資通安全法律案例彙編

第 15 輯

行政院國家資通安全會報技術服務中心

中華民國 107 年 12 月

序

近年來資通科技發展迅速，其應用與影響範圍更已深入各種層面，舉凡一般民眾之日常生活、企業與政府之發展及運作，隨處可見資通科技之影響及其所帶來之效益。惟於享受資通科技帶來便利之同時，對於其背後所潛藏之資通安全風險亦不可輕忽。有鑑於資通安全對於數位時代之重要性，資通安全管理法已於107年6月6日經總統令公告，並自108年1月1日起開始施行。而行政院亦公布國家資通安全發展方案(106-109年)，提出包含：「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」及「孕育優質資安菁英人才」等四項推動策略。配合政府嶄新資通安全政策、法律之推行，各界宜強化資通安全法制意識。

「行政院國家資通安全會報技術服務中心」(以下簡稱技服中心)長期協助我國政府推動資通安全工作，自91年起即開始編撰「資通安全法律案例宣導彙編」，並於107年邁入第15輯(以下簡稱本輯)。本輯之內容編排仍維持以「資訊保護」、「資訊公開」、「資訊監察」及「資訊應用」等四大主軸，收錄近期重要時事案例，並透過法律概念剖析與資通安全管理觀念宣導之結合，期能增進讀者對於資通安全之重視與理解。

本輯為增加相關案例素材之豐富度與實用性，所編蒐之案例即以各種不同角度著手，收錄多則國內外重要事件，使讀者能了解其工作、生活各層面所可能接觸之資通安全相關法律、規範及制度，例如：美國亞特蘭大市政府遭勒索病毒SamSam攻擊、臉書保護個人資料不力、歐盟GDPR上路、資通安全管理法、無人載具實驗條例之制定等，並以我國法制規範之觀點出發，進行解析與提出相關之資通安全管理及注意要領。

誠摯希望本輯案例彙編，能提供政府機關與社會大眾豐富與實用之資通安全法制與管理資訊，並進一步建構良好的資通安全法律與管理觀念。

行政院國家資通安全會報 技術服務中心

吳啟文 主任 謹識

吳啟文

凡例

壹、本彙編案例依其內容及相關法律觀點之重要內容，分為以下類別：

一、資訊保護（Security）

二、資訊公開（Disclosure）

三、資訊監察（Monitors）

四、資訊應用（Application）

貳、本案例編碼共 5 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年分三碼及案例流水編碼兩碼；以利讀者在案例與評量間對照參考。

壹、資訊保護（SECURITY）---------- 1

遭勒索病毒攻擊 美亞特蘭大市政癱瘓 5 天---------- 3

臉書保護個資不力 祖克柏：我很抱歉---------- 7

主管機關駁斥手機廠商：「未取得」資安認證！---------- 11

名店資料被駭　女客遭詐騙 28 萬控店家未通知---------- 15

遭澳洲稱 5G 危及國家安全 中國大陸通訊設備大廠聲明反擊---------- 19

勞務採購洩密 機關之承辦人遭判刑 1 年 2 個月---------- 25

商業電子郵件詐騙橫行，美國逮捕 74 名嫌犯---------- 29

又見商業間諜！上市科技大廠機密外洩 損失高達 38 億---------- 33

包商小油坑架 200 萬天線 軍方雷達站訊號全都錄---------- 37

歐盟個資法上路 台灣爭取列入白名單---------- 41

公務防駭 近萬機關資安納管 預告資安法 6 大子法草案---------- 45

民眾個資、公所公文拿去墊菜？市府：查明後將懲處---------- 50

資產兆元以上銀行應設獨立法遵與資安單位---------- 54

貳、資訊公開(DISCLOSURE)----------59

性侵犯沒匿名權！ 波蘭公開性侵犯個資---------- 60

立院三讀通過 起訴書一審後公開---------- 65

補助社團疑黑箱作業　市府：依法網路公告---------- 69

行政機關通過「政治檔案條例」草案　政黨、附隨組織所持檔案將歸國有---------- 74

機關審議討論過程原則可錄音錄影---------- 78

空污法新制上路---------- 81

參、資訊監察(MONITORS)----------89

用側錄軟體蒐證告員工 老闆先被判 3 月徒刑---------- 90

扣押已結束的通訊內容 須搜索票或扣押裁定---------- 94

建置手機監控系統 執法機關：絕無可能任意擷取資料 ---------- 98

德國全面禁止兒童智能手錶----------102

奧克蘭通過全美最嚴謹監控監察法----------106

肆、資訊應用(APPLICATION) ---------- 111

上下班塞車有解？ 北市「智慧路燈」上線----------112

立院三讀通過民航法修正案，無人機使用需註冊納管----------116

金管會新春修法 悠遊卡網路刷卡通了----------120

立法院通過無人載具實驗條例，最長實驗 4 年----------124

首例金融創新實驗 已遞件申請----------128

用聲音完成電子簽章 法人獲獎----------134

伍、自我評量---------- 139

是非題----------140

選擇題----------148

壹、資訊保護（Security）

類別：資訊保護【案號：S10701】

遭勒索病毒攻擊 美亞特蘭大市政癱瘓 5 天

【焦點話題】

美國亞特蘭大市政府於 2018 年 3 月遭勒索病毒 SamSam 攻擊，雖然緊急報案和供水系統等仍正常運作，但與民生息息相關之線上繳費等系統仍受到嚴重影響。駭客要求該市政府支付價值 5.1 萬美金的比特幣，並限期一週內付款，方予以解索。亞特蘭大市政府表示不會支付贖金，並已掌握駭客的身分，且無員工或其他個人資料外洩，但也因勒索病毒攻擊，市政府除原分配 3,500 萬美元的 IT 預算，將追加 950 萬美元，用以恢復受衝擊之市政系統。

【參考資料來源：自由電子報，107/3/29；iThome，107/6/11】

【重點摘要】

1. 比特幣被認為是去中心化的電子加密貨幣，多數國家則認為比特幣屬於虛擬商品，並非貨幣，而我國亦採低度監理的原則，不視比特幣為貨幣，而是虛擬商品，貨幣間的交易，屬於商品與商品間的交換。
2. 為降低資安事件發生之風險，組織應定期進行資安訓練，宣導資訊安全事件對組織之影響，以及預防、因應之方式等資訊。

【法律觀點】

本案之 SamSam 勒索軟體，係透過「變更」使用者電腦或其設備之電磁紀錄，以達癱瘓政府機關電腦、設備之效果，而刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」，因此有關侵入他人電腦，進行檔案加密、變更電磁紀錄之部分，行為人可能因而構成妨害電腦使用罪。

其次，按刑法第 346 條規定：「意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付者，處六月以上五年以下有期徒刑，得併科一千元以下罰

金。以前項方法得財產上不法之利益，或使第三人得之者，亦同。」而比特幣被認為是去中心化的電子加密貨幣[1]，我國採取低度監理的原則，不視比特幣為貨幣，而是虛擬商品，以虛擬貨幣交易購買商品時，屬於商品與商品間的交換，也就是以物易物[2]，因此，駭客除侵入電腦之行為外，另要求被害人給付貨幣（本案為比特幣），方解除加密狀態，也就是以比特幣作為勒索政府單位支付以解除癱瘓的對價，故亦觸犯刑法第 346 條之罪。

另外，此種利用惡意程式癱瘓公務機關電腦之情形，因行為人之妨害電腦使用行為係針對公務機關所為，因此依刑法第 361 條之規定：「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。」更要加重刑度。

【管理 Tips】

「電子化政府」是政府機關運用資訊與通信科技形成網網相連，並透過不同資訊服務設施（包括電話、網際網路、公用電腦站等），對機關、企業及民眾在其方便之時間、地點及方式下，提供自動化服務之總體概念[3]。但在建立電子化政府提供政府服務時，應將資訊安全列為重要事項，以確保資料、系統、設備及網路安全[4]。本案中，為恢復受勒索病毒攻擊之市政系統，亞特蘭大市須增加 950 萬美元之支出，因此，如何強化資訊管控措施是所有組織均需面對之課題。

而資訊控管區分為事前及事後，事前控管包括平日定期進行教育訓練，宣導資訊安全事件對組織的影響、拒絕下載來路不明的盜版軟體、注意社交工程郵件以及

---

[1] 去中心化係相對於中心化而言，去中心化出現在擁有眾多節點的系統中，透過每一個獨立的節點處理資訊，而非在單一中心處理，以比特幣而言，透過網路技術，使得比特幣的製造和發行都不以對中央發行機構的信任為基礎，任何人只要運行比特幣軟體，就可以參與其製造，因此，在沒有一個中心的中央發行機構的發行，而是以所有非中心的運行比特蔽體的個人為製造，這就是為什麼比特幣被稱為去中心化的虛擬貨幣。

[2] https://www.ithome.com.tw/news/119603，金管會為何選擇對虛擬貨幣發展採取低度監理原則?(瀏覽日期：2018 年 7 月 17 日)。

[3] 第一階段電子化政府計畫（87 至 89 年度），https://www.ndc.gov.tw/cp.aspx?n=D88BA19D378B30C4&s=1F6D9F3EEABADB1D（瀏覽日期：2018 年 6 月 13 日）。

[4] 臺北市政府資訊安全管理規範第 1 條：「臺北市政府為強化所屬各機關（以下簡稱各機關）資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，特訂定本規範。」

重要資料時常備份外，組織亦可透過諸如定期檢查「安全性更新」或限制員工使用網際網路等主動之網路控制措施，均可有效降低侵害發生；而當資安事件發生後，應及時通報並且迅速進因應，同時保存相關紀錄做為證據，並於改善缺失後，從事件中學習相關經驗，以降低未來再度發生事故之風險。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.7.2.2　資訊安全認知、教育及訓練

(1) 標準內容：　組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2) 適用說明：　如果組織對其員工或相關之承包者能進行有效之教育訓練，而使本案電腦受侵害之相關人員，平時均恪守教育訓練之指示，善盡社交工程之注意、軟體之定期更新等事項，應可有效降低惡意軟體所造成之受害程度。

- A.12.2.1　防範惡意軟體之控制措施

(1) 標準內容：　應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。

(2) 適用說明：　新興之惡意軟體攻擊日益頻繁，組織平時即應針對相關惡意攻擊軟體進行預防性工作，且熟捻遭攻擊後之因應措施，本案中，如組織能隨時讓電腦和軟體保持最新狀態，對於點擊連結或下載資料或開啟電子郵件附件或圖片時能格外小心，或可有效避免系統遭受侵害。

- A.12.3.1　資訊備份

(1) 標準內容：　應依議定之備份政策，定期取得資訊、軟體及系統的影像

備份複本，並測試之。

(2) 適用說明： 為避免無法預期之資料毀損或侵害，以降低損失風險，定期進行相關資料之有效備份是防止資訊損失的最後防線，本案中，若組織善盡對於相關資訊之備份，於電腦遭受攻擊後，相關資訊仍得以保存，所受損失亦可減少。

● A.13.1.1 網路控制措施

(1) 標準內容： 應管理及控制網路，以保護資訊系統及應用。

(2) 適用說明： 現今網路空間之陷阱層出不窮，若得以適當將部分有問題之網域限制連網，亦可降低惡意程式由網頁攻擊之風險，本案中，如組織如可將對外連網與內部資料電腦予以實體切割，將內部資料電腦之連網採取限制或是根本性的禁止非必要連網活動，將可有效降低重要電腦設備遭植入惡意軟體等造成系統受侵害之可能性。

類別：資訊保護【案號：S10702】

臉書保護個資不力 祖克柏：我很抱歉

【焦點話題】

社群網站臉書（Facebook）執行長祖克柏（Mark Zuckerberg）針對英國諮詢機構「劍橋分析」(Cambridge Analytica)以不當手段獲取海量臉書用戶資料，最終導致臉書計有 8,700 萬名用戶個資外洩，以及未能有效打擊假新聞所造成的傷害，向歐洲議會道歉。祖克柏表示本於「歐盟通用資料保護規則」（GDPR）精神，臉書將依照新規定調整至符合歐盟通用資料保護規則之要求，並推出多項新功能，包括特殊「清除歷史」鈕，允許用戶刪除所有儲存的暫存檔或瀏覽歷史。

【參考資料來源：中央社，107/5/23】

【重點摘要】

1. 組織於蒐集個人資料時，依個人資料保護法第 8 條規定，應告知當事人蒐集目的、蒐集資料類別、個人資料利用之期間、地區、對象及方式、當事人權利及行使方式以及不提供個資之權益影響等相關事項，俾使當事人能知悉其個人資料被他人蒐集之情形。

2. 依個人資料保護法第 20 條規定，合法蒐集的個人資料，原則上仍應在蒐集之特定目的必要範圍內為之，也就是於蒐集時所告知當事人的特定目的，僅在特定情形下得為特定目的外之利用。

【法律觀點】

「劍橋分析事件」起源於劍橋大學研究人員 Aleksandr Kogan 的研究公司 Global Science Research(GSR)在 2013 年打造了一款名為「thisisyourdigitallife」的性格分析臉書應用程式，並透過臉書使用者下載，該程式取得了 30 萬名臉書用戶的居住位置及「按讚」內容等個人資料，並依當時臉書使用者政策，進而取得這些用戶好友的個人資料，共計超過 5000 萬人的個資，而 GSR 再與英國資料分析業者劍橋分析(Cambridge Analytica)分享所取得

的資料。

不過，據臉書表示，該程式在使用者下載時其實是有同意提供個人資料予程式設計者以及第三方單位作為「學術用途」使用，因此 GSR 取得個人資料是經過使用者同意的，而依臉書使用者與臉書之間的使用者條款，GSR 取得該程式使用者的好友個人資料也是符合相關規定，但因劍橋分析於使用個人資料時，並未依照與程式使用者間的承諾，僅供學術用途，因此，事件之爭議係有問題的資料使用，而非資料之違法取得。

考量個人資料之蒐集涉及當事人隱私權益，為使當事人知悉個人資料被何人蒐集及其蒐集之目的等資訊，故我國個人資料保護法（下稱個資法）規定，除有免為告知之法定情形外

[1]，組織於蒐集個人資料時，應告知當事人諸如蒐集目的、蒐集資料類別、個人資料利用之期間、地區、對象及方式、當事人權利及行使方式以及不提供個資之權益影響[2]等相關事項，俾使當事人能知悉其個人資料被他人蒐集之情形，並了解到最終個人資料會被何人利用、如何利用、在哪些地方被利用以及利用的期間為何，也就是個人資料被蒐集、處理及利用的情況應予透明化。同時，當事人若對於其個人資料欲主張停止蒐集、處理或利用等相關權利時，組織亦應予以配合[3]。

而合法蒐集的個人資料，不代表可以任意使用，原則上仍應在蒐集之特定目的必

1 個人資料保護法第 8 條第 2 項：「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、告知將妨害第三人之重大利益。五、當事人明知應告知之內容。」

2 個人資料保護法第 8 條第 1 項:「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。」

3 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。」

要範圍內為之，如有超出特定目的範圍，僅得在特定情形下得為特定目的外之利用[4]。

本案若發生於我國，按個資法規定，對於個人資料之利用，如無可為特定目的外利用之特定情形卻為特定目的外利用，則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[5]。

【管理 Tips】

消費者在使用網路上的免費服務時，為避免個人資料外洩或其他不利益情事之發生，應妥善知悉使用者條款內容。而網路服務業者提供免費服務，從而蒐集個人資料時，亦應注意是否符合個人資料保護法等相關法令規範。

而組織於利用個人資料時，亦應注意：一、應確認蒐集個人資料時，所告訴被蒐集者之告知事項內容，尤其是蒐集個人資料之特定目的，以及個人資料利用之期間、地區、對象及方式，因這是在利用個人資料時，所應遵守之事項。二、如果在上開個人資料蒐集目的中，找不到所要利用的特定目的時，則應確認有無得為特定目的外之利用的情形。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.18.1.1　適用之法規及契約的要求事項之識別

4 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識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

5 個人資料保護法第 47 條略以：「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，按次處新臺幣五萬元以上五十萬元以下罰鍰：三、違反第二十條第一項規定。」

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 本案如發生在我國，組織應明確識別相關法令，並依相關法令之要求執行業務，方可確保其工作之合法性。

ISO 29100：2011（CNS29100）

● 5.6 利用、持有及揭露原則

(1) 標準內容： 堅持利用、持有及揭露限制原則，意指下列事項。

- PII 之利用、持有及揭露(包括移轉)限制於為履行特定、明確及合法目的所必要者。

- 除非適用之法律明確要求不同的目的，否則將 PII 之利用限制於蒐集之前 PII 控制者所規定之目的。

持有 PII 之時間長度，僅為滿足所陳述目的必要的長度，並於之後安全地將其破壞或匿名化。

- 一旦所陳述目的逾期，但依適用法律要求保留下，鎖住(亦即將 PII 歸檔、保全及免除進一步處理)所有 PII。

當 PII 於國際間傳輸時，PII 控制者亦知悉所有跨國傳輸之國家或當地額外特定要求。

(2) 適用說明： 本案中，GSR 將所蒐集到的個人資料提供與劍橋分析，雖 GSR 有告知蒐集之目的以及可能提供所蒐集到的個人資料予第三方，但如 GSR 提供給劍橋分析之目的與 GSR 蒐集個資時告知被蒐集者之目的不同時，將是目的外利用之行為，而違反利用原則。

類別：資訊保護【案號：S10703】

主管機關駁斥手機廠商：「未取得」資安認證！

【焦點話題】

日前外國資安業者指出一款名為「RottenSys」的惡意程式入侵了全球約 500 萬台的 Android 手機，其中不乏知名大廠中招。隨後，手機廠商則刊出聲明，指其產品皆取得主管機關認證並合格上市，並無安全之虞。惟對此主管機關則發出新聞稿表示：「依電信法第 42 條第 1 項規定，針對手機之電信介面、電磁相容及電氣安全進行型式認證檢測，檢測範圍並不含手機內建軟體之資安檢測」。換言之，主管機關之電磁檢驗因性質與軟體不同，並無法為手機的資安能力背書。此外，主關機關雖有推動手機內建軟體之資安檢測，範圍包含出廠預載軟體、授權銷售商加載軟體，以及無圖示軟體等，但目前該手機廠商所生產之手機款式並未取得上述手機內建軟體之安全認證。主管機關呼籲各手機廠商不得以通過主管機關之「型式認證」，混稱其手機內建軟體亦取得「資安保證」，而應自主辦理智慧型手機內建軟體之資通安全認證。

【參考資料來源：自由電子報，107/3/28】

【重點摘要】

1. 電信法第 42 條、電信終端設備審驗辦法以及依其所訂定之行動寬頻業務寬頻終端設備技術規範，均在處理針對實體設備之相關問題，而設備內所載之軟體並無直接相關。

2. 智慧型手機系統內建軟體資通安全檢測技術規範對智慧型手機之安全分層訂定檢測項目，包括：資料使用授權、資料儲存保護、資料遺失保護、程式身分辨識、程式信任來源、程式執行授權、程式執行安全、協定使用授權、協定傳輸保護、協定執行安全、系統操作授權、系統身分辨識、系統執行安全、金鑰管理保護以及演算法強度要求等，通過分級檢測後方得稱通過該層級之安全檢測技術規範，符合各層級之程度資安要求。

【法律觀點】

電信法係為健全電信發展，增進公共福利，保障通信安全及維護使用者權益而制定[1]，同法第 42 條則要求連結第一類電信之電信終端設備應符合一定技術規範[2]，同時電信終端設備則指任何數位或類比設備，其以無線或有線傳輸媒介，與公眾電信網路之終端點介接，並以光或電磁波方式進行通信之設備[3]，因此，現代人日常生活不可或缺的智慧型手機亦包括在內，業者於製造、販售時亦須符合法規要求。

而電信法所要求於我國販售之電信終端設備應通過相關技術規範，該要求主要係為確保：[4]，一、不得損害第一類電信事業之電信機線設備或對其機能造成障礙；二、不對第一類電信事業之電信機線設備之其他使用者造成妨害；三、第一類電信事業設置之電信機線設備與使用者連接之終端設備，應有明確之責任分界；四、電磁相容及與其他頻率和諧有效共用；五、電氣安全，防止網路操作人員或使用者受到傷害。綜合上開要求，係為處理實體設備之相關問題，而依電信法第 42 條第 1 項及電信終端設備審驗辦法第 4 條第 2 項所訂定之「行動寬頻業務寬頻終端設備技術規範」，則仍係以電信法第 42 條所要求的實體設備及使用者的傷害訂定測試項目及合格標準[5]，包括功率限制等實體設備之測試，其所要求之技術規

---

[1] 電信法第 1 條：「為健全電信發展，增進公共福利，保障通信安全及維護使用者權益，特制定本法；本法未規定者，依其他法律之規定。」

[2] 電信法第 42 條第 1 項：「連接第一類電信事業所設電信機線設備之電信終端設備，應符合技術規範，並經審驗合格，始得輸入或販賣；其技術規範由電信總局訂定公告之。」

[3] 電信終端設備審驗辦法第 2 條第 1 款。

[4] 電信法第 42 條第 3 項：「第一項技術規範之訂定，應確保下列事項：一、不得損害第一類電信事業之電信機線設備或對其機能造成障礙。二、不對第一類電信事業之電信機線設備之其他使用者造成妨害。三、第一類電信事業設置之電信機線設備與使用者連接之終端設備，應有明確之責任分界。 四、電磁相容及與其他頻率和諧有效共用。五、電氣安全，防止網路操作人員或使用者受到傷害。」

[5] 行動寬頻業務寬頻終端設備技術規範第 5 條略以：「5. 測試項目及合格標準：5.1 功率限制…；5.2 發射頻譜波罩…：5.3 傳導帶外輻射發射限制…；5.4 相鄰頻道洩漏功率比…；5.5 頻率容許差度…；5.6 電磁波能量比吸收率…；5.7 電波功率密度…；5.8 電磁相容…；5.9 電氣安全…；5.10 手機端連接介面…；5.11 充電器端連接介面…；5.12 充電線…；5.13 充電器電性要求…；5.14 災防告警細胞廣播訊息接收功能…；5.15 IMEI 號碼及唯一保證書…」。

範與手機內建軟體之資安檢測並無相關。

因此，本案之手機製造商所聲稱通過資安認證與實際狀況並不相符，消費者於購買時僅能確認智慧型手機本身的硬體安全性應屬無虞，但並無法據以認定已符合足夠之資安認證，如其需符合相關資安標準，仍應滿足如「智慧型手機系統內建軟體資通安全檢測技術規範」等對於智慧型手機系統內建軟體之檢測。

【管理 Tips】

網路與通訊無遠弗屆，智慧型手機基於高度可攜性與便利性，有效提升生產力與工作效率，但隨之而來，使用者也必須面對智慧型手機上網後所帶來的資安威脅。有鑒於此，國家通訊傳播委員會於 106 年 3 月參考國際標準 ISO/IEC 15408 及歐美等國之作法，發布「智慧型手機系統內建軟體資通安全檢測技術規範」[6]，作為智慧型手機製造商、經銷商、電信業者及資通安全檢測實驗室辦理檢測之依據。

相關業者依上開規範之要求，在開發過程中或辦理檢測時，將手機系統及其內建軟體進行測試，並將安全等級區分為初級檢測、中級檢測以及高級檢測[7]，並依其檢測條件、檢測方法及所對照之判定標準，進行通過與否之確認。而依據國際間對智慧型手機安全之分層概念，將智慧型手機安全分層區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層等五個層別，考量不同層別可能面臨的資通安全風險有所不同，對各層別分別訂定檢測項目[8]，包括：資料使用授權、資料儲存保護、資料遺失保護、程式身分辨識、程式信任來源、程式執行授權、程式執行安全、協定使用授權、協定傳輸保護、協定執行安全、系統操作授權、系統身分辨識、系統執行安全、金鑰管理保護以及演算法強度要求等項目。開發者依上開文件之要求，在開發過程中，應注意到各層別之檢測項目之注意事項[9]，

[6] 通傳基礎字第 10663004370 號。

[7] 智慧型手機系統內建軟體資通安全檢測技術規範 3。

[8] 智慧型手機系統內建軟體資通安全檢測技術規範 2.2。

[9] 智慧型手機系統內建軟體資通安全檢測技術規範 6.2。

以確保智慧型手機系統及其內建軟體，符合現階段資通安全要求。

【相關標準】

ISO 27001：2013（CNS 27001）

- 14.2.1 保全開發政策

(1)標準內容： 應建立軟體及系統開發之規則，並應用至組織內之開發。

(2)適用說明： 行動裝置上網佔有率已超越桌機，智慧型手機之相關營收亦年年成長，而製造商因開發智慧型手機必載內建軟體方可驅動，因此無論是出廠預載軟體、銷售商加載軟體或是無圖示軟體，均可依據主管機關所提供之開發 APP 相關資安規範，建立自己的 APP 開發規則，使所開發之 APP 符合法規要求。

類別：資訊保護【案號：S10704】

名店資料被駭　女客遭詐騙 28 萬控店家未通知

【焦點話題】

台北糕餅名店 107 年 1 月發生會員資料遭盜取事件，導致不少會員接到詐騙電話，一名王小姐表示，她日前接到一通自稱糕餅名店客服人員之來電，該人員稱因資料輸入錯誤，每月會從其帳戶扣款 1800 元會費，隨後又接到一名自稱銀行客服之來電，要求王小姐到 ATM 進行變更操作，避免被扣除會費，她信以為真，將戶頭內共 28 萬元存款，全數匯到對方帳戶，事後聯絡糕餅名店，才驚覺自己遭受詐騙。糕餅名店客服表示發現雲端會員遭駭客盜取後，隨即於官網公告，並逐一發送簡訊及電子郵件通知會員，且擔心會員沒收到，每三至五天就發送一次，雖糕餅名店強調，被盜取的僅有會員訂購單資料並沒有個資，目前也只有一名受害者，但公司資料被盜是事實，也已強化電腦之加密機制，避免再有資料外洩情況。

【參考資料來源：三立新聞網，107/3/12】

【重點摘要】

1. 依個人資料保護法第 12 條規定，公務機關或非公務機關管理之個人資料，如有被竊取、洩漏、竄改或其他侵害者，應於查明後通知當事人，以使當事人得以知悉個人資料遭違法侵害之情事，並及時採取補救措施或提起救濟。
2. 按個人資料保護法施行細則第 22 條規定，個資外洩事件之通知方式，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，且如果費用所需過鉅時，亦得考量技術之可行性及當事人隱私之保護後，以網際網路、新聞媒體或其他適當之公開方式為之。

【法律觀點】

近年來個人資料外洩事故頻傳，當組織違反個人資料保護法(下稱個資法)規定，

導致相關事故發生時，為免損害擴大，個資法即要求該組織應查明後，以適當方式通知當事人[1]。故組織違反個資法致個資外洩時之通知，所應作為之事項如下：首先，應於查明事件相關事項後，組織則可採言詞、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，若通知費用所需過鉅時，亦得考量技術之可行性及當事人隱私之保護(不揭示可直接或間接識別當事人之個人資料)，以網際網路或新聞媒體或其他適當之公開方式[2]，通知當事人個人資料被侵害之事實及已採取之因應措施[3]，此外，若組織屬網際網路零售業或網際網路零售平台業者，除前段應通知之項目，須另外提供「諮詢服務專線」[4]，且如所發生者為重大事故，更應依主管機關指定之機制進行通報及進行後續處理[5]。

就本案而言，應先確認該公司是否為登記資本額為新臺幣 1,000 萬元以上之股份有限公司或已受指定之公司或商號[6]，如是，則據「網際網路零售業及網際網路

[1] 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。」

[2] 個人資料保護法施行細則第 22 條第 1 項：「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。」

[3] 個人資料保護法施行細則第 22 條第 2 項：「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。」

[4] 法務部 105 年 04 月 20 日法制字第 10502506140 號函釋，要旨：「各中央目的事業主管機關應針對轄下所有特許行業，依個人資料保護法第 27 條規定訂定相關個資檔案安全維護計畫及辦法，而相關辦法就業者對於當事人通知義務事項，應明定通知內容包含『個資外洩之事實、業者所採取之因應措施及所提供之諮詢服務專線』等。」

[5] 網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法第 8 條第 1 項第 4 款。

[6] 網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法第 2 條第 1 項：「本辦法所稱網際網路零售業，指以網際網路方式零售商品，且登記資本額為新臺幣一千萬元以上之股份有限公司，或受經濟部（以下簡稱本部）指定之公司或商號。但不包括應經特許、許可或受專門管理法令規範之行業。」。其立法理由為「考量一定規模以上之業者，其擁有之個人資料已占大宗，且考量業者之經營成本，爰本辦法將適用之範圍，限制在一定資本額以上之股份有限公司。」但依該條立法理由二可知，為使經濟部能有效管理，縱非前開一定資本額以上之股份有限公司，如其已發生個人資料外洩等事故，或經濟部認有加強管理之必要時，亦得指定公司或商號適用該辦法。

零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」之規定[7]，以及參照前述法務部要求之相關事項，該糕餅名店應將個資外洩之事實、所採取之因應措施及後續供當事人查詢之專線與其他查詢管道，通知受影響之當事人。

【管理 Tips】

一般來說，發生個資事故時，對內必須向上通報，予以適當調查及處理，以防止事態的蔓延及擴大；對外則視事故之嚴重性，決定是否需要對外發布相關訊息。另外，組織所發生之資訊安全事件涉及個人資料被竊取、洩漏、竄改或其他侵害時，則應在查明事件原因後告知當事人，且當組織為網際網路零售業時，必須依法告知應對措施及服務專線。同時，除解決個案問題外，組織也需進行問題核心之分析，並以此為借鏡，降低再次發生類似事件之機率。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.16.1.2 通報資訊安全事件

(1)標準內容： 應循適切之管理管道，儘速通報資訊安全事件。

(2)適用說明： 資安事件、事故發生時，儘速透過適當窗口通報予相關單位、主管機關，以降低事件、事故發生之衝擊。本案如係涉及網際網路零售時，事發單位依網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法第 8 條之規定，於發現個資外洩後儘速通報予權責機關，並將相關內容一併通知當事

[7] 網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法第 8 條：「前條因應措施，應包括個人資料被竊取、竄改、毀損、滅失或洩漏等事故之應變機制，其內容應對下列事項為具體規定：一、降低、控制事故對當事人造成損害之作法。二、適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形，及後續供當事人查詢之專線與其他查詢管道。三、避免類似事故再次發生之矯正及預防機制。四、發生重大事故時，即時依本部公告或持續通報事故之處理情形與避免類似事故再次發生之矯正及預防機制。」

人，應可有效降低個資外洩所造成之損害風險。

類別：資訊保護【案號：S10705】

遭澳洲稱 5G 危及國家安全 中國大陸通訊設備大廠聲明反擊

【焦點話題】

澳洲政府於 2012 年禁止某中國大陸通訊設備廠供應其全國寬頻網路（National Broadband Network, NBN），於 2018 年 5 月更是力阻該通訊設備廠建造澳洲與索羅門群島間的網路纜線。澳洲政府此舉恐是擔憂中國大陸企業掌控其通訊基礎設施，並於近期的 5G 通訊設施投標案仔細審查該廠。而該通訊設備廠澳洲區董事長及董事發表聯合聲明反擊澳洲政府，表示：「我們是一家獨立經營的公司，並沒有其他的單位參與，在我們運營的 170 國家的每一個國家，我們都遵守所在國的法律和規則。不這樣做的話，我們的業務一夜之間就完了。[1]」而英國、加拿大、紐西蘭皆已接受該公司的 5G 測試提案，願意評估、確認是否遵守數位安全協定。

【參考資料來源：自由電子報，107/6/18、Reuters，107/6/18】

【重點摘要】

1. 標的屬於財物採購時，依臺灣地區與大陸地區人民關係條例第 35 條第 3 項規定，並非所有與大陸地區的貿易行為均予以禁止，但允許輸出入之品項以及管理等應遵行事項授權須由有關主管機關擬訂，並報請行政院核定。

2. 標的屬於工程及技術服務採購中資訊服務採購時，依行政院公共工程委員會工程企字第 10400024613 號函要求，需求單位應先行評估採購標的是否屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」，而經濟部投資審議委員會所公告「具敏感性或國安（含資安）疑慮之業務範疇」包括能源類、水資源類、通訊傳播類、交通類、金融與銀行類、緊急救援與醫院類、中央政府與地方機關與科技園區與工業區中被選定之重要系

[1] "We are a private company, owned by our employees with no other shareholders. In each of the 170 countries where we operate, we abide by the national laws and guidelines. To do otherwise would end our business overnight."

