國土及公共治理季刊第 3 卷第 4 期，2015
- ▶ 公司治理中個人資料保護與管理制度的建立-從直接蒐集與間接蒐集樣態談起，萬國法律第 181 期，2012
- ▶ 給科技研發與創新服務者的個資運用藍圖 (合著)，商周出版，2011
- ▶ 歐盟通訊匯流管制革新經驗對我國之政策意涵—以歐盟與英國隨選視訊服務 (VOD) 規範為例，收錄於「歐洲聯盟經貿政策之新頁」專書，國立台灣大學出版中心，2011.05
- ▶ 匯流管制革新下隨選視訊節目規範趨勢之探討 (李淳、顧振豪)，收錄於 2010 年第五屆全國法學實證研究研討會論文集，2010.05
- ▶ 優質網路社會基礎法制初探 (王郁琦、顧振豪)，收錄於「第 21 屆近代工程技術暨第 28 屆中美工商聯合會議」論文集，2006.09
- ▶ RFID 應用與相關法制問題研析 - 個人資料在商業應用上的界限，科技法律透視，第 18 卷第 5 期，2006.05
- ▶ 我國促進高速寬頻網路發展之法制建議--固定網路用戶迴路的相關爭議與法制建議，收錄於「建構行動生活基礎法制研討會」，經濟部技術處，2005.11
- ▶ 從法規及經營面探討電力線通訊開放的相關問題 - 從美國聯邦通訊委員會的管制措施談起，科技法律透視，第 17 卷第 9 期，2005.09

場次一 與談人

鄧惟中

國家傳播通訊委員會 | 委員

專長領域

網路通訊協定

資訊安全

網路安全

虛擬實境

專業經歷

日本東京大學大學院情報理工學系研究科 | 特任研究員

碩琦科技股份有限公司研發技術處 | 經理

國立臺灣科技大學資訊工程學系 | 教授

相關著作

- ▶ Hadziq Fabroyir, Wei-Chung Teng*, "Navigation in virtual environments using head-mounted displays: Allocentric vs. egocentric behaviors," Computers in Human Behavior, vol. 80, pp. 331-343, Elsevier, March, 2018.
- ▶ Rayi Yanu Tara, Wei-Chung Teng*, "Improving the visual momentum of tethered viewpoint displays using spatial cue augmentation," Intelligent Service Robotics, Springer, vol. 10, is. 4, pp. 313-322, May, 2017.
- ▶ Rayi Yanu Tara, Wei-Chung Teng*, "A Suitability Evaluation of Controlling 3D Map Viewpoint by Gamepad Orientation for Remote Navigation," IEEE Access, vol. 5, pp. 10686-10693, April, 2017.
- ▶ Komang Oka Saputra, Wei-Chung Teng*, Takaaki Nara, "Hough Transform-Based Clock Skew Measurement by Dynamically Locating the Region of Offset Majority," IEICE Transactions on Information and Systems, vol. E99-D, no. 8, August 2016.

場次一 與談人 **李世德**

國家發展委員會 | 參事

專長領域

個人資料保護
政府資訊公開

學歷

政治大學法碩士
東吳大學法學士

專業經歷

- ▶ 台歐盟適足性諮商會議成員
- ▶ APEC 隱私權保護小組（APEC Privacy Subgroup）成員
- ▶ 法務部個人資料保護法修正草案研修小組成員
- ▶ 司法院行政訴訟及懲戒廳專門委員
- ▶ 法務部法律事務司科員、編審、科長
- ▶ 最高法院法官助理
- ▶ 全台法律事務所律師
- ▶ 86 年律師高考及格
- ▶ 86 年特種考試法務部調查局調查人員考試通過

場次一 與談人

余啟民

東吳大學 法律系 | 副教授兼科技暨智慧財產權法律研究中心主任

專長領域

英美契約法及侵權行為法

數位資安及人工智慧法律

國際商事交易及投資

專業經歷

東吳大學法律系 | 專任副教授

東吳大學電子計算機中心 | 主任

相關著作

- ▶ 余啟民，〈從電子商務角度看我國第三方支付法律與實務發展〉，《全國律師》，第 19 卷第 2 期（2015）

場次一 與談人

陳奕廷

景翊科技股份有限公司 | 總經理

專長領域

ITS 及 Telematics、GIS、資訊、通信等相關技術之整合應用

Open Data

資料經濟

交通大數據應用分析

專業經歷

台灣智慧運輸協會 | 理事

台灣車聯網協會 | 理事

台灣 Open Data 聯盟 | 副會長

TTIA 無人機應用與管理小組 | 召集人

場次一 與談人

楊立偉

意藍資訊股份有限公司 | 董事總經理

專長領域

大數據與商業分析
資料庫及語意分析技術
知識管理
數位行銷

專業經歷

台大工管系暨商研所 | 兼任助理教授
資訊及通信國家標準技術委員
意藍資訊股份有限公司 | 董事總經理
龍捲風科技 | 董事總經理

相關著作

- 楊立偉,《社群大數據：網路聲量、口碑及輿情分析》，前程文化出版，第二版（2020年）

場次一 與談人 **趙祖佑**

財團法人工業技術研究院 產業科技國際策略發展所 | 總監

專長領域

台灣/全球半導體產業、微機電元件、雲端運算、巨量資料等科技應用趨勢分析與研究

數位經濟發展趨勢、跨領域科技發展議題與前瞻、數位科技商業模式創新與新創

專業經歷

工業技術研究院 產經中心(IEK)

跨域創新研究群 | 副總監

電子與系統研究組

-科技應用與服務研究部 | 經理

-零組件研究部 | 經理

-半導體研究部 | 產業分析師

臺灣飛鷹航太事業股份有限公司 | 副理

淡江大學 ITS 研究中心 | 研究員

相關著作

- ▶ 從 CES 2020 窺探全球新創發展趨勢 (2020)
- ▶ 以人為本的科技服務新生態 (2020)
- ▶ 創新顛覆：從 CES 2020 窺探全球新創發展趨勢 (研討會簡報) (2020)
- ▶ 以新科技服務新創公司，幫助台灣服務業與中小製造業 (2020)
- ▶ 新世代數位生活樣貌下科技發展新思維 (2019)
- ▶ 運用新興科技加速服務業科技化之策略路徑 (2019)
- ▶ 眺望 2020 系列 | 運用新興科技加速服務業數位轉型的新探索 (2019)

場次一 主講人

孫鈺婷

財團法人資訊工業策進會 科技法律研究所 | 專案經理

專長領域

通訊傳播匯流法制

個人資料保護與資料開放運用

專業經歷

財團法人資訊工業策進會科技
法律研究所 | 專案經理

財團法人資訊工業策進會科技
法律研究所 | 法律研究員

相關著作

- ▶ 孫鈺婷，〈加拿大財政部發布開放銀行第一階段公眾意見諮詢結果〉，
《科技法律透析》，第 32 卷第 4 期（2020）
- ▶ 孫鈺婷，〈國際資安防護政策趨勢探討 - 關於「主動式網路防禦」〉，
《科技法律透析》，第 32 卷第 1 期（2020）
- ▶ 孫鈺婷，〈加州消費者隱私法實施前的討論 - 關於美國聯邦隱私法之
制定〉，《科技法律透析》，第 31 卷第 7 期（2019）
- ▶ 孫鈺婷，〈區塊鏈於歐盟一般資料保護規則適法性與隱私保護困境〉，
《科技法律透析》，第 30 卷第 12 期（2018）
- ▶ 孫鈺婷，〈歐美資料跨境傳輸推動進程 - 隱私盾協議首次年度審查完
成〉，《科技法律透析》，第 30 卷第 03 期（2018）
- ▶ 孫鈺婷，〈新加坡個人資料保護法制推動進程 - 以資料保護信任環境
促進數位經濟發展〉，《科技法律透析》，第 30 卷第 01 期（2018）
- ▶ 孫鈺婷，〈金融監理沙盒申請案例之觀察 - 以英國與新加坡為例〉，
《科技法律透析》第 29 卷第 08 期（2017）
- ▶ 孫鈺婷，〈創新科技應用之國際監管法制發展 - 從高度管制產業觀
察〉，《科技法律透析》，第 29 卷第 06 期（2017）

通傳產業為何不做資料經濟？

國家通訊傳播委員會 鄧惟中

1

有線TV 擬採收視率分潤

2020-08-06 01:24 經濟日報 / 記者黃晶琳／台北報導

+ 有線電視

讚 0 分享 分享



有線電視產業紛亂多年，國家通訊傳播委員會（NCC）主委陳耀祥昨（5）日表示，未來規劃以收視率進行收視分潤，並強化傳播產業資料庫，納入收視率等數據，做為未來調處的客觀數據。

NCC昨天舉行新任委員上任記者會，陳耀祥與副主委翁柏宗，委員王維菁、林麗雲、孫雅麗、鄧維中、蕭祈宏等人出席。外界關注如何讓台灣發展成5G大國，促進有線電視產業改革，黨政軍條款及資安等議題。

陳耀祥坦言，有線電視產業十多年來累積不少問題，包含頻道公平上下架、分組付費等，都是未來政策推動跟修法重點。

<https://udn.com/news/story/7241/4758957>

2

本公司向來重視資訊安全與個資保護！

- 對訂戶收視相關資料之蒐集、處理、利用及其執行透明化，向消費者揭露等，皆符合法令及所定處理程序，並確保訂戶收視行為之隱私保護。
- 以高規格制定資訊安全機制，導入 **ISO 27001及ISO 27011**。於106年通過**BSI**公司驗證，並連續 2 年通過複驗。
- 對訂戶個資及收視相關資料之利用及資安維護，指定資訊安全長及專責人員辦理。
- 於通過之ISO27001驗證中已建立個資保護相關機制，預於2年內導入個資保護管理系統，以建置完整之管理機制。

不做與做了等於沒做

- 傳統的有線電視系統業者不碰用戶收視行為
 - 沒有蒐集，就不用做個資保護
- 轉型中的MSO引進第三方服務，還是不想碰用戶收視行為
 - 遠端監控、居家保全
 - 智慧音箱、智慧家庭
 - 遠距醫療、即時健診
 - 當然還有OTT TV