統。

3. 依資通安全管理法第 9 條、資通安全管理法施行細則第 4 條之規定，受資通安全管理法納管之對象於辦理資通系統建置、維運或資通服務提供之委外時，應有相關之注意事項。

【法律觀點】

政府採購法之立法目的在於提升採購效率與功能，確保採購品質[2]。因此機關辦理採購時，得依實際需要，設定投標廠商之基本資格，且如為特殊或巨額之採購，須由具有相當經驗、實績、人力、財力、設備等之廠商始能擔任者，得另規定投標廠商之特定資格[3]，藉以確保採購品質[4]。

然而，因為我國與大陸間的特殊關係，因此在為政府採購時仍應特別注意。

標的屬於財物採購時，依臺灣地區與大陸地區人民關係條例第 35 條第 3 項[5]規定，並非所有與大陸地區的貿易行為均予以禁止，但允許輸出入之品項以及管理等應遵行事項授權須由有關主管機關擬訂，並報請行政院核定。而依該項所訂定之臺灣地區與大陸地區貿易許可辦法則對可輸入之大陸地區物品為正面表列[6]，如非

---

[2] 政府採購法第 1 條：「為建立政府採購制度，依公平、公開之採購程序，提升採購效率與功能，確保採購品質，爰制定本法。」

[3] 政府採購法第 36 條：「機關辦理採購，得依實際需要，規定投標廠商之基本資格。特殊或巨額之採購，須由具有相當經驗、實績、人力、財力、設備等之廠商始能擔任者，得另規定投標廠商之特定資格。外國廠商之投標資格及應提出之資格文件，得就實際需要另行規定，附經公證或認證之中文譯本，並於招標文件中訂明。第一項基本資格、第二項特定資格與特殊或巨額採購之範圍及認定標準，由主管機關定之。」

[4] 民間業者之採購係屬於民事契約，原則上並不需適用政府採購法，但如屬於公立學校、公營事業辦理採購時，仍適用政府採購法之相關規定。

[5] 臺灣地區與大陸地區人民關係條例第 35 條第 3 項：「臺灣地區人民、法人、團體或其他機構，經主管機關許可，得從事臺灣地區與大陸地區間貿易；其許可、輸出入物品項目與規定、開放條件與程序、停止輸出入之規定及其他輸出入管理應遵行事項之辦法，由有關主管機關擬訂，報請行政院核定之。」

[6] 臺灣地區與大陸地區貿易許可辦法第 7 條第 1 項：「大陸地區物品，除下列各款規定外，不得輸入臺灣地區：一、主管機關公告准許輸入項目及其條件之物品。二、古物、宗教文物、民族藝術品、民俗文物、藝術品、文化資產維修材料及文教活動所需之少量物品。三、自用之研究或開發用樣品。四、依大陸地區產業技術引進許可辦法規定准許輸入之物品。五、供學校、研究機構及動物園用之動物。六、保稅工廠輸入供加工外銷之原物料與零組件，及供重整後全數外銷之物品。七、加工出口區及科學工業園區廠商輸入供加工外銷之原物料與零

屬允許得由大陸地區輸入台灣地區之品項者，即不得輸入，而其中得輸入之品項並不包括資通安全設備，且依主管機關公告准許輸入品項亦必須以不危害國家安全及對相關產業無重大不良影響者為限[7]。

而如標的屬於工程及技術服務採購中資訊服務採購時，依行政院公共工程委員會工程企字第 10400024613 號函要求，各機關辦理資訊服務採購，需求單位應先行評估採購標的是否屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」，並於簽辦採購文件中載明，如屬前開業務範疇者，應依「投標廠商資格與特殊或巨額採購認定標準」第 4 條第 1 項第 6 款[8]規定，確實於招標文件載明不允許經濟部投資審議委員會公告之陸資資訊服務業參與。

而目前經濟部投資審議委員會所公告「具敏感性或國安（含資安）疑慮之業務範疇」[9]包括能源類、水資源類、通訊傳播類、交通類、金融與銀行類、緊急救援與醫院類、中央政府與地方機關與科技園區與工業區中被選定之重要系統。

此外，資通安全管理法經行政院核定於 108 年 1 月 1 日施行，若相關機關、單位屬該法所納管之對象，於辦理資通系統建置、維運或資通服務提供之委外時，應針對受託者及相關內容妥適進行注意及監督。

綜上可知，如案例中之情形發生於我國，則我國政府機關應依資通安全管理法之規定，妥適選任廠商及進行相關監督，並判斷該案屬單純財物採購或是資訊服務採購，如是單純財物採購，因所採購品項係屬涉及資通安全之設備，並不在臺灣地區與大陸地區貿易許可辦法中得為採購的正面表列清單，依法不得採購；而如

組件，及供重整後全數外銷之物品。八、醫療用中藥材。九、行政院新聞局許可之出版品、電影片、錄影節目及廣播電視節目。十、財政部核定並經海關公告准許入境旅客攜帶入境之物品。十一、船員及航空器服務人員依規定攜帶入境之物品。十二、兩岸海上漁事糾紛和解賠償之漁獲物。十三、其他經主管機關專案核准之物品。」

[7] 臺灣地區與大陸地區貿易許可辦法第 8 條第 1 項：「主管機關依前條第一項第一款公告准許輸入之大陸地區物品項目，以符合下列條件者為限：一、不危害國家安全。二、對相關產業無重大不良影響。」

[8] 投標廠商資格與特殊或巨額採購認定標準第 4 條第 1 項第 6 款：「機關依第二條第二款訂定與履約能力有關之基本資格時，得依採購案件之特性及實際需要，就下列事項擇定廠商應附具之證明文件或物品：...六、其他法令規定或經主管機關認定者。」

[9] https://www.moeaic.gov.tw/download-file.jsp?do=BP&id=HmkGoSBaCyY= ，具敏感性或國安(含資安)疑慮之業務範疇。

為資訊服務採購，因通訊傳播中通訊網路維運支援相關系統屬於「具敏感性或國安(含資安)疑慮之業務範疇」，故亦不允許經濟部投資審議委員會公告之陸資資訊服務業[10]參與。

【管理 Tips】

按行政院公共工程委員會針對政府採購訂定多項範本，包括資訊服務採購契約範本，因此政府機關在辦理與資訊及通訊安全有關採購時，得應循辦理，而資訊服務採購契約範本針對於廠商之資訊安全責任[11]有下列規定：

1.廠商應遵守行政院所頒訂之各項資訊安全規範及標準，並遵守機關資訊安全管理及保密相關規定。此外機關保有對廠商執行稽核的權利。

2.廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

3.契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄。

4.廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。

5.廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。

6.廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合機關對系統品質及資訊安全的要求。

7.廠商如違反第 1 目至第 6 目規定，應適用第 15 條之違約責任，並就機關所受

[10] https://www.moeaic.gov.tw/download-file.jsp?do=BP&id=seb8R5JfT+w= ，陸資投資資訊產業事業清冊（107 年 5 月 21 日更新）

[11] 資訊服務採購契約範本第 16 條第 19 項。（106 年 7 月 13 日版本）

損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。

受資通安全管理法納管之對象，辦理資通系統建置、維運或資通服務提供之委外時，應注意之相關事項，依資通安全管理法施行細則第 4 條之規定，如下：

1.受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

2.受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

3.受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

4.受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

5.受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

6.受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

7.委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

8.受託者應採取之其他資通安全相關維護措施。

9.委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

一般民間組織如需相類似的資安服務，或可參考資訊服務採購契約範本，並參照

資通安全管理法之相關規定，作為廠商之資訊安全責任依據。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.7.1　聘用前

(1)標準內容：　確保員工及承包商瞭解其將承擔之責任，且適任其角色。

(2)適用說明：　委託承包商提供資訊服務，在現代專業分工下相當常見。政府機關於選任資訊服務之承包商時，須依照政府採購之相關規範挑選合適的承包商或限定承包商之資格；一般組織亦可仿此精神，在選定委外廠商時，進行必要之背景調查，並汰除不合適之廠商，以保障組織採購資訊服務之安全與品質。

類別：資訊保護【案號：S10706】

勞務採購洩密 機關之承辦人遭判刑 1 年 2 個月

【焦點話題】

政府機關之承辦人於任內辦理勞務採購招標案，涉嫌於招標前自行或透過行政秘書將評選委員遴選名單透漏予有意投標之廠商閱覽、挑選，並協助該廠商順利得標。該承辦人一審時依公務員洩密罪遭判刑 2 年半且不得易科罰金，經上訴後，臺灣高等法院高雄分院認定其僅單純洩密，無法證明有其他圖利情事，改判 1 年 2 個月徒刑，並可易科罰金定讞，而涉嫌協助遞送委員遴選名單之行政秘書，一審遭判 6 個月徒刑、廠商總經理則判 9 個月徒刑，皆可易科罰金。

【參考資料來源：新頭殼，107/1/23、臺灣高等法院高雄分院 107 年度聲再字第 25 號刑事裁定、臺灣高等法院高雄分院 106 年度上易字第 479 號刑事判決】

【重點摘要】

1. 政府採購法第 34 條規定，招標文件原則於公告前應予保密；對底價、廠商名稱、家數等，在標案公告後至開標前仍須保密；而於開標至決標之期間，對於底價仍應予以保密；決標後除有特殊情形外，應予公開底價。

2. 按採購評選委員會組織準則第 2、3、6 條規定，機關採限制性招標辦理公告金額以上之委託專業服務、技術服務或資訊服務的採購時，應就各該採購案成立採購評選委員會，但因該委員會涉有訂定或審定招標文件之評選項目、評審標準及評定方式；辦理廠商評選；協助機關解釋與評審標準、評選過程或評選結果有關之事項，因此，委員名單，於開始評選前應予保密，於評選出優勝廠商或最有利標後，方予以解密。

【法律觀點】

現行政府機關辦理工程、財物、勞務[1]等採購之招標方式[2]共分為公開招標、選擇

[1] 政府採購法第 2 條：「本法所稱採購，指工程之定作、財物之買受、定製、承租及勞務之委任或僱傭等。」

性招標及限制性招標三種，採取公開招標或選擇性招標時，必須將招標公告或辦理資格審查之公告刊登於政府採購公報並公開於資訊網路[3]，有關必須公告之內容[4]則包括：案號、機關、及其他重要資訊，而招標文件指機關為邀請廠商投標所準備之相關文件，其內容應包括投標廠商提交投標書之一切必要資料[5]，諸如投標須知、投標標價清單、投標廠商聲明書等資料。

而限制性招標係指不經公告，邀請二家以上廠商比價或一家廠商議價之招標方式，因此，在招標階段不必上網公告。若機關辦理公告金額以上之委託專業服務、技術服務、資訊服務及辦理設計競賽，需選出優勝者而採限制性招標時[6]，有成立採購評選委員會[7]之必要，而委員會之任務即為訂定或審定招標文件之評選項目、評審標準及評定方式、辦理廠商評選、協助機關解釋與評審標準、評選過程或評選結果有關之事項等[8]故委員會之名單，於開始評選前應予保密，於評選出優勝

---

[2] 政府採購法第 18 條「採購之招標方式，分為公開招標、選擇性招標及限制性招標。本法所稱公開招標，指以公告方式邀請不特定廠商投標。本法所稱選擇性招標，指以公告方式預先依一定資格條件辦理廠商資格審查後，再行邀請符合資格之廠商投標。本法所稱限制性招標，指不經公告程序，邀請二家以上廠商比價或僅邀請一家廠商議價。」

[3] 政府採購法第 27 條第 1 項：「機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報並公開於資訊網路。公告之內容修正時，亦同。」

[4] 政府採購公告及公報發行辦法第 7 條：「依本法第二十七條第一項規定辦理之招標公告，應登載下列事項：一、有案號者，其案號。二、機關之名稱、地址、聯絡人 (或單位) 及聯絡電話。三、招標標的之名稱及數量摘要。有保留未來後續擴充之權利者，其擴充之期間、金額或數量。四、招標文件之領取地點、方式、售價及購買該文件之付款方式。五、收受投標文件之地點及截止期限。六、公開開標者，其時間及地點。七、須押標金者，其額度。八、履約期限。九、投標文件應使用之文字。一〇、招標與決標方式及是否可能採行協商措施。一一、是否屬公告金額以上之採購。一二、是否適用我國所締結之條約或協定。一三、廠商資格條件摘要。一四、財物採購，其性質係購買、租賃、定製或兼具二種以上之性質。一五、是否屬公共工程實施技師簽證者。一六、其他經主管機關指定者。」

[5] 政府採購法第 29 條第 3 項：「第一項文件內容，應包括投標廠商提交投標書所需之一切必要資料。」

[6] 政府採購法第 22 條第 1 項第 9、10 款：「機關辦理公告金額以上之採購，符合下列情形之一者，得採限制性招標：...九、委託專業服務、技術服務或資訊服務，經公開客觀評選為優勝者。十、辦理設計競賽，經公開客觀評選為優勝者。」

[7] 採購評選委員會組織準則第 2 條：「機關為辦理下列事項，應就各該採購案成立採購評選委員會 (以下簡稱本委員會) ：一、本法第二十二條第一項第九款或第十款規定之評選優勝者。二、本法第五十六條規定之評定最有利標或向機關首長建議最有利標。」

[8] 採購評選委員會組織準則第 3 條第 1 項：「本委員會應於招標前成立，並於完成評選事宜且無待處理事項後解

廠商後，則予解密[9]。

於本案例中，承辦人明知政府機關辦理採購，載有標案計畫內容之招標文件不得於公告前交付，且於評選委員會辦理評選前，不得洩漏評選委員資料，更不應配合廠商圈選評選委員，而使其於評選委員會開始評選前得悉評選委員人選，該等文書及消息均係中華民國國防以外應祕密者，應予保密，承辦人使廠商閱覽遴選名單，供其挑選評選委員，使廠商於評選委員會開始評選前即知悉評選委員會之成員，犯有刑法洩漏國防以外之秘密罪[10]，故遭處有期徒刑 1 年 2 個月。

【管理 Tips】

為避免發生廠商於招標前即取得招標文件知悉其內容，採購法第 34 條[11]明文招標文件原則於公告前應予保密。而為防止廠商藉先行了解底價及其他競爭者之資料，而造成不公平之現象，對底價、投標廠商名稱、數量等，於標案公告至開標前仍須保密，而在開標後因審標或減價之需要，可能無法立即決標，而後至決標前，對於底價仍應予以保密；最末，基於透明化之需要，底價於決標後除有特殊情形外，應予公開[12]。

因此，承辦政府採購案件，組織應建立標準作業流程，並明確告知同仁相關規則，尤其是涉及法律規範者，應納入工作規則，訂定內部罰則，並透過教育訓練，以

散，其任務如下：一、訂定或審定招標文件之評選項目、評審標準及評定方式。二、辦理廠商評選。三、協助機關解釋與評審標準、評選過程或評選結果有關之事項。」

9 採購評選委員會組織準則第 6 條：「本委員會委員名單，於開始評選前應予保密。但經本委員會全體委員同意於招標文件中公告委員名單者，不在此限。本委員會委員名單，於評選出優勝廠商或最有利標後，應予解密；其經評選而無法評選出優勝廠商或最有利標致廢標者，亦同。」

10 刑法第 132 條第 1 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。」

11 政府採購法第 34 條：「機關辦理採購，其招標文件於公告前應予保密。但須公開說明或藉以公開徵求廠商提供參考資料者，不在此限。機關辦理招標，不得於開標前洩漏底價，領標、投標廠商之名稱與家數及其他足以造成限制競爭或不公平競爭之相關資料。底價於開標後至決標前，仍應保密，決標後除有特殊情形外，應予公開。但機關依實際需要，得於招標文件中公告底價。機關對於廠商投標文件，除供公務上使用或法令另有規定外，應保守秘密。」

12 政府採購法第 34 條 87 年立法理由。

及宣導等方式，使相關人員知曉其嚴重性，該等人員如不能堅守品操、善盡保密義務，並謹慎依法辦理採購作業，即有可能觸法而面臨相關刑責，殊值戒慎。

【相關標準】

ISO27001：2013（CNS27001）

- A.7.2.2　資訊安全認知、教育及訓練

(1)標準內容：　組織所有員工及相關之約用人員，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2)適用說明：　組織應透過諸如教育訓練等方式，確保其人員等，於平時即妥善了解組織之相關政策及法律、法規等規範。若本案之組織平時均有對其人員進行教育訓練，確保相關員工了解若違反相關規定之嚴重性，對於因人為因素而造成之洩密風險，應可有效降低。

- A 18.1.1　適用之法規及契約的要求事項之識別

(1)標準內容：　對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明：　組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。本案如承辦人能清楚了解政府機關辦理採購之相關規範要求，對於所承辦業務具有保密義務而不洩漏評選委員資料，應可避免涉犯法規遭致判刑的結果。

類別：資訊保護【案號：S10707】

商業電子郵件詐騙橫行，美國逮捕 74 名嫌犯

【焦點話題】

美國司法部與聯邦調查局宣布，在全球三大洲破獲國際商業電子郵件詐騙(Business E-mail Compromise, BEC)活動。BEC 又稱為網路金融詐騙，常見手法為鎖定具有企業之財務權限員工進行詐騙，該類詐騙手法源自奈及利亞，現已遍布全球。美國將此次逮捕行動稱為 Operation Wire Wire，除了美國司法部與聯邦調查局之外，美國特勤局、美國財政部金融犯罪防治署等單位均全力配合行動，共同逮捕計 74 名嫌犯，緝獲近 240 萬美元之不法所得，並追回約 1,400 萬美元贓款。

【參考資料來源：Department of Justice，107/6/11；iThome，107/6/12】

【重點摘要】

1. 商業電子郵件詐騙又稱變臉詐騙，其指透過社交工程或是電腦入侵企業電子信箱，再設法詐騙其跨國合作廠商匯款的一種新型態詐騙，其流程通常是透過社交工程攻擊特定組織，進入組織後透過潛伏監控以瞭解並分析作業流程，最終利用對於組織的瞭解以執行詐騙。
2. 社交工程雖利用人性弱點以騙取重要資料，讓人防不勝防，但能隨時保持提高警覺，不輕易開啟可疑電子郵件，開啟後不隨意下載電子郵件的附件檔及不隨意點擊郵件夾帶的超連結，應可大幅將網路攻擊阻絕於外，使資安風險降至最低。

【法律觀點】

近年來電子郵件詐騙已從針對不特定多數人進化至針對特定人士及組織。尤以俗稱變臉詐騙的商業電子郵件(BEC)詐騙為大宗，進而造成組織重大損失。變臉詐

騙[1]是一種新型態的詐騙，係指透過社交工程或電腦入侵組織之電子信箱，再設法詐騙其跨國合作廠商匯款，以達到詐騙目的。

變臉詐騙的手法[2]通常是犯罪集團透過魚叉式網路釣魚攻擊[3]等社交工程攻擊進入組織網路，接著可能會花數週或數月時間來研究組織之合作廠商、財務系統和高階主管之電子郵件溝通風格，甚至是高階主管之旅行時程。當時機成熟時，詐騙者會透過高階主管之電子郵件帳號發送假郵件予財務部門，指示該部門要求合作廠商匯款 至詐騙者指定之帳戶。而財務部門則依指示將款項匯入該帳戶，但實際上被害者已將款項轉移至詐騙者控制之另一帳戶。而變臉詐騙之攻擊對象多具有跨國合作情形，其主因在於利用組織時常需與具時差之外國客戶聯繫之特性，當事件發生時，難以即時發現，而發現時亦難以回復。

據此亦可判斷變臉詐騙慣用的三個階段：社交工程攻擊、潛伏監控與執行詐騙。而上開三個階段則各有其觸法之虞。首先，犯罪集團鎖定特定組織進行社交工程入侵他人電腦，並進行潛伏、監控、研究及分析，此舉恐觸犯刑法第 358 條妨害電腦使用罪[4]，得處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。其次，犯罪集團假冒特定人士向合作廠商請求匯款之詐騙行為，亦恐構成刑法第 339 條第 1 項普通詐欺罪[5]，得處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。綜上，若行為人利用非法手段侵入他人電腦並行詐騙致他人損失者，應論以妨害電腦使用罪、詐欺取財罪，數罪併罰之。

---

[1] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)，(瀏覽日期：2018 年 6 月 27 日)

[2] Business E-Mail Compromise - Cyber-Enabled Financial Fraud on the Rise Globally，https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise ，(瀏覽日期：2018 年 6 月 27 日)

[3] 魚叉式網路釣魚係指針對特定對象的網路釣魚，而非一般的網路釣魚，且因其具有特定對象，故可判斷使用魚叉式網路釣魚的發動者應具有針對該特定對象的特殊原因，進而造成更大的損害。

[4] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[5] 刑法第 339 條第 1 項：「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。」

【管理 Tips】

現代科技日新月異，利用網路通訊更是方便快捷，網路攻擊亦與時俱進，而攻擊對象亦從不特定多數人轉變為針對更具利益之特定目標，進行攻擊，且因愈來愈多的網路攻擊具有潛伏並觀察組織作業之特性，以至最終執行破壞時，造成之損害更是難以抵擋。

因此對組織而言，如何將網路攻擊阻絕在外是相當重要的課題，社交工程雖利用人性弱點以騙取重要資料，讓人防不勝防，但能隨時保持提高警覺，不輕易開啟可疑電子郵件，開啟後不隨意下載電子郵件的附件檔及不隨意點擊郵件夾帶的超連結，應可大幅將網路攻擊阻絕於外，並有效降低資安風險。

【相關標準】

ISO27001：2013（CNS27001）

- A.7.2.2　資訊安全認知、教育及訓練

(1)標準內容：　組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2)適用說明：　組織對其員工或相關之約用人員進行有效之教育訓練，使組織成員得清楚了解資訊安全之重要性，使其組織成員面對社交工程郵件時能提高警覺，避免危險作為，應可有效將威脅阻絕於外。

- A.14.1.2　保全公共網路之應用服務

(1)標準內容：　應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議或未經授權揭露與修改。

(2)適用說明：　組織對於成員使用公共網路上傳送的應用服務，如線上郵件應用服務等，應謹慎使用，組織更可用限制使用的方式，例如禁止使用此類公共網路之應用服務，以避免陷入社交

工程或其他詐欺活動之可能。

類別：資訊保護【案號：S10708】

又見商業間諜！上市科技大廠機密外洩 損失高達 38 億

【焦點話題】

林姓工程師任職於上市科技大廠近 11 年，主要負責動態隨機存取記憶體(DRAM) 產品研發。去年 3 月，轉往大陸發展的許姓前主管遊說林男跳槽，並允諾高薪，但要求林男必須提供 DRAM 專業報告。林男受重金引誘下決定離職，並於離職前破解公司電腦防火牆，以手機竊取公司多達 11.5GB 的內部資料，離職後又向另一名李姓離職員工索取該科技大廠與其他公司共同研發的 DRAM 機密資料，導致上市科技大廠損失 38 億元，返台後隨即遭檢警約談，並以涉嫌違反營業秘密法起訴。

【參考資料來源：聯合報，107/7/21】

【重點摘要】

1. 按照最高法院 106 年度台上字第 441 號民事判決指出，實務上認為具有秘密性（非一般涉及該類資訊之人所知）、經濟價值（因其秘密性而具有實際或潛在之經濟價值）、保密措施（所有人已採取合理之保密措施），且可用於生產、銷售或經營之資訊，即屬營業秘密。
2. 按照檢察機關辦理重大違反營業秘密法案件注意事項第 2 點指出，涉犯侵害營業秘密罪，且為上市、上櫃公司或經我國政府認許之外國公司所有之營業秘密，其經濟價值逾新臺幣 1,000 萬元以上之重大違反營業秘密法案件，因其影響甚鉅，勢必成為社會焦點，因此要求由專責檢察官偵辦，以儘速分案偵辦。

【法律觀點】

營業祕密法第 2 條[1]規定，營業祕密係指方法、技術、製程、配方、程式、設計

[1] 營業祕密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛

或其他可用於生產、銷售或經營之資訊，且非一般涉及該類資訊之人所知者、因其秘密性而具有實際或潛在之經濟價值者，而所有人已採取合理保密措施者。據此，實務上認為具有秘密性、經濟價值、保密措施，且可用於生產、銷售或經營之資訊，即屬營業秘密法第 2 條所規定，得作為該法保護之對象[2]。

行為人意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而以不正方法取得、無權而重製、使用或洩漏、或應刪除銷毀而不為等方式侵害他人或他公司營業秘密者，即可能構成營業秘密法第 13-1 條[3]侵害營業秘密罪，最高得處以 5 年以下有期徒刑，並得併科最高 1,000 萬元罰金。且如係行為人不法取得我國人之營業秘密，其意圖係於域外使用，將嚴重影響我國產業之國際競爭力，因此同法第 13-2 條[4]規定對於意圖在外國、大陸地區、香港或澳門使用，而犯第 13-1 條第 1 項各款之罪者，處 1 年以上 10 年以下有期徒刑，並得併科最高 5,000 萬元罰金。

又檢察機關鑒於重大違反營業秘密法案件影響產業倫理與競爭秩序甚鉅，為兼顧重大營業秘密之保障、社會公共利益及人權維護，亦發布檢察機關辦理重大違反營業秘密法案件注意事項[5]。其重大違反營業秘密法案件[6]係指犯營業秘密法第 13-1 條、第 13-2 條，且為上市、上櫃公司或經我國政府認許之外國公司所有營

在之經濟價值者。三、所有人已採取合理之保密措施者。」

[2] 最高法院 106 年度台上字第 441 號民事判決。

[3] 營業祕密法第 13-1 條第 1 項：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣一百萬元以上一千萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。二、知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。三、持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。四、明知他人知悉或持有之營業秘密有前三款所定情形，而取得、使用或洩漏者。」

[4] 營業祕密法第 13-2 條第 1 項：「意圖在外國、大陸地區、香港或澳門使用，而犯前條第一項各款之罪者，處一年以上十年以下有期徒刑，得併科新臺幣三百萬元以上五千萬元以下之罰金。」

[5] 檢察機關辦理重大違反營業秘密法案件注意事項第 1 點立法說明。

[6] 檢察機關辦理重大違反營業秘密法案件注意事項第 2 條：「本注意事項所稱重大違反營業秘密法案件，指犯營業秘密法第十三條之一、第十三條之二之罪，且符合下列情形之一者：(一) 營業秘密為上市、上櫃公司或經我國政府認許之外國公司所有。(二) 營業秘密經濟價值逾新臺幣一千萬元以上。(三) 其他經各檢察機關檢察長核定。」

業秘密，其經濟價值逾新臺幣 1,000 萬元以上。也因為該重大案件影響甚鉅，勢必成為社會焦點，因此要求由專責檢察官偵辦[7]，並儘速分案偵辦[8]，而以維護公共利益或保護合法權益之必要時，亦可適度發布新聞[9]。

本案中，林男原任職於上市科技大廠，因離職而盜取其「動態隨機存取記憶體(DRAM)產品測試技術」等機密資料，並將該資料攜至中國大陸 DRAM 廠任職，意圖在大陸地區使用，而據上市科技大廠表示，其所損失之金額可能高達 38 億，因而符合營業祕密法第 13-2 條的加重規定，並應由專責檢察官儘速偵辦，以維重大營業秘密之保障。

【管理 Tips】

針對營業秘密保護，業界所提出之營業祕密管理指針，從四大面向「政策」、「內容」、「人員」、「環境及設備相關」等管理重點，建立營業秘密管理措施或機制。亦即從營業秘密管理政策擬定、營業秘密產出 / 使用 / 流通等管理、內 / 外部人員保密規範、存放營業秘密的環境與設備控管等四大構面加以規範。

就本案而言，組織應訂定營業祕密管理政策，並定期檢驗營業秘密管理的執行現況，並透過明確定義營業祕密及建立清單，以要求組織人員負有保密約定或競業禁止等約定，再從環境及設備等相關管理下，建立實體與虛擬二方面之保護機制，以降低營業祕密外洩之風險。

【相關標準】

ISO27001：2013（CNS27001）

- A.18.1.1　適用之法規及契約的要求事項之識別

---

[7] 檢察機關辦理重大違反營業秘密法案件注意事項第 3 點：「檢察機關應指派專責檢察官偵辦重大違反營業秘密法案件。　　法務部或其他機關舉辦營業秘密法相關研習，並應優先遴派專責檢察官參加。」

[8] 檢察機關辦理重大違反營業秘密法案件注意事項第 4 點第 1 項：「檢察機關就重大違反營業秘密法案件應於收文後儘速分案，並即交專責檢察官辦理。」

[9] 檢察機關辦理重大違反營業秘密法案件注意事項第 18 點：「重大違反營業秘密法案件，為維護公共利益或保護合法權益，而認有適度發布新聞之必要時，得聽取告訴人或被害人意見，並避免透露有關營業秘密之實質內容。」

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織在業務開發時應瞭解並依循其應適用之法令，以避免觸法。以本案例而言，組織應熟悉營業祕密三原則，並善用保密約定或競業禁止等約定，以保障自身權益。

- A.18.2.2 安全政策及標準之遵循性

(1)標準內容： 管理人員應以適切之安全政策、標準及所有其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。

(2)適用說明： 組織應在建立管理制度時，應以具備適當的管理政策，使組織得以依循，以本案為例，應訂定營業秘密管理規定及相關配套程序，於明確營業秘密管理範圍及對象下，進行營業秘密的內容、人員、環境及相關設備等管理，並據以遵循。

類別：資訊保護【案號：S10709】

包商小油坑架 200 萬天線 軍方雷達站訊號全都錄

【焦點話題】

國家科技研發機構於 105 年招標無線電設備採購案，科技公司於投標前夕為確保價值 200 萬的設備能正常運作，竟將天線架於國軍雷達站附近，警方發現立刻通知國安機關派員到場勘查，發現該組天線設備係由美商國家儀器公司製造，具有指向性功能與頻譜分析儀，除能偵測分析頻譜訊號，更有測錄功能，經解密分析，確定蒐錄的訊號中包含多筆軍方專用的軍事跳頻無線電訊號，惟經查該科技公司未將機密外洩，且其林姓負責人及許姓員工皆坦認犯行，故地檢署分別為緩起訴及不起訴處分。

【參考資料來源：自由時報，106/11/27】

【重點摘要】

1. 按照國家機密保護法第 4 條規定，國家機密等級區分為絕對機密、極機密以及機密，其區別在於洩漏後對國家安全或利益造成非常重大損害（全面性危害）、重大損害（對國家安全或利益產生嚴重影響）或損害（對國家安全或利益產生影響）等不同程度。
2. 按照國家機密保護法施行細則第 21 條規定，傳遞國家機密時，實體傳遞以人員親自持送為原則，必要時得派人員護送，或以外交郵袋或雙掛號函件傳遞；電子通信工具傳遞則應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞。

【法律觀點】

攸關國家安全或利益之資訊，應建立國家機密保護制度，予以妥善保護[1]。然而，並非任何公務資訊皆屬國家機密保護法所保護之客體，必須係基於國家安全或利

[1] 國家機密保護法第 1 條。

益而有保護必要者，且經核定為機密等級的資訊，才屬「國家機密」[2]。

然而，國家機密等級區分為絕對機密、極機密以及機密，其區別在於洩漏後對國家安全或利益造成不同程度之傷害[3]。就非常重大損害而言，係指造成全面性危害之情形[4]，重大損害則指對國家安全或利益產生嚴重影響之情形[5]，而損害指國家安全或利益產生影響之情形[6]。而核定之權限係由「絕對機密」、「極機密」、「機密」等事項，對其損害國家安全或利益之程度，分層規定其核定權人[7]。

---

[2] 國家機密保護法第 2 條：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[3] 國家機密保護法第 4 條：「國家機密等級區分如下：一、絕對機密適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。　二、極機密　適用於洩漏後足以使國家安全或利益遭受重大損害之事項。　三、機密適用於洩漏後足以使國家安全或利益遭受損害之事項。」

[4] 國家機密保護法施行細則第 5 條：「本法第四條第一款所稱非常重大損害，指有下列各款情形之一：一、造成他國或其他武裝勢力，以戰爭、軍事力量或武裝行為敵對我國。　二、使軍事作戰遭受全面挫敗。　三、造成全國性之暴動。　四、中斷我國與邦交國之外交關係或重要友好國家之實質關係。　五、喪失我國在重要國際組織會籍。　六、其他造成戰爭、內亂、外交或實質關係重大變故，或危害國家生存之情形。」

[5] 國家機密保護法施行細則第 6 條：「本法第四條第二款所稱重大損害，指有下列各款情形之一：一、中斷或破壞我國與他國軍事交流、軍事合作或軍事協定之推展。　二、使單一軍（兵）種或作戰區聯合作戰遭受挫敗。　三、危害從事或協助從事情報工作人員之身家安全，或中斷、破壞情報組織之運作。　四、使政府通信、資訊之保密技術、設備、設施遭受破解或破壞。　五、中斷或破壞與大陸地區、香港或澳門之協議或談判。　六、嚴重不利影響我國與邦交國之外交關係或友好國家之實質關係。　七、破壞我國在重要國際組織享有之會員地位或重大權益。　八、破壞洽談中之建交案、條約案、協定案或加入國際組織案。　九、中斷或破壞我國與他國經貿之諮商、協議、談判或合作事項。　十、其他使國家安全或利益相關政務發展產生嚴重影響之情形。」

[6] 國家機密保護法施行細則第 7 條：「本法第四條第三款所稱損害，指有下列各款情形之一：一、有利他國或減損我國情報蒐集、研析、處理或運用。　二、減損整體國防武力，或破壞建軍備戰工作推展。　三、使作戰部隊、重要軍事設施或主要武器裝備之安全遭受損害。　四、不利影響與大陸地區、香港或澳門之交流活動。　五、不利影響與邦交國之外交關係或友好國家之實質關係。　六、妨礙洽談中之建交案、條約案、協定案、諮商案、合作案或加入國際組織案。　七、其他使國家安全或利益相關政務發展產生影響之情形。」

[7] 國家機密保護法第 7 條：「國家機密之核定權責如下：一、絕對機密由下列人員親自核定：(一)總統、行政院院長或經其授權之部會級首長。　(二)戰時，編階中將以上各級部隊主官或主管及部長授權之相關人員。　二、極機密由下列人員親自核定：(一)前款所列之人員或經其授權之主管人員。　(二)立法院、司法院、考試院及監察院院長。　(三)國家安全會議秘書長、國家安全局局長。　(四)國防部部長、外交部部長、行政院大陸委員會主任委員或經其授權之主管人員。　(五)戰時，編階少將以上各級部隊主官或主管及部長授權之相關人員。　三、機密由下列人員親自核定：(一)前二款所列之人員或經其授權之主管人員。　(二)中央各院之部會及同等級之行、處、局、署等機關首長。　(三)駐外機關首長；無駐外機關首長者，經其上級機關授權之主管人員。　(四)戰時，編階中校以上各級部隊主官或主管及部長授權之相關人員。　前項人員因故不能執行職務時，由其

經核定為國家機密之資訊，在標示、知悉、持有、使用、收發、傳遞、保管、複製、移交、銷毀及解除等作為，均應依法辦理。對於保管國家機密之場所或區域，基於維護國家機密之必要，得禁止或限制人員或物品進出，且為能周密管制及有效維護，得採取其他必要之管制措施[8]，並對國家機密之維護隨時或定期查核，及應指派專責人員辦理國家機密之維護事項[9]，以加強國家機密之維護。於傳遞時，實體傳遞以人員親自持送為原則，必要時得加派人員護送，或以外交郵袋、雙掛號函件傳遞；若以電子通信工具傳遞國家機密時，應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞[10]。

而上開管制之目的在於避免國家機密遭洩漏，以維護國家安全，因此本法亦規定，洩漏或交付國家機密者，最重處 7 年有期徒刑[11]，刺探或收集國家機密者，最重亦可處 5 年有期徒刑[12]。

本案之林姓負責人及其員工係為參與政府標案，先行測試設備，雖經查其等側錄之無線電訊號包含機密級之軍事機密，惟未查友洩漏之情事，僅得論以刺探國家機密罪，且考量被告等人並未造成國家安全危害，因此檢察官未為起訴，僅分別以緩起訴即不起訴處分之。

【管理 Tips】

從組織角度加以觀察，本案可從兩個重點加以思考。首先是資訊分級，因資源有限，組織無法就所有的資料給予相同規格的保護，故組織必須依照資料檔案重要

職務代理人代行核定之。」

[8] 國家機密保護法第 19 條立法理由二。

[9] 國家機密保護法第 20 條：「各機關對國家機密之維護應隨時或定期查核，並應指派專責人員辦理國家機密之維護事項。」

[10] 國家機密保護法施行細則第 21 條：「國家機密之傳遞方式如下：一、在機關內相互傳遞，屬於絕對機密及極機密者，由承辦人員親自持送。二、在機關外傳遞，屬於絕對機密或極機密者，由承辦人員或指定人員傳遞，必要時得派武裝人員或便衣人員護送。屬於機密者，由承辦人員或指定人員傳遞，或以外交郵袋或雙掛號函件傳遞。　　依前項第二款規定，由承辦人員或指定人員傳遞者，事先應作緊急情形之銷毀準備。國家機密非由承辦人員親自持送傳遞者，應密封交遞。以電子通信工具傳遞國家機密者，應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞。」

[11] 國家機密保護法第 32 條第 1 項：「洩漏或交付經依本法核定之國家機密者，處一年以上七年以下有期徒刑。」

[12] 國家機密保護法第 34 條第 1 項：「刺探或收集經依本法核定之國家機密者，處五年以下有期徒刑。」

性之不同，予以適當的保護，以避免資源之浪費。

另一方面，則是資料傳送之安全性，原則上，易發生資料外洩之節點有三，分為資料傳入、資料儲存以及資料傳出之階段，其中資料傳輸即佔兩部分，因此資訊傳送安全性係屬資訊管理中之重要一環，宜透過有效加密機制或保密裝備，以強化相關資料傳輸時的安全，避免遭到破解或竊取。除考量傳輸安全外，資料儲存之後台設備亦應同等視之，包括定期維護硬體設備與更新系統、防毒軟體版本，且保持監控並留下紀錄追蹤，均為有效的管控措施。

【相關標準】

ISO27001：2013（CNS27001）

- A.13.2.3　電子傳訊

  (1)標準內容：　應切適保護電子傳訊時所涉及之資訊。

  (2)適用說明：　組織應在進行資訊傳輸時，應具備有效的保密措施，避免資訊外洩，以本案為例，所被告透過無線電將資訊予以截取，但因加密方式完備而內容並無外洩，可見有效的保密措施是保護傳訊內容的良好方法。

- A.8.2.1　資訊之分級

  (1)標準內容：　資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

  (2)適用說明：　組織應依照其保有資訊之價值、重要性等，將資料進行分級，以利後續發展資訊管理。以本案為例，無線電蒐錄之訊號係為國家機密，應依國家機密保護法要求，將資料區分為絕對機密、極機密及機密。

類別：資訊保護【案號：S10710】

歐盟個資法上路 台灣爭取列入白名單

【焦點話題】

史上最嚴格的歐盟個人資料保護規定（GDPR）正式上路，該規定適用於各行業並採取高罰鍰，政府相關部會總動員，對於影響最大的跨境傳輸，決定兩路並進，爭取列入歐盟認可的「白名單」國家，以降低對廠商衝擊。

繼反洗錢、反避稅浪潮後，反個資外洩亦成為全球趨勢，GDPR 適用對象不僅是於歐盟設點的企業，境外若有蒐集或處理歐盟民眾個資者，亦受規範。新規定對科技、金融、航運、電商等，將大幅提升法遵成本，甚至形成貿易障礙。我國政府亦高度重視，並由國發會主政採相關因應措施，首先爭取加入歐盟認可的跨境傳輸「白名單」。再於各部會成立諮詢、輔導窗口，協助產業因應 GDPR，並密切觀察 GDPR 執行情況、檢討國內個資法，以及評估成立個資保護專責單位。

【參考資料來源：經濟日報，107/5/16】

【重點摘要】

1. 按照一般資料保護規範第 45 條(General Data Protection Regulation, art. 45)規定，進行與歐盟國家間的個資國際傳輸時之適足性評估時應考量：1.法治、對人權與基本自由之尊重、一般與部門之相關立法；2.有一個或以上存在且有效運作獨立監管機關；3.參與或簽署關於個人資料保護之國際協定或其他具法律拘束力之合約。
2. 未通過與歐盟國家間的個資國際傳輸時的適足性評估時，就必須要由控管者或處理者提供適當保護措施，或經同意、契約合意、基於資料主體之利益、公共利益或是法律上之必要等情形下，方得進行。

【法律觀點】

在全球化的時代，企業多會透過業務委外以降低營運成本，例如在甲國製造產品，

販賣至乙國再由丙國進行客服，此時，企業所擁有的個人資料於國與國之間流動將無可避免，而歐盟於今年 5 月上路的一般資料保護規則(General Data Protection Regulation,下稱 GDPR)，對於個人資料跨境傳輸具有相關規定。

對企業而言，因 GDPR 的保護對象為歐盟境內之資料主體，因此當個人資料之控管者(controller)或處理者(processor)在歐盟境內所為之個人資料處理活動，均屬其規範範圍，縱使控管者或處理者非設於歐盟境內，但其對於歐盟境內之資料主體提供商品或服務，或對於資料主體於歐盟內進行監控，亦受 GDPR 規範[1]。由上可知，無論組織是否設立在歐盟境內，只要活動涉及其範圍內之個人資料蒐集時，就必須遵守 GDPR。

然為保護歐盟的資料主體，GDPR 在跨境傳輸設有嚴格限制，首先，歐盟採「原則禁止、例外允許」模式[2]，也就是資料僅於控管者及處理者遵循特定條件下，方得進行跨境傳輸，除此之外不得為之。

而使資料得以跨境傳輸之重要條件即係通過歐盟執委會認定移轉之場所得以完善進行資料保護，也就是必須進行適足性評估，當一國家經認定得以完善進行資料保護時，往後的對於於該國與歐盟間之資料移轉，即無需獲得特別授權[3]。該適足性評估之考量要件包括[4]：1.法治、對人權與基本自由之尊重、一般與部門之相關立法；2.有一個或以上存在且有效運作獨立監管機關；3.參與或簽署關於個人資料保護之國際協定或其他具法律拘束力之合約。

但如某國家未通過歐盟之適足性評估，原則上歐盟境內之資料即不得對該國為跨境傳輸，此時，必須要控管者或處理者自行提供適當保護措施，方得為資料的國際傳輸。而所謂的適當保護措施包括：公務機關或機構間有法律拘束力且得執行之辦法、有拘束力之企業守則、標準資料保護條款、行為守則或通過經核准之驗證機制[5]。而在沒有經過適足性評估也欠缺適當保護措施之情形下，就必須經同

[1] General Data Protection Regulation, art. 3.

[2] General Data Protection Regulation, art. 44.

[3] General Data Protection Regulation, art. 45 §1.

[4] General Data Protection Regulation, art. 45 §2.

[5] General Data Protection Regulation, art. 46.

意、契約合意、基於資料主體之利益、公共利益或是法律上之必要等情形下，方得進行資料傳輸[6]。

歐盟新法通過後，從國家角度而言，通過適足性評估可以避免個別企業在與歐盟國家進行時，必須單獨通過各項要求，也因此，各國政府均以爭取加入歐盟認可之跨境傳輸「白名單」為目標，成立個人資料保護專案辦公室，希冀能加速成為通過適足性評估的國家。

【管理 Tips】

就組織在面對個人資料國際傳輸時，應確認的事項包括：是否屬於國際傳輸、我國法上（包括中央目的事業主管機關）有無規範、資料接收或來源國有無規範、傳輸過程的監督管理、內部審核並留存相關紀錄。

首先，國際傳輸的定義於我國是指將個人資料作跨國（境）之處理或利用[7]，因此不論所傳輸的對象是否為同一組織之分支機構均屬之。其次，傳輸前應考量所屬產業有無特別限制、是否屬於限制傳輸之國家或地區，並再確認資料接收國或來源國有無相關規範，例如 GDPR 對於歐盟地區的個人資料國際傳輸受有嚴格限制，在不符其規範之狀況下，資料是無法進行國際傳輸的。在傳輸的過程中應注意將資料傳送路徑、儲存方式及過程等予以紀錄留存，而後續監督管理及審核之方式，亦必須加以注意，藉以提升及強化資訊傳輸之安全性。

【相關標準】

ISO27001：2013（CNS27001）

- A.13.2.1 資訊傳送政策及程序

(1)標準內容： 應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。

[6] General Data Protection Regulation, art. 49.

[7] 個人資料保護法第 2 條第 6 款。

(2)適用說明： 組織對於資訊傳送時，應具備正式之傳送政策、程序及控制措施，藉以保護資訊傳送的安全。而歐盟新規對於未通過適足性評估的組織，在進行國際資訊傳送時，要求要具備有拘束力之企業守則等適當保護措施即屬之。

類別：資訊保護【案號：S10711】

公務防駭 近萬機關資安納管 預告資安法 6 大子法草案

【焦點話題】

106 年台灣公部門遭網路攻擊成功的案例共有 360 件，其中高達八成來自中國網軍攻擊。政府視資安為國安，為防止政府機關資安遭中國等其他網軍攻擊，進而推動資安法制化，訂定「資通安全管理法」。

「資通安全管理法」於 107 年 5 月 11 日經立法院三讀通過，並於同年 6 月 6 日正式公布該法，由於資通安全管理法施行需要準備期，目前由該法之主管機關─行政院暫定於 108 年 1 月 1 日施行。

行政院亦於 107 年 7 月 9 日起辦理資通安全管理法相關之 6 個子法草案之 60 天預告作業[1]，於 8 至 9 月間同步舉辦多場座談會，並將子法草案置於「眾開講」平台，若各界對於子法有疑慮或建議，均可以座談會或「眾開講」平台提出相關建議；在彙整各界意見後，將進行相關子法之發布及備查作業。估計全國將有近一萬個中央與地方政府其及下轄的各公務機關、公立學校等，將受該法規範。

【參考資料來源：自由時報，107/7/4；iThome，107/7/15】

【重點摘要】

1. 我國於 107 年 6 月公布資通安全管理法，規範對象包括：公務機關及特定非公務機關，公務機關係指除軍事機關與情報機關外，依法行使公權力之中央、地方機關（構）或公法人，而特定非公務機關則指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

2. 資通安全責任等級分級辦法將資安責任區分成 A、B、C、D、E 總共 5 個等級。而各機關應依其自身對應之等級，從管理面、技術面以及認知與訓練等面向，進行其應辦事項。

[1] 行政院 107 年 11 月 21 日院臺護字第 1070213547 號令，已發布資通安全管理法各子法。

【法律觀點】

為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益[2]，我國於 107 年 6 月公布資通安全管理法，並定自 108 年 1 月 1 日施行，該法所規範之對象包括公務機關與特定非公務機關，公務機關係指除軍事機關與情報機關外，依法行使公權力之中央、地方機關 (構) 或公法人[3]，而特定非公務機關則指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。而資通安全管理法所規範之重點包括主管機關之權責[4]、公務及特定非公務機關之資通安全管理、以公私協力推動國家資通安全發展[5]，以及委外辦理資通服務之管理[6]。

就公務機關而言，應符合其所屬資通安全責任等級的要求，訂定、修正及實施資

---

[2] 資通安全管理法第 1 條。

[3] 資通安全管理法第 3 條第 5 款。

[4] 資通安全管理法第 2 條「本法之主管機關為行政院。」第 5 條「主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。　前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。」第 6 條「主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。 前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。」第 7 條「主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之。 主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。 特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。」第 8 條「主管機關應建立資通安全情資分享機制。 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。」

[5] 資通安全管理法第 4 條「為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：一、資通安全專業人才之培育。二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。三、資通安全產業之發展。四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。　前項相關事項之推動，由主管機關以國家資通安全發展方案定之。」。

[6] 資通安全管理法第 9 條「公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。」。

通安全維護計畫[7]，並設置資通安全長負責資通安全事務[8]，每年向上級或監督機關提出資通安全維護計畫實施情形[9]，為因應資通安全事件，公務機關更應訂定通報及應變機制，以利於事件發生時之通報與調查[10]。而特定非公務機關部分，亦須符合其所屬資通安全責任等級的要求，訂定、修正及實施資通安全維護計畫[11]，並訂定資通安全事件之通報及應變機制，並以是否屬於關鍵基礎設施提供者進行區分，其主要差別在於，包括提出資通安全維護計畫實施情形、受稽核以及提出改善報告等，受有監督管理等均係關鍵基礎設施提供者應受友或辦理之義務，而其關鍵基礎設施提供者以外之特定非公務機關，僅於中央目的事業主管機關要求時，方有相同之受監督管理義務[12]。

---

[7] 資通安全管理法第 10 條「公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」

[8] 資通安全管理法第 11 條「公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。」

[9] 資通安全管理法第 12 條「公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形;無上級機關者，其資通安全維護計畫實施情形應送交主管機關。」

[10] 資通安全管理法第 14 條「公務機關為因應資通安全事件，應訂定通報及應變機制。 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。 公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。」

[11] 資通安全管理法第 16 條第 2 項「關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」;同法第 17 條第 1 項「關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」

[12] 資通安全管理法第 16 條第 3 項以下「關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。 中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。 關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關。 第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。」;同法第 17 條第 2 項以下「中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。 前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。」

就罰則部分，如特定非公務機關未訂定、修正或實施資通安全維護計畫，或違反其必要事項；未提出資通安全維護計畫實施情形；未提出改善報告；未訂定通報及應變機制或違反其必要事項；未提出資安事件調查、處理及改善報告或違反其規定；違反資安事件通報內容之規定時，處其 10 萬至 100 萬元罰鍰[13]，對資安事件知情不報者，最高更可處 500 萬元罰鍰，並限期改正[14]。

【管理 Tips】

主管機關已正式對外發布包括：《資通安全管理法施行細則》、《資通安全責任等級分級辦法》、《資通安全事件通報及應變辦法》、《特定非公務機關資通安全維護計畫實施情形稽核辦法》、《資通安全情資分享辦法》以及《公務機關所屬人員資通安全事項獎懲辦法》等 6 個資通安全管理法子法。

其中資通安全責任等級分級辦法則是將資安責任依照各機關所涉業務資料、資通系統分成 A、B、C、D、E 總共 5 個等級。而各公務機關與特定非公務機關應依其自身對應之等級，從管理面、技術面以及認知與訓練進行其應辦事項。

縱非屬上開受資通安全管理法規範之非公務機關，仍可依資通安全責任等級分級辦法，就自身所面臨到之風險加以分析並依其內容予以辦理，亦不失於對資通安全的良好控管措施。

---

[13] 資通安全管理法第 20 條「特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰：一、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫必要事項之規定。二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。三、未依第七條第三項、第十六條第五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條第六項或第十七條第四項所定辦法中有關改善報告提出之規定。四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八條第四項所定辦法中有關通報及應變機制必要事項之規定。五、未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。 六、違反第十八條第四項所定辦法中有關通報內容之規定。」

[14] 資通安全管理法第 21 條「特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。」

【相關標準】

ISO27001：2013（CNS27001）

- A.7.2.3　懲處過程

(1)標準內容：　應具備正式及以傳達之懲處過程，以對違反資訊安全之員工採取行動。

(2)適用說明：　資通安全管理法將違反相關規定者予以明定其情形，並分為罰鍰處分，如以國家作為一個整體組織，則個別違反規定之機關則可類比於其員工，違反規定時，國家就必須對其採取行動，以保障組織的資通安全。

- A.18.1.1　適用之法規及契約的要求事項之識別

(1)標準內容：　對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明：　資通安全管理法通過後，對於公務機關及特定非公務機關將是全新的挑戰，各組織除母法外，對於相對應的六個子法亦應有所認知，方能於其正式施行後確切遵行以符合相關要求。

類別：資訊保護【案號：S10712】

民眾個資、公所公文拿去墊菜？市府：查明後將懲處

【焦點話題】

林姓女子表示日前收到果菜市場的得標菜貨，打開檢查時發現有一疊紙張，起初原以為是廢紙，本想利用背面空白處寫字，卻驚覺該紙張上竟載有地方區公所的函文、地方環保機關的結業證書，以及地方社福卡申請表等文件，其中可見民眾的身份證件影本、住址、手機號碼等基本資料。該地方市政機關則表示，公文銷毀應依照既定程序執行，承諾會檢討資料外洩之情形，並已要求各單位清查，若有人為疏失，將進行懲處，同時緊急回收外洩資料，也向民眾致歉。

【參考資料來源：自由時報，107/6/27】

【重點摘要】

1. 按個人資料法施行細則第 22 條規定，個資外洩事件之通知方式，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，且如果費用所需過鉅時，亦得考量技術之可行性及當事人隱私之保護後，以適當公開方式通知。

2. 資通安全事件通報及應變辦法第 4 條第 1 項規定，資通安全事件發生後，受規範之公務機關與特定非公務機關，均必須要在知悉資通安全事件的 1 小時內，依照主管機關指定的方式及對象，進行資通安全事件之通報；及同辦法第 6 條第 1 項規定：若是第一級或是第二級資安事件，權責機關在接獲通報 8 小時內進行資安事件等級的審核，事件機關則在知悉後 72 小時內完成損害控制或恢復作業；若是第三級或是第四級資安事件，則必須在接獲通報 2 小時內完成審核，知悉後 36 小時內完成損害控制或恢復作業。

【法律觀點】

按個人資料保護法（下稱個資法）第 2 條規定，得以直接或間接識別該個人之資

料即為個人資料（下稱個資）[1]，對於個資之蒐集、處理皆必須符合法定要件，且原則上不得為特定目的外之利用。公務機關保有個人資料者，應指定專人辦理安全維護事項[2]，而當其未針對保有之個資採行適當安全措施，導致資料被竊取、竄改、毀損、滅失或洩漏時，則如非公務機關一般，可能須負擔行政[3]及民事[4]等相關責任，相關公務員恐亦面臨遭懲處[5]。於事故發生時，公務機關應先查明相關事項，並於事件查明後，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，若通知費用所需過鉅時，亦得斟酌技術之可行性及當事人隱私之保護後，以網際網路或新聞媒體等適當方式[6]，通知當事人個資被侵害之事實及因應措施[7]。

除個人資料保護法之外，本年度行政院發布之《資通安全事件通報及應變辦法》即是在處理公務機關與特定公務機關間，對資通安全事件所應進行之通報及應變方式。

該辦法將資通安全事件依是否屬於核心業務以及事件之嚴重程度等因素，區分為四級[8]，

---

[1] 個人資料保護法第 2 條第 1 款：「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。」

[2] 個人資料保護法第 18 條：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

[3] 個人資料保護法第 48 條第 4 款：「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：...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。」。

[4] 個人資料保護法第 29 條第 1 項略以：「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。」

[5] 公務員懲戒法第 2 條：「公務員有下列各款情事之一，有懲戒之必要者，應受懲戒：一、違法執行職務、怠於執行職務或其他失職行為。　二、非執行職務之違法行為，致嚴重損害政府之信譽。」

[6] 個人資料保護法施行細則第 22 條第 1 項：「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。」

[7] 個人資料保護法施行細則第 22 條第 2 項：「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。」

[8] 資通安全事件通報及應變辦法第 2 條第 1 項：「資通安全事件分為四級。」

而資通安全事件發生後，受規範之公務機關及特定非公務機關，必須於知悉資通安全事件後 1 小時內，依照主管機關指定的方式及對象，進行資通安全事件通報[9]；而通報為第一級或第二級的資安事件，權責機關應於接獲通報後 8 小時內完成資安事件等級之審核，事件機關則於知悉事件後 72 小時內完成損害控制或復原作業；若是第三級或第四級資安事件，則必須於接獲通報 2 小時內完成審核，事件機關則應於知悉事件後 36 小時內完成損害控制或復原作業[10]。而公務機關與特定非公務機關完成損害控制或復原作業後，仍應續行調查及處理，並提出調查、處理及改善報告[11]，以作為後續改善之依據。

本案中，涉事機關除應盡個資法所規範之義務外，再者，個人資料亦屬資通安全事件通報及應變辦法所稱之敏感資訊[12]，因此其洩漏後，其資通安全事件等級恐自第三級起跳。

【管理 Tips】

[9] 資通安全事件通報及應變辦法第 4 條第 1 項：「公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。」；第 11 條第 1 項：「特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。」

[10] 資通安全事件通報及應變辦法第 5 條第 1 項：「主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：一、通報為第一級或第二級資通安全事件者，於接獲通報後八小時內。　二、通報為第三級或第四級資通安全事件者，於接獲通報後二小時內。」；第 6 條第 1 項：「公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象，辦理通知業務：一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。　二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。」；第 12 條第 1 項：「中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：一、通報為第一級或第二級資通安全事件者，於接獲通報後八小時內。　二、通報為第三級或第四級資通安全事件者，於接獲通報後二小時內。」；第 13 條第 1 項：「特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式，辦理通知業務：一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。　二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。」

[11] 資通安全事件通報及應變辦法第 6 條第 2 項：「公務機關完成前項作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。」第 13 條第 2 項：「特定非公務機關完成前項作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。」

[12] 資通安全事件通報及應變辦法第 2 條立法理由 3：「所稱敏感資訊，指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。」

預防勝於治療，當資安事件發生時，應當如何有效應變並非一蹴可及，因此，透過適當安全演練等預防機制有其必要性，而在資通安全事件通報及應變辦法中亦要求公務機關與特定非公務機關，應配合主管機關規劃、辦理資通安全演練作業，而其項目可能包括社交工程演練、資通安全事件通報及應變演練、網路攻防演練、情境演練以及其他必要之演練等，透過適當的演練，可使機關對於資通安全事件之預防與應變更臻完備。

縱非屬上開受資通安全管理法規範之非公務機關，仍可依資通安全事件通報及應變辦法，辦理自身的資通安全演練，避免資安事件發生時難以應變，此亦不失於對資通安全的良好控管措施。

【相關標準】

ISO27001：2013（CNS27001）

- A.16.1.2 通報資訊安全事件

  (1)標準內容： 應循適切之管理管道，儘速通報資訊安全事件。

  (2)適用說明： 資安事件發生時，應儘速透過主管機關所指定之方式通報，以降低事件、事故發生之衝擊。本案應依規定於發現個資外洩後於 1 小時內通報主管機關，且因涉及個人資料，故於查明後亦應將相關內容通知當事人。

- A8.2.1 資訊之分級

  (1)標準內容： 資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。

  (2)適用說明： 組織宜依照其保有資料之價值、法規要求等，將資料進行分級並為此制定合適的管理方法。以本案為例，組織得依照其個人資料之揭露程度及是否含特種個資等方向進行分級。