上網+看電視+遠端監控一次搞定
每月只要**\$1299**

1G 高速網路
在家開Party、親朋好友一起用手機、電腦、平板上網也超順暢！

Wi-Fi 六
有線電視首推1G雲端置家中Wi-Fi6無線上網環境、傳輸量提升4倍
延遲時間減少75%！玩雲端遊戲、看海量線上影音全部更順暢

60M	120M	200M	500M
\$799 起	\$999 起	\$1049 起	\$1199 起
第四台 多送130台衛星電視頻道 30台智慧電視輕鬆看	免費建置家庭無線網路 有線、無線通通吃到飽	myVideo 家庭月租2年免費 觀看、近2萬部影劇看 到底	120M以上、最新 GOOGLE 智慧馬路帶回家

全速率串辦、立即升級A1 BOX機上盒
看電影、YouTube、玩遊戲一機搞定

https://www.wujuneha5168.url.tw/product_1257245.html

4

蒐集了也不利用

什麼時候才要學Netflix？

- 自選20/50，前幾個月哪些頻道沒看或幾乎沒看？
- 知道我最常看電視的時段&節目，幫我推薦頻道/電影
- 依照收視頻率調整頻道排列



中華電信MOD 自選餐 自選・自組・真自由

MOD自選餐費率說明
提供三種方案「自選20」、「自選50」、「全選」，約150個頻道自由選
可依需求選擇方案、依喜好挑選頻道，想看什麼就選什麼，每個月還可以換頻道喔！

自選20	自選50	全選
從自選餐中挑選20個頻道 精打細算小資首選	從自選餐中挑選50個頻道 寵愛自己任意選	總收視頻道數約190個 多元需求一次滿足
200元/月	300元/月	350元/月

註：自選餐頻道如有異動，以MOD平臺實際提供為準。自選餐收視費按月繳費用，不含網路費及MOD平台服務費。

5

為什麼不做用戶資料蒐集？

- 法遵成本
- 個資外洩風險增大
- 特許行業，不用做數位轉型照樣賺錢
 - 做資料經濟的動機不足



暗網交易論壇 全球唯一的中文暗網 担保交易平台，交易无忧！

尚未设置封面图或
下方查看附件图片
No-pictures

立即购买 查看已购物品

购买用户	数量	购买金额	状态	购买时间
simonlee	1件	1美元	购买成功	2020-10-17
Ray584066	1件	1美元	购买成功	2020-10-17
allin021	1件	1美元	购买成功	2020-10-17
ShadowMoon	1件	1美元	购买成功	2020-10-17
otseaz9	1件	1美元	购买成功	2020-10-17

1 2 下一页

共有交易记录8条

本站最后由 modR 于 2020-10-17 02:43 AM 编辑

先放出几千条样本，
17年数据。
用户姓名、客户性别、客户生日、客户身份证、是否外国人、购买服务套餐、联系电话1、联系电话2、联系电话3、客户邮

6

電信產業資料經濟的例子

但是仍沒有可獲利且具規模的服務

- 利用電信帳單作信用評等
 - 2003年中華電+凱基銀「金融小白」
- 利用手機連線的基地台定位
 - Covid-19防疫，也可轉換為軌跡服務



7

Over The Top MyData

- 沒有比智慧型手機更精確的觀察者
- 使用者有辦法得知/管理她的隱私？有辦法知道哪個APP更值得信任？

他們都在偷聽 **Facebook**承認錄下你的聊天內容，還找人聽寫！

亞馬遜雇人監聽你與智慧音箱Alexa的對話，Google也定期聽取人工智慧語音助理錄下的談話內容，蘋果Siri也被爆出在未告知使用者的情況下，偷錄對話。不只是你的語音助理，現在連你的文字內容，他們都在偷聽。

臉書竊聽？美教授：講完就收到廣告不是巧合是偷聽

2019-08-18



<https://www.cw.com.tw/article/5096477>

8

消費者賦能

才是發展資料經濟的長久之道

9

工業技術研究院

Industrial Technology
Research Institute

通傳資料應用與法制整備研討會

資料經濟與產業推動關鍵議題探討

趙祖佑 組長兼研究總監

工研院產科國際所

2020/11/10



資料經濟與產業推動關鍵趨勢-1 以資料為核心的產業數位轉型

數位轉型核心精神在因應數位科技對產業、市場及生產服務活動的顛覆，思考企業未來經營策略轉變方向，進而尋求新興數位工具以及資料的加值運用，故以資料為核心的數位轉型通常伴隨新價值、新服務的出現。



版權宣告©工業技術研究院

2020/11/8

2

資料經濟與產業推動關鍵趨勢-2

資料驅動新經濟時代之商業模式創新

2019年百事公司成立Foodservice Digital Lab部門，針對小型餐飲供應商(如餐廳、小型食品零售店)提供產品銷售之顧問服務，成為公司驅動產業資料服務化獲利之新動能。



版權宣告©工業技術研究院

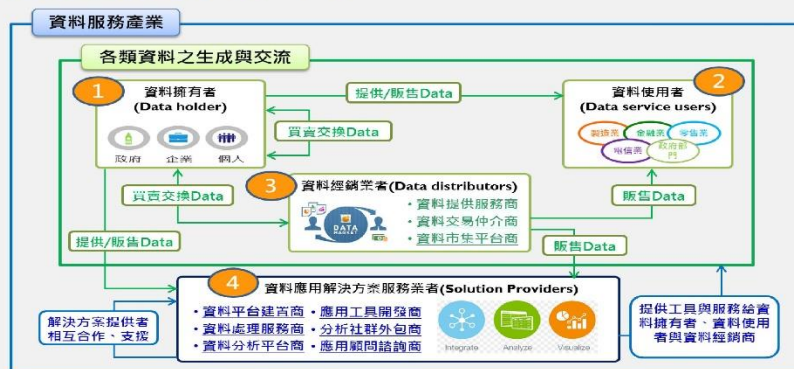
2020/11/8

3

資料經濟與產業推動關鍵趨勢-3

資料生態系的建構與基礎環境

完整的資料經濟生態系是未來數位經濟的重要核心，需要：資料服務產業(資料擁有者、資料經銷商與、資料應用解決方案提供者)、資料使用者(即市場端之消費者)以及外部環境支援，缺一不可。



版權宣告©工業技術研究院

2020/11/8

4

小結

完備資料經濟發展的關鍵要素檢視

以資料為核心的 產業數位轉型

- 企業內部資料之落實與資料分析能力
- 分散式/跨境資料管理與運用
- 跨部門/跨產業之資料互通與融合

資料驅動新經濟時代之 商業模式創新

- 創新商業模式與資料價值之衡量
- 各種資料源之所有權確認
- 資料取得與授權再運用範圍

資料生態系的建構與 基礎環境

- 完善的資料服務與生態系以及第三方服務之營業範疇
- 公共資料取得之合法使用範圍
- 資安基礎環境(包含技術性與非技術性)

敬請指教!!



通傳產業資料應用與法制研析 —資料經濟下個人資料的流通與應用

孫鈺婷 專案經理

財團法人工業策進會 科技法律研究所

2020.11.10



2020 © 資訊工業策進會 Institute for Information Industry



報告大綱

01

資料經濟國際趨勢

- 全球資料經濟發展趨勢
- 歐洲資料戰略(European Data Strategy)
- 從資料經濟中觀察涉及個人的資料
 - 何謂公民資料？
- 形塑資料經濟相關政策議題與法律規範
 - 資料移動性與GDPR資料可攜權

02

資料經濟下個人資料流通與應用—以英國為例

- 英國國家資料戰略
 - 資料流通應用關鍵：資料可用性(Data availability)
- 英國智慧資料(Smart Data)
 - 開放銀行到開放金融
 - 開放通訊

03

展望未來

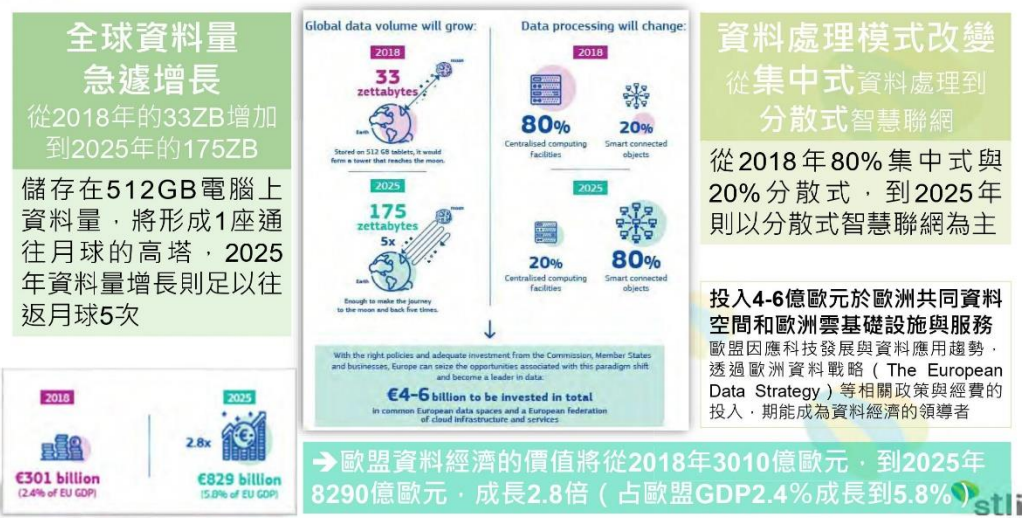
- 我國資料流通與應用現況
- 借鏡英國：資料驅動經濟



2020 © 資訊工業策進會 Institute for Information Industry



全球資料經濟發展趨勢



資料來源：European Commission, The European Data Strategy

4

2020 © 資訊工業發展協會 Institute for Information Industry stli

歐洲資料戰略(European Data Strategy)

- 建立單一資料市場(single market for data)，確保歐洲的全球競爭力 and 資料主權



從資料經濟中觀察涉及個人的資料：何謂公民資料？



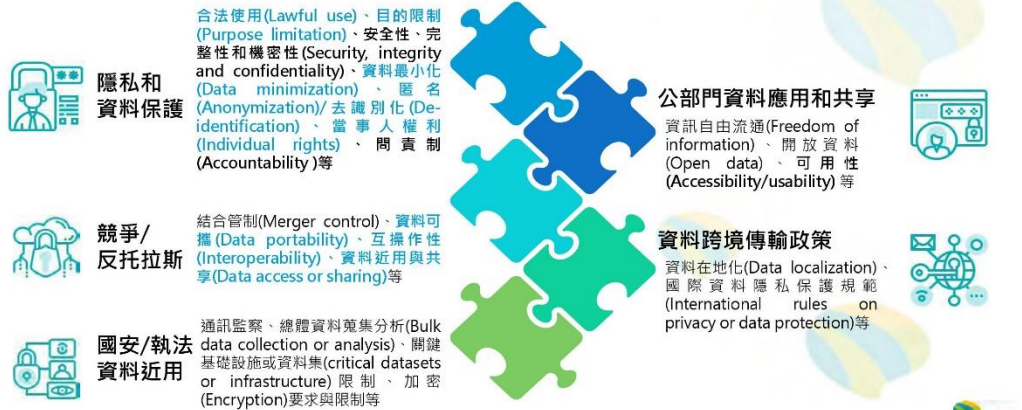
參考英國政府科學辦公室(Government Office for Science)2020/9發布「公民資料生態系的未來」(The Future of Citizen Data Systems)報告，整理涉及個人的資料，該報告稱「公民資料」(citizen data)，範圍相較於資料保護法規「個資」更廣泛，相關示例如下：

1. 唯一識別符（如身分證字號、護照號碼等）
2. 共享識別符（如姓名、出生日期、地址等）
3. 生物識別資料（如DNA、指紋等）
4. 透過服務或設備生成資料：醫療、金融、教育或其他紀錄
5. 透過觀察所得
 - 網路瀏覽歷史記錄、cookie、IP、影像資料...
 - 公用事業使用資料
 - 透過IoT蒐集資料設備資料
 - 消費者資料、網路社群媒體資料、位置資料...
6. 從個人相關資料分析得出推論、預測和假設
7. 與個人相關的Metadata（何時、如何生成資料）
8. 去識別化資料(De-identified data)
9. 群集資料(aggregate data)



形塑資料經濟相關政策與法律規範

- 影響資料經濟發展因素，如政策、法規、新興技術、創新商業模式等
- 各國對於資料經濟發展所提出相關政策與法律規範係為關鍵，整理如下：



資料來源：Government Office for Science, The Future of Citizen Data Systems, p17

2020 © 資訊工業策進會 Institute for Information Industry



資料經濟下資料移動性與GDPR資料可攜權



- 資料流通應用並非一蹴可幾，目前國際上透過Open Banking機制，來實踐金融領域資料流通應用
- 英國2019年Smart Data Review，重點在於如何利用資料可攜改善消費者體驗

資料來源：Her Majesty's Treasury (HM Treasury), Unlocking digital competition: Report of the Digital Competition Expert Panel (2019), p68-69

2020 © 資訊工業策進會 Institute for Information Industry



英國國家資料戰略(National Data Strategy)



英國2020/9發布國家資料戰略，釋放資料的價值，推動資料能更好、更安全、更具創新性應用，改善社會和公共服務，成為資料驅動創新的領導者



資料流通應用關鍵：資料可用性(Data availability)



資料可用性：確保公私部門、第三方組織以及各自之間的適當資料近用、流通和再利用

針對「經濟社會的資料可用性」(Data availability for the economy and society) 相關研究顯示：

- 目前市場上的資料應用尚未完全實現資料價值，政府干預仍有其必要性
- 資料過度集中和缺乏互操作性，導致數位市場競爭和創新不彰

(根據研究參考：Online platforms and digital advertising Market study interim report, Data platform and digital advertising Market study interim report, DATA MOBILITY: The potential for data portability growth opportunity for the UK economy...)

經濟社會的資料可用性之推動——智慧資料(Smart Data)：使消費者能與獲授權的第三方簡單、安全地共享資料，從而使第三方服務提供者(third party service provider, TPPs)能提供創新服務

- 鼓勵新競爭者進入市場，驅動創新資料服務，並降低創新者的壁壘，同時保護消費者權益
- 英國資料保護法賦予消費者權利，即參照GDPR資料可攜權規定
- Smart Data代表對資料可攜權擴展，提供共享消費者資料框架
 - 應消費者要求向TPP提供資料，以API安全共享資料，在確認消費者身份，且TPP收到其明確同意後共享
 - 適當情況下，企業和TPP間可以常態性傳輸資料
 - 遵守技術標準、資料格式，確保互操作性並減輕TPP障礙
 - 必要時，除消費者資料外，提供產品和性能資料，以實現創新
- 英國2019年Smart Data Review重點：如何改善消費者對於其資料控制與應用

加速開發創新的資料驅動服務，包含建立新的智慧資料部門，並衍生應用於能源和通訊領域



利用資料和技術幫助弱勢消費：監管者得於資料受到適當保護的情況下，協助弱勢消費者

確保消費者資料受到保護：對TPP資料保護要求，使消費者對創新資料驅動服務的信任，以減少TPP負擔

11

2020 © 資訊工業策進會 Institute for Information Industry

英國Smart Data典範：開放銀行(Open Banking)



- 英國競爭及市場管理局(CMA)發布「零售銀行業市場調查的最終報告」(Retail banking market investigation Summary of final report) 調查結果指出：英國大型銀行間競爭疲弱，且銀行間帳戶轉換成本高、資訊不夠透明，因此推動改革制定開放銀行標準(Open Banking Standard)
- 由英國9大銀行(CMA9) 出資成立開放銀行實施組織(Open Banking Implementation Entity, OBIE)
 - 其主要任務即在制定開放銀行API與共同標準，使消費者資料透過開放API提供給獲授權的第三方服務提供者(TPPs)
- 英國開放銀行的下一步「開放金融」(Open finance)
 - 開放金融將開放銀行的資料共享和第三方資料近用概念，擴展到更廣泛的金融產品服務(退休金、投資保單、資產管理等)
 - 改變消費者和企業使用金融服務的方式，使其更輕鬆地比較價格、產品功能以及轉換產品或服務提供者
 - 公眾意見諮詢於2020/10/1結束



- Open Banking從2016年推動至今超過100萬的消費者，200家以上服務提供者，估計消費者的年度總收益達120億英鎊，中小企業60億英鎊
- 未來英國政府除了金融產業，也將借鑒Open Banking推動經驗，拓展到其他產業，如能源與電信等資料

12

2020 © 資訊工業策進會 Institute for Information Industry

英國Ofcom：開放通訊(Open Communications)

英國通訊傳播管理局 (The Office of Communications, Ofcom) 於2020/8/4-11/10進行「開放通訊：使人們能夠透過創新服務共享資料」(Open Communications: Enabling people to share data with innovative services) 公開意見徵詢

Figure 1: Open Communications in summary



開放通訊：使消費者能將通訊資料與獲授權第三方簡單安全地共享

- 消費者應能控制其所共享之資料，且必須獲其同意
- 要求業者共享更多有關產品的資料，確保提供TTP可用資料
- 任何經認可第三方都得依消費者的要求近用其資料

Next step將持續與利益相關者溝通：

- 考量訂定相關法律（如何監管、標準化消費者和產品資料？）
- 如何確保資料移動安全性與消費者控制權限？
- 如何降低實施開放通訊的成本，以達到開放通訊效益？
- 循序漸進開放資料，如風險低但對消費者有較高利益的資料...

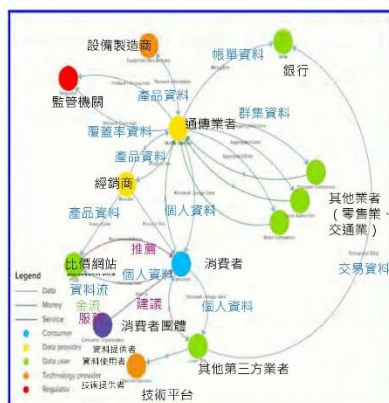


13

2020 © 資訊工業策進會 Institute for Information Industry

英國通傳產業資料生態與開放通訊範圍

英國開放資料研究所(Open Data Institute, ODI)2020/8發表「開放通訊：電信領域的開放式可信賴資料生態系」(Open communications: an open trustworthy data ecosystem for the telecommunications sector)報告



ODI 通傳產業資料生態的例示

該報告整理ODI與產業代表討論，聚焦如何使人們和企業共享有關其使用通訊服務相關資料，與加值利用資料的效益與風險

- 通訊資料生態系中的「資料」包含：
 - **開放資料** (如產品資訊、商店位置等，還有Ofcom發布固網、行網覆蓋範圍、業者服務品質等資料)
 - **共享、非開放資料** (如安全憑證和通話紀錄等)
- 通傳資料生態系「參與者」以不同方式創造價值，報告提出應思考：
 - 消費者如何在通傳市場得到其所需的服務/產品
 - 各類通傳業者與第三方如何在資料生態系中近用資料並獲利

英國Ofcom開放通訊將提供2大類資料：

- **消費者資料(customer data)**：如消費者姓名、地址、資費(tariff)、服務合約相關資訊、使用經驗等
- **產品資料(product data)**：產品詳細資訊 (合約內容、費用、加值服務)、速度、服務品質 (覆蓋率、可用性) 以及消費者的總體客戶體驗詳細資料等
- 範圍包含市話(landline)、固網、行網與付費電視(pay TV services)的獨立和套餐(standalone and bundled)服務的以上2類資料

第一頁 ODI, Open communications: an open trustworthy data ecosystem for the telecommunications sector. <http://odi.org.uk/content/odis/2020/08/04/open-communications-ecosystem-report>. Ofcom, Final.pdf

2020 © 資訊工業策進會 Institute for Information Industry



Figure 4: Illustration of an account management service using Open Communications

英國開放通訊：第三方服務提供案例

案例1：產品服務之比較推薦

消費者直接與其他業者共享其資料，接收適合其需求的產品服務建議

案例2：帳戶整合

- 整合消費者在不同業者間所擁有的帳戶和產品的資料（甚至是公用事業繳費）
- 幫助消費者管理和掌握其通訊服務相關帳戶（開放銀行也有類似服務模式），且應獲其同意與第三方持續共享資料