類別：資訊保護【案號：S10713】

資產兆元以上銀行應設獨立法遵與資安單位

【焦點話題】

金融主管機關於 106 年底邀集金控、銀行業者參與公聽會，討論金控與銀行內部控制及稽核制度實施辦法，要求資產兆元以上的銀行應設立獨立的法遵部門、吹哨人保護機制及資安專責單位。107 年 3 月 31 日所發布之金融控股公司及銀行業內部控制及稽核制度實施辦法，已於同年 9 月 30 日正式施行，該辦法為提昇銀行業者對資訊安全之重視，明定銀行業者須設置資訊安全專責單位及主管，負責資安相關工作，並依其規模大小進行差異化管理，以降低資安風險。

【參考資料來源：聯合新聞網，106/12/7、金融監督管理委員會新聞稿，107/3/20】

【重點摘要】

1. 金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條規定，銀行業應設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備，而資產總額達兆元以上的銀行，應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管。

2. 資通安全管理法第 17 條規定，中央目的事業主管機關得要求所管特定非公務機關，在符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，且得要求特定非公務機關提出資通安全維護計畫實施情形，更得稽核其實施情形。

【法律觀點】

近年銀行資安事件發生頻頻，從 ATM 到國際匯款系統屢遭駭客入侵，為此，

金融監督管理委員會（下稱金管會）特於 107 年 3 月 31 日發布新修正之金融控股公司及銀行業內部控制及稽核制度實施辦法，並於同年 9 月 30 日施行。

該辦法要求銀行業者應設置資訊安全專責單位及主管，且不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備[1]，而資產總額達兆元以上的銀行，應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管[2]，該資訊安全專責單位並應獨立於原本的資訊單位外且組織地位相當。

資訊安全專責單位所負責的業務包括：規劃、監控及執行資訊安全管理作業，而專責單位主管必須與其他高階主管，共同將資訊安全執行情形做成資訊安全整體執行情形聲明書，提報董事會[3]，聲明書則要求該銀行提出應加強事項、改善措施以及預定完成改善日期[4]，且資訊安全專責單位人員亦應受一定時數的資訊安全專業課程訓練或職能訓練[5]。對此，只要屬於金融控股公司或銀行業者，無論是公營銀行或民營銀行均需要符合上開規定，以維資訊安全。

且如該銀行為如臺灣銀行[6]等公營銀行時，因 107 年 6 月 6 日所公布的資通

---

[1] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條第 1 項本文。

[2] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條第 2 項。

[3] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條第 3 項：「銀行業資訊安全專責單位負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，由資訊安全專責單位主管與董(理)事長(主席)、總經理、總稽核聯名出具資訊安全整體執行情形聲明書（附表二），並於會計年度終了後三個月內提報董(理)事會。」

[4] 資訊安全整體執行情形說明書。

[5] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條第 4 項：「銀行業資訊安全專責單位人員，每年至少應接受十五小時以上資訊安全專業課程訓練或職能訓練。總機構、國內外營業單位、資訊單位、財務保管單位及其他管理單位之人員，每年至少須接受三小時以上資訊安全宣導課程。」

[6] 臺灣銀行為臺灣金融控股股份有限公司持股百分之百之銀行，而臺灣金融控股股份有限公司為財政部持股百分之百之國營事業，按大法官釋字第 41 號解釋文：「國營事業轉投於其他事業之資金，應視為政府資本，如其數額超過其他事業資本百分之五十者，該其他事業即屬於國營事業管理法第三條第一項第三款之國營事業。」因此臺灣銀行屬國營事業。而資通安全管理法第 3 條第 6 款：「六、特定非公

安全管理法規定中央目的事業主管機關得要求所管特定非公務機關[7]，在符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，且得要求特定非公務機關提出資通安全維護計畫實施情形，更得稽核其實施情形[8]，因此公營銀行除提報董事會外，亦可能會面臨主管機關之要求提出其資通安全維護計畫實施情形。

【管理 Tips】

行政院於 107 年 11 月 21 日正式對外發布資通安全管理法相關子法，其中資通安全管理法施行細則第 6 條[9]已對資通安全維護計畫所應包括之事項予以明列並說明，而資通安全維護計畫之事項係以 PDCA（Plan-Do-Check-Act 的簡稱，係指按規劃、執行、查核與行動作為管理依據）為原則，與 CNS 27001 資訊安全管理系統相仿[10]，一般組織縱非該

務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」因此公營事業即國營事業屬於資通安全管理法之特定非公務機關。

[7] 資通安全管理法第 3 條第 7 款：「特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」

[8] 資通安全管理法第 17 條：「關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。　中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。　中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。　前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。」

[9] 資通安全管理法施行細則第 6 條第 1 項：「本法第十條、第十六條第二項及第十七條第一項之資通安全維護計畫，應包括下列事項：一、核心業務及其重要性。　二、資通安全政策及目標。　三、資通安全推動組織。　四、專責人力及經費之配置。　五、公務機關資通安全長之配置。　六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。　七、資通安全風險評估。　八、資通安全防護及控制措施。　九、資通安全事件通報、應變及演練相關機制。　十、資通安全情資之評估及因應機制。　十一、資通系統或服務委外辦理之管理措施。　十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。　十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。」

[10] 以「資通安全政策及目標」而言，CNS27001 5.2 政策即要求最高觀禮階層應建立資訊安全政策，又以「資通安全風險評估」而言，CNS27001 6.1.2 資訊安全風險評鑑則是要求組織應定義及應用資訊安

法所定義之公務機關或特定非公務機關，亦可將其作為組織內資訊安全管理之建置參考。

【相關標準】

ISO27001：2013（CNS27001）

- A.18.2.2 安全政策及標準之遵循性

(1)標準內容：管理人員應以適切之安全政策、標準及所有其他安全要求事項，定期審查其責任範圍內之安全處理及程序之遵循性。

(2)適用說明：管理人員必須定期審查其責任範圍內之安全處理及程序之遵循性，而金融控股公司及銀行業內部控制及稽核制度實施辦法亦要求資訊安全專責單位審查相關事項，以將前一年度資訊安全整體執行情形做成報告，使高階主管得以出具執行情形聲明書。

- A.7.2.1 資訊安全認知、教育及訓練

(1)標準內容：組織所有員工及相關承包商，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2)適用說明：組織可透過教育訓練等方式，確保其成員能適切瞭解組織之相關政策、程序以及與其相關之適當知識，而金融控股公司及銀行業內部控制及稽核制度實施辦法即有要求銀行業資訊安全專責單位人員，每年至少應接受 15 小時以上資訊安全專業課程訓練或職能訓練。總機構、國內外營業單位、資訊單位、財務保管單位及其他管理單位之人

全風險評鑑。

員，每年至少須接受 3 小時以上資訊安全宣導課程。

貳、資訊公開(Disclosure)

類別：資訊公開【案號：D10714】

性侵犯沒匿名權！ 波蘭公開性侵犯個資

【焦點話題】

近日，波蘭政府為維護兒童安全，公佈 768 名兒童性犯罪者名單，只要登入波蘭司法部的網站[1]，任何人皆可透過該網站查看性犯罪者之個人資料，除有姓名及清楚臉部照片外，還包含性犯罪者的性別、罪名、刑期、出生年月日、甚至連出生地及現居地址等資料也一併釋出。公佈資料，但此舉亦引來人權團體的抗議，認為曝光身分將使出獄後的性犯罪者更難融入社會，也可能讓性犯罪者陷入報復攻擊的人身危險之中。然而，波蘭當局仍堅持公佈該名單的用意是為保護兒童，性犯罪者必須承擔嚴重的後果，包括褫奪匿名的權利。

【參考資料來源：聯合新聞網，107/1/9】

【重點摘要】

1. 兒童及少年福利與權益保障法第 97 條規定，對於兒童及少年如有強迫、引誘、容留或媒介兒童及少年為猥褻行為或性交行為，得以公布行為人之姓名；而性侵害防制條例第 23-1 條則規定，有下列情形，該管警察機關得將其身分資訊登載於報紙或以其他方法公告：1. 性侵害犯罪加害人經直轄市、縣(市)主管機關通知，無正當理由不到場或拒絕接受評估、身心治療或輔導教育，而屆期仍不履行；2.性侵害犯罪加害人經直轄市、縣(市)主管機關通知，無正當理由不按時到場接受身心治療或輔導教育，而屆期仍不履行；3.性侵害犯罪加害人未依規定定期辦理登記、報到、資料異動或接受查訪或接受之時數不足，而屆期仍不履行；4.判決有罪之性侵害犯罪加害人逃亡或藏匿經通緝者。

2. 性侵害犯罪防治法亦規定中央主管機關應建立全國性侵害加害人之檔案資料，

[1] Sex Offenders Register The Public Register，https://rps.ms.gov.pl/en-US/Public#/home(瀏覽日期：2018 年 6 月 18 日)。

並在一定情況下，基於維護公共利益及社會安全之目的，於登記期間得供特定人員查閱，故中央主管機關仍有建立檔案資料之責。

【法律觀點】

性侵害犯罪防治法之立法目的在於防治性侵害犯罪及保護被害人權益[2]。兒童及少年性剝削防制條例之立法目的則在於為防制兒童及少年遭受任何形式之性剝削[3]，保護其身心健全發展[4]，及兒童及少年福利與權益保障法之立法目的則在於為促進兒童及少年身心健全發展，保障其權益，增進其福利[5]。上述三法均對於防治性侵害或性剝削則均有所規定，因此，就性犯罪加害人之規範則必須考慮到平衡加害人權益以及被害人身心健全發展，而是否予以公告加害人之姓名等相關資訊亦應據此判斷。

目前我國對於性侵害或性剝削犯罪行為人之資訊必要時是得以公開或公告的，雖然該類資訊屬於政府資訊公開法所定義的資訊[6]，但因政府資訊公開法第 2 條[7]將其本身認定為普通法，而有其他法律時優先適用，故對於性侵害或性剝削犯罪行為人之資訊，雖其公開或提供是有侵害個人隱私之情形[8]，但在符合其他法律的規定時是得以公開的。

就現行法而言，目前有二處係針對性侵害或是性剝削加害人公告姓名等身分資訊

---

[2] 性侵害犯罪防治法第 1 條。

[3] 兒童及少年性剝削防制條例第 2 條第 1 項：「本條例所稱兒童或少年性剝削，係指下列行為之一：一、使兒童或少年為有對價之性交或猥褻行為。二、利用兒童或少年為性交、猥褻之行為，以供人觀覽。三、拍攝、製造兒童或少年為性交或猥褻行為之圖畫、照片、影片、影帶、光碟、電子訊號或其他物品。四、使兒童或少年坐檯陪酒或涉及色情之伴遊、伴唱、伴舞等行為。」

[4] 兒童及少年性剝削防制條例第 1 條。

[5] 兒童及少年福利與權益保障法第 1 條。

[6] 政府資訊公開法第 3 條「本法所稱政府資訊，指政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。」

[7] 政府資訊公開法第 2 條「政府資訊之公開，依本法之規定。但其他法律另有規定者，依其規定。」

[8] 政府資訊公開法第 18 條第 1 項第 6 款「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：...六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。」

之相關規定，分別是性侵害犯罪防治法以及兒童及少年福利與權益保障法。首先，依性侵害犯罪防治法第 23-1 條規定，有下列情形，該管警察機關得將其身分資訊登載於報紙或以其他方法公告：1.性侵害犯罪加害人經直轄市、縣（市）主管機關通知，無正當理由不到場或拒絕接受評估、身心治療或輔導教育，而屆期仍不履行； 2.性侵害犯罪加害人經直轄市、縣（市）主管機關通知，無正當理由不按時到場接受身心治療或輔導教育，而屆期仍不履行；3.性侵害犯罪加害人未依規定定期辦理登記、報到、資料異動或接受查訪或接受之時數不足，而屆期仍不履行； 4.判決有罪之性侵害犯罪加害人逃亡或藏匿經通緝者[9]。其次，就兒童及少年福利與權益保障法第 97 條規定，強迫、引誘、容留或媒介兒童及少年為猥褻行為或性交者，或是其他不正當行為者，主管機關得公布其姓名或名稱[10]。不過前開條文均僅係「得」公告，而非如已刪除之兒童及少年性剝削防制條例第 34 條[11]之「應」公告。

目前中央主管機關針對性侵害事件已建立案件資料庫管理系統[12]，並在一定情況下，基於維護公共利益及社會安全之目的供特定人員查閱[13]。而依法地方政府社會局亦得公布強迫、引誘、容留或媒介兒童及少年為猥褻行為或性交者之姓名，

[9] 性侵害犯罪防治法第 23-1 條第 1 項前段「第二十一條第二項之被告或判決有罪確定之加害人逃亡或藏匿經通緝者，該管警察機關得將其身分資訊登載於報紙或以其他方法公告之。」

[10] 兒童及少年福利與權益保障法第 97 條「違反第四十九條各款規定之一者，處新臺幣六萬元以上三十萬元以下罰鍰，並得公布其姓名或名稱。」

[11] 兒童及少年性交易防制條例（即現行法之兒童及少年性剝削防制條例）第 34 條第 1 項規定「犯第二十二條至第二十九條之罪，經判刑確定者，主管機關應公告其姓名、照片及判決要旨。」惟已於修法後刪除，其理由主為「現行「兒童及少年福利與權益保障法」第四十九條第一項第三款、第八款、第九款、第十一款、第十五款，實已概括本條例所規範之各類兒童及少年為性剝削之犯罪態樣，地方主管機關並得依同法第九十七條規定公布行為人姓名。故本條例毋庸重複規範，爰予刪除。」惟該條除公布行為人姓名外，尚包括照片，仍略有差異，至於照片不予公佈之原因在於目前刑事犯並無公告照片之規定，且實務上亦有取得照片之困難，致直轄市、縣（市）主管機關因無法取得照片而延宕公告，有失公告之時效，爰刪除應公告照片之規定。

[12] 性侵害犯罪防治法第 4 條第 1 項第 5 款「中央主管機關應辦理下列事項：...五、性侵害事件各項資料之建立、彙整、統計及管理。」

[13] 性侵害犯罪防治法第 23 條第 4 項「登記期間之事項，為維護公共利益及社會安全之目的，於登記期間得供特定人員查閱。」

目前亦已有一定成果[14]。

【管理 Tips】

政府機關蒐集資料，建立資料庫並公開涉及個人資料之政府資訊時，已構成個人資料之蒐集、處理及利用，惟行政機關基於犯罪防治之目的，建立全國性侵犯的檔案資料並在一定情況下公開，以建構全面防護網應屬合宜。因此，權衡相關法令之規定，確認所公開之資料否符合法規所要求，並衡酌犯罪防治以及當事人個人隱私保障之重要性，則為風險判斷之必要條件。

政府機關執行此類業務之過程中，本於資訊公開之原則，應保障民眾知的權利，但由於政府機關所掌握之資訊遠大於所應公開之資訊，因而需有完善的資訊管理程序與個人資料保護評估作業，僅公開法規所規定之必要資料，以達到資訊保護與資訊公開之平衡。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.18.1.4　個人可識別資訊之隱私及保護

(1) 標準內容：　應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2) 適用說明：　依性侵害犯罪防治法規定中央主管機關針對性侵害事件已建立案件資料庫管理系統，但該資料庫僅在特定情形下，基於維護公共利益及社會安全之目的供特定人員查閱，而非任何人均得隨意查詢，目的即在於確保個人可識別資訊之隱私及保護。

ISO 29100：2011（CNS29100）

[14] 台北市政府社會局違反兒少法公告，https://dosw.gov.taipei/News.aspx?n=926F2E666D71D89B&sms=F0A015F5CA923CDA（瀏覽日期：2018 年 6 月 18 日）。

● 5.5　資料極小化

(1) 標準內容：　個人可識例資料之處理及揭露，僅確保採用、"僅知(need-to-know)"原則，在合法目的下對揭露必要之資料。(摘錄)

(2) 適用說明：　對於違反兒童及少年福利與權益保障法之加害人，主管機關於公開其個人資料時時，僅得依法揭露姓名，其他如照片或住址等資訊，因已刪除兒童及少年性交易防制條例（即現行法之兒童及少年性剝削防制條例）第 34 條，故不得揭露之。

● 5.6　利用、持有及揭露限制

(1) 標準內容：　個人可識別資訊之利用及揭露，僅限於為履行特定、明確且合法目的所必要。(摘錄)

(2) 適用說明：　縱使依法政府有資訊公開之要求，個人資料之揭露仍應係符合性侵害犯罪防治法或兒童及少年福利與權益保障法所要求者方得為之。

類別：資訊公開【案號：D10715】

立院三讀通過 起訴書一審後公開

【焦點話題】

立法院於 107 年 5 月三讀通過「法院組織法第八十三條條文修正案」，未來高等法院以下各級法院及其分院地檢署，應於第一審判決後，公開起訴書。另外，立法院同時三讀通過民事訴訟法在內的多項修正案，例如過去法院公告一定要刊登於新聞報紙，修法通過後公告亦可公布於法院網站。

現行法律已規定法院應公開裁判書，「法院組織法第八十三條條文修正案」通過後，明確規定在第一審判決後，應公開起訴書，以落實司法改革國是會議有關資訊透明化的結論[1]。

【參考資料來源：自由電子報，107/5/23】

【重點摘要】

1. 裁判書全文包含當事人及訴訟關係人之身分證統一編號等個人資料，為平衡「人民知的權利」與「個人資訊隱私權」之衝突，並顧及公開技術有其極限，避免執行上窒礙難行，因此於法院組織法第 83 條立法理由要求，原則上自然人之姓名應予公開，但於公開技術可行範圍內，得限制裁判書內容中自然人之出生年月日、身分證統一編號、住居所及其他足資識別該個人之資料。
2. 為兼顧公眾利益及當事人權益，於法院組織法第 83 條第 3 項要求高等法院以下各級法院及其分院檢察署，應於第一審裁判書公開後，公開起訴書，以透過資訊之透明化達到檢視檢察官起訴品質之目的。

【法律觀點】

[1] 司法改革會議第四分組編號 4-3 議題「公開透明的司法」子題「3.起訴書全面公開，刑事判決書記載起訴檢察官姓名」，2017.04.28 第五次會議決議：「在我國未來刑事訴訟法採起訴狀一本制度之後，起訴書應於起訴公告或公布後即時上網公開；在採起訴狀一本制度之前，起訴書應於一審判決之後上網公開。但如經被告要求，或檢察官已將起訴事實提供媒體報導，或媒體已主動報導者，則應立即上網公開。」

人民有知的權利，裁判書之公開係監督司法審判之有效機制，也因此法院組織法第 83 條第 1 項規定各級法院及分院應定期出版公報或以其他適當方式，公開裁判書。因此，現行規定已有針對裁判書公開之要求，但基於人性尊嚴之維護、個人主體性之確保及人格之自由發展，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃人民為不可或缺之基本權利，而受憲法第 22 條所保障。裁判書全文包含當事人及訴訟關係人之身分證統一編號等個人資料，此屬資訊隱私權之保護範圍，為平衡「人民知的權利」與「個人資訊隱私權」之衝突，並顧及公開技術有其極限，避免執行上窒礙難行，因此規定原則上自然人之姓名應予公開，但於公開技術可行範圍內，得限制裁判書內容中自然人之出生年月日、身分證統一編號、住居所及其他足資識別該個人之資料[2]。

而原本的法院組織法僅處理法院的裁判書，也就是僅於監督司法審判之判決品質，然刑事訴訟法課以檢察官於依偵查所得證據足認被告有犯罪嫌疑時，應提起公訴之「法定性義務」，亦要求檢察官必須就於被告有利及不利之情形一律注意之「客觀性義務」。檢察官在刑事訴訟程序中所擔綱之角色，非僅僅為一造當事人，更必須居於法律守護者之角色，為刑事訴訟案件之開啟及進行把關。從而，應透過資訊之透明化，使公眾得藉由對起訴書所載犯罪事實、證據及所犯法條等事項為公開檢驗，以加強對檢察官履行法定性及客觀性義務之監督[3]。

因此，為兼顧公眾利益及當事人權益，107 年度增訂法院組織法第 83 條第 3 項[4]，要求高等法院以下各級法院及其分院檢察署，應於第一審裁判書公開後，公開起訴書，以透過資訊之透明化達到檢視檢察官起訴品質之目的，並強化社會公眾監

[2] 法院組織法第 83 條 99 年立法理由二。

[3] 法院組織法第 83 條 107 年立法理由二。

[4] 法院組織法第 83 條第 3 項:「高等法院以下各級法院及其分院檢察署，應於第一審裁判書公開後，公開起訴書，並準用前二項規定。」而之所以僅有高等法院以下各級法院及其分院檢察署於第一審裁判書公開後，方有公開起訴書之義務，其原因在於刑事訴訟法第 4 條規定「地方法院於刑事案件，有第一審管轄權。但左列案件，第一審管轄權屬於高等法院：一、內亂罪。二、外患罪。三、妨害國交罪」因此，具有第一審管轄權之法院僅有高等法院及地方法院，而最高法院並無任何犯罪之第一審管轄權，故依附於各級法院之檢察署而言，需要起訴的亦依各級第一審法院定之，亦因之法院組織法之新增條文不會出現最高法院檢察署之起訴書。

督檢察官之職權行使。

【管理 Tips】

政府資訊對外公開是必要的，但在公開資料時仍應採取妥適之管制，而非任意性全面公開，亦應衡酌其公開之目的及手段，因此政府機關執行此類業務過程中，本於資訊公開之原則，應保障民眾知的權利，但由於政府機關所掌握之資訊遠大於應公開之資訊，因而需有完善的資訊管理程序與個人資料保護評估作業，僅辦理法規所要求之必要公開資料且降低其所涉及個人隱私之部分，或採取去識別化等作業，以期達到資訊保護與公開之平衡。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.18.1.4　個人可識別資訊之隱私及保護

(1)標準內容：　應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2)適用說明：　新法上路後，檢察署於公開起訴書時，建議依法揭露姓名等必要事項，其他如得以識別特定自然人之資料則宜限制公開，以確保個人可識別資訊之隱私及保護。

ISO 29100：2011（CNS29100）

- 5.5　資料極小化

(1)標準內容：　資料極小化密切連結「蒐集限制」原則，但不僅如此，「蒐集限制」意指被蒐集之有限資料與特定目的相關連，「資料極小化」則嚴格限制將 PII 之處理極小化，堅持資料極小化原則，意指以下列方式設定及實作資料處理程序與 ICT 系統。

- 將所處理之 PII、隱私權利害相關者及 PII 揭露對象或

可存取 PII 之人員數目最小化。

- 確保採用「僅知(need-to-know)」原則，亦即於 PII 處理之合法目的框架下，宜僅對執行正式職務所必要之人員賦予 PII 存取權限。
- 使用或提供視為預設選項，只要不涉及 PII 當事人知識別的互動及交易，儘可能降低其行為之可觀察性並限制所蒐集 PII 的可連結性。
- ”一旦 PII 處理之目的終止，無法定要求保有 PII，或是實務上需如此做時，即刪除或廢棄 PII。

(2)適用說明： 檢察署於限制公開相關事項之理由即在於對起訴書所載犯罪事實、證據，及所犯法條等事項為公開檢驗，因此其他非屬於需檢驗之事項，如自然人之身份證統一編號，為顧及當事人權益，宜限制公開。

類別：資訊公開【案號：D10716】

補助社團疑黑箱作業　市府：依法網路公告

【焦點話題】

市議會進行市政總質詢，市議員提及社會局所提供之補助民間社團及區公所辦理各項活動之經費資料，其中部分資訊遭去識別化處理，市議員抨擊蓄意隱匿，迴避議會監督。社會局局長對此則表示，該等資料，涉及政府內部函稿與簽呈資料，依法不予提供；且顧及相關資料與法人之經營資訊有關，必須部分以去識別化處理，以保障法人權益，此外亦強調政府機關應依法行政，即依法應公開、可公開之資料已公告於網路，而社會局網站所公告之補助社團經費明細，已包括依規定與格式標示受補助社團名稱、金額、核准補助日期及補助事項等，為法律範圍內可完全公開之部分。

【參考資料來源：NOWnews，107/6/22】

【重點摘要】

1. 按政府資訊公開法第 18 條意旨，政府機關做成決定前之內部擬稿與個人、法人或團體營業上秘密或經營事業有關之資訊，原則限制公開，但在對公益有必要的情況下，是可以公開的，也就是就該政府資訊涉及公益程度，及其應受人民監督必要性之高低作為判斷，如所涉公益程度越高，則應受人民監督必要性亦隨之增高，此時則可能需要公開。
2. 綜政府資訊公開法第 7、18 條與最高行政法院 102 年度判字第 147 號判決理由，政府機關判斷是否應將政府資訊予以公開區可分為五個層次。第一，該資訊其是否為政府資訊；第二，是否為應主動公開之資訊；第三，是否為應限制或不予提供之資訊；第四、必要時，衡量公益與私益決定是否公開；第五、資訊分離原則，就可公開部份予以提供。

【法律觀點】

依照政府資訊公開法第 7 條規定[1]，包括支付或接受之補助等政府資訊，除有同法第 18 條限制公開或不予提供之事由外，均屬政府應主動公開之資訊，雖「補助」一詞，並未於政府資訊公開法另為立法定義，惟補助金係由政府以預算補助下級機關或人民，此涉及公共資源分配及平等原則，故列為應主動公開資訊[2]。

而政府資訊公開法第 18 條[3]對於資訊公開範圍限制，則希望以列舉限制範圍之方式，在資訊公開與資訊限制間取得平衡，兼顧國家整體利益、公務之執行及個人之隱私[4]。本案例中，社會局以作成意思決定前之機關內部資料及公開資訊將侵害法人或團體之權利，故將資料限制公開，即係援引政府資訊公開法第 18 條第 3

[1] 政府資訊公開法第 7 條：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：一、條約、對外關係文書、法律、緊急命令、中央法規標準法所定之命令、法規命令及地方自治法規。二、政府機關為協助下級機關或屬官統一解釋法令、認定事實、及行使裁量權，而訂頒之解釋性規定及裁量基準。三、政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號。四、行政指導有關文書。五、施政計畫、業務統計及研究報告。六、預算及決算書。七、請願之處理結果及訴願之決定。八、書面之公共工程及採購契約。九、支付或接受之補助。十、合議制機關之會議紀錄。　　前項第五款所稱研究報告，指由政府機關編列預算委託專家、學者進行之報告或派赴國外從事考察、進修、研究或實習人員所提出之報告。第一項第十款所稱合議制機關之會議紀錄，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單。」

[2] 法務部 98 年 8 月 26 日法律字第 0980024475 號函釋。

[3] 政府資訊公開法第 18 條：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。二、公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。四、政府機關為實施監督、管理、檢 (調) 查、取締等業務，而取得或製作監督、管理、檢 (調) 查、取締對象之相關資料，其公開或提供將對實施目的造成困難或妨害者。五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資料，其公開或提供將影響其公正效率之執行者。六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。八、為保存文化資產必須特別管理，而公開或提供有滅失或減損其價值之虞者。九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。政府資訊含有前項各款限制公開或不予提供之事項者，應僅就其他部分公開或提供之。」

[4] 政府資訊公開法第 18 條 94 年立法理由一：「資訊公開與限制公開之範圍互為消長，如不公開之範圍過於擴大，勢將失去本法制定之意義；惟公開之範圍亦不宜影響國家整體利益、公務之執行及個人之隱私等，爰於本條第一項列舉政府資訊限制公開或提供之範圍，以資明確。」

款及第 7 款之規定。

首先，依政府資訊公開法第 18 條第 1 項第 3 款規定，政府機關作成意思決定前，內部意見或與其他機關間之意見交換等政府資訊，如予公開或提供，恐礙該機關最後決策且易滋困擾，故限制公開或提供[5]，縱使已為決定後，仍應不予公開[6]。其次，同條第 1 項第 7 款規定，屬於秘密或經營事業有關之資訊時，因該等資訊公開或提供將有侵害該個人、法人或團體之權利、競爭地位或其他正當利益時，為保護當事人之權益，應限制公開或不予提供[7]。

綜上規定均有相同但書，係對於公益有必要之情形，即可得公開，換言之，該政府資訊涉及公益程度越高，其應受人民監督必要性亦隨之增高。本案例中，政府機關認為受要求公開之資訊，其部份涉及政府內部文件而不予提供，他部份則涉有法人之經營資訊，依政府資訊公開法第 18 條第 2 項之資訊分離原則，僅就可公開部份提供。如此判斷檔案之資訊所涉事項、資訊之時間性，衡量申請人閱覽之公益，及政府機關所主張之有礙該機關之最後決定之作成、易茲生後遺症、經營事業有關之資訊、工商秘密等要件後，若將之公開造成之損害大於公共利益時，即可依規定限制公開[8]。

【管理 Tips】

政府資訊公開之目的，係以建立政府資訊公開之制度，便利人民共享及公平利用

---

[5] 政府資訊公開法第 18 條 94 年立法理由四：「政府機關之內部意見或與其他機關間之意見交換等政府資訊，如予公開或提供，因有礙該機關最後決定之作成且易滋困擾，例如對有不同意見之人加以攻訐，自應限制公開或不予提供，惟對公益有必要者，自不在限制範圍之列，以求平衡，爰為第一項第三款之規定。」

[6] 最高行政法院 101 年度判字第 171 號判決：「惟查依政府資訊公開法第 18 條第 1 項第 3 款規定，政府機關作成意思決定前，內部單位之擬稿或準備作業，除係意思決定作成之基礎事實外，應限制公開或提供，其立法目的在於此等機關內部意見或與其他機關間之意見交換等政府資訊，如予公開或提供，因有礙該機關之最後決定之作成及易茲生後遺症，例如對有不同意見之人加以攻訐，自應限制公開或提供。準此，因該類資訊係政府機關作成意思決定前之擬稿或準備作業，於政府機關作成意思決定後，仍有上開規定之適用。」

[7] 政府資訊公開法第 18 條 94 年立法理由八：「個人、法人或團體營業上秘密或其經營事業有關之資訊，該等資訊之公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益時，為保護當事人之權益，該等政府資訊亦應限制公開或不予提供；惟如對公益有必要或為保護人民生命、身體、健康有必要者，自不在限制範圍，爰為第一項第七款之規定。」

[8] 最高行政法院 102 年度判字第 147 號判決。

政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督[9]，因此，對於政府資訊屬於應主動公開或應人民申請而公開之資訊，以及政府資訊屬於應限制公開或不予提供之資訊，政府機關應有所瞭解，並知悉其理由，以確保其公開或不公開均符合法律規定，機關應盤點其所持有之政府資訊，依是否為政府資訊公開法規定需予以公開之政府資訊加以列冊管考。