Figure 5: Illustration of a service to help financially vulnerable customers, using Open Communications

案例3：帳戶管理

- 協助消費者在接近服務契約終止或價格上漲時，提醒消費者，並結合案例1比較推薦服務，提供消費者後續選擇
- 應獲消費者同意與第三方持續共享其資料

案例4：協助財務困難的消費者

若有財務困難消費者選擇透過如慈善機構、資產管理等第三方尋求幫忙，並與第三方共享其資料



Figure 6: Illustration of an account aggregator using Open Communications



Figure 7: Illustration of a service to help financially vulnerable customers, using Open Communications

資料來源：Open Communications: Enabling people to share data with innovative services. 625.07.25.25

15

2020 © 資訊工業策進會 Institute for Information Industry

展望未來

我國資料流通與應用現況

借鏡英國：資料驅動經濟

16



我國資料流通與應用現況



金管會2019年推動開放銀行

- 採取鼓勵銀行與外部機構合作開發金融服務，以「自願自律」三階段漸進式實施
- 2019/9 第一階段開放「公開資料查詢」
- 2020年邁入下一階段「消費者資訊查詢」與「交易面資訊」，將涉及消費者個人資料、交易資料等，預計 2020 年底前第二階段可上線



國發會2020年推動數位服務個人化(MyData)

- 推動個人資料自主運用，讓人民可自行下載運用個人化資料或單次即時同意傳輸給第三方運用，創造精準數位服務
- 經身分驗證及同意後，在個資安全與隱私保護下，平臺提供民眾多元化個人資料下載及線上介接服務，讓保存在政府機關內的資料，回歸民眾合理運用

- 依我國個人資料保護法第3條規定之當事人權利，目前並無資料可攜權
- 未來於各領域推動資料共享時，亦得參酌國際推動經驗，雖規範與模式可能略有不同，但皆應保護消費者權益，尤其是資料安全與隱私保護，期能持續發展創新蓬勃的數位經濟

個資法第3條規定「當事人就其個人資料依法規定行使之下列權利，不得預先拋棄或以特約限制之：

- 一、查詢或請求閱覽。
- 二、請求製給複製本。
- 三、請求補充或更正。
- 四、請求停止蒐集、處理或利用。
- 五、請求刪除。」



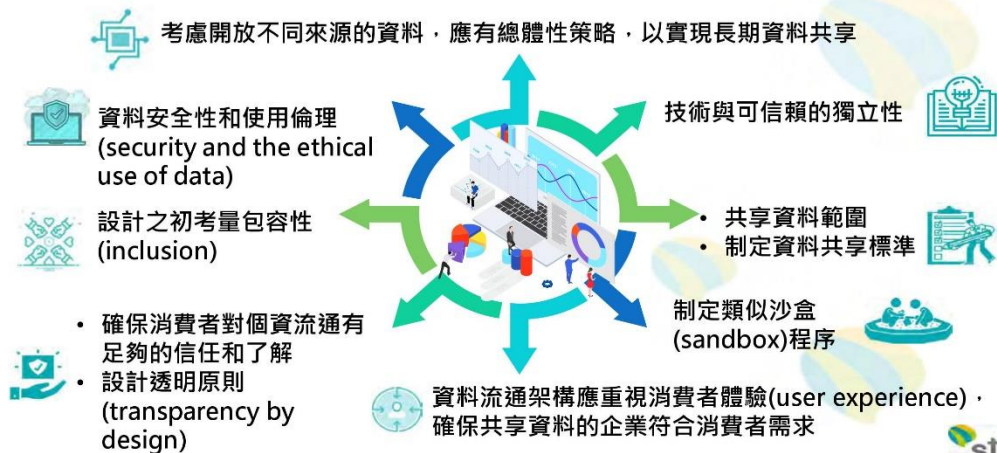
17

2020 © 資訊工業策進會 Institute for Information Industry



借鏡英國：資料驅動經濟

參考英國經驗，促進真正資料驅動的經濟，英國數位競爭專家小組報告與TechUK相關建議如下：



18

2020 © 資訊工業策進會 Institute for Information Industry



Thank you



2020 © 資訊工業策進會 Institute for Information Industry

場次二 主持人 **葉奇鑫**

達文西個資暨高科技法律事務所 | 所長暨主持律師

專長領域

個人資料保護法與 GDPR

科技法律

資安法規

網路犯罪

數位鑑識與蒐證

網路交易安全

電子商務相關法規

專業經歷

達文西個資暨高科技法律事務所 | 所長

電腦稽核協會 | 理事長

東吳大學法律研究所 | 兼任助理教授

國發會 | 個資法諮詢委員

智慧財產局 | 著作權顧問暨調解委員

場次二 與談人

郭文忠

國立臺北大學 經濟系 | 教授

專長領域

財務經濟
財務理論
個體經濟理論
電信經濟學
媒體經濟學
公共經濟學
互聯網與媒體

專業經歷

國家通訊傳播委員會 | 委員
國立臺北大學經濟學系 | 教授
國立臺灣大學國際企業學系 |
兼任助理教授
元智大學財務金融學系 | 專任
助理教授

相關著作

- ▶ “Downs Meets d’Aspremont and Company: Convergence versus Differentiation in Politics and the Media,” Wen-Chung Guo, Fu-Chuan Lai, Wing Suen (2018, Aug). *International Journal of Industrial Organization*, forthcoming.
- ▶ “Prices, Locations and Welfare when an Online Retailer Competes with Heterogeneous Brick-and-mortar Retailers,” Wen-Chung Guo, Fu-Chuan Lai, *Journal of Industrial Economics*, 2017 (June), 65 (2), 439-468.

場次二 與談人

劉定基

國立政治大學 法律系 | 副教授

專長領域

憲法
通訊傳播法
個人資料保護法
政府資訊公開法

專業經歷

國立政治大學法律學系 | 專任
副教授

相關著作

- ▶ 劉定基，〈The Past, Present, and Future of the Right to Information Privacy: A Comparative Law Perspective〉，收錄於〈釋憲七十週年國際學術研討會論文集〉，司法院（2020）
- ▶ 劉定基，〈試評「數位通訊傳播法」草案〉，收錄於彭芸、葉志良主編《匯流、治理、通傳會論文集》，新北市：風雲論壇（2018.8）
- ▶ 劉定基，〈大數據與物聯網時代的個人資料自主權〉，《憲政時代》，第4期（2017）

場次二 與談人

林雅惠

凱擘股份有限公司 法務法規室 | 處長

專長領域

通訊傳播政策與法律

專長領域

凱擘股份有限公司法務法規室 | 處長

相關著作

- ▶ 江耀國主編，江耀國、葉志良、林孟楠、蕭景騰、陳人傑、陳志宇、張志鵬、林雅惠合著，《電信法》，台北：新學林（2017）
- ▶ 《科技法律未知的境界》（合著），台北：新學林（2006）
- ▶ 《資訊、電信與法律》（合著），台北：元照（2004）
- ▶ 《數位法律科技大未來》（合著），台北：書泉（2004）

場次二 與談人

李和音

遠傳電信 法務法規暨採購群 | 資深副總經理

專長領域

具有橫跨法律、電信等經驗，涵蓋銷售，銷售運營，商務運營及法務等領域

專業經歷

遠傳電信法務法規暨採購群 | 資深副總經理

場次二 與談人 林冠宇

財團法人資訊工業策進會 科技法律研究所 | 組長

專長領域

個人資料保護法

科專法令

智財技轉

專業經歷

財團法人資訊工業策進會科技
法律研究所 | 組長

財團法人資訊工業策進會科技
法律研究所 | 專案經理

財團法人資訊工業策進會科技
法律研究所 | 法律研究員

松江專利商標事務所 | 法務專員

相關著作

- ▶ 林冠宇，〈美國專利訴訟趨勢與科技專案研發成果運用之法制研析〉，
《科技法律透析》，第 30 卷第 10 期（2018）
- ▶ 林冠宇，〈簡評歐洲法院認定 Uber 商業模式為運輸服務之判決〉，
《科技法律透析》，第 30 卷第 2 期（2018）
- ▶ 林冠宇，〈歐盟循環經濟新展望與推動進程〉，《科技法律透析》，第
29 卷第 5 期（2017）
- ▶ 林冠宇，〈美國第七巡迴上訴法院伊利諾運輸貿易協會訴芝加哥市政
府案之判決評析 - 與德國法蘭克福地方法院計程車派車聯盟訴優步案
就行政管制思維之比較〉，《科技法律透析》，第 29 卷第 2 期
（2017）
- ▶ 林冠宇，〈【產業創新法制系列 - 消除法令灰色地帶】日本企業實證
特例制度與法律保留原則之調和〉，《科技法律透析》，第 28 卷第 12
期（2016）
- ▶ 林冠宇，〈美國佛羅里達州認定 Uber 與其招募駕駛間成立獨立合約
員工關係〉，《科技法律透析》，第 28 卷第 4 期（2016）

場次二 主講人 **王慕民**

達文西個資暨高科技法律事務所 | 合夥律師

專長領域

GDPR 合規遵循

個資適法性查檢與矯正

個資委外稽核

個資管理制度建置

個資保護衝擊評估

個資法律顧問

個資法認知教育訓練

專業經歷

達文西個資暨高科技法律事務所 | 合夥律師

BS10012 個資管理系統主導稽核員

通傳產業應用與 法遵運作

與談人：郭文忠

通傳產業應用與法制整備研會

創新與資料經濟

- 破壞性創新：取代效果大、既有產業衝擊與轉型。如自駕車取代司機
- 新產品或服務：如AR、VR娛樂
- 成本降低或效率提昇：如製造業5G應用

通傳產業應用與法制整備研會

創新可能衍生之爭論

- 壟斷或濫用市場影響力：Google、Youtube等
- 破壞性創新之產業調整與資源重分配
- 侵犯隱私、擔心遭資料蒐集者濫用資料

通傳產業應用與法制整備研會

資料蒐集與利用

- No data, no data economy.
- 過往通傳產業之高度監理
- 資料蒐集受限於資源、法遵、法規不明確

通傳產業應用與法制整備研會

資料蒐集、利用之法規明確性

- 去識別化之程度
- 非基於營業目的
- 執行業務所必須
- 經當事人同意

通傳產業應用與法制整備研會

我國面臨數位經濟之轉換與挑戰 I

1. 數位轉換並無捷徑，逐步尋求適合台灣之數位轉換方式。
2. 社會經常低估由資通訊科技(ICT)為前導的轉型所帶來的長期經濟成長力: 中小企業不願意投資、人民抗拒數位轉換
3. 公共政策必須預防法規: 政府組織偏向於僵化