就此，政府機關依法可將政府資訊是否得以公開區分五個層次。第一點：確保其是否為政府資訊；第二點：是否為應主動公開之資訊；第三點：是否為應限制或不予提供之資訊；第四點：必要時，衡量公益與私益決定是否公開；第五點：資訊分離原則，就可公開部份予以提供。

【相關標準】

ISO27001：2013（CNS27001）

- A.8.1.1　資產清冊

(1)標準內容：　應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。

(2)適用說明：　組織為釐清其持有之資產，以及對於該等資產進行妥適之分類、分級等管理措施，對於其所持有之資產應予以分類並製表列冊，以供需要時得以快速檢驗。本案政府機關對於其所管之資訊，平時即應妥適進行盤點並列冊管考，其中屬限制公開或不予提供者加註理由，使政府人員知悉。

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容：　對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為

[9] 政府資訊公開法第 1 條：「為建立政府資訊公開制度，便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與，特制定本法。」

符合此等要求之作法。

(2)適用說明： 組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。本案之政府機關即屬熟悉政府資訊公開法對於是否為應限制或不予提供之政府資訊有所瞭解，但如對於限制公開與公益間之衡平有更進一步闡述，將更為恰當。

類別：資訊公開【案號：D10717】

行政機關通過「政治檔案條例」草案　政黨、附隨組織所持檔案將歸國有

【焦點話題】

行政院於 107 年 5 月通過配套促進轉型正義條例之政治檔案條例草案，未來除政黨、其附隨組織及黨營機構所保管的政治檔案將收歸國有外，包括 228 事件、動員戡亂體制、戒嚴體制相關檔案或各類紀錄文件將解密公開。「政治檔案條例」草案送請立法院審議後，將請權責機關積極與立法院朝野各黨團溝通協調，早日完成立法程序。另請各部會配置適當資源，督促所屬機關(構)落實政治檔案之清查及整理，以利儘速移轉國家發展委員會檔案局管理。

【參考資料來源：台灣好新聞，107/5/17】

【重點摘要】

1. 按政治檔案條例草案第 8 條規定，得申請或調閱政治檔案者包括檔案當事人、非檔案當事人、政府機關等。其中就檔案當事人或其繼承人而言，其本人所涉案件，除特殊狀況外，均得全部閱覽、抄錄及複製；次按，政治檔案條例草案第 9 條規定，非檔案當事人原則需採分離原則，將檔案內容抽離或遮掩處理後，方提供閱覽、抄錄或複製。再按，政治檔案條例草案第 10 條規定而政府機關辦理檔案借調時，除借調機密檔案，應先經原移轉機關同意外，原則係全部提供。

2. 按政治檔案條例草案第 11 條規定，政治檔案中所載公務員、證人、檢舉人及消息來源的姓名、化名、代號及職稱，應該提供閱覽、抄錄或複製，藉由資訊公開，以落實轉型正義，還原歷史真相。

【法律觀點】

政治檔案條例草案第 1 條開宗明義說明，其目的係為辦理政治檔案之徵集、整理、

保存、開放應用、研究及教育[1]。而政治檔案[2]則指：動員戡亂、戒嚴體制下涉及之政治事件、財產變動或司法平復等各類檔案及紀錄文件。經促進轉型正義委員會審定為政治檔案時，無論原持有檔案者為政黨、其附隨組織或黨營機構，均應於指定期限內移歸檔案局管理[3]，惟政黨以外之私人與團體所持有之政治檔案，不強制徵集，而以捐贈、收購或受託保管等方式納為國家檔案典藏[4]。

而依該草案第 7 條之規定，所有保密逾 30 年的政治檔案，除適用國家機密保護法第 24 條永久保密等法規[5]外，皆應視為解除機密。而可申請或調閱政治檔案者，包括檔案當事人、非檔案當事人之個人或團體及政府機關，就檔案當事人或其繼承人而言，其本人所涉案件，不論檔案是否屆滿 30 年，除有依法核定為機密檔案、經移轉機關表示嚴重影響國家安全、利益、對外關係之推動或經其他檔案當事人或其繼承人表示不予公開之私人文書外，全部均得閱覽、抄錄及複製[6]。但非檔案當事人則受有限制，原則需將涉及同草案第 8 條第 2 項與第 3 項規定，提供申請人於指定場所閱覽、抄錄，俟複製時，檔案內容抽離或遮掩處理後提供閱覽、抄錄或複製[7]。而政府機關借調時則規定除經移轉機關表示借調恐影響國家

---

[1] 政治檔案條例草案第 1 條：「為辦理政治檔案之徵集、整理、保存、開放應用、研究及教育，特制定本條例」

[2] 政治檔案條例草案第 1 條第 1 款：「政治檔案：指由政府機關（構）、政黨、附隨組織及黨營機構所保管，自中華民國三十四年八月十五日起至八十一年十一月六日止，與二二八事件、動員戡亂體制、戒嚴體制相關之檔案或各類紀錄文件；其包括已裁撤機關（構）之檔案。」

[3] 政治檔案條例草案第 6 條第 1 項：「政黨、附隨組織及黨營機構持有政治檔案，經促進轉型正義委員會審定為國家檔案者，應於該會指定期限內移歸檔案局管理，並由該會、檔案局及持有檔案之政黨、附隨組織及黨營機構依審定清冊作成紀錄。」

[4] 政治檔案條例草案第 3 條立法理由一後段：「至政黨以外之私人團體所持有之政治檔案，基於尊重人民財產權，不強制徵集，而依現行『私人或團體捐贈珍貴文書獎勵辦法』、『國家發展委員會檔案管理局受託保管及收購私人或團體珍貴文書要點』以捐贈、收購或受託保管等方式納為國家檔案典藏。」

[5] 政治檔案條例草案第 7 條第 2 項：「政治檔案於保密期限屆滿或解密條件成就時，自動解除機密；保密逾三十年仍列機密等級者，除原移轉機關敘明有保密義務之法規外，視為解除機密。」

[6] 政治檔案條例草案第 8 條第 2 項：「依前項規定申請之政治檔案，除有下列情形之一外，檔案局應於指定場所提供閱覽、抄錄或複製：一、經依法核定為機密檔案。　二、經移轉機關（構）表示有嚴重影響國家安全、利益或對外關係推動之虞。　三、經其他檔案當事人或其繼承人表示不予公開之私人文書。」

[7] 政治檔案條例草案第 9 條第 1 項：「非檔案當事人申請閱覽、抄錄或複製政治檔案，依下列方式提供：一、屆滿三十年之政治檔案，依前條第二項及第三項規定辦理。　二、未屆滿三十年之政治檔案，依前條第二項規定辦理；有前條第三項涉及個人隱私者，應經該個人同意，始得於指定場所提供閱覽、抄錄或複製。」

安全、利益或對外關係之推動、經檔案當事人或其繼承人表示不予公開之私人文書外，原則全部提供；借調機密檔案者，應先經原移轉機關同意[8]。

該草案亦明文政治檔案中所載公務員、證人、檢舉人及消息來源的姓名、化名、代號及職稱，應提供閱覽、抄錄或複製，藉由資訊公開，以落實轉型正義，還原歷史真相[9]。當然，因申請或借調政治檔案所知悉之檔案內容，應依相關法律保護規定使用之，包括個人資料保護法、著作權法或其他相關法規均應遵守[10]。

檔案是保存歷史真實紀錄之重要資料，不僅是政府資訊，亦是國家資產與社會公器，希冀政治檔案條例通過後，得於資訊公開、知的權利、資訊保護及公平正義間取得平衡，以面對歷史真相。

【管理 Tips】

政治檔案之保全與開放應用是政府重要政策，亟需藉由完整之管理與應用制度，以妥善辦理其保存與開放，而透過特定資訊的分級與限制瀏覽，則可避免將非必要資訊外流，並採取分離處理，以降低若不慎於檔案傳遞時發生個資外洩之損害及風險。

考量資訊管理之需求，組織亦應制定存取控制政策，透過權限分級設定，限制及管理不同等級帳號對於資訊及應用系統之存取權，並將機敏性資料予以分級控管，以避免發生無權限者進行資料存取，以及透過資料本身之遮蔽與隱藏，以及限制系統輸出之資訊內容，使存取者無法一窺資料全貌，此時縱有無權限者以其他方式取得資料，亦可降低其取得之資料效用。

【相關標準】

ISO27001：2013（CNS27001）

[8] 政治檔案條例草案第 10 條第 1 項。

[9] 政治檔案條例草案第 11 條：「政治檔案中所載公務員、證人、檢舉人及消息來源之姓名、化名、代號及職稱，應提供閱覽、抄錄或複製。」

[10] 政治檔案條例草案第 15 條：「因申請或借調政治檔案所知悉之檔案內容，應依相關法律保護規定使用之。違反前項規定者，依有關法律處罰。」

- A.9.1.1 存取控制政策

(1)標準內容： 存取控制政策應依據業務與資訊安全的要求來建立、文件化及覆核。

(2)適用說明： 組織應明確定訂定存取控制政策，視需要針對不同業務內容建立不同等級的存取控制政策以加以控管，藉以規範組織內部可以觸及到機敏資料的人員，控制個別使用者的存取權限，避免無權限者存取。

- A.18.1.4 個人可識別資訊之隱私及保護

(1)標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2)適用說明： 組織應辨識出個人資料以及相關法定要求，以確保個人可是別資訊之隱私及保護，以政治檔案條例草案為例，雖政治檔案中所載公務員、證人、檢舉人及消息來源的姓名、化名、代號及職稱，應該提供閱覽、抄錄或複製，但足資辨識個人隱私資料，如身分證字號、縣市以下地址等，仍應於分離後方提供複製。

類別：資訊公開【案號：D10718】

機關審議討論過程原則可錄音錄影

【焦點話題】

環境保護機關所舉辦之環境影響評估會議時常成為民眾參與的重點，不僅開放錄音、錄影，並於 106 年 8 月起更進一步啟動線上直播。然而，當時之內政機關於資訊公開之態度卻與之不同。以致中科汙染搜查線、地球公民基金會、草山生態文史聯盟等全台超過 50 個公民團體共同發起記者會，重批內政機關對於公民參與國土利用相關審議委員會有諸多限制，且拒絕民眾錄音、錄影，故而要求內政機關應修改相關規定。對此，內政主管機關已於 106 年 8 月 24 日發布實施國土空間計畫審議會議及會場管理要點，原則上審議會議的公開討論過程皆可錄音錄影，僅有委員內部討論時，民眾、相關代表及記者皆須要離席。

【參考資料來源：環境資訊中心，106/7/21】

【重點摘要】

1. 民眾於審查會議公開討論過程中自行錄音錄影，其所製成之資訊，因非屬於政府機關於職權範圍所作成的資訊，故非政府資訊；而由政府錄音錄影時，雖屬政府資訊，但因審議小組會議屬於機關內部為審議及研究為審議個別案件而設置之任務編組，非為機關組織型態者，因此其所作成之政府資訊並不屬於合議制機關之會議紀錄，而無必要公開。

2. 依政府資訊公開法第 5 條規定，政府資訊應依本法主動公開或應人民申請提供之，及同法第 6 條規定，與人民權益攸關之施政、措施及其他有關之政府資訊，以主動公開為原則，並應適時為之。因此，相關會議紀錄雖非「應」主動公開項目，然而，如無第 18 條第 1 項規定各款應限制公開或不予提供之事由者，仍得主動或應人民申請提供之。

【法律觀點】

為為貫徹政府資訊公開制度、便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與[1]，因此，政府資訊，應以主動公開為原則[2]，僅有例外情形下方得限制公開。

政府資訊係指政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息[3]。依政府資訊公開法第 7 條規定，包括合議制機關之會議紀錄等政府資訊，除有同法第 18 條限制公開或不予提供之事由外，均屬政府應主動公開之資訊[4]，其中，合議制機關係指該機關決策階層由權限平等並依法獨立行使職權之成員組成者（如公平交易委員會）[5]，而合議制機關之會議紀錄則指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單[6]。

本案中，於審查小組會議公開討論過程中進行錄音錄影，可分成由民眾錄音錄影或政府錄音錄影，由民眾錄音錄影者，因非屬於政府機關於職權範圍所作成的資訊，故非政府資訊；而由政府錄音錄影者，依法雖屬於政府資訊，惟依法務部法律字第 0090047712 號函意旨，因其所召開的審議小組會議雖是合議制[7]，但屬

---

[1] 政府資訊公開法第 1 條。

[2] 政府資訊公開法第 6 條：「與人民權益攸關之施政、措施及其他有關之政府資訊，以主動公開為原則，並應適時為之。」

[3] 政府資訊公開法第 3 條。

[4] 政府資訊公開法第 7 條第 1 項第 10 款：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：...十、合議制機關之會議紀錄。」

[5] 法務部 100 年 12 月 06 日法律字第 1000029002 號說明二：「二、按政府資訊公開法（以下簡稱本法）第 7 條第 1 項規定：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：...三、政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號。...十、合議制機關之會議紀錄。」又同法第 7 條第 3 項規定：「第 1 項第 10 款所稱合議制機關之會議紀錄，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單。」所稱「合議制機關」，指該機關決策階層由權限平等並依法獨立行使職權之成員組成者（如行政院公平交易委員會）。」

[6] 政府資訊公開法第 7 條第 2 項：「第一項第十款所稱合議制機關之會議紀錄，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單。」

[7] 內政部土地徵收審議小組設置要點第 6 點第 1 項：「本小組需有過半數委員之出席，始得開會，並有出席委員

於機關內部為審議及研究案件而設置之任務編組，非為機關組織型態者，因此其所作成之政府資訊並不屬於合議制機關之會議紀錄[8]，而無必要公開。

考量人民知的權利之保障，主管機關除已將相關會議紀錄公開供民眾查詢外[9]，更已 106 年修訂相關會議及會場管理要點[10]，允許出列席人員若於會議中有有攝影、錄影或錄音之需求時，於簽到時告知會議工作人員後，可在非委員討論階段之議程中進行之[11]，嗣後如有相類似需求，出列席人員即可依相關規定進行攝影、錄影或錄音，藉以強化一般民眾對公共事務之瞭解、信賴及進行監督。

【管理 Tips】

政府資訊公開之目的，在於增進一般民眾對公共事務之瞭解、信賴及監督，故機關應確實知悉政府資訊公開法所規範之政府資訊，應於何種情形主動公開或經人民申請而提供，以及限制公開或不予提供者。

政府機關為確保其資訊公開或不公開均符合法律規定，並應建立完善之資料盤點流程，分類盤點出機關所持有之政府資訊，確認公開與非公開之項目，避免失誤之發生。

過半數之同意始得決議；可否同數時，由主席裁決。」

[8] 法務部 91 年 01 月 10 日法律字第 0090047712 號：「按依行政程序法第四十五條第一項第八款規定，行政機關持有或保管之合議制機關之會議紀錄，應主動公開。其所稱「合議制機關之會議紀錄」，指該機關決策階層由權限平等並依法獨立行使職權之成員組成者(如行政院公平交易委員會)，其所審議議案之案由、決議內容及出席會議成員名單(行政資訊公開辦法第四條第五項參照)。至都市計畫委員會對於審議或討論之案件雖屬合議制(各級都市計畫委員會組織規程第九條規定參照)，但屬機關內部為審議及研究都市計畫而設置之任務編組，因非為機關組織型態者，並不屬之。故主旨所揭資料，尚無首揭行政程序法第四十五條第一項第八款規定之適用。」

[9] 主管機關目前係將相關會議紀錄均有公開，係依政府資訊公開法第 5 條：「政府資訊應依本法主動公開或應人民申請提供之。」、第 6 條：「與人民權益攸關之施政、措施及其他有關之政府資訊，以主動公開為原則，並應適時為之。」因此，會議紀錄雖非「應」主動公開項目，然如無第 18 條第 1 項各款應限制公開或不予提供之事由者，仍得主動或應人民申請提供之。

[10] 內政部 106 年 9 月 14 日台內地字第 1061305502 號函。

[11] 內政部土地徵收審議小組會議及會場管理要點第 4 點第 2 項：「出列席人員於會議進行中有攝影、錄影或錄音之需求，應於簽到時告知會議工作人員，且以委員討論前之議程為限。其中攝影、錄影應於會場指定區域進行，並不得妨礙與會人員之發言或會議流程。」

政府機關執行與人民涉有重大關係之審查會議時，本於資訊公開之原則，應保障民眾知的權利，但為避免影響機關決定之作成，或是可能侵害個人隱私情形之發生時，仍應對公開之資訊加以限制，而僅公開必要之資訊，以期符合資訊公開之意義。

【相關標準】

ISO27001：2013（CNS27001）

- A.8.1.1　資產清冊

(1)標準內容：　應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。

(2)適用說明：　組織為釐清其持有之資產，以及對於該等資產進行妥適之分類、分級等管理措施，對於其所持有之資產應予以分類並製表列冊，以供需要時得以快速檢驗。本案政府機關對於其所管之資訊，平時即應妥適進行盤點並列冊管考，並對其中屬限制公開或不予提供者，加註說明。

- A.18.1.1　適用之法規及契約的要求事項之識別

(1)標準內容：　對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明：　組織在業務開發時應瞭解並依循其應適用之法令，以避免觸法。以本案例而言，政府機關在資訊公開前，必須瞭解所掌握的資訊為何，是否得以公開，以避免在無法源依據下公開不得公開之政府資訊。

類別：資訊公開【案號：D10719】

空污法新制上路

【焦點話題】

眾所矚目的空氣污染防制法（下稱空污法）修正案，於 107 年 6 月 25 日完成三讀程序，並在同年 8 月 1 日經總統令公布，使我國空氣污染防制工作，邁向新里程。空污法自民國 64 年公布施行迄今，期間歷經 8 次修正，逐步建構我國空氣污染管制制度。然而，最近一次大幅修正是在 91 年間，至今也已逾 16 年，現行的條文已不符時代需求及民眾期待，因此予以檢討修正。主管機關表示，此次修法其中有 5 大亮點，包括：增訂好鄰居條款、工廠源頭管制機制、增加移動污染管制措施、提高罰則，以及追繳不法利得與吹哨者條款，要求工廠公開污染排放等相關資訊，以供全民監督，並從空氣品質改善規劃、污染源的源頭管制與中間管理，至管末處理及應變，全面予以補強。

【參考資料來源：行政院環境保護署，107/6/26、總統府公報，107/8/1】

【重點摘要】

1. 空氣污染防制法第 24 條規定，如公私場所具有經中央主管機關指定公告之固定污染源，應於設置或變更前，檢具空氣污染防制計畫，向主管機關委託之機關申請及取得設置許可證，並依許可證內容進行設置或變更，主管機關在許可證核發前，應將申請資料登載於公開網站，供民眾查詢並表示意見，作為核發許可證之參考。

2. 空氣污染防制法第 98 條規定，公私場所遭令停止污染源之操作、停工或經主管機關令改善而自報停工者時，應於恢復污染源操作或復工前，檢具試車(於正式營運前，先行試用)計畫，向主管機關申請試車，該試車計畫亦應刊載於主管機關所指定之公開網站，供民眾查詢，以利利害關係人及公益團體表示意見。

【法律觀點】

空污法第 1 條開宗明義表示其立法目的係為防制空氣污染，維護生活環境及國民

健康，以提高生活品質。然而，近年來空氣污染議題逐漸受到重視，現行空氣污染防制法主要定訂於民國 91 年間，距今十年有餘，更因社經環境變遷、污染管制需求不同，已然不符合時代需求，權責機關進而對此進行大幅調修。

然而，對於法規之修訂，民眾不免有其疑慮，故主管機關亦召開相關說明會[12]。而此次修訂重點包括：增訂好鄰居條款[13]；增訂工廠源頭與管末雙重管制機制[14]；增訂好社區條款[15]；加重罰則[16]；增訂不法利得追繳及吹哨者條款[17]等。

---

[12] 空污法修法說明會各場次議程表：https://www.google.com/url?q=https://www.epa.gov.tw/DO/DownloadController.Attach.asp%3Fxpath%3Dpublic/Attachment/8810128539.docx&sa=U&ved=0ahUKEwiSm4-jqJ7dAhUCerwKHdwBCo4QFggJMAI&client=internal-uds-cse&cx=013428823787310676217:rraz5xrilpk&usg=AOvVaw0Tz9pM9gvS1E2-zhQ1yzxi （本共四場，惟因中南部遭受豪雨襲擊成災，故暫取消其中三場）

[13] 空氣污染防制法第 7 條：「中央主管機關應訂定空氣污染防制方案，並應每四年檢討修正。　　直轄市、縣（市）主管機關應依前條規定及前項方案擬訂空氣污染防制計畫，報中央主管機關核定後公告之，並應每四年檢討修正。　　前項空氣污染防制計畫之擬訂，直轄市、縣（市）主管機關應考量空氣污染物流通性質，會商鄰近直轄市、縣（市）主管機關定之。」；第 33 條第 3 項：「公私場所應擬訂空氣污染突發事故緊急應變措施計畫，並定期檢討，報經直轄市、縣（市）主管機關核定後切實執行。」

[14] 空氣污染防制法第 20 條第 3 項：「第一項排放標準應含有害空氣污染物，其排放標準值應依健康風險評估結果及防制技術可行性訂定之。」；第 28 條第 1 項：「公私場所固定污染源所使用之燃料及輔助燃料，含生煤或其他中央主管機關指定公告者，應符合中央主管機關所定燃料種類混燒比例及成分之標準，並申請及取得直轄市、縣（市）主管機關核發之使用許可證，始得為之；其使用情形，應作成紀錄，並依規定向直轄市、縣（市）主管機關申報。」；第 6 條第 3 項：「三級防制區內，既存之固定污染源應削減污染物排放量；新設或變更之固定污染源污染物排放量達一定規模者，應採用最佳可行控制技術，其屬特定大型污染源者，應採用最低可達成排放率控制技術，且新設或變更之固定污染源污染物排放量應經模式模擬證明不超過污染源所在地之防制區及空氣品質同受影響之鄰近防制區污染物容許增量限值。」

[15] 空氣污染防制法第 40 條：「各級主管機關得視空氣品質需求及污染特性，因地制宜劃設空氣品質維護區，實施移動污染源管制措施。　　前項移動污染源管制得包括下列措施：一、禁止或限制特定汽車進入。　二、禁止或限制移動污染源所使用之燃料、動力型式、操作條件、運行狀況及進入。　三、其他可改善空氣品質之管制措施。　　第一項移動污染源管制措施由直轄市、縣(市)主管機關擬訂，報中央主管機關核定後公告之。」；第 3 條第 2 款：「污染源：指排放空氣污染物之物理或化學操作單元，其類別如下：(一)移動污染源：指因本身動力而改變位置之污染源。　(二)固定污染源：指移動污染源以外之污染源。」；第 36 條第 2 項：「前項排放標準，由中央主管機關會商有關機關定之；並得視空氣品質需求，加嚴出廠十年以上交通工具原適用之排放標準。」；第 80 條第 3 項：「逾應檢驗日起六個月仍未實施定期檢驗、未依規定申請複驗或複驗仍不合格者，經直轄市、縣（市）主管機關通知限期改善，屆期未完成改善者，處新臺幣三千元以上六萬元以下罰鍰；經直轄市、縣（市）主管機關再通知限期改善，屆期仍未完成改善者，得移請公路監理機關註銷其牌照。」

[16] 空氣污染防制法第 51 條：「違反第三十三條第一項未立即採取緊急應變措施或不遵行直轄市、縣（市）主管

然而，為求落實資訊公開，此次修正參酌司法改革國是會議[18]之建議[19]，一體適用至其他政府公部門，並從管制面加以著手，將公私場所固定污染源之相關資訊予以公開，就固定污染源之設置而言，如公私場所具有經中央主管機關指定公告之固定污染源，應於設置或變更前，檢具空氣污染防制計畫，向主管機關委託之機關申請及取得設置許可證，並依許可證內容進行設置或變更，主管機關在許可證核發前，應將申請資料登載於公開網站，供民眾查詢並表示意見，作為核發許可證之參考[20]。

而於本法修正內容生效前已設置具有固定污染源者，應於規定期限內完成設置自動監測設施，連續監測其操作或空氣污染物排放狀況，並向主管機關申請認可；其經指定公告應連線者，其監測設施應於規定期限內完成與主管機關連線，並公

機關依第三十三條第二項所為之命令，因而致人於死者，處無期徒刑或七年以上有期徒刑，得併科新臺幣三千萬元以下罰金；致重傷者，處三年以上十年以下有期徒刑，得併科新臺幣二千五百萬元以下罰金；致危害人體健康導致疾病者，處六月以上五年以下有期徒刑，得併科新臺幣二千萬元以下罰金。」

[17] 空氣污染防制法第 86 條：「違反本法義務行為而有所得利益者，除應依本法規定裁處一定金額之罰鍰外，並得於所得利益之範圍內，予以追繳。　為他人利益而實施行為，致使他人違反本法上義務應受處罰者，該行為人因其行為受有財產上利益而未受處罰時，得於其所受財產上利益價值範圍內，予以追繳。　行為人違反本法上義務應受處罰，他人因該行為受有財產上利益而未受處罰時，得於其所受財產上利益價值範圍內，予以追繳。　前三項追繳，由為裁處之各級主管機關以行政處分為之；所稱利益得包括積極利益及應支出而未支出或減少支出之消極利益，其核算及推估辦法，由中央主管機關定之。」；第 94 條：「人民或團體得敘明事實或檢具證據資料，向直轄市、縣（市）主管機關檢舉公私場所違反本法規定之行為，或使用中汽車排放空氣污染物情形。　前項檢舉及獎勵之辦法，由直轄市、縣（市）主管機關定之。　被檢舉對象屬公私場所，且經查證檢舉屬實並處以罰鍰者，其罰鍰金額達一定數額時，得以實收罰鍰總金額收入之一定比例，提充獎金獎勵檢舉人。　直轄市、縣（市）主管機關對於第一項檢舉人之身分應予保密。」

[18] 司改國是會議第四分組決議：參與、透明、親近的司法，4-3.公開透明的司法。

[19] 空氣污染防制法修正草案總說明三。

[20] 空氣污染防制法第 24 條：「公私場所具有經中央主管機關指定公告之固定污染源，應於設置或變更前，檢具空氣污染防制計畫，向直轄市、縣（市）主管機關或中央主管機關委託之機關申請及取得設置許可證，並依許可證內容進行設置或變更。　前項固定污染源設置或變更後，應檢具符合本法相關規定之證明文件，向直轄市、縣(市)主管機關或經中央主管機關委託之機關申請及取得操作許可證，並依核發之許可證內容進行操作。直轄市、縣（市）主管機關或經中央主管機關委託之機關，應於前二項許可證核發前，將申請資料登載於公開網站，供民眾查詢並表示意見，作為核發許可證之參考。　固定污染源設置與操作許可證之申請、審查程序、審查原則、公開內容、核發、撤銷、廢止、中央主管機關委託或終止委託及其他應遵行事項之辦法，由中央主管機關定之。」

開於主管機關網站[21]，且公私場所應將含空氣污染防制計畫及空氣污染防制設施說明書、燃料使用許可證及依本法申報之資料、與環境工程技師、空氣污染防制專責人員及環境檢驗測定機構之證號資料，以及突發事故緊急應變措施計畫之固定污染源設置與操作許可證，公開於中央主管機關指定之網站，而主管機關亦得在指定網站公開公私場所、環境工程技師、空氣污染防制專責人員、環境檢驗測定機構查核、處分之個別及統計資訊[22]。

而當污染源未經合法登記、許可，或其情節重大之情形時，主管機關應公開情節重大之公私場所，停止並追回一切優惠措施[23]。且如公私場所遭令停止污染源之操作、停工或經主管機關令改善而自行報請停工者時，應於恢復污染源操作或復工前，檢具試車計畫，向主管機關申請試車[24]，該試車計畫亦應刊載於主管機關

---

[21] 空氣污染防制法第 22 條第 1 項：「公私場所具有經中央主管機關指定公告之固定污染源者，應於規定期限內完成設置自動監測設施，連續監測其操作或空氣污染物排放狀況，並向直轄市、縣（市）主管機關申請認可；其經指定公告應連線者，其監測設施應於規定期限內完成與直轄市、縣(市)主管機關連線，並公開於直轄市、縣（市）主管機關網站。」

[22] 空氣污染防制法第 35 條：「公私場所應將直轄市、縣（市）主管機關核發之固定污染源設置與操作許可證，其應含空氣污染防制計畫及空氣污染防制設施說明書;燃料使用許可證及依本法申報之資料,與環境工程技師、空氣污染防制專責人員及環境檢驗測定機構之證號資料，以及突發事故緊急應變措施計畫，公開於中央主管機關指定之網站。但涉及國防機密或經公私場所向直轄市、縣(市)主管機關申請核准之工商機密者，不在此限。各級主管機關得於中央主管機關指定之網站，公開公私場所、環境工程技師、空氣污染防制專責人員、環境檢驗測定機構查核、處分之個別及統計資訊。　　前二項資訊公開方式及工商機密審查之辦法，由中央主管機關定之。」。

[23] 空氣污染防制法第 96 條：「第三十條第一項第一款、第五十九條、第六十一條、第六十二條第一項、第六十四條、第六十五條第一項、第六十七條第二項及第六十八條所稱之情節重大，指有下列情形之一者： 一、未經合法登記或許可之污染源，違反本法之規定。 二、經處分後，自報停工改善，經查證非屬實。 三、一年內經二次限期改善，仍繼續違反本法規定。 四、大量排放空氣污染物，嚴重影響附近地區空氣品質。 五、排放之空氣污染物中含有害空氣污染物質，有危害公眾健康之虞。 六、以未經固定污染源操作許可證核定之排放管道排放空氣污染物,或調整廢氣排放流向,致空氣污染物未經許可證核定之收集或處理設施排放。 七、其他嚴重影響附近地區空氣品質之行為。　　各級主管機關應公開依前項規定認定情節重大之公私場所，由提供優惠待遇之目的事業主管機關或各該法律之主管機關停止並追回其違規行為所屬年度之優惠待遇,並於其後三年內不得享受政府之優惠待遇。　　前項所稱優惠待遇，包含中央或地方政府依法律或行政行為所給予該事業獎勵、補助、捐助或減免之租稅、租金、費用或其他一切優惠措施。」