我國面臨數位經濟之轉換與挑戰 II

1. 新數位產品和服務模式對既有商業模式之衝擊: 破壞性創新或監理落差之套利
2. 人們是否能接受對生活方式之轉變: 遠距工作與教學、勞動力之取代、產業轉型與退場
3. 個資和隱私保護
4. 與社會倫理之衝突

各產業數位經濟之挑戰

Retail

Increasing the use of big data analytics and personalization

Providing unique in-store experience such as AR/VR

Improving smart logistics and in-store operational optimization

Agriculture

Increasing the use of technology in smart farming

Changing agricultural techniques and improving supply chain tracking

Improving connectivity between different pieces of equipment players

各產業數位經濟之挑戰

Media & Entertainment

1. Improving quality of content, speed of streaming and download
2. Increasing interactive and immersive forms of entertainment
3. Improving communication with customers and other partners
4. Expanding digital content through new platforms and new market players

數位轉型其他挑戰

數位世界之壟斷議題

資安威脅、駭客入侵

掌握資料者是否濫用

虛擬世界犯罪、網路詐騙

自駕車安全性

數位轉型與城鄉落差、數位落差

企業與政府之預算限制

主事者缺乏數位轉型之正確認知與概念

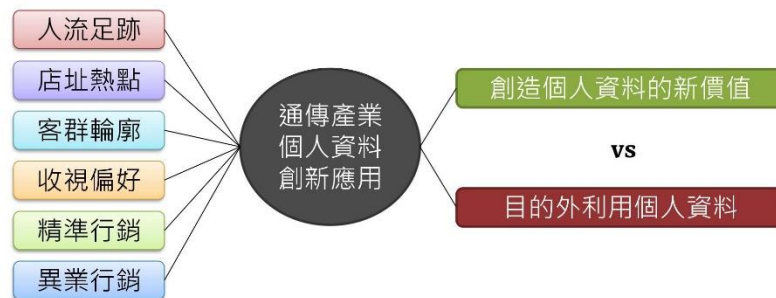
通傳產業資料應用 與法遵運作



達文西個資暨高科技法律事務所
王慕民 律師

2020/11/10 於通傳資料應用與法制整備研討會

資料應用的優勢也是資料應用的劣勢



實務上2個解答-1

資料匿名

常見技術

- 抑制 — 將整欄列資料刪除(非隱藏)
- 隱碼 — 以特定符號取代部分字元
- 泛化 — 模糊、區間，降低準確性
- 置換 — 將資料重新排列
- 干擾 — 修改資料，略為失真
- 聚合 — 將多人資料轉換為統計值

官方實務

- 英國 / 匿名化資料保護風險管理守則 2012
- 歐盟 / 匿名化技術意見書 2014
- 加拿大 / 結構化資料去識別指引 2016
- 日本 / 匿名情報處理指南 2016
- 新加坡 / 資料匿名基本技術指南 2018
-

實務上2個解答-2

當事人同意

注意事項

- 任意性 — 可自由決定是否同意
- 特定性 — 一個目的，一個同意
- 知情性 — 清楚揭露隱私聲明
- 明確性 — 積極表達的同意
- 可撤回 — 可用相同方式撤回同意
- 留證據 — 保留同意的證據

常見瑕疵

- 任意性 — 不同意就不能申辦服務
- 特定性 — 網綁多個目的
- 知情性 — 空白同意 / 文字難懂
- 明確性 — 不反對的默示同意
- 可撤回 — 沒有撤回同意機制
- 留證據 — 沒有完整規劃保留證據方式

管理制度難以滿足創新應用的法遵性

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

- 108年+109年，30間通傳業者訪查經驗
- 個人資料管理制度PIMS一個資利用程序書
 - 利用個人資料應與蒐集目的相符，但有下列情形不在此限：
 - ① 法律明文規定。
 - ② 為增進公共利益所必要。
 - ③ 為免除當事人之生命、身體、自由或財產上之危險。
 - ④ 為防止他人權益之重大危害。
 - ⑤ 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。
 - ⑥ 經當事人同意。**(如何取得同意？如何記錄？如何撤回同意？)**
 - ⑦ 有利於當事人權益。

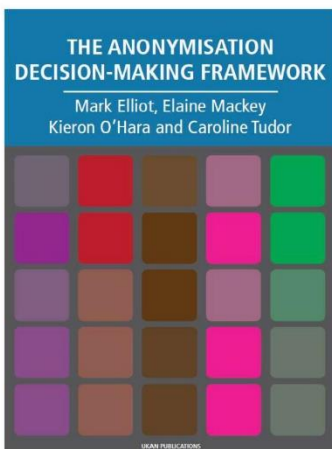
- 去識別技術不在制度範圍
- 取得同意程序缺乏操作性

通傳產業資料應用與法遵運作 @通傳資料應用與法制整備研討會_109.11.10

5

建議1：建立匿名決策機制

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



UK Anonymisation Network (UKAN) / 匿名化決策框架

- ① 描述資料情狀
- ② 識別法律義務
- ③ 清查資料
- ④ 盤點資料應用方式
- ⑤ 善盡倫理義務
- ⑥ 建立資料應用風險評估程序
- ⑦ 選擇對外提供資料的控制程序
- ⑧ 識別參與者並規劃程序
- ⑨ 安排後續行動
- ⑩ 規劃事故應變措施

通傳產業資料應用與法遵運作 @通傳資料應用與法制整備研討會_109.11.10

6

建議2：當事人同意內部審查

	目標	留意事項
1	客戶可自由選擇同意或不同意，不影響既有使用服務的權益	即便客戶不同意，仍可申辦服務，或原有服務效能不受影響
2	客戶可針對不同目的，分別表示同意或不同意	不同目的分開列出，不綑綁同意
3	客戶可清楚理解目的、涉及的個資範圍、不同意對權益的影響	在取得同意之前，清楚、友善揭露利用資料的目的、範圍及不同意的影響
4	客戶以積極、明確的行為表達同意	客戶必須以特定行為表達同意，可搭配雙因驗證方式取得證據
5	客戶可使用相同管道/方式撤回同意	如何給予同意，就該如何撤回同意
6	公司可保存客戶表示同意的證據	證據便於識別、便於取得

通傳產業資料應用與法遵運作 @通傳資料應用與法制整備研討會_109.11.10

7

謝謝聆聽

THANKS FOR YOUR ATTENTION

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

王慕民 律師

電話：02-2367-0902

信箱：service@davinci.idv.tw

地址：台北市中正區衡陽路51號6樓之9



歡迎訂閱【達文西個資週報】



場次三 主持人

陳人傑

財團法人電信技術中心 | 主任

專長領域

通訊傳播監理政策及法規

競爭法

資訊法

專業經歷

財團法人電信技術中心研究企劃組 | 研究員

東吳大學法律學系碩士在職專班 | 兼任助理教授

輔仁大學財經法律學系 | 兼任助理教授

財團法人資訊工業策進會科技法律中心 | 組長

相關著作

- ▶ 陳人傑，《廣播電視集中化管制規範之比較研究—以德國、英國法制為中心》，臺灣大學法律學研究所博士論文（2013）
- ▶ 江耀國主編，江耀國、葉志良、林孟楠、蕭景騰、陳人傑、陳志宇、張志鵬、林雅惠合著，《電信法》，台北：新學林（2017）

場次三 與談人

孫雅麗

國家通訊傳播委員會 | 委員

專長領域

網際網路與行動通訊
資訊安全
惡意程式分析與鑑識
網路與系統效能評估與分析

學歷

美國加州大學洛杉磯分校
Computer Science
Department 博士
美國加州大學洛杉磯分校
Computer Science
Department 碩士
國立臺灣大學資訊工程學系畢業

專業經歷

- ▶ 國立臺灣大學資訊管理學系教授
- ▶ 美國貝爾通訊研究室 (Bell Communications Research Inc.) 研究員 (Member of Technical Staff)
- ▶ 行政院科技會報科技計畫首席評議專家
- ▶ 國立臺灣大學計算機及資訊網路中心主任
- ▶ 國立臺灣大學資訊管理系系主任兼所長
- ▶ 科技部第二期能源國家型科技計畫能源主軸中心共同召集人
- ▶ 科技部中央政府科技發展計畫審議作業資通訊建設群組委員
- ▶ 國家通訊傳播委員會電信事業普及服務基金管理委員會委員
- ▶ 教育部臺灣學術網路北區資訊安全維運中心主持人
- ▶ 教育部臺灣學術網路管理委員會委員
- ▶ 考試院考選部高等暨普通考試典試委員
- ▶ 臺北市市政顧問
- ▶ 臺北市悠遊卡股份有限公司董事
- ▶ 財團法人資訊工業策進會董事
- ▶ 中央銀行資訊業務推動委員會委員

場次三 與談人

李寧修

中國文化大學 法律學系 | 教授

專長領域

憲法
行政法
資訊法
警察法

專業經歷

中國文化大學法律學系 | 教授

相關著作

- ▶ 李寧修，〈個人資料合理利用模式之探析：以健康資料之學術研究為例〉，《臺大法學論叢》，第 49 卷第 1 期（2020）
- ▶ 李寧修，〈警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例〉，《臺大法學論叢》，第 48 卷第 2 期（2019）
- ▶ 李寧修，〈國家機關及立法委員聲請法規範憲法審查〉，《世新法學》，第 12 卷第 1 號（2018）
- ▶ 李寧修，〈中央與地方之立法權限劃分及其爭議：以食品安全法制為例〉，《法學叢刊》，第 63 卷第 4 期（2018）
- ▶ 李寧修，〈論國會調查權之革新與展望〉，《政大法學評論》，第 154 期（2018）
- ▶ 李寧修，〈選舉期間民調管制之界限〉，《東海法學研究》，第 54 期（2018）

場次三 與談人

江耀國

中原大學 財經法律學系 | 教授

專長領域

個資法
網路法律
廣電法律
電信法律
資訊法律
行政法
憲法

專業經歷

國家通訊傳播委員會 | 法規諮詢
委員會委員
行政院新聞局 | 法規委員會委員
國家通訊傳播委員會 | 廣播電視
節目暨廣告諮詢會議委員
交通部電信顧問小組會議
(TAB) | 委員

相關著作

- ▶ 江耀國、黃子宴 (2019) · 〈個人資料的概念與匿名化：一個認識論的觀點〉· 《東海大學法學研究》· 第 58 期 (2019)
- ▶ 江耀國 · 〈過猶不及的立法 — 個人資料保護法爭議問題研析〉· 《法令月刊》· 第 65 卷第 8 期 (2014)

場次三 與談人 **鍾國強**

中華電信股份有限公司 法律事務處 | 副總經理

專長領域

電信法規
經營策略
行動通信
衛星通信

專業經歷

中華電信公司經營規劃處
中華電信公司網路處
電信總局技術處

場次三 與談人

曾更瑩

理律法律事務所 | 合夥律師

專長領域

個資與隱私保護
電子商務
網際網路法律
電信
金融科技
共享經濟
OTT
電子支付

專業經歷

現任
台灣網路治理論壇 | 副主席/
常務理事

臺灣網路暨電子商務產業發展
協會 (TiEA) | 監事

NII 財團法人中華民國國家資
訊基本建設產業發展協進會 |
董事

相關著作

- ▶ Privacy & Cybersecurity in Taiwan, GTDT – Market Intelligence - Privacy & Cybersecurity (2020)
- ▶ 理律新知：電信管理法自民國 109 年 7 月 1 日起正式實施, Lee and Li Newsletter (2020)
- ▶ The International Comparative Legal Guide to: Data Protection 2020 - Chapter 39 Taiwan, ICLG to: Data Protection (2020)
- ▶ 立院三讀防疫期間違反隔離檢疫命令得公布個資, LEE & LI Bulletin (2020.4)
- ▶ The Legal 500: Doing Business In: Taiwan (2020)

場次三 與談人 **宋佩珊**

財團法人資訊工業策進會 科技法律研究所 | 副主任

專長領域

個人資料保護與管理
資通安全管理
資料加值應用與前瞻科技 (包括物聯網、醫療科技)

專業經歷

財團法人資訊工業策進會科技
法律研究所 | 副主任
國家安全會議 | 助理研究員

相關著作

- ▶ 宋佩珊，〈遠距醫療照護保險補助機制之研析〉，《科技法律透析》(2012)
- ▶ 宋佩珊，〈資通訊技術結合醫療器材之法律議題研析--借鏡美國醫療器材驗證檢驗機制〉，《科技法律透析》(2011)
- ▶ 宋佩珊 (合著)，〈各國個人醫療資訊隱私標準之法制研析〉，《醫事法學》(2010)
- ▶ 宋佩珊，〈個人醫療資訊隱私保護之立法趨勢探究--以美國、加拿大為例〉，《科技法律透析》(2010)
- ▶ 宋佩珊，〈遠距健康照護之法律議題研析〉，《科技法律透析》(2009)
- ▶ 宋佩珊，〈美國隱私標章與個人資料管理機制研析〉，《科技法律透析》(2009)
- ▶ 宋佩珊，〈迎接高齡化世代 遠距照護規範受矚目〉，《生技與醫療器材報導》(2009)

場次三 主講人 **王德瀛**

財團法人資訊工業策進會 科技法律研究所 | 專案經理

專長領域

個人資料保護
人工智慧
資料開放
生技領域法制議題

專業經歷

財團法人資訊工業策進會科技
法律研究所 | 專案經理

財團法人資訊工業策進會科技
法律研究所 | 法律研究員

相關著作

- ▶ 王自雄、王德瀛，〈COVID-19 與全球公衛治理 - WHO 的衰頹與新典範的崛起〉，《科技法律透析》，第 32 卷第 5 期（2020）
- ▶ 王德瀛，〈行動醫療軟體的上市前規範：美國經驗〉，《月旦醫事法報告》，第 30 期（2019）
- ▶ 王德瀛，〈初探遺傳資訊隱私保護發展〉，《月旦醫事法報告》，第 25 期（2018）
- ▶ 王德瀛，〈精神衛生法強制住院侵害身心障礙者自由權 - 身心障礙者權利公約初次國家報告國際審查〉，《科技法律透析》，第 29 卷第 12 期（2017）
- ▶ 王德瀛，〈強制蒐集人體生物資料的人權標準 - 聯合國人權事務委員會的見解〉，《科技法律透析》，第 28 卷第 11 期（2016）
- ▶ 王德瀛，〈美國基改食品標示新發展 - 強制標示與否的拔河〉，《科技法律透析》，第 28 卷第 7 期（2016）

通傳資料應用與疫情防制

COVID-19 全球大流行下的科技減災與調適

孫雅麗 委員

國家通訊傳播委員會 (Taiwan National Communications Commission, NCC)

November 10, 2020 通傳資料應用與法治整備研討會

Outline

- 科技減災
- 科技調適
- 結語

Copyright 2020 YLSun

2

利用追蹤科技降低疫病傳播

- The goal is to use technology to help public health authorities fight COVID-19
 - Traditional methods - Longer time, human resources, etc.
- Use cases
 - Apple, Google - Contact Tracing System including app
 - Taiwan - Geo-fencing System
- Containing the spread of infections, augmenting the efforts
- The purpose is to quickly notify and alert people who might not know directly.
- The systems are built with participants' privacy and security control to the design.

Copyright 2020 YLSun

3

Apple, Google - Contact Tracing System

- A participant's device such as smart phone
 - 1) Regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier – a string of random numbers that are not tied to a user's identity.
 - 2) Rotate the random numbers every 10-20 minutes for additional protection
 - 3) Nearby devices of other participants will be listening for these beacons and broadcast theirs as well.
 - 4) When receiving other's beacons, the device will record and securely store that beacons on the device.
 - 5) Periodically (e.g., at least once a day), the Contact Tracking System will download a list of keys for the beacons that have been verified as belonging to people confirmed as positive for COVID-19.
 - 6) Participant's device checks the list of beacons it has recorded against the list downloaded.
 - 7) If there is a match, participant may be notified and advised to steps to take next.

Copyright 2020 YLSun

4

Privacy Protection by Design

- Participants
 - opt-in and opt-out any time
- The system does **NOT** track user's location.
- Using **Bluetooth** to detect if two users are near each other; no revealing locations of the users' smart phones
- **No** identity of the smart phones
- All of the exposure notification matching **happens on user's device**.

Copyright 2020 YLSun

5

Regulation

- For Public health authorities that use the system, they **MUST** meet specific criteria around privacy, security and data use.

Copyright 2020 YLSun

6

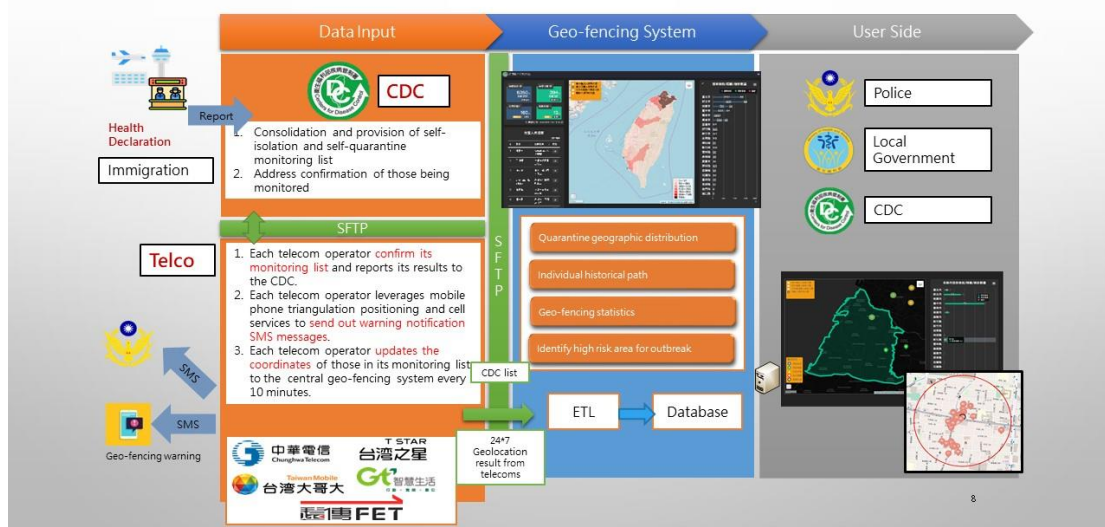
Taiwan: Geo-fencing System

- The goal is to track the people who are undertaking **safety measures**, such as **self-quarantine** and **self-isolation** so to break the chain of transmission.
- The system works through **mobile phone signals**, **mobile phone triangulation positioning** and **cell services** for target individual positioning and movement tracking.
- In the early implementation, every self-quarantine person received a Chung-Hua Telecom cell phone. Later, the personal cell phone is used.

Copyright 2020 YLSun

7

System Architecture



8

Geo-fencing System

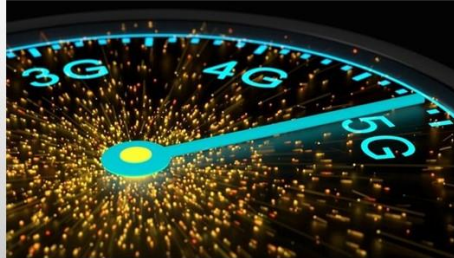


9

科技調適 隱私保護與資安 (Privacy and Security)

10

5G is not simply
“4G on steroids.”



Copyright 2020 YLSun

It is Transformational !

(“The technology will spawn
an **intelligent ecosystem** of
connected devices,
harvesting **massive amounts of data**
that will **change the way**
we live and work.”)

11

5G : a major driving force for digital transformation

- **Digital business** is the creation of *new* business designs by **blurring the digital and physical worlds**.
 - Business model disruption
 - Business moment opportunities
 - Time-to-market imperatives
- **Intelligence and Productivity**
- IoT and M2M communications (**Smart-X: factory, city, home, etc.**) require supporting of *tens of thousands of connected devices*.