[24] 空氣污染防制法第 97 條：「公私場所經直轄市、縣（市）主管機關依第五十九條、第六十一條、第六十二條第一項、第六十四條、第六十五條第一項、第六十七條第二項或第六十八條令停止污染源之操作、停工（業）或經直轄市、縣（市）主管機關令改善而自報停工（業）者，應於恢復污染源操作或復工（業）前，檢具試車

所指定之公開網站[25]，供民眾查詢，使利害關係人及公益團體得以表示意見。亦即自污染源設置申請開始、使用期間監督、到停工後復工階段，本法修正後，均要求透過資訊公開，使人民得瞭解運作情形，以避免資訊不透明。且為使人民能更瞭解周遭環境情形以及政府作為，本次修法亦要求政府將石化工業區[26]及特殊性工業區[27]所在地區之空氣品質監控原始資料及空氣污染防制費實際支用情形公開[28]。且政府負有輔導污染源改善之義務，輔導成果應每年公開於指定網站，並定期檢討[29]。

空氣污染防制帶入了資訊公開，使民眾瞭解所身處地區環境資訊是本法大幅翻新中的一點，也期許將來相關子法修正後，能確實落實空污法的精神，以維護人民知的權利。

【管理 Tips】

隨著社會的進步，民眾需要透過不斷獲取新知，因應時代變遷。然而，居住環境優劣亦是民眾於生活中所重視之課題之一，從而透過法律規定將民眾周邊環境資訊揭露，使民眾得清楚了解其居住環境品質。

計畫，向直轄市、縣（市）主管機關申請試車，經直轄市、縣（市）主管機關核准後，始得進行試車；並於試車期限屆滿前，檢具符合排放標準之證明文件，報經直轄市、縣（市）主管機關評鑑合格後，始得恢復操作或復工（業）。　　前項試車、評鑑及管理事項之辦法，由中央主管機關定之。」

[25] 空氣污染防制法第 98 條：「公私場所應將依前條第一項所提出之試車計畫，登載於中央主管機關所指定之公開網站，供民眾查詢。　　直轄市、縣（市）主管機關為前條第一項核准前，應給予利害關係人及公益團體表示意見，作為直轄市、縣（市）主管機關核准之參考；以會議方式審查者，於會議後應作成會議紀錄，並公開登載於中央主管機關指定之網站。」

[26] 空氣污染防制法第 13 條：「中央主管機關應於石化工業區所在之鄉鎮市區、各級主管機關應選定適當地點，設置空氣品質監測站，定期公布空氣品質狀況及其原始資料。　　前項空氣品質監測站設置及監測之準則，由中央主管機關定之。」

[27] 空氣污染防制法第 15 條：「特殊性工業區開發者，應於區界內之四周規劃設置緩衝地帶及適當地區設置空氣品質監測設施。　　前項特殊性工業區之類別、緩衝地帶、空氣品質監測狀況記錄、申報、監測設施設置規範、記錄及申報之標準，由中央主管機關定之。　　中央主管機關應定期公布前項申報狀況及其原始資料。」

[28] 空氣污染防制法第 18 條第 4 項：「第一項空氣污染防制費支用項目實際支用情形，應公開於中央主管機關指定之網站。」

[29] 空氣污染防制法第 50 條：「各種污染源之改善，由各目的事業主管機關輔導之，相關輔導成果，應每年公開於中央主管機關指定之網站，並定期檢討之。」

而空污法針對污染源管制之資訊公開,係自污染源設置申請時起、使用期間監督、證明提供、到停工後復工階段，均一併考量，亦如同組織在進行風險管控時，應以整體運作流程為考量，且對各式風險類別進行掌握，以強化組織之應變能力並於風險發生時得以降低損失。

【相關標準】

ISO27001：2013（CNS27001）

- A.6.1.3 與權責機關之聯繫

  (1)標準內容： 應維持與相關權責機關之適切聯繫。

  (2)適用說明： 空污法於本次修訂後，對於具有固定污染源之公私場所賦予一定程度的資訊公開義務，而該資訊公開均需與主管機關配合方得執行，如公私場所向主管機關委託之機關申請及取得設置許可證，主管機關在許可證核發前，應將申請資料登載於公開網站，即屬需與權責機關相互配合，方得完成法律義務之情形，因此必須維持與相關權責機關之適切聯繫。

- A.18.1.1 適用之法規及契約的要求事項之識別

  (1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

  (2)適用說明： 組織應瞭解並依循其應適用之法令，進行相關業務之執行,以避免觸法。新法修訂後,常是各組織遵法的陣痛期,但也是所必須的，而公私場所具有固定污染源者，於本次修法後的資訊公開義務相形加重，各公私場所待子法修訂後，亦應配合執行。

參、資訊監察(Monitors)

類別：資訊監察【案號：M10720】

用側錄軟體蒐證告員工 老闆先被判 3 月徒刑

【焦點話題】

台中市某生技公司黃姓負責人，於公司電腦內安裝「X-fort」側錄軟體，可側錄「即時通」、「Skype」、「line」等電腦與手機同步之通訊及對話內容，遂因黃男懷疑陳姓職員涉嫌將公司檔案拷貝帶走，提出控告妨害商業秘密，並提供陳女與他人之「Skype」談話內容予檢方偵辦，因而將非法監控員工之行為曝光，黃男雖辯稱安裝該軟體僅為了保護商業秘密，並非監控個人隱私，且陳女早知悉公司有安裝該軟體。法官則認為，黃男安裝該軟體，理應知道此舉恐會側錄個人隱私，有侵害他人隱私之虞，則依違反通訊保障及監察法判處 3 個月徒刑。

【參考資料來源：自由時報，107/5/29；臺灣臺中地方法院 107 年度訴字第 531 號判決】

【重點摘要】

1. 通訊保障及監察法之立法目的在於保障人民秘密通訊自由及隱私權不受非法侵害，因此適用範圍並非僅限制政府機關，針對違法監察他人通訊者，其犯罪行為主體並未規定限於公務員，而亦包括一般人民。
2. 私人違法通訊監察者一樣會違反通訊保障及監察法，但私人違法監察所取得之證據是否不得使用，則應視情況而定，由法官於具體個案為比例原則加以判斷是否採用，而非一律禁止。

【法律觀點】

我國以通訊保障及監察法（下稱通保法）作為政府機關進行通訊監察之依據，其立法目的在於保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序[1]。但，既然通保法之立法目的在於保障人民秘密通訊自由及隱私權不受非法侵害，因此並非僅限制政府機關，針對違法監察他人通訊者，其犯罪

[1] 通訊保障及監察法第 1 條。

行為主體並未限於公務員，而是將一般人民亦包括在內[2]。因此，非法進行通訊監察者如為一般民眾，即可能觸犯刑法第 315-1 條之無故竊錄罪[3]及通保法第 24 條第 1 項之非法監察罪。

惟以非法監察方式所取得之證據，具備證據能力與否，可將其區分為政府之非法監察或是私人之非法監察，二者雖均屬非法監察而為法律所禁止，但其效力並不相同。

偵查機關若欲實施通訊監察，根據通保法規定，僅得在特定類型案件範圍內，諸如危害國家安全、經濟秩序或社會秩序情節重大，且不能或難以其他方法蒐集或調查證據者，方可向法院聲請通訊監察書而進行通訊監察[4]。因此若屬政府無通

---

[2] 最高法院 101 年台上字第 3416 號刑事判決:「按通訊保障及監察法第 24 條第 1 項規定，違法監察他人通訊者，處五年以下有期徒刑，其犯罪行為主體並未規定限於公務員；參酌同條第 2 項所規範之對象，為執行或協助執行通訊監察之公務員或從業人員，第 3 項則為前 2 項營利犯罪之行為人，足見其第 1 項之處罰對象應係針對一般人民；又同法第 30 條復規定同法第 24 條第 1 項之罪，須告訴乃論，苟同法第 24 條第 1 項之犯罪主體限於公務員，則公務員違法監察他人通訊，不僅侵犯被害人之隱私權，更違背公務員之忠實義務，有辱官箴，實不宜規定為告訴乃論之罪，足見同法第 24 條第 1 項之罪所規範之行為人，應為一般人民」。

[3] 刑法第 315-1 條「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[4] 通訊保障及監察法第 5 條第 1 項：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。一、最輕本刑為三年以上有期徒刑之罪。二、刑法第一百條第二項之預備內亂罪、第一百零一條第二項之預備暴動內亂罪或第一百零六條第三項、第一百零九條第一項、第三項、第四項、第一百二十一條第一項、第一百二十二條第三項、第一百三十一條第一項、第一百四十二條、第一百四十三條第一項、第一百四十四條、第一百四十五條、第二百零一條之一、第二百五十六條第一項、第三項、第二百五十七條第一項、第四項、第二百九十八條第二項、第三百條、第三百三十九條、第三百三十九條之三或第三百四十六條之罪。三、貪污治罪條例第十一條第一項、第四項關於違背職務行為之行賄罪。四、懲治走私條例第二條第一項、第二項或第三條之罪。五、藥事法第八十二條第一項、第四項或第八十三條第一項、第四項之罪。六、證券交易法第一百七十三條第一項之罪。七、期貨交易法第一百十二條或第一百十三條第一項、第二項之罪。八、槍砲彈藥刀械管制條例第十二條第一項、第二項、第四項、第五項或第十三條第二項、第四項、第五項之罪。九、公職人員選舉罷免法第一百零二條第一項第一款之罪。十、農會法第四十七條之一或第四十七條之二之罪。十一、漁會法第五十條之一或第五十條之二之罪。十二、兒童及少年性剝削防制條例第三十二條第一項、第三項、第四項、第五項之罪。十三、洗錢防制法第十一條第一項至第三項之罪。十四、組織犯罪防制條例第三條第一項後段、第二項後段、第六條或第十一條第三項之罪。十五、陸海空軍刑法第十四條第二項、第十七條第三項、第十八條第三項、第十九條第三項、第二十條第五項、第二十二條第四項、第二十三條第三項、第二十

訊監察書之非法通訊監察所取得之內容及其衍生證據，依同法第 18-1 條第 3 項[5]之規定，不得於偵查、司法或任何程序中使用，即無證據能力，以避免政府濫行監聽取證。

但於私人進行之非法監察部分，雖通保法對私人非法通訊監察有所規範，非法進行通訊監察者一樣會觸法，但對私人而言，並沒有如第 5 條、第 6 條或第 7 條之核發通訊監察書之要求，因此並無通保法第 18-1 條之適用，亦即並無因違反通保法規定而不得作為證據之情形，此時應由法官於具體個案為比例原則加以判斷是否採用，而非一律禁止[6]。

本案中，黃姓負責人雖因違反通保法遭判 3 個月有期徒刑，但因其所非法取得的證據在法官依比例原則判斷後，仍可能於他案使用，陳女是有可能遭受到妨害商業秘密罪之不利益。

【管理 Tips】

側錄軟體本身係直接載於使用者之硬體上，而控管所有周邊裝置、網路行為等，並記錄操作行為，因此使用該硬體人員之行為均受到記錄，但組織並非一定不得進行通訊監察，符合相關程序下，仍得辦理之。

首先，宜考量通保法第 3 條[7]規定之合理期待，先行告知成員將使用相關軟體為紀錄保存，並聲明「禁止使用通訊軟體作私人聊天使用」、「禁止將公司文件洩漏予非必要人員」等，使員工已無從期待其通訊內容不被公司蒐集。

四條第二項、第四項、第五十八條第五項、第六十三條第一項之罪。十六、營業秘密法第十三條之二第一項、第二項之罪。十七、森林法第五十二條第一項、第二項之罪。十八、廢棄物清理法第四十六條之罪。」

[5] 通訊保障及監察法第 18-1 條第 3 項「違反第五條、第六條或第七條規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據或其他用途，並依第十七條第二項規定予以銷燬。」

[6] 臺灣高等法院臺中分院 100 年度上易字第 1593 號刑事判決「偵查機關違法偵查蒐證與私人不法取證，乃兩種完全不同之取證態樣，兩者所取得之證據排除與否，理論基礎及思維方向均非可等量齊觀，私人不法取證，難以證據排除法則作為其排除之依據及基準，故應認私人所取得之證據，原則上無證據排除原則之適用。惟如私人故意對被告使用暴力、刑求等方式，而取得被告之自白或證人之證述，因違背任意性，且有虛偽高度可能性，基於避免間接鼓勵私人以暴力方式取證，例外排除該證據之證據能力。」

[7] 通訊保障及監察法第 3 條第 2 項：「前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」

其次，組織仍應考量成員之隱私與組織機密安全間之平衡為原則，以相當性、必要性等原則為依歸，訂定內部處理準則及有效之管理措施，以避免相關疏漏、誤失之發生，更應將依據內部處理準則及員工規則等辦理通訊監察之相關紀錄予以留存，降低將來訟爭之風險。

【相關標準】

ISO27001：2013（CNS27001）

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。本案如被告能清楚了解通保法規範要求，知悉該法係對一般人亦適用，可先以口頭或書面告知公司電腦內有安裝側錄軟體一事，則可能使告訴人喪失通訊內容不被公司蒐集的期待可能性，而不致敗訴。

類別：資訊監察【案號：M10721】

扣押已結束的通訊內容 須搜索票或扣押裁定

【焦點話題】

2015 年 8 月，檢警查出陳姓、洪姓男子 2 人經營地下六合彩簽賭站，讓賭客以中華電信「hiBox」電子郵件網路傳真下單，但因賭博罪是輕罪，不可聲請通訊監察書，檢警則以「調取票」向中華電信調閱 324 張賭客傳真簽單影像做為證據。然最高法院認為，通訊監察書只適用於「現時或未來發生」的通訊內容，而「過去已結束」的通訊內容，應回歸刑事訴訟法搜索、扣押程序，由於涉及民眾通訊隱私，偵查單位不宜未經法院介入就直接調閱，應向法官聲請核發搜索票或扣押裁定，才能搜索、扣押當事人「過去已結束」的通訊內容，包括 LINE 的已讀訊息。

【參考資料來源：自由電子報，107/5/30】

【重點摘要】

1. 通訊保障及監察法第 5 條所定辦理及准許通訊監察所需具備之要件，包括重罪原則、必要性、關聯性、令狀原則、事中監督以及事後通知等；而同法第 11-1 條准許聲請調取票之要件則為重罪原則、必要性、關連性及令狀原則，二者差異在於准許調取票之聲請並無事中監督以及事後通知。

2. 依通訊保障及監察法第 11-1 條規定，調取票所能調取之客體乃通信紀錄及通信使用者資料，而最高法院 106 年度台非字第 259 號刑事判決闡述，通訊保障及監察法所規範之通訊監察，重在過程，應限於「現時或未來發生」之通訊內容，並不包含「過去已結束」之通訊內容，偵查機關如欲取得「過去已結束」之通訊內容，應回歸適用刑事訴訟法，並依刑事訴訟法搜索扣押相關規定為之。

【法律觀點】

我國之通訊監察相關規範，係以通訊保障及監察法（下稱通保法）作為政府機關進行通訊監察之依據，依照通保法規定，當調查發現相關情事可能危害國家安全、經濟秩序或社會秩序之情節重大、通訊內容與案件相關，且無法以其他方式進行調查時，得發通訊監察書進行監察。而如果僅需要通信紀錄或使用者資料時，則發調取票調取之[1]。

有關通保法准許通訊監察之要件如下：一、重罪原則，最輕本刑三年以上有期徒刑之罪及其他所列舉之重罪者[2]；二、必要性，須無法以其他方式為調查者；三、關聯性，通訊內容與案件相關者；四、令狀原則，須視情況由法院或綜理國家情報工作機關首長核發通訊監察書，由情報機關首長核發者，並須經法院事後補行同意；五、事中監督[3]，每十五日至少作成一次以上之報告書；六、事後通知，通訊監察結束後應通知受監察人[4]。

另外，通保法准許聲請調取票之要件[5]如下：一、重罪原則，最重本刑三年以上有期徒刑之罪；二、必要性；三、關連性，有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性；四、令狀原則，應以書面聲請該管法院核發，

[1] 按通訊保障及監察法第 5 條規定，通訊監察書於偵查中均由檢察官依司法警察機關聲請或依職權以書面聲請該管法院核發。而同法第 11-1 條則規定調取票係檢察官應以書面聲請該管法院核發調取票；或司法警察官報請檢察官許可後，向該管法院聲請核發調取票；又或在特定重罪下，得由檢察官依職權或司法警察官向檢察官聲請同意後，調取通信紀錄。

[2] 通訊保障及監察法第 5 條第 1 項略以：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。…」

[3] 通訊保障及監察法第 5 條第 4 項：「執行機關應於執行監聽期間內，每十五日至少作成一次以上之報告書，說明監聽行為之進行情形，以及有無繼續執行監聽之需要。檢察官或核發通訊監察書之法官並得隨時命執行機關提出報告。法官依據經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原核發之通訊監察書。」

[4] 通訊保障及監察法第 15 條第 1 項：「第五條、第六條及第七條第二項通訊監察案件之執行機關於監察通訊結束時，應即敘明受監察人之姓名、住所或居所、該監察案件之第十一條第一項各款及通訊監察書核發機關文號、實際監察期間、有無獲得監察目的之通訊資料及救濟程序報由檢察官、綜理國家情報工作機關陳報法院通知受監察人。如認通知有妨害監察目的之虞或不能通知者，應一併陳報。」

[5] 通訊保障及監察法第 11-1 條第 1 項：「檢察官偵查最重本刑三年以上有期徒刑之罪，有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性時，除有急迫情形不及事先聲請者外，應以書面聲請該管法院核發調取票。聲請書之應記載事項，準用前條第一項之規定。」

縱有急迫情形不及事先聲請者亦須於急迫原因消滅後補行聲請。

綜上而述，二者相較的差異在於事中監督及事後通知，其主因在於調取票僅調取「通信紀錄或使用者資料」，如電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄；而通訊監察書則可取得文字、影像、聲音、言論談話、郵件書信等「實質通訊內容」。由此可知，調取票係針對於過去已結束之通信紀錄或使用者資料，而通訊監察書則是為現時或未來發生之通訊內容，並不及於過去已結束的資料[6]。

本案中，由最高法院[7]之說明可知，如需要現時或未來發生之通訊內容應以通訊監察書為之；過去已結束之通信紀錄應以調取票為之；過去已結束之通訊內容則應以搜索、扣押之方式為之，而對於現時或未來發生之通信紀錄，因其並不存在亦無法預測，除非依附現時或未來發生之通訊內容的通訊監察，否則並無此選項。

【管理 Tips】

基於人性尊嚴與個人主體性維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權為憲法第 22 條所保障之基本權。就個人秘密不受侵擾部分，憲法第 12 條特別規定秘密通訊自由之保障，乃隱私權保障之具體態樣及重要內容。

因此，公務機關於涉及隱私權部份之處理應特別注意，並在資訊保護與資訊 (通訊)監察間取得平衡，而通訊內容與通信紀錄或使用者資料間，因通訊內容涉及對於個人隱私權之侵害程度大於通信紀錄或通信使用者資料，故對於「過去已結束」之通訊內容，原則上應向法院聲請核發扣押裁定，不得逕以提出或交付命令

---

[6] 按通訊保障及監察法第 3-1 條第 1 項：「本法所稱通信紀錄者，謂電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。」，可知通信紀錄係使用服務後所產生之紀錄，故屬「過去已結束」之紀錄。而最高法院 106 年台非字第 259 號刑事判決引述司法院釋字第 631 號解釋理由書，並將理由書所謂之「監控與過濾」應係對於「現時或未來發生」之通訊方能為之，對於「過去已結束」之通訊內容，則無從「監控與過濾」。益徵大法官解釋所指稱之通訊監察係針對「現時或未來發生」之通訊，不及於「過去已結束」之通訊。

[7] 最高法院 106 年台非字第 259 號刑事判決。

之函調方式取得，方屬保障人民一般隱私權。而向法院透過司法權之監督，得以確認所監察之範圍是否適當，以保障相關人員之權益。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。本案中檢方所要調取的是經由電腦伺服器儲存傳真影像而傳送訊息，涉及「通訊之實質內容」，檢察機關應對於法規之適用更加清楚了解，以符合依法行政原則。

類別：資訊監察【案號：M10722】

建置手機監控系統 執法機關：絕無可能任意擷取資料

【焦點話題】

執法機關預計斥資 5 億元建置「新世代行動網路 App 偵查相關系統中程計畫」，遭外界質疑有監控全民之虞。執法機關表示，依通訊保障及監察法相關規定，電信事業有協助執行通訊監察之義務，通訊設備應具配合執行監察之功能，目前各家電信業者已陸續完成升級為 4G 電信系統，但執法機關因通訊監察系統仍屬 3G，不符未來科技使用，因此執行提升計畫，配合升級為 4G 系統，則過去建置的 2G 系統已於 107 年 6 月淘汰。且執法機關於執行時受有通訊保障及監察法規範，不得任意監聽或擷取民眾手機資料。若需向檢察官及法官聲請核發通訊監察書，亦須為涉及最輕本刑為 3 年以上有期徒刑罪責者。此外，監察資訊需同步傳送至臺灣高等法院，以備稽核，無任意擷取民眾手機資料之疑慮。

【參考資料來源：自由時報，106/11/2】

【重點摘要】

1. 按通訊保障及監察法施行細則第 26 條規定，第一類電信事業者所建置的通訊系統，應符合執法機關之監察需求，如為現有設備不足者，執法機關評估電信事業業務及設備設置情形，向其提出需求，並由其建置之，如為新設、新增或擴充通訊系統，則由執法機關提出監察需求，讓電信事業擬定建置計畫，經由確認後辦理建置，建置完成後則應經確認符合需求功能，方得開始運作。

2. 電信業者之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但亦以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性，此按通訊保障及監察法施行細則第 14 條可知。

【法律觀點】

我國通訊監察相關規範，係以通訊保障及監察法（下稱通保法）作為政府機關進行通訊監察之依據；依通保法規定，於特定重罪之情形時，當調查發現相關情事可能危害國家安全、經濟秩序或社會秩序情節重大，或該通訊內容具有相當理由可信與案件相關，且不能或難以其他方式進行調查時，得發通訊監察書進行監察[1]。另外，根據通保法規定[2]，為進行通訊監察，電信事業有協助執行通訊監察之義務，該義務包括電信事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助[3]。

目前各家電信業者之電信系統均自 3G 升級為 4G，且於 107 年 6 月已將 2G 系統淘汰，並希望於 107 年年底將 3G 系統終止[4]。然執法機關現行的通訊監察系統仍屬 3G，為使通訊監察不致因為系統淘汰而中斷，因此通保法施行細則第 26 條[5]則要求，第一類電信事業者所建置的通訊系統，應符合執法機關之監察需求，

---

[1] 通訊保障及監察法第 5 條第 1 項略以：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。…」

[2] 通訊保障及監察法第 14 條：「通訊監察之執行機關及處所，得依聲請機關之聲請定之。法官依職權核發通訊監察書時，由核發人指定之；依第七條規定核發時，亦同。　　電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。　　前項因協助執行通訊監察所生之必要費用，於執行後，得請求執行機關支付；其項目及費額由交通部會商有關機關訂定公告之。電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。　　前項協助建置通訊監察系統所生之必要費用，由建置機關負擔。另因協助維持通訊監察功能正常作業所生之必要費用，由交通部會商有關機關訂定公告之。」

[3] 通訊保障及監察法施行細則第 26 條第 1 項：「本法第十四條第二項所稱協助執行通訊監察之義務，指電信事業及郵政事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備及本施行細則所定之其他配合事項。」

[4] 參考網址：https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&is_history=0&pages=0&sn_f=39080，(瀏覽日期：107 年 6 月 29 日)

[5] 通訊保障及監察法施行細則第 26 條第 2 項至第 4 項：「國家通訊傳播委員會應將本細則施行前經特許或許可設置完成之第一類電信事業之通訊系統及通訊網路等相關資料，提供予法務部調查局或內政部警政署評估其所需之通訊監察功能後，由法務部調查局或內政部警政署依第一類電信事業之業務及設備設置情形，向第一類電信事業提出需求；第一類電信事業應即依該需求，擬定所需軟硬體設備、建置時程及費用之建置計畫，與法務部調查局或內政部警政署協商確定後辦理建置。必要時，由國家通訊傳播委員會協助之。第一類電信事業於本細則施行前已經同意籌設或許可之新設、新增或擴充通訊系統，於本細則施行時尚未完成籌設或建置者，於其通

如現有設備不足者，執法機關應評估電信事業業務及設備設置情形，向其提出需求，並由其建置之，若須新設、新增或擴充通訊系統時，則由執法機關提出監察需求，讓該電信事業擬定建置計畫，經確認後辦理建置，建置完成後則應經檢核，確認符合需求功能後方得開始運作。

為達到有效監管之目的，執法機關於 106 年底提出「建置新世代行動網路 App 偵查相關系統中程計畫」[6]，自 107 年至 109 為期三年，所提出之 107 年年度目標為建置 4G M 化定位系統及行動網路應用服務鑑析系統，目的即在配合第一類電信業者之系統更換，使新的通訊系統具有配合執行監察之功能。

本計畫中，電信業者之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務，而該等義務以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性[7]。

【管理 Tips】

通訊保障及監察法之立法目的即包括確保國家安全，維護社會秩序，並非完全禁止通訊監察，為了有效監察，透過第三方之協助亦是在所難免，因此，電信業者於通訊監察即佔有一定的角色。

惟在行動通訊的時代，科技越形發達，對於電信業者的仰賴相形降低，以 M 化定位系統而言，該系統並不需要透過電信業者即可偵測特定手機，而偵測特定手機位置資訊仍屬通保法第 3-1 條[8]的「通信紀錄」，而受通保法規範[9]。故政府機

訊系統開始運作前，應依前項之規定擬定配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫及辦理建置，並於其通訊系統開始運作時同時協助執行通訊監察。本細則施行前交通部已公告受理特許經營之第一類電信業務，其經核可籌設者，亦同。第一類電信事業新設、新增或擴充通訊系統者，為確認其通訊系統具有配合執行監察之功能，應由法務部調查局或內政部警政署提出監察需求，該電信事業儘速擬定應配合執行通訊監察所需軟硬體設備、建置時程及費用之建置計畫，經法務部調查局或內政部警政署與該電信事業協調確定後，由國家通訊傳播委員會核發建（架）設許可證（函）後辦理建置，並經國家通訊傳播委員會與法務部調查局或內政部警政署確認符合通訊監察功能後，於其通訊系統開始運作時同時協助執行通訊監察。」

[6] http://117.56.91.94/KMPublic/readdocument.aspx?documentId=279684 ，(瀏覽日期：107 年 6 月 29 日)

[7] 通訊保障及監察法第 14 條第 4 項。

[8] 通訊保障及監察法第 3-1 條第 1 項：「本法所稱通信紀錄者，謂電信使用人使用電信服務後，電信系統所產生

關在進行通訊監察時，雖不需透過電信業者即可進行，但仍應考量是否有通保法或其他相關法規之適用，降低觸法可能。

【相關標準】

ISO27001：2013（CNS27001）

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。本案中所涉及的是電信業者對於通訊監察之配合義務，執法機關與電信業者均應瞭解所涉法律及應用範圍，對於建置通訊設備之必要性及流程操作應予以瞭解，俾符合依法行政原則。

之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。」

[9] 在 103 修法前，通信紀錄並未受到通保法規範，故亦有認為位置資訊不受到通保法規範之論點(http://news.ltn.com.tw/news/local/paper/722677 ，瀏覽日期：：107 年 6 月 30 日)，惟修法後明確表示為保障憲法第十二條人民秘密通訊自由並落實司法院大法官會議第 631 號解釋意旨，將通信紀錄納入通訊監察法制範圍內，因此通訊紀錄自此已受到通保法規範，需經必要程序方得合法調取。

類別：資訊監察【案號：M10723】

德國全面禁止兒童智能手錶

【焦點話題】

德國電信監理機構宣布，德國全面禁止販售兒童智能手錶，其因兒童智能手錶具有錄音功能，此功能原先是設計給家長用以掌握孩童動靜，但家長亦可能透過該功能秘密監聽孩童所在環境，甚至部分家長會藉機監聽老師上課內容。該錄音功能雖有利家長知悉其兒童之周遭狀況，惟亦衍伸出隱私權侵害之疑慮，故予以列為禁用之裝置。

【參考資料來源：自由時報，106/11/18】

【重點摘要】

1. 按通訊保障及監察法第 3 條規定，通訊包括：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信；二、郵件及書信；及，三、言論及談話。因此只要是符合上面任一情形，又有事實足認受監察人對其通訊內容有隱私或秘密之合理期待時，就是通保法所要保障的通訊。

2. 依通訊保障及監察法第 29 條意旨，監察者如非通訊之一方，亦無取得任一方同意，即監聽通訊內容或將通訊內容錄音時，將可能構成違法監察他人通訊罪，以及妨害秘密罪。

【法律觀點】

通訊保障及監察法（下稱通保法）第 1 條即開宗明義，為保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。而其中「祕密通訊自由」係為憲法[1]所保障的權利，而隱私權雖非憲法明文列舉之權利，惟為保障個人生活私密領域免於他人侵擾，大法官亦認為係屬憲法第 22 條所保

[1] 憲法第 12 條：「人民有秘密通訊之自由。」

障之權利[2]。

依照通保法之定義，所謂通訊[3]包括：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信；二、郵件及書信；及，三、言論及談話。因此，只要符合上述任一情形，且有事實足認受監察人對其通訊內容有隱私或秘密之合理期待時，係屬通保法所要保障之通訊。

然而，通訊監察係以截收監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之，但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材[4]。於本案提及之兒童智慧手錶具有位置定位、雙向通話、及遠程監聽等功能[5]，換言之，手機可以遙控該手錶予以錄製周圍之環境音，並自動發送到配對的手機，因此當兒童智慧手錶開啟通話、監聽等功能，即可能符合前述通訊監察之定義。

依通保法之相關規定，監察者為通訊之一方或已得通訊之一方事先同意，且非出於不法目的者，則相關的監察行為將不被處罰[6]。本案所提及之兒童智慧手錶，其出發點雖是確保兒童安全以使家長安心，但因其功能眾多，如追蹤位置或遠程監聽等功能及可能有侵害個人隱私之虞，又若安全機制有所疏漏，則可能因系統遭駭入，反而致使兒童暴露於危險之下，或可能監聽到他人言論及談話，而使該等人員之隱私權和秘密通訊自由受到侵害，可能構成通保法第 24 條第 1 項[7]違法

---

[2] 參照大法官釋字第 585 號理由書：「...其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五 0 九號、第五三五號解釋參照）。」

[3] 通訊保障及監察法第 3 條：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。　前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」