Cyber-Physical System (CPS)

Source: Gartner

Copyright 2020 YLSun

12

(IIoT) (工業物聯網): Siemens

- Use 5G for Siemensstadt factory in Berlin and plant in Erlangen
 - Enable machinery and equipment to communicate directly
 - Exploit the **Mindsphere platform** to *manage and analyze processes, and find ways to operate more efficiently.*
- **Security**
 - 設備商 (security by design, built-in security functions)
 - 系統整合商 (網路、系統、平台、應用)、營運/維運階段)



Copyright 2020 YLSun

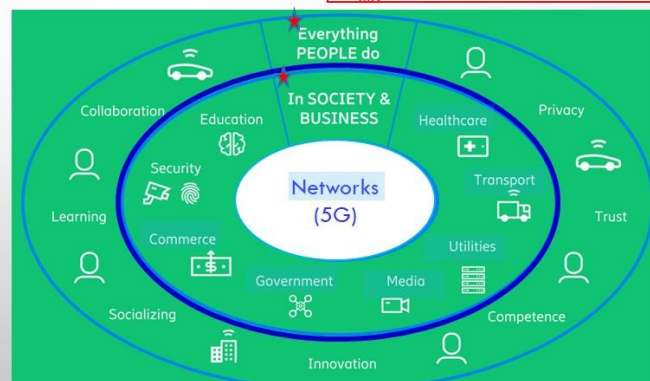
13

數位 (5G) 時代的資安風險與威脅

- Cyber Physical System, digital twin
- 數位時代，資安風險與威脅升高！
- 隱私與資料保護更形重要。
- **How to manage the risks?**

Privacy and Security Concerns of

- Unauthorized collection of data from the network about who is doing what
- Surveillance by adversaries
- Human rights violations and abuses
- Third-party data use (e.g., advertisements) etc.



Copyright 2020 YLSun

14

結語（1／2）

- COVID-19 pandemic 加速數位化與數位轉型（產業、企業、社會、個人）
 - 例如員工回不來、用學生工、遠距上班、遠距教學
- 數位時代（5G）
 - 萬物聯網、數位化、智能化；數位企業、數位經濟、數位-X
 - 資安風險與威脅升高！
 - 隱私與資料保護更形重要。
- The battle is just on ...
 - 資料蒐集、儲存、處理、利用；隱私保護 vs. 數據經濟、打擊犯罪
 - 資安（國安）
 - 風險管理（Manage the risks）

Copyright 2020 YLSun

15

結語（2／2）

數位時代國家、經濟、科技、產業的發展

Q: What specific ***national strategy, policies and legal framework*** are necessary for our nation, society and economy in digital era to **ensure a high level of security and resilience?**

A: 數位時代下的數位安全政策、法規、制度、管理、技術（機制）

Copyright 2020

16



通傳資料應用與疫情防制議題研析 COVID-19全球大流行下的科技減災與調適

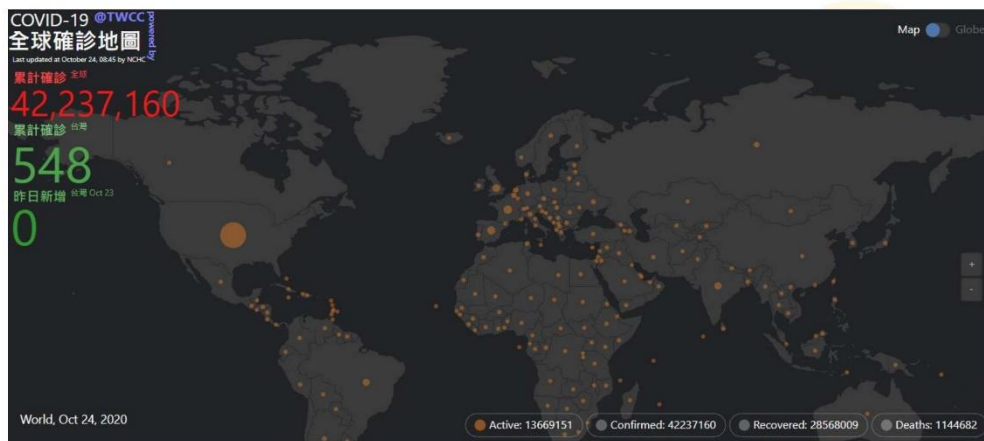
王德瀛 專案經理

財團法人資訊工業策進會科技法律研究所

2020.11



資訊工業策進會 Institute for Information Industry



1

2020 © 資訊工業策進會 Institute for Information Industry



疫情下的減災與調適

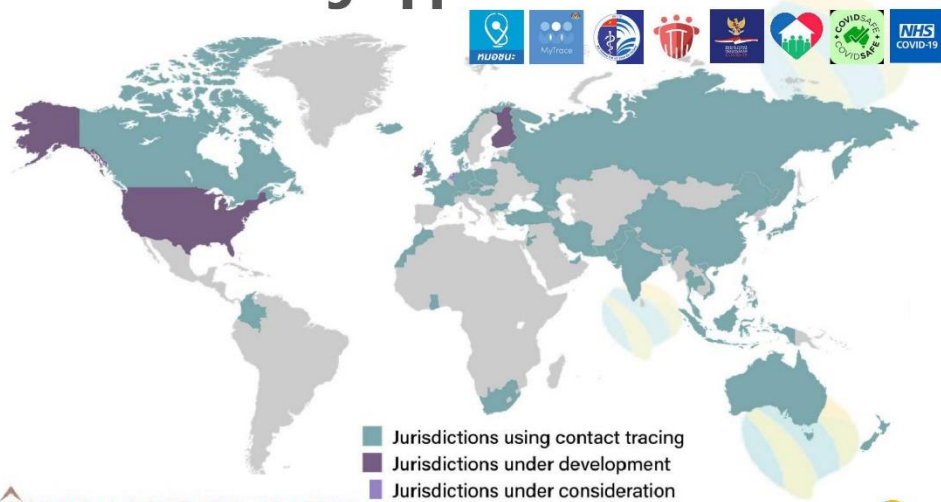


2

2020 © 資訊工業策進會 Institute for Information Industry

減災：利用追蹤科技降低疫病傳播

Contact Tracing Apps



NORTON ROSE FULBRIGHT

<https://www.nortonrosefulbright.com/en/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy>



3

2020 © 資訊工業策進會 Institute for Information Industry



調適：全面加速數位轉型

Low-Touch Economy

電子商務



工作



教育



外送

4

2020 © 資訊工業策進會 Institute for Information Industry



疫情下的減災與調適

減災

調適

以資料的流動
追蹤人的流動

以資料的流動
取代人的流動



5

2020 © 資訊工業策進會 Institute for Information Industry



減災：以資料的流動，追蹤人的流動



6

2020 © 資訊工業策進會 Institute for Information Industry



接觸史追蹤科技的興起



- ◆ 2/08 杭州推推出「健康碼」
- ◆ 2/18 政府要求市民和進入杭州者使用
- ◆ 利用位置資訊、政府資料串連判斷健康風險，蒐集位置、身份證號、臉部識別等資料
- ◆ 擴及至少20於個省級行政區，並有多地考慮常態化使用

- ◆ 4/10 Apple 與Google 聯手推出「接觸史追蹤應用程式框架」(CTF)
- ◆ 以自願下載：開啟為基礎，交換使用者經雜湊金鑰，在自願告知傳染基礎下，通知曾接觸之使用者
- ◆ 許多國家接觸史追蹤Apps的基礎

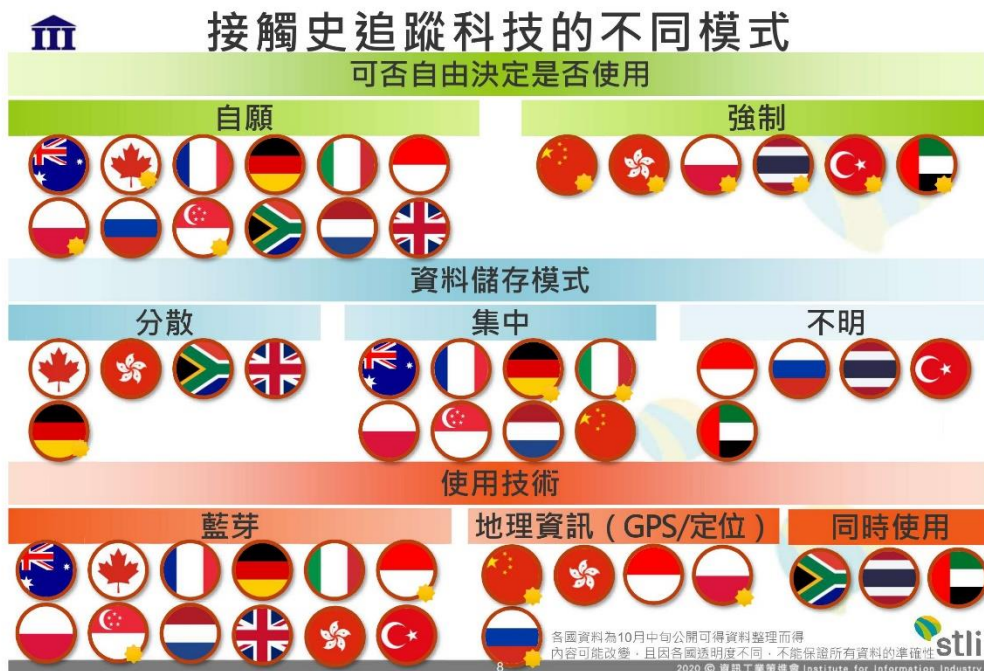


- ◆ 4/21 歐洲資料委員會 (EDPB) 提出「COVID-19疫情下使用位置資料及接觸追蹤工具指引」
- ◆ 接觸追蹤Apps 應以自願為基礎，基於當事人同意或經法律規定要求當事人使用
- ◆ 應嚴格限制資料蒐集範圍、利用期限，並進行資料保護影響評估
- ◆ 如以資料交換方式蒐集資料，應使用假名化唯一識別符，並依照疫病性質定期更新