[4] 通訊保障及監察法第 13 條第 1 項：「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」

[5] https://24h.pchome.com.tw/prod/DYAI4F-A9008L1RL (瀏覽日期：2018 年 7 月 2 日)

[6] 通訊保障及監察法第 29 條：「監察他人之通訊，而有下列情形之一者，不罰：一、依法律規定而為者。二、電信事業或郵政機關（構）人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

[7] 通訊保障及監察法第 24 條第 1 項：「違法監察他人通訊者，處五年以下有期徒刑。」

監察他人通訊罪。

除了通保法之相關規範外，智慧手錶的監控者若無故利用工具或設備窺視、竊聽，或以錄音、照相、錄影或電磁紀錄竊錄使用者非公開之活動、言論、談話或身體隱私部位者時，亦有可能成立刑法第 315 條之 1 的妨害秘密罪。

本案兒童智慧手錶可能可使父母對於兒童之安全更加放心，但也可能更使兒童暴露於風險下，且父母在使用相關設備時亦應為相當注意，若不慎侵害他人祕密通訊自由或隱私權時，可能須負相關法律責任。

【管理 Tips】

組織購入資訊設備前，須於採購前檢視相關報告及技術文件，確認是否符合採購需求，以及是否有危害組織權益之風險。如發現該設備有諸如使組織機密洩漏或遭竄改之可能時，基於風險控制之考量，應該執行風險規避，排除該設備之採購，但如已購入或該設備為組織運作所必須者，則應採取相對應之控管機制或其他補償性措施，以降低風險或進行風險轉嫁

此外，組織實際運行資訊設備時，亦應確保其安全性，定期執行必要之安全檢查措施，如有任何異常，則應在保固範圍內請求產品開發商進行確實檢測以及修補，避免第三方透過弱點入侵，造成組織網路暴露於風險之下。

【相關標準】

ISO27001：2013（CNS27001）

- A.13.1.2　網路服務之安全

(1)標準內容：　應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外提供。

(2)適用說明：　組織應確保無論是內部或外部服務，其所使用之網路已具備相關安全機制，以進行網路服務之管理與安全維護，當

設備需要透過網際網路進行資料傳輸時，因此應具備相當之通訊安全措施，避免第三方透過弱點入侵導致相關損害。

- A.18.1.1　適用之法規及契約的要求事項之識別

(1)標準內容：　對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明：　組織在業務開發時應瞭解並依循其應適用之法令，以避免觸法。以本案例而言，當組織在開發兒童智能手錶時，並未清楚認知到其所應適用之法律，導致當政府機關下達禁止兒童使用智慧手錶要求時，組織將蒙受損失。

類別：資訊監察【案號：M10724】

奧克蘭通過全美最嚴謹監控監察法

【焦點話題】

美國奧克蘭市議會於 2013 年成立區域警示中心，建立多重感測監控系統，整合包含奧克蘭港監控攝影機、熱成像設備、車牌照辨識系統、槍聲感測器、閉路攝影機、市立學校監控攝影機以及公路攝影機等設備。而在該監控系統建置後，奧克蘭市議會隨後成立隱私諮詢委員會(Privacy Advisory Commission, PAC)，執法機關如為取得個人隱私資訊，便需經過隱私諮詢委員會(PAC)同意。日前，奧克蘭市議會更進一步通過購買與使用監察設備條例，當該市市議會欲撥預算或試圖尋求外部資金採購用於影響隱私之軟硬體時，皆須通知隱私諮詢委員會。

【參考資料來源：iThome，107/5/10】

【重點摘要】

1. 奧克蘭市議會成立隱私諮詢委員會(PAC)，其職責包括提供針對監察設備購買時的諮詢與技術援助、為隱私與資訊保護相關立法起草、對現有與規劃中的監察設備提交年度策略報告、提供其他地區隱私立法與資訊、召開公聽會、就區域警示中心的功能及政策進行審查。
2. 奧克蘭市議會成立隱私諮詢委員會(PAC)，其職責包括提供針對監察設備購買時的諮詢與技術援助、為隱私與資訊保護相關立法起草、對現有與規劃中的監察設備提交年度策略報告、提供其他地區隱私立法與資訊、召開公聽會、就區域警示中心的功能及政策進行審查。

【法律觀點】

奧克蘭市議會於 2014 年 3 月成立一個特設的諮詢委員會—區域警示中心(Domain Awareness Center, DAC)，區域警示中心(DAC)位於緊急操作中心(Emergency Operations Center, EOC)內，該區域警示中心(DAC)可收集監控影

像、音頻和數據的即時串流，同時該議會亦提出 7 項建議[1]，其中二項關鍵建議為：一、成立隱私諮詢委員會，以提供有關於區域警示中心(DAC)或區域警示中心隱私與資訊政策的相關指導。二、考慮訂定全市監察技術條例，以便市政府就未來所有監察技術的隱私和政策進行公開討論和決策。據此，奧克蘭市議會於 2016 年 1 月成立隱私諮詢委員會(Privacy Advisory Commission, PAC)，該隱私諮詢委員會(PAC)之職責[2]包括提供針對監察設備購買時的諮詢與技術援助、研擬隱私與資訊保護相關規範、提交現有與所規劃之監察設備年度策略報告、提供其他隱私立法與資訊、召開公聽會、審查區域警示中心(DAC)之功能及政策。

2018 年奧克蘭市議會更進一步通過購買與使用監察設備條例，該條例將監察技術[3]定義為，設計或主要用於蒐集、保留、分析、處理或共享音頻，電子、視覺、位置、熱、嗅覺、生物識別軟體、電子設備、使用電子設備的系統或類似物，例如：蜂窩站點模擬器、車牌自動識別系統、槍聲定位系統、人臉辨識軟體、熱成像系統、隨身相機、社群網路分析軟體、步態分析軟體；透過遠端錄音或錄影的攝影機。更包括以監控社群網路服務或預測犯罪活動，或以犯罪、生物識別為目的的軟硬體。

就建置監察技術之程序上，可從隱私諮詢委員會(PAC)以及市議會二者加以觀察：就隱私諮詢委員會(PAC)而言，市議會必須於尋求或募集監察技術資金或向其他非政府機關徵求監察技術提案前通知隱私諮詢委員會(PAC)主席，而該委員會則應將該項目列入其下一次會議議程，以供討論並決定是否批准。而當採行新的監察技術時，奧克蘭市議會必須向隱私諮詢委員會(PAC)提交監督影響報告，並經其審查，而既有之監察技術，則必須定期向隱私諮詢委員會提出監察技術清單，並據以提交監察影響報告，使該委員會得以確認該技術是否得持續使欲[4]。就奧

---

1 https://www.oaklandca.gov/services/boards-and-commissions-index/privacy-advisory-commission-index/dac-draft-privacy-policy-public-comments (瀏覽日期：2018 年 7 月 6 日)

2 OAKLAND CITY COUNCIL ORDINANCE NO. 13349 C.M.S. SECTION 2. (2015)

3 OAKLAND CITY COUNCIL ORDINANCE NO.13489 C.M.S art.9.64.010 §10 (2018)

4 OAKLAND CITY COUNCIL ORDINANCE NO.13489 C.M.S art.9.64.020 (2018)：「「"Surveillance Technology"

克蘭市議會而言，當市議會接受州或聯邦的資金、實物或其他捐贈用於監察技術時、獲得新的監察技術時、未經批准使用監察技術或據此而來之資訊、與其他非政府機關簽訂協議以取得、共享或以其他方式使用監察技術或其提供的資訊，均需經過市議會批准方得為之[5]。綜上而言，以該市之規定，如欲使用新監察技術等，需先經由隱私諮詢委員會(PAC)同意，再經市議會批准。

觀我國現行之相關法規，似未有該等規定，於數位化日漸盛行之當下，或可參考外國立法進行法規之增修，引進外部審查單位，當政府在使用可能侵害個人隱私的技術時加以審核，以降低政府侵害個人隱私之風險。

【管理 Tips】

若組織要健全成長，適當之監督有其必要性，可有助於健全各單位之責任歸屬。

從監督之角度觀之，可分為內部監督與外部監督，內部監督是藉由組織內部之行政控制，例如上級對下級單位之控制，以確保程序順利進行，又或是藉由人事、財務等方式，對於人員或採購予以適法性監督；而外部監督則可透過獨立董事，協助董事會作出對公司股東最有利之決策，又或是外部會計師之財務查核，藉以達到資訊揭露及透明化的效果。就奧克蘭市的作法，透過隱私諮詢委員會(PAC)的外部監督，可降低政府侵害人民的風險。

除此之外，從監督的時間點來看，可分為事前監督、事中監督、事後監督。事前監督，是指在組織某項活動付諸實施之前，對其決策的預防性監督；事中監督，是指在執行決策過程中所進行的監督；事後監督，是指決策完成後之驗證檢討。就奧克蘭市之作法，在進行監察技術之採購時，事前需經審查批准，進行中需提

---

means any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software. 」」

[5] OAKLAND CITY COUNCIL ORDINANCE NO.13489 C.M.S art.9.64.030 (2018)

交監督影響報告，而已經運作部分，則是要定期提出清單，並提交報告並據以檢討是否持續。

準此，組織宜透過適當的監督機制，確保工作過程之正確性與完整性，如果有任何缺漏亦可早期發現予以應變調整。

【相關標準】

ISO27001：2013（CNS27001）

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織應識別所適用關於資訊監察之相關法令，並確認應作為及不作為之事項，本案中，奧克蘭市訂定嚴格的購買與使用監察設備條例，則市議會即應遵守此條例，在採購新的監察技術或就既有監察技術的評估，就必須要符合相關規定。

- A.17.1.2 實作資訊安全持續

(1)標準內容： 組織應建立、文件化、實作及維持過程、程序及控制措施，以確保不利情況期間所要求之資訊安全持續等級。

(2)適用說明： 依本案為例，奧克蘭市議會應系統性的建立並維持相關程序及控制措施，並將其妥善記錄以確保資訊安全。

肆、資訊應用(Application)

類別：資訊應用【案號：A10725】

上下班塞車有解？ 北市「智慧路燈」上線

【焦點話題】

北市府計畫於 2019 年斥資 1.4 億元建置 1.26 萬盞智慧路燈，範圍涵蓋信義、松山、中山、內湖及南港等 5 大行政區，有別於一般路燈僅用來照明，智慧路燈結合邊緣運算應用，進行遠端即時監控管理。同時，該市府亦計畫 3 年內將全市 16 萬盞路燈智慧化，未來的路燈除可能具備 5G 網路、車潮人流分析、PM2.5 偵測等功能外，甚至傳出可以「人臉辨識」，但因涉及隱私與資安疑慮，引發熱議。該市府亦強調，相關措施會遵守個資法等規定，不會配置造成隱私疑慮之人臉辨識功能。

【參考資料來源：TVBS 新聞網，107/5/28】

【重點摘要】

1. 如果於公開場所或公開活動中僅以影音資料方式蒐集個人臉部特徵，但並不與其他個人資料結合時，則屬於個人資料保護法第 51 條所稱是個人資料，但不適用個人資料保護法的情形，則該蒐集行為並不適用個人資料保護法。
2. 邊緣運算是一種分散式運算的架構，其可減少雲端運算頻寬負荷或斷線所產生的風險，更因為在本地裝置端蒐集資料時同時進行資料處理，因此可以選擇僅將必要資料上傳至雲端透過資料中心加以處理，而將涉及個人資料之部份予以過濾分析、匿名保留於本地裝置端，可減少個人資料移轉時外洩風險。

【法律觀點】

現階段智慧型 LED 路燈系統之功能包括：自動量測路燈電力數據、調光及自我故障偵測等功能，後續規劃與 Google 電子地圖結合並導入可攜式裝置，配合財產管理 E 化，可供線上即時報修以加速路燈修復時間[1]。但因政府單位可能將之納

[1] 臺北市政府工務局施政兩週年績效報告。

入人臉辨識等功能，而產生侵犯個人權利之爭議。

依個人資料保護法第 2 條之規定，個人資料為：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。人臉辨識之目的在於將出現於影像系統中之個人予以特定，故可能因個人之主要特徵而得識別個人，或以其他得以直接方式識別該個人，無論屬何者均為個人資料保護法所稱之個人資料。

而個人資料保護法規定在蒐集個人資料時，必須要具備特定目的，符合法定情形並履行告知義務，如此方為合法之個人資料蒐集，惟並非所有個人資料皆受到個人資料保護法之保護。按個人資料保護法第 51 條規定，有二情形不適用個人資料保護法，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，本款係指一般正常個人或家庭社交活動，例如，為舉辦國中同學會，而蒐集畢業同學的聯絡方式；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，本款重點則在於公開以及未與其他個人資料結合之影音資料，例如，路口監視器在未與其他個人資料結合前所拍攝到的人臉，上開二者均屬於「是個人資料，但不受到個人資料保護法所規範」的情形[2]。

本案中，北市府原欲利用人臉辨識等功能作為智慧路燈的未來發展，惟考量人臉辨識技術引發侵害個資隱私的疑慮，而暫不考慮採用，此或許是一時之解，不過，如果僅以影音資料蒐集人流或人臉部資料，但並不與其他個人資料結合，則亦符合現行個人資料保護法。

[2] 按歐盟於本年度所施行之一般隱私保護規則（general data protection regulation, GDPR）中所定義之個人資料係指係指有關識別或可得識別自然人（「資料主體」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具（第 4 條第 1 款）。但其亦有排除適用之規定，包括於歐盟法外治權領域之活動、由會員國所進行屬於歐盟條約第二章第 5 節範圍內之活動、當事人所為單純之個人或家庭活動以及主管機關為達預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的（包括為維護及預防對於公共安全造成之威脅）之作為（第 2 條第 2 項）。因此，於本案中之市府蒐集人臉資訊，如得直接或間接地識別該自然人，則仍有可能屬於 GDPR 所稱之個人資料，而如無符合其排除適用之規定時，則有違反 GDPR 之可能。

【管理 Tips】

邊緣運算是一種分散式運算的架構，將應用程式、數據資料與服務的運算，由網路中心節點，移往網路邏輯上的邊緣節點來處理[3]，之所以運算架構會由中心化導向去中心化，主要的原因是當原始資料愈來愈多，如果仍然使用單一資料中心處理，將使得資料中心的負擔持續增加，但是資料中心是否能夠負荷已有疑義，再加上如果資料必須從蒐集處一路傳送到資料中心，後由資料中心加以處理後再將命令發送給終端裝置，中間網路傳輸時所可能造成的遲延，將使得命令的時效性產生疑義。因此，將資料運算下放至離資料來源更近的節點，使資料分析的速度能加快，省去額外的網路傳輸的時間成本，使用者獲得資料的時間將會縮短。

與此同時，邊緣運算不僅可減少雲端運算頻寬負荷或斷線所產生的風險，更因為在本地裝置端蒐集資料時同時進行資料處理，因此可以選擇僅將必要資料上傳至雲端透過資料中心加以處理，而將涉及個人資料之部份予以過濾分析、匿名保留於本地裝置端，不上傳至雲端，可減少個人資料移轉時外洩風險，不過也因為分散保存資料，因此如設備係外露於一般人均可觸及之處，將產生將個人資料上傳至雲端時不同的風險，例如因為設備失竊所導致的資料外洩，建置者亦應予以考量，例如以實體隔離，讓一般人無法接觸到該設備。

【相關標準】

ISO 27001：2013（CNS 27001）

- A. 14.1　資訊系統之安全要求事項

(1)標準內容：　確保資訊系統係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。

(2)適用說明：　組織對於所建置之系統，應確保使用者及相關資訊之隱私具備一定程度之有效保護，本案中，若在設計智慧路燈系

[3] 維基百科：http://www.law.ncku.edu.tw/NL/Pages/sample.aspx（瀏覽日期：2018 年 6 月 17 日）。

統，妥善納入資料運用方式，甚或是不予設計人臉辨識功能，則可將個人資料洩漏風險降至最低。

- A.18.1.4　個人可識別資訊之隱私及保護

(1)標準內容：　應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2)適用說明：　本案所涉之主要爭點在於智慧路燈系統所可能蒐集到的人臉辨識功能，因其係以影音方式蒐集，故如未與其他個人資料相結合則屬於「是個人資料，但不適用個人資料保護法所規範」之情形，但如之後結合其他個人資料而成為個人資料時，其相關作為仍應確保符合個資法之要求。

類別：資訊應用【案號：A10726】

立院三讀通過民航法修正案，無人機使用需註冊納管

【焦點話題】

立法院於 107 年 4 月 3 日三讀通過《民用航空法》部分條文修正案，增訂「遙控無人機」專章管理規定，首度將無人機納入管理。未來擁有重量二百五十公克以上的無人機，需辦理註冊，並將註冊號碼標明在機體上明顯處，操作人需取得民航局發給的操作證，才可使用；若在禁航區、限航區及航空站飛行場四周操作無人機，最重處一百五十萬元罰鍰，並可沒收無人機。另外，民航局亦承諾將開發行動裝置應用程式 App，整合台灣禁航區域及相關資訊，方便無人機操作者查詢使用。

【參考資料來源：科技新報，107/4/4】

【重點摘要】

1. 民用航空法第 2 條第 26 款定義之遙控無人機係指自遙控設備以信號鏈路進行飛航控制之無人航空器。
2. 為求有效管理，民用航空法第 99-10 條要求最大起飛重量高於 250 公克以上等之遙控無人機，操作者必須以真實姓名及聯絡方式，向主管機關註冊。

【法律觀點】

遙控無人機之風行，時聞有致飛安、公安、國安等問題之虞，例如：於機場四周管制範圍內，有礙飛航安全物體係依民航法處理；撞毀他人建築物時，建築物所有權人得依照民法請求損害賠償；於要塞堡壘地帶之禁航區內為非法偵查時，則依要塞堡壘法加以規範[1]，適用上未必均能及時妥適處置遙控無人機所引發的問題。為求對相關問題能有更切合實際之處理，立法院於 107 年 4 月 3 日通過「民

[1] 要塞堡壘地帶法第 4 條第 1 款：「第一區內之禁止及限制事項：一、非受有國防部之特別命令，不得為測量、攝影、描繪、記述及其他關於軍事上之偵察事項。…」

用航空法」部分條文修正草案，為遙控無人機訂定專章。

民航法修正條文將遙控無人機定義為：指自遙控設備以信號鏈路進行飛航控制或以自動駕駛操作或其他經民航局公告之無人航空器[2]。而自然人所有之最大起飛重量 250 公克以上之遙控無人機及政府機關（構）、學校或法人所有之遙控無人機，必須向民航主管機關註冊，並將註冊號碼標明於遙控無人機上顯著之處；而操作最大起飛重量達一定重量之遙控無人機，或政府機關（構）、學校或法人所有之遙控無人機，其操作人應經測驗合格，由民航局發給操作證後，始得操作[3]。因遙控無人機係以信號鏈路進行飛航控制，他人不易預測其實際運作狀態，為避免因人為控制或資通設備發生故障，進而影響飛航及國家安全，故該法亦限制遙控無人機之活動範圍，日後將由民航主管機關公告禁止使用遙控無人機之區域[4]；此外亦明定從事遙控無人機活動應遵守之規定[5]，包括遙控無人機距地表高度不得逾四百呎、不得以遙控無人機投擲或噴灑任何物件等。在新法修正通過後，因遙控無人機造成損害時，遙控無人機之所有人依規定必須負絕對責任[6]，亦即縱使所有人無故意或過失，例如，因為天災而導致損害發生，所有人仍應要負損害

[2] 民用航空法修正條文第 2 條第 26 款：「遙控無人機：指自遙控設備以信號鏈路進行飛航控制或以自動駕駛操作或其他經民航局公告之無人航空器。」

[3] 民用航空法修正條文 99-10 條第 1 項：「自然人所有之最大起飛重量二百五十公克以上之遙控無人機及政府機關（構）、學校或法人所有之遙控無人機，應辦理註冊，並將註冊號碼標明於遙控無人機上顯著之處，且一定重量以上遙控無人機飛航應具射頻識別功能。」

[4] 民用航空法修正條文 99-13 條第 1 項：「禁航區、限航區及航空站或飛行場四周之一定距離範圍內，禁止從事遙控無人機飛航活動；航空站或飛行場四周之一定距離範圍由民航局公告之。」

[5] 民用航空法修正條文第 99-14 條第 1 項：「從事遙控無人機飛航活動應遵守下列規定:一、遙控無人機距地表高度不得逾四百呎。二、不得以遙控無人機投擲或噴灑任何物件。三、不得裝載依第四十三條第三項公告之危險物品。四、依第九十九條之十七所定規則之操作限制。五、不得於人群聚集或露天集會遊行上空活動。六、不得於日落後至日出前之時間飛航。七、在目視範圍內操作，不得以除矯正鏡片外之任何工具延伸飛航作業距離。八、操作人不得在同一時間控制二架以上遙控無人機。九、操作人應隨時監視遙控無人機之飛航及其周遭狀況。十、應防止遙控無人機與其他航空器、建築物或障礙物接近或碰撞。」

[6] 民用航空法修正條文第 99-15 條第 1、2 項：「操作遙控無人機而致他人死傷，或毀損他人財物時，不論故意或過失，遙控無人機所有人應負賠償責任；其因不可抗力所生之損害，亦應負責。自遙控無人機上落下或投下物品，致生損害時，亦同。遙控無人機所有人將其遙控無人機交由他人操作所生之損害，由所有人及操作人負連帶賠償責任。」

賠償責任。

【管理 Tips】

遙控無人機所涉資安問題在於設計不當或駭客入侵所導致之危害，因遙控無人機之資料傳輸多採用未經加密之方式傳送，因此駭客入侵系統時，很容易便可截取其中資料，並成功取得遙控無人機的控制權，而導致人民生命及財產的損失之風險。

而當駭客入侵多具有一定目的，尤其現階段多家廠商已開始嘗試以遙控無人機作為運輸工具，包括運送血液、藥品或食品，更提高駭客對此類設備的攻擊意向，因此遙控無人機的資通安全問題已成為網路安全新興風險議題，故相關產品之開發單位於產品設計時，應將資通安全相關事項加入產品功能中，例如將遙控無人機的 Wi-Fi 數據進行加密，採取密碼保護機制，而使用者於產品使用時，亦須注意相關資通安全相關措施，以避免或抵禦駭客攻擊等侵害行為而導致之損失。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.11.2.8 無人看管的資訊設備

  (1)標準內容： 使用者應確保無人看管之設備具適切保護。

  (2)適用說明： 因遙控無人機可能之運行方式可能為人為操控，抑或為自動運行，而為確保遙控無人機設備之安全性，遙控無人機操作者應確保遙控無人機在運行過程中有適當保護措施，以新修法為例，應在目視範圍內操作，不得以除矯正鏡片外之任何工具延伸飛航作業距離，降低成為無人看管的資訊設備風險。

- A.13.1.2 網路服務之安全

  (1)標準內容： 應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部

或委外提供。

(2)適用說明： 遙控無人機設備若需透過網際網路等進行資料傳輸以為控制，應具備相當之通訊安全措施，例如對其 Wi-Fi 數據進行加密，以避免遭到駭客攻擊等入侵，並造成其他損害。

類別：資訊應用【案號：A10727】

金管會新春修法 悠遊卡網路刷卡通了

【焦點話題】

因應電子票證從「線下」走入「線上」發展，金管會預告「電子票證應用安全強度準則」部分條文修正草案，讓電子票證與電子支付機構的管理法規風險控管強度趨於一致。金管會銀行局表示，此次修正有兩大重點，一是為因應電子票證有使用於網際網路交易的業務需求，調整「線上即時交易」及「非線上即時交易」的用詞定義，以利業者遵循；二是為線上刷卡安全，新增電子票證交易「來源辨識性」防護措施的安全設計機制，擴大民眾使用電子票證之場域，讓電子票證也可用於網路交易及行動支付。此次還放寬電子票證之端末設備感應距離，以利快速完成交易，提升民眾支付便利性及優化使用體驗，將電子票證之端末設備感應距離由現行之 4 公分、6 公分以及 10 公分以下之不同限制，統一放寬至「10 公分以下」。

【參考資料來源：中時電子報，107/2/22】

【重點摘要】

1. 電子票證應用安全強度準則第 4 條規定將即時交易類型區分為「線上即時交易」及「非線上即時交易」，二者係以即時儲存地為區分，「線上即時交易」係指電子票證餘額及交易紀錄即時儲存於發行機構端，而將電子票證餘額及交易紀錄即時儲存於電子票證端者則為「非線上即時交易」。
2. 電子票證應用安全強度準則第 11 條規定，統一放寬電子票證端末設備感應距離至 10 公分以下，讓電子票證方便於行動支付使用，以利快速完成交易，提升持卡人交易便利性。

【法律觀點】

金融監督管理委員會(下稱金管會)在 107 年 2 月研訂「電子票證應用安全強度準

則」修正草案，並自同年 3 月 31 日起公布施行。本次修正重點，包括因應電子票證使用於網際網路交易之業務需求，修正納入電子票證餘額及交易紀錄之區分標準，並因應上開需求，新增對電子票證交易來源辨識性防護措施；放寬電子票證端末設備感應距離，以利快速完成交易，且為因應新興科技發展與新型態資安風險，並整合電子支付機構與電子票證發行機構管理法制之風險控管，修正各項安全需求之安全設計規定[1]。

依修正前電子票證應用安全強度準則之規定，原本的「線上即時交易」係指持卡人利用電子設備或通訊設備，透過各種網路型態，經由機構即時連線進行交易，而「非線上即時交易」則指持卡人持電子票證，不與發行機構即時進行連線，而利用各種介面類型於端末設備進行交易。本次為明確區分電子票證使用於網際網路線上交易與實體通路線下交易，因此修正定義，明定線上即時交易[2]除合法性之驗證須透過連線送回發行機構處理外，交易紀錄及電子票證餘額並須即時儲存於發行機構端；非線上即時交易[3]不需與發行機構即時連線，交易紀錄及電子票證餘額即時儲存於電子票證端。

為配合電子票證使用於網際網路交易，本次修法參酌電子機構交易安全設計規定，新增部份對電子票證交易來源辨識性防護措施[4]，修正網際網路應用系統設計[4]及行動裝置應用程式設計[5]之要求，以利業者明確遵循，進行相關業務規劃及風險

---

[1] 電子票證應用安全強度準則部份條文修正總說明四：參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」相關規定，修正發行機構提供「網際網路應用系統、行動裝置應用程式」、採用「條碼掃描技術、用戶代號及固定密碼來確認電子票證網際網路交易之訊息來源」等各項安全需求之安全設計規定。

[2] 電子票證應用安全強度準則第 4 條第 2 款：「線上即時交易：係指透過各種網路型態，經由特約機構、加值機構或直接與發行機構即時連線進行交易，並將電子票證餘額及交易紀錄即時儲存於發行機構端者，包含特約機構與發行機構間、加值機構與發行機構間、加值機構或特約機構與其所屬之端末設備間之即時訊息傳輸。」

[3] 電子票證應用安全強度準則第 4 條第 4 款：「非線上即時交易：係指利用各種介面類型，於端末設備進行交易，並將電子票證餘額及交易紀錄即時儲存於電子票證端，而不需與發行機構即時連線者。」

[4] 電子票證應用安全強度準則第 7 條，107 年 3 月立法理由一「因應電子票證使用於網際網路交易，參酌『電子支付機構資訊系統標準及安全控管作業基準辦法』第七條第三款有關 C 類交易安全設計規定，增修第三款第一目 C1 及第二目 C2 防護措施之安全設計規定，以確認各項交易之來源辨識性。」。

[4] 電子票證應用安全強度準則第 9 條第 6 款第 1 目。

[5] 電子票證應用安全強度準則第 9 條第 6 款第 3 目。

控管措施。又，為擴大民眾使用電子票證之場域，讓電子票證方便於行動支付使用，以利快速完成交易，因此統一放寬末端設備的感應距離為 10 公分以下，並明定發行機構應有效防止特約機構不當扣款[6]。

本準則修正後，就消費者端而言，應可有效提升民眾支付便利性及優化使用體驗，就業者端而言，若使業者在電子支付機構端與電子票證發行機構端採行統一作法，可藉之降低開發及維護成本。

【管理 Tips】

金管會為因應電子票證使用於網際網路交易之業務需求及新興科技之運用趨勢，兼顧電子票證使用便利性及安全性，並逐步整合電子支付機構與電子票證發行機構管理法制之風險控管，將二者相關內容調整趨於一致，以利建構實體與虛擬支付工具融合發展之支付生態圈[7]，因此修正電子票證應用安全強度準則，並貼近電子支付機構資訊系統標準及安全管控作業基準之規定，避免造成業者過大負擔，例如：加強對消費者與平台之間的身分驗證機制[8]，與帳號及固定密碼之安全設計規定[9]，皆為其所整合的部份。

準此，因電子票證發行機構得以掌握消費者的金流與資訊流，電子票證使用上的安全管理顯得尤為重要，其等將面臨許多資訊安全的隱憂，而本次修正係為確實保護交易安全，並兼顧資訊安全管理、業者法遵成本及消費者體驗等三方面。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.13.2.2　資訊傳送協議

---

[6] 電子票證應用安全強度準則第 11 條第 4 款。

[7] 電子票證應用安全強度準則部分條文 107 年 3 月修正總說明。

[8] 電子票證應用安全強度準則第 7 條第 2 款，本條係參照電子支付機構資訊系統標準及安全控管作業基準辦法第 7 條第 3 款，107 年 3 月第 7 條立法理由一。

[9] 電子票證應用安全強度準則第 14 條第 2 款，本條係參照電子支付機構資訊系統標準及安全控管作業基準辦法第 5 條第 2 項，107 年 3 月第 14 條立法理由。

(1)標準內容： 協議應詳細闡述組織與外部各方間營運資訊之安全傳送。

(2)適用說明： 組織進行資訊傳送時，必須驗證身分並確保文件內容的完整，在電子票證應用中，所對於身分驗證的要求可以密碼、實體設備、生物特徵等方式達成資訊傳送時之身分驗證。

- A.13.2.3 電子傳訊

(1)標準內容： 應適切保護電子傳訊時所涉及之資訊。

(2)適用說明： 在進行電子傳訊時，應視所涉及之資訊內容，採取必要且適當的方式以保護之，因電子票證可進行線上或線下交易，故所採取的保護方式亦隨之不同，如電子票證應用安全強度準則第 6 條，即針對線上即時消費交易、非線上即時消費交易、線上即時加值交易、非線上即時加值交易、票證款項移轉交易及帳務清算及結算交易等交易方式，個別採取適切的保護。