7

2020 © 資訊工業策進會 Institute for Information Industry



不斷辯證的隱私意涵

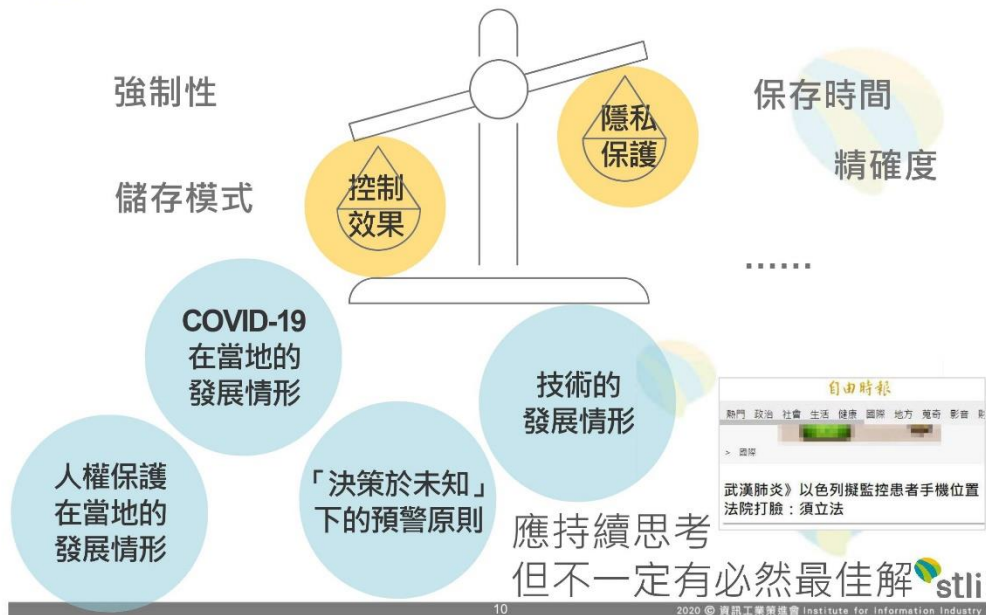
- 隱私與其他空間、人的期待與互動有關，不是靜態、固定的，而是持續辯證的。
- 隱私案件的處理，除重視辯證過程的公平合理外，更要重視時間空間脈絡。

葉俊榮，〈探尋隱私權的空間意涵——大法官對基本權利的脈絡論證〉
《中研院法學期刊》，18期，頁1-40，2016。

2020 © 資訊工業策進會 Institute for Information Industry stli



COVID-19下的隱私辯證



調適：以資料的流動，取代人的流動



低接觸經濟的新未來

流程的數位化



資料與資訊的數位化



互動溝通的數位化



人、資料、流程 大幅的
以通訊的方式進入數位世界 

12

2020 © 資訊工業策進會 Institute for Information Industry



新時代的資料應用新挑戰

當 人、資料、流程 大幅的
以通訊的方式進入數位世界.....

越多的人、越多的流程帶來更多新的風險...
不只是技術就可以解決的風險



流程基於風險的重新設計、組織面的編排與人力訓練
將越來越重要



13

2020 © 資訊工業策進會 Institute for Information Industry



小結



14

2020 © 資訊工業策進會 Institute for Information Industry



科技減災與調適：我們的機會



減災

運用滲透率極高的手機進行接觸史追蹤以成為多國運用手段。各國制度設計因應在地脈絡各有不同

調適

疫情帶來的「低接觸經濟」，人、資料、流程大幅數位化，對資料保護帶來新的挑戰，除了技術，我們更該重視流程與組織規劃

我們的機會

打完上半場，在「相對不緊急」的時候，更能思考科技防疫的合理界線，並針對流程、組織進行數位化下的重新設計



15

2020 © 資訊工業策進會 Institute for Information Industry



Thank you



2020 © 資訊工業策進會 Institute for Information Industry

參考書目

中文參考資源

1. 財團法人資訊工業策進會科技法律研究所，「個資保護 2.0」，書泉（2019）。

外文參考資源

1. Advisory Guidelines for the Telecommunication Sector, PDPC, <https://www.pdpc.gov.sg/guidelines-and-consultation/2017/10/advisory-guidelines-for-the-telecommunication-sector>.
2. Advisory Guidelines on Enforcement of Data Protection Provisions, PDPC, <https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-enforcement-of-data-protection-provisions>.
3. Blog: ICO regulatory sandbox, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/first-reports-published-from-the-regulatory-sandbox/>.
4. Call for evidence: Regulatory Sandbox, ICO, <https://ico.org.uk/media/about-the-ico/consultations/2259746/regulatory-sandbox-call-for-evidence.pdf>.
5. Data Protection Trustmark Certification, IMDA, <https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification>.
6. Department for Digital, Culture, Media & Sport, National Data Strategy, <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-1-3>.
7. Ethical Principles for Digital Media and Technology Design in the New Normal, WEF,

- http://www3.weforum.org/docs/WEF_Ethical_Principles_2020.pdf.
8. European Commission, A European strategy for data, <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>.
 9. European Commission, Proposal for a Regulation on European data governance (Data Governance Act), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2102.
 10. European Commission, Proposal for a Regulation on European data governance (Data Governance Act), <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act>.
 11. Facebook (2020), Communicating About Privacy: Towards People-Centered and Accountable Design.
 12. Guide on Active Enforcement, PDPC, <https://www.pdpc.gov.sg/help-and-resources/2019/05/guide-on-active-enforcement>.
 13. Guide to Accountability under the Personal Data Protection Act, PDPC, <https://www.pdpc.gov.sg/help-and-resources/2019/07/guide-to-accountability-under-the-personal-data-protection-act>.
 14. IBA Research (2019), 54 TECHNOLOGYTRENDS TO WATCHIN 2020.
 15. Open communications: an open trustworthy data ecosystem for the telecommunications sector, ODI, <https://theodi.org/article/open-communications-an-open-trustworthy-data-ecosystem-for-the-telecommunications-sector-report/>.
 16. Our key areas of focus for the Regulatory Sandbox 2020-2021, ICO, <https://ico.org.uk/media/for-organisations/documents/2618112/our-key-areas-of-focus-for-regulatory-sandbox.pdf>.
 17. Personal Data Protection (Amendment) Bill, Singapore, <https://sso.agc.gov.sg/Bills-Supp/37-2020/Published/20201005?DocDate=20201005#legis>.

18. Regulatory Sandbox Final Report: FutureFlow, ICO,
<https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf>.
19. Regulatory Sandbox Final Report: Heathrow Airport Ltd. , ICO,
<https://ico.org.uk/media/for-organisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf>.
20. Regulatory Sandbox Final Report: Jisc, ICO,
<https://ico.org.uk/media/for-organisations/documents/2618023/jisc-regulatory-sandbox-final-report.pdf>.
21. Regulatory Sandbox Final Report: Onfido, ICO,
<https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf>.
22. The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision, NEF,
https://neweconomics.org/uploads/files/NEF_DATA-INADEQUACY.pdf.
23. WEF (2020), 10 Principles of Mobility Data Operationalization.
24. WEF (2020), A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy WHITE PAPER.
25. WEF (2020), Understanding Value in Media: Perspectives from Consumers and Industry.
26. My Data Intelligence ,〈 パーソナルデータの預託と活用をする情報銀行を生活者と企業が体験！大規模「情報銀行トライアル企画」スタート 〉, 2019/7/23 , https://www.mydata-intelligence.co.jp/news/2019/07/20190703_01.html.
27. NTT Data ,〈 情報銀行を活用したパーソナルデータ同意管理サービスの実証実験を開始 〉, 2020/04/28 ,
<https://www.nttdata.com/jp/ja/news/release/2020/042800/>.

28. 〈「情報信託機能の認定スキームの在り方に関する検討会」の論点について〉(2017), 総務省,
http://www.soumu.go.jp/main_content/000553637.pdf.
29. 〈国内初の情報銀行、サービス開始 購買履歴など提供〉(2019), 産経新聞社,
<https://www.sankei.com/economy/news/190703/ecn1907030015-n1.html>
30. 一般社団法人日本 IT 団体連盟, 〈日本 IT 団体連盟、「情報銀行」認定(第1弾)を決定〉, 2019/06/26,
<https://itrenmei.jp/topics/2019/3646/>.
31. 一般社団法人日本 IT 団体連盟, 〈日本 IT 団体連盟、「情報銀行」認定(第2弾)を決定〉, 2019/12/25,
<https://www.itrenmei.jp/topics/2019/3652/>.
32. 一般社団法人日本 IT 団体連盟, 〈日本 IT 団体連盟、「情報銀行」認定(第3弾)を決定〉, 2020/02/17,
<https://www.itrenmei.jp/topics/2020/3657/>.
33. 一般社団法人日本 IT 団体連盟, 〈日本 IT 団体連盟、初の通常認定となる「情報銀行」認定(第4弾)を決定〉,
2020/03/12, <https://www.itrenmei.jp/topics/2020/3662/>.
34. 日立トップ, 〈個人データの活用の新しい仕組み「情報銀行」の実現に向けた実証実験を開始〉, 2018/09/10,
<https://www.hitachi.co.jp/New/cnews/month/2018/09/0910.html>.
35. 石山大晃, 日本国内のデータ利活用に係る昨今の制度検討の状況, 富士通総研,
<https://www.fujitsu.com/jp/group/fri/business/topics/data-economy/regulation-domestic/>.
36. 庄司昌彦, 〈我が国における データ活用に関する意識調査〉, 第6回データ流通・活用ワーキンググループ,
http://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/dai6/siryou1.pdf.
37. 首相官邸, 〈未来投資戦略 2017〉, 2017/6/9,

https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf.

38. 株式会社日立製作所，〈情報銀行に係る日立の実証実験について〉，2019/02/12，<file:///C:/Users/cindyhsu/Desktop/000600133.pdf>
39. 情報信託機能の認定スキームの在り方に関する検討会，〈情報信託機能の認定に係る指針 ver1.0〉，
<https://www.meti.go.jp/press/2018/06/20180626002/20180626002-2.pdf>.
40. 情報信託機能の認定スキームの在り方に関する検討会，〈情報信託機能の認定に係る指針 ver2.0〉，
<https://www.meti.go.jp/press/2019/10/20191008003/20191008003-3.pdf>.