類別：資訊應用【案號：A10728】

立法院通過無人載具實驗條例，最長實驗 4 年

【焦點話題】

立法院為因應無人載具科技興起及國際發展趨勢於 107 年 11 月通過「無人載具科技創新實驗條例」，創新實驗時間原則為 1 年，最長可延至 4 年，並援引監理沙盒精神，營造合理且安全的創新測試場域，該條例未來經三讀通過、發布並生效後，於自駕車、無人機等進行創新實驗時，將可排除部分交通法規之適用，以促進相關產業發展。

【參考資料來源：科技新報，107/4/2】

【重點摘要】

1. 按無人載具科技創新實驗條例第 3、9 條規定，創新實驗係指以創新應用為目的之無人載具科技、服務及營運之實驗，申請創新實驗期間原則為一年，必要時可申請延長一年，有修正現行法必要性，可再額外延長，全程實驗期間最多以四年為限。

2. 無人載具之風險從資訊面而言，是可能遭駭客透過無線通訊入侵，造成事故發生；就技術面而言，無人載具尚屬發展中的科技，因此必須承受因技術尚未完備造成錯誤的風險；就法規面而言，仍有許多相關規定有待主管機關訂定，有意於此之組織亦應注意避免風險。

【法律觀點】

為鼓勵無人載具科技之研究發展與應用，建構完善且安全之創新實驗環境，以促進產業技術及創新服務之發展[1]，立法院通過無人載具科技創新實驗條例（下稱本條例）。依本條例之規定，創新實驗係指以創新應用為目的之無人載具科技、

[1] 無人載具科技創新實驗條例第 1 條：「為鼓勵無人載具科技之研究發展與應用，建構完善且安全之創新實驗環境，以促進產業技術及創新服務之發展，特制定本條例。」（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

服務及營運之實驗[2]。其申請創新實驗期間原則為一年，必要時可申請延長一年，若目的事業主管機關認定具有修正現行法必要性，可額外申請延長，以利申請者可繼續從事無人載具的創新服務及營運行為，全程實驗期間最多以四年為限[3]。且為排除法規障礙，本草案亦於實驗期間排除法律、法規命令或行政規則中之處罰規定[4]，以打造友善法規環境。

當然並非任何創新實驗均是無限制的准許，因此本草案亦規定申請創新實驗必須經由經濟部召開審查會議，邀集政府機關(構)代表、法律專家學者等[5]，針對創新實驗之創新性、法令、條件、資格、安全性及風險控管進行審查[6]。

而其中安全性及風險控管則是透過限制無線通訊應用及管理[7]、必要時的實地訪

---

[2] 無人載具科技創新實驗條例第 3 條第 3 款：「本條例用詞定義如下：三、創新實驗：指以創新應用為目的之無人載具科技、服務及營運之實驗。」(中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過)

[3] 無人載具科技創新實驗條例第 9 條：「主管機關核准辦理創新實驗之期間以一年為限。申請人得於該創新實驗期間屆滿六十日前，檢具理由並說明具體成效，向主管機關申請核准展延。　前項展延以一次為限，最長不得逾一年。但創新實驗內容經中央目的事業主管機關於審查會議認定應修正相關法律者，展延不以一次為限，其全部創新實驗期間不得逾四年。　主管機關應於原核准辦理創新實驗之期間屆滿前，作成核准或駁回展延申請之決定，並將決定以書面通知申請人。　前條第二項及第三項規定，於前項準用之。」(中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過)

[4] 無人載具科技創新實驗條例第 22 條第 1 項：「申請人於創新實驗期間，於主管機關核准創新實驗之範圍內辦理創新實驗者，其創新實驗行為不適用核准決定載明排除適用之法律、法規命令或行政規則規定。」(中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過)

[5] 無人載具科技創新實驗條例第 6 條第 1 項：「主管機關就創新實驗申請、第九條第一項申請展延及第十條申請變更之案件，應召開審查會議；會議成員，包括跨部會目的事業主管機關、中央、地方政府或相關機關（構）代表、法律專家學者及無人載具科技或產業領域之專家學者。」(中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過)

[6] 無人載具科技創新實驗條例第 7 條：「主管機關對於創新實驗之申請，應審查下列項目：一、具有創新性。二、確認屬於依現行法規無法取得目的事業主管機關許可或核准之範疇，及為進行創新實驗而應排除適用之法律、法規命令或行政規則。三、具有於開放性場域實驗之可行性，並已提出曾於模擬或封閉性場域測試之相關經驗及數據分析資料。四、可有效提升交通運輸服務或系統之效率、提升安全或降低經營及使用成本。五、已提出維持交通順暢及確保交通安全之因應措施。六、已評估潛在風險並定有相關因應措施，及其他與創新實驗計畫相關之安全或風險控管措施。七、建置參與實驗者及實驗利害關係人之保護措施，並預為準備適當補償。八、其他經審查會議決議應由申請人提出說明之事項。」(中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過)

[7] 無人載具科技創新實驗條例第 13 條：「可供創新實驗運用之無線電頻率與其地理範圍、實驗期限及其他相關條件，由中央目的事業主管機關公告之。　申請人取得創新實驗核准後，始得使用經核准指配之無線電頻率。創

查、人為方式介入控制之次數及原因之通報、實驗紀錄留存[8]、申請人於開始執行測試前之公告、場域安全及事故處理[9]、適當及充足之資訊安全措施[10]及個人資料保護[11]、參與實驗契約之相關規範[12]，等方式加以控管。

【管理 Tips】

無人載具科技係利用人工智慧與移動載具結合，發展各式創新科技，為人們民眾帶來便利，例如無人機送貨或無人車載客等不同創新作法，此科技之應用可以帶來龐大的經濟效益，同時亦隱藏不同層面之風險。

以資訊面而言，無人載具運作之控制係透過其搭載之感測器蒐集數據，傳輸到載具中進行分析、處理及決策，並透過網路將數據分析回傳至雲端進行調整，此時

新實驗所需電信管制射頻器材輸入管理、通訊干擾處理及其他相關電信監理事項，由通訊傳播主管機關辦理之。」（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

[8] 無人載具科技創新實驗條例第 14 條：「申請人應遵守本條例規定及主管機關核准創新實驗時要求申請人辦理之事項，並應依主管機關指示說明創新實驗情形。主管機關於必要時得實地訪查，申請人不得規避、妨礙或拒絕。

申請人於創新實驗期間，應每月通報以人為方式介入無人載具之控制權次數及原因，以作為主管機關評估創新實驗安全性之參考。 申請人應蒐集及留存創新實驗期間之紀錄資料，並應自創新實驗期間屆滿後留存至少三年。主管機關基於創新實驗安全或公共利益之必要，得命申請人提供相關資料。（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

[9] 無人載具科技創新實驗條例第 15 條：「申請人應於創新實驗開始執行測試前，於媒體或電子網站公告實驗相關資訊，並於無人載具或實驗場域以適當方式進行告示。 創新實驗期間發生安全事故時，申請人除應依相關法律負賠償責任外，並應主動即時暫停實驗且通報主管機關及交通主管機關事故之發生及後續處理方式。 前項事故發生後，主管機關經會同交通主管機關評估並確保安全無虞後，始得同意續行實驗。 有關申請人於創新實驗開始前之資訊公告與告示、事故發生後之通報程序、暫停實驗之程序及其他相關事項之辦法，由主管機關會同中央交通主管機關定之。」（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

[10] 無人載具科技創新實驗條例第 16 條：「申請人於創新實驗期間應配合創新實驗業務性質，採行適當及充足之資訊安全措施，確保資訊蒐集、處理、利用及傳輸之安全。（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

[11] 無人載具科技創新實驗條例第 17 條：「申請人蒐集、處理或利用個人資料，應遵守個人資料保護法之相關規定。」（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

[12] 無人載具科技創新實驗條例第 18 條：「申請人與參與實驗者於創新實驗期間訂定參與實驗契約，應本於公平合理、平等互惠及誠信原則。 前項契約條款顯失公平者，該部分條款無效；契約條款如有疑義時，應為有利於參與實驗者之解釋。 申請人於創新實驗期間應盡善良管理人之注意義務。」（中華民國 107 年 11 月 30 日立法院第 9 屆第 6 會期第 11 次會議通過）

恐遭第三方透過無線通訊駭入,所造成之危害將遠大於一般連網設施事故;其次，就技術面而言，無人載具尚屬發展中之科技，必須承受因技術尚未完備而發生錯誤之風險，以無人車為例，則必須承擔因技術未成熟所造成之人傷財損，這些均屬技術面需解決之課題；第三，就法規面而言，目前法規雖以大量鬆綁為導向，但依本草案之規定，諸如可供創新實驗運用之無線電頻率、地理範圍、實驗期限及其他條件、相關電信監理事項、資訊公告與告示、事故發生後之通報程序、暫停實驗之程序及其他相關事項之規定，仍有待主管機關訂定。

因此，對於有意於無人載具科技的廠商，對於資訊面、技術面以及法規面均應有所留意，以降低創新實驗時所可能產生之風險。

【相關標準】

ISO27001：2013（CNS27001）

- A.13.2.3　電子傳訊

  (1)標準內容：　應適切保護電子傳訊時所涉及之資訊。

  (2)適用說明：　無人載具係需要透過網際網路進行資料傳輸,因此在進行資料傳輸時應具備適當的保護,以避免遭到駭客攻擊等入侵導致相關損害。

- A.18.1.1　適用之法規及契約的要求事項之識別

  (1)標準內容：　對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

  (2)適用說明：　組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。目前無人載具創新實驗條例已送立法院審查，有意發展無人載具之組織，應適時瞭解後續發展，以適時申請佔得先機。

類別：資訊應用【案號：A10729】

首例金融創新實驗 已遞件申請

【焦點話題】

金融管理機關為推動金融科技，於 107 年初完成立法並公布「金融科技發展與創新實驗條例」，其相關子法亦於同年 4 月底陸續施行，台灣成為全球首個成文法推動金融監理沙盒之國家。金融管理機關指出，監理沙盒措施可提供產業與政府間之溝通對話機制、法規調適機制、扶植金融創新及加速創新商轉等功能。而該條例上路後，於 107 年 6 月已出現首宗遞件案與 36 件諮詢輔導案件，其中不乏科技業者與金融業者，送件後，需經過審查委員會為期 60 天之審核後進行准駁，最快於 107 年第三季即將有第一個金融創新實驗案例上路。

【參考資料來源：中國時報，107/6/19】

【重點摘要】

1. 按照金融科技發展與創新實驗條例第 3 條規定，創新實驗係指以科技創新或經營模式創新方式從事屬於需主管機關許可、核准或特許之金融業務實驗。次按金融科技發展與創新實驗條例第 9 條規定，其申請創新實驗期間原則以一年為限，必要時得申請延長六個月，有修正現行法必要性，可再額外延長，全程實驗期間不得逾三年。

2. 為使創新實驗能從實驗階段得以正式上路，主管機關認定創新實驗內容具有創新性、有效提升金融服務之效率、降低經營及使用成本或提升金融消費者及企業之權益時，亦有義務針對申請案所涉及之管制法令進行檢討研修，如認有修正必要時，就必須在創新實驗屆滿後三個月內提交修正草案報院審查，以排除法規障礙。

【法律觀點】

透過當代科技創新，使金融服務或商品之效率性與普及性更為提升的「金融科技」，

已成為全球創新產業之新趨勢。因此，為建立安全之金融科技創新實驗(以下簡稱創新實驗)環境，以科技發展創新金融商品或服務，促進普惠金融及金融科技發展，並落實對參與創新實驗者(以下簡稱參與者)及金融消費者之保護[1]，因此我國於 107 年 1 月通過並公佈「金融科技發展與創新實驗條例」(下簡稱本條例)。

所謂創新實驗，係指以科技創新或經營模式創新方式從事屬於需主管機關許可、核准或特許之金融業務實驗[2]。其申請創新實驗期間原則以一年為限，必要時得申請延長六個月，若主管機關認定創新實驗內容具有修正現行法必要性，可再額外延長，以利申請者可繼續從事金融科技的創新服務及營運，然全程實驗期間不得逾三年[3]。

為排除法規障礙，本條例於實驗期間得排除相關法規之處罰[4]，以打造友善法規環境。而主管機關除受理創新實驗之申請外，當認定創新實驗內容具有創新性、有效提升金融服務之效率、降低經營及使用成本或提升金融消費者及企業之權益時，亦有義務針對申請案所涉及之管制法令進行檢討研修，如認有修正之必要時，須於創新實驗屆滿後三個月內提交修正草案報行政院審查[5]。

---

[1] 金融科技發展與創新實驗條例第 1 條。

[2] 金融科技發展與創新實驗條例第 2 條。

[3] 金融科技發展與創新實驗條例第 9 條：「主管機關核准辦理創新實驗之期間以一年為限。申請人得於該創新實驗期間屆滿一個月前，檢具理由向主管機關申請核准延長；延長以一次為限，最長不得逾六個月。但創新實驗內容涉及應修正法律時，其延長不以一次為限，全部創新實驗期間不得逾三年。 主管機關應於原核准辦理創新實驗之期間屆滿前，作成核准或駁回前項申請之決定，並將決定以書面通知申請人。」。

[4] 金融科技發展與創新實驗條例第 26 條：「申請人於創新實驗期間，依主管機關核准創新實驗之範圍辦理創新實驗者，其創新實驗行為不適用下列處罰規定：「一、銀行法第一百二十五條。二、電子支付機構管理條例第四十四條或第四十六條。三、電子票證發行管理條例第三十條第一項、第三項、第四項或第二項有關違反同條例第四條第一項規定。四、信託業法第四十八條。五、票券金融管理法第六十一條有關違反同法第六條規定。六、證券交易法第一百七十五條第一項有關違反同法第十八條第一項、第四十四條第一項規定，或第一百七十七條第一項有關違反同法第四十五條第二項規定。 七、期貨交易法第一百十二條第五項第三款至第五款。 八、證券投資信託及顧問法第一百零七條或第一百十條。 九、保險法第一百六十七條或第一百六十七條之一。」。

[5] 金融科技發展與創新實驗條例第 17 條：「創新實驗具有創新性、有效提升金融服務之效率、降低經營及使用成本或提升金融消費者及企業之權益者，主管機關應參酌創新實驗之辦理情形，辦理下列事項：一、檢討研修相關金融法規。二、提供創業或策略合作之協助。三、轉介予相關機關（構）、團體或輔導創業服務之基金。

然而，創新實驗之申請亦不宜毫無審查機制，因此本條例規定申請創新實驗必須經由主管機關召開審查會議，邀集專家、學者及相關機關(構)代表[6]，根據創新實驗申請之範圍、期間及規模，針對創新性[7]、提昇金融服務效率[8]、風險評估[9]、參與者之保護措施[10]等項目進行實質審查[11]，主管機關並訂定「金融科技創新實驗管理辦法」以說明上開各項目之意義，使有意於創新實驗者，能真正瞭解應注意事項。

近年來，許多金融先進國家為因應金融科技發展趨勢，提出監理沙盒制度，賦予業者在風險規模可控的環境內，測試其金融創新產品、業務、商業模式及供應機制，且其所從事活動不受一般法規之限制，我國此次立法立意亦在於此，希冀能發展台灣成為國際創新基地，培育出國際級企業及專業的金融創新人才。

【管理 Tips】

從定義上來說，任何與金融相關的科技皆可稱為金融科技，透過科學、材料和人力資源，以執行金融服務，以及包括網路銀行、線上支付、理財機器人等皆屬金融科技之一環。。而金融科技或多或少會利用網際網路執行金融服務，於帶來龐大的經濟效益之同時，亦隱藏許多資訊安全層面之風險。

因此，組織欲申請金融創新實驗時，應參考金融科技創新實驗辦法，依規定建立管理制度。首先，組織在申請創新實驗時，必須進行風險評估，以及建立包括個

主管機關認需修正相關金融法律時，至遲應於創新實驗屆滿後三個月內，完成相關金融法律之修正條文草案，並報請行政院審查。」

[6] 金融科技發展與創新實驗條例第 6 條。

[7] 金融科技創新實驗管理辦法第 6 條。

[8] 金融科技創新實驗管理辦法第 7 條。

[9] 金融科技創新實驗管理辦法第 8 條。

[10] 金融科技創新實驗管理辦法第 9 條。

[11] 金融科技發展與創新實驗條例第 7 條：「為促進金融科技創新發展，並維護公共利益，主管機關對於創新實驗之申請應根據創新實驗之範圍、期間及規模，審酌下列要件： 一、屬於需主管機關許可、核准或特許之金融業務範疇。 二、具有創新性。 三、可有效提升金融服務之效率、降低經營及使用成本或提升金融消費者及企業之權益。 四、已評估可能風險，並訂有相關因應措施。 五、建置參與者之保護措施，並預為準備適當補償。 六、其他需評估事項。」

人資料保護以及資訊安全維護之管理機制[12]。其次，在創新實驗過程中也必須確保資訊之蒐集、處理、利用及傳輸之安全，並防止非法入侵、取得、竄改、毀損業務紀錄或個人資料，及建置第三方入侵資訊系統對參與者之通報及損害賠償機制[13]。而後，當創新實驗期間屆滿後，組織必須將創新實驗結果函報主管機關由主管機關召開評估會議進行結果評估，此時必須就參與者之權益保障及資訊安全控管作業提出說明[14]。

【相關標準】

ISO27001：2013（CNS27001）

● 6.1.2 資訊安全風險評鑑

(1)標準內容： 組織應定義及應用資訊安全風險評鑑過程於下列事項中。

(a) 建立及維持包括下列準則之資訊安全風險準則。

(1) 風險接受準則。

(2) 履行資訊安全風險評鑑之準則。

(b) 確保重複之資訊安全風險評鑑產生一致、有效及適於比較之結果。

(c) 識別資訊安全風險。

(1) 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與漏失資訊之機密性、完整性及可用性相關聯之風險。

(2) 識別風險擁有者。

[12] 金融科技創新實驗管理辦法第 14 條。

[13] 金融科技創新實驗管理辦法第 18 條。

[14] 金融科技發展與創新實驗條例第 16 條。

(d)分析資訊安全風險。

(1)評鑑若 6.1.2(c)(1)中所識別之風險實現時，可能導致之潛在後果。

(2)評鑑 6.1.2(c)(1) 中所識別之風險發生的實際可能性。

(3)決定風險等級。

(e)評估資訊安全風險。

(1)以 6.1.2(a)中所建立之風險準則，比較風險分析結果。

(2)訂定已分析風險之風險處理優先序。

組織應保存關於資訊安全風險評鑑過程之文件化資訊。

(2)適用說明： 建立風險評鑑是組織於無法預見之風險發生時，所應該進行的必要程序，以避免造成損害之發生及擴大。而金融科技創新實驗管理辦法亦已明確規定申請人必須落實風險管理機制，藉由風險管理，以兼顧金融市場秩序及保護參與者之權益。

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織應瞭解並依循適用之法令，執行相關業務，以避免觸法。目前金融科技發展與創新實驗條例已施行，相關配套辦法亦已上路，組織如欲投入相關產業，應熟悉該條例之

規定。

類別：資訊應用【案號：A10730】

用聲音完成電子簽章 法人獲獎

【焦點話題】

106 年度台北國際發明暨技術交易展，發明競賽獎正式揭曉，國內資訊工業法人計有 3 項技術獲發明競賽獎。其中，將語音生物特徵應用於電子文件簽章，更獲得「鉑金獎」肯定。此專利應用語音生物特徵（Biometrics）建立簽署者自然人與電子文件簽章之間的高強度關聯性，有效將生物特徵轉化於應用安全層面，並符合電子簽章法的高安全需求，而可進行電子文件簽章。

【參考資料來源：中央社，106/9/30】

【重點摘要】

1. 依電子簽章法第 9 條與第 10 條規定，以數位簽章簽署電子文件時，除需雙方同意外，亦應以經主管機關核定或許可之憑證機構依法簽發之憑證為之。
2. 電子簽章法係以「電子簽章」為立法基礎，而不以「數位簽章」為限，其目的即在於因應諸如生物科技等電子鑑別技術之創新發展，因此利用任何電子技術製作之電子簽章及電子文件，只要功能與書面文件及簽名、蓋章相當，皆可使用。

【法律觀點】

電子簽章法通過後，原本應以書面作為之法律行為，只要透過當事人約定，而電子文件內容可完整呈現，且日後取出可供查驗[1]，又無法令或行政機關所公告排除適用電子文件或電子簽章時[2]，電子簽章與電子文件即可取代傳統簽名、蓋章

[1] 電子簽章法第 4 條第 2 項：「依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。」

[2] 電子簽章法第 4 條第 3 項本文：「前二項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。」；同法第 6 條第 3 項本文：「第一項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。」；同法第 9 條第 2 項本文：「前項規定得依法令或行政機關之公告，排除其適用或就其應用

與書面，並具備法律效力。

端視電子簽章法第 2 條第 2 款規定：「電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。」，同條第 3 款規定：「數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。」等規定，可知，數位簽章係屬電子簽章其中一類。

而同法第 9 條第 1 項規定：「依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。」及同法第 10 條規定：「以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第一項之效力：一、使用經第十一條核定或第十五條許可之憑證機構依法簽發之憑證。二、憑證尚屬有效並未逾使用範圍。」因此，以數位簽章簽署電子文件時，除需雙方同意外，應以經主管機關核定或許可之憑證機構依法簽發之憑證為之。

然，因數位簽章僅係電子簽章之一種，電子簽章法立法時即說明，基於技術中立性原則[3]，電子簽章法係以「電子簽章」為立法基礎，而不以「數位簽章」為限[4]，其目的即在於因應諸如生物科技等電子鑑別技術之創新發展。利用任何電子技術製作之電子簽章及電子文件，只要功能與書面文件及簽名、蓋章相當，皆可使用[5]。以現今科技而言，包括指紋、虹膜甚至是聲紋等方式，只要能夠辨識及確認電子文件簽署人身分、資格及電子文件真偽，在雙方同意下均有可能作為電子簽章之依據。

隨著資訊化的時代，人與人之間不一定要實體接觸到才能進行各項業務，透過電

技術與程序另為規定。但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。」

[3] 技術中立原則係指在制定法律原則方向須具有前瞻性，不可獨厚特定技術，在立法上不能對技術發展造成限制或偏袒效果，因此我國電子簽章法採取較廣之定義，將任何可確保資料在傳輸或儲存過程中之完整性及鑑別使用者身分之技術，皆可用來製作電子簽章，並不以「數位簽章」為限。

[4] 立法院公報第 90 卷第 38 期委員會紀錄第 177 頁，數位簽章與電子簽章兩者指涉的內容並不一樣，數位簽章係專指以「非對稱型密碼技術」所製作之電子簽章，電子簽章之意義則較廣泛，例如可以個人的生物特徵如指紋、眼紋及聲紋來達到簽章之目的。

[5] 電子簽章法立法總說明。

子簽章等方式進行社會活動，有助於提昇民眾使用各項服務的便利性，更有利業者之服務推動及競爭力提升，現今科技技術不斷創新，於可預見的未來，使電子簽章之應用將更為便利。

【管理 Tips】

因電子簽章法要求「以」數位簽章技術簽署電子文件時，必須是憑證機構依法簽發，方具有依法令規定應簽名或蓋章之效力，但並未限制電子簽章方式簽署時之處理方式，因此組織如欲透過其他「電子簽章」方式為簽名或蓋章時，當相對人同意時，亦非不得為之。

依電子簽章法第 9 條亦規定，在公平合理的情形下得依法令或行政機關之公告，排除電子簽章之適用或排除適用電子簽章之相關應用技術與程序[6]。而目前各機關亦針對其所主管之法令予以公告排除適用事項，以財政部為例，將擔保品之提供...等事項作為排除適用電子文件及電子簽章之項目[7]，而金管會亦將公開公司發行公司年報...等事項作為排除適用之項目[8]。

無論是以數位簽章或聲紋辨識等方式所作之電子簽章，其目的皆為提高身分驗證之控制點，使其更具安全防護功效。組織在實施以電子簽章替代紙本簽章時，應先瞭解其適法性，是否可以採用電子簽章替代，再因應個別情況尋找合適之電子簽章方式，而該方式如以具備適當的加密技術，確保資訊具備機密性、完整性、不可否認性與鑑別性等保護時，宜可作為適法之電子簽章。**【相關標準】**

ISO27001：2013（CNS27001）

- A.10.1.1 使用密碼式控制措施

(1)標準內容： 應發展及落實政策，關於資訊保護之密碼式控制措施的使用。

[6] 電子簽章法第 9 條第 2 項：「前項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。」

[7] 財政部 107 年 3 月 30 日台財關字第 1071006706 號函釋。

[8] 金融監督管理委員會 106 年 12 月 20 日金管證發字第 10600477961 號函釋。

(2)適用說明： 即指是適當的加密控制措施，目的在於適當的加密措施，以確保資訊具備機密性、完整性、不可否認性與鑑別性等保護時，以作為適法之電子簽章。

- A.18.1.1 適用之法規及契約的要求事項之識別

(1)標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2)適用說明： 組織應了解並依其適用之法令，進行相關業務之管理及執行，避免觸法。本案例中，就數位簽章與電子簽章兩者各有不同限制，組織應就其適用法律清楚識別。

伍、自我評量

是非題

1. (O) 德德一時貪圖好玩，利用最新勒索病毒 HowHow 癱瘓台北市政府內部系統，雖未造成市府重大損失，但德德的行為仍涉犯刑法第 359 條破壞電磁紀錄罪。**【資訊保護 S10701】**

   解析：依刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」，另按刑法第 361 條規定：「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。」且因台北市政府為公務機關，故德德恐觸犯刑法並得加重其刑。

2. (O) 在我國，即便透過合法程序蒐集個人資料，亦不代表該個人資料即可任意使用。**【資訊保護 S10702】**

   解析：依個人資料保護法第 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。」，另按同法第 20 條第 1 項規定：「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。」綜上而言，合法蒐集之個人資料不得任意利用。

3. (O) 國際間，將智慧型手機安全分層區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層。**【資訊保護 S10703】**

   解析：依據智慧型手機系統內建軟體資通安全檢測技術規範 2.2 明訂：「本規範依據國際間對智慧型手機安全之分層概念，將智慧型手機區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層五個層別，考量不同層別可能面臨的資訊安全風險有所不同，故對各層別分別訂定檢測項目。各檢測層別之安全性說明如下：**資料層**（Information/Data）：資料之安全性主要包含資料的傳送、儲存或使用等相關安全，並應確保使用者資料避免遭系統內建軟體未經授權之蒐集、分享、使用、刪除、竄改及儲存。；**應用程式層**（APPs）：應用程式之安全性主要包含程式信任來源、執行授權等相關安全，並應確保內建軟體避免未經授權存取系統資源。；**通訊協定層**（Protocol）：通訊協定之安全性主要包含無線傳

輸技術及通訊協定等相關安全，並應確保使用者對資料之傳輸、周邊設備之連接的可控管性。；**作業系統層**（Operating System）：作業系統之安全性主要包含作業系統相關服務與身分辨識等相關安全，並應確保作業系統對系統資源之保護、提醒，並讓使用者於知情的狀況下進行更新。**硬體層**（Hardware）：硬體之安全性主要包含金鑰與演算模組等安全，並應確保金鑰管理、存放之保護，及演算法之安全強度符合國際規範，並讓使用者於知情的狀況下進行更新。」故答案為正確。

4. (O) 近年來個人資料外洩事故頻傳，依照我國個人資料保護法之規定，若組織發生外洩事故時，應查明後利用適當方式通知當事人。**【資訊保護 S10704】**

   解析：按個人資料保護法第 12 條規定：「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。」故答案為正確。

5. (O) 資訊服務採購如內含具敏感性或國安(含資安)疑慮之業務範疇，不得允許陸資資訊服務業者參與。**【資訊保護 S10705】**

   解析：依行政院公共工程委員會工程企第 10400024613 號函要求：「機關辦理資訊服務採購，如屬經濟部投資審議委員會公告『具敏感性或國安(含資安)疑慮之業務範疇』，於招標文件載明不允許經濟部投資審議委員會公告之陸資資訊服務業者參與，屬投標廠商資格與特殊或巨額採購認定標準第 4 條第 1 項第 6 款規定情形。」故答案為正確。

6. (X) 台北市政府為行政訴訟委任案而辦理公開招標，其承辦人應須將招標公告刊登於市府大廳公告資訊欄。**【資訊保護 S10706】**

   解析：依政府採購法第 27 條第 1 項：「機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報並公開於資訊網路。公告之內容修正時，亦同。」承辦人應將招標公告刊登於政府採購公報及資訊網路，故答案為錯誤。

7. (O) 電子郵件詐騙盛行，民眾應對於電子郵件保持警覺，不隨意開啟可疑電子郵件並下載其附件檔或點擊郵件內附的超連結，得有效降低風險。**【資訊保護 S10707】**

   解析：電子郵件詐騙又稱變臉詐騙，其犯罪集團透過社交工程等方式入侵電腦或電子郵件，模仿組織溝通風格待時機成熟進行詐騙。則常見的社交工程工程：電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼或利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式，故答案正確。

8. (X) 小方為能順利謀求高薪，遂利用自己在公司掌握的技術資料投奔新東家，並將該資料攜至位於中國之新東家使用，係因該資料為境外使用，並未破壞國內之市場規則，小方

應屬合法。**【資訊保護 S10708】**

解析：依營業秘密法第 2 條規定：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」及同法第 13-2 條第一項：「意圖在外國、大陸地區、香港或澳門使用，而犯前條第一項各款之罪者，處一年以上十年以下有期徒刑，得併科新臺幣三百萬元以上五千萬元以下之罰金。」是以，小方之行為係屬違法，故答案為錯誤。

9. (X) 為健全國家機密保護制度，並確保國家安全及利益，凡是公務資訊皆應列為國家機密，並依法保管之。**【資訊保護 S10709】**

解析：依國家機密保護法第 2 條：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」然而，並非所有公務資訊皆與國家安全或利益相關，故答案為錯誤。

10. (O) 歐盟最嚴格的個人資料保護規定來勢洶洶，無論組織是否設立於歐盟境內，只要與其交易而有蒐集到歐盟居民之個人資料時，即必須遵守 GDPR。**【資訊保護 S10710】**

解析：依照 GDPR 法規，無論是否個人資料處理活動發生於歐盟境內，只要涉及歐盟居民之個人資料，即應遵守該規定。

11. (O) 我國於 107 年 6 月公布資通安全管理法，並針對公務機關及特定非公務機關加以規範，其中特定非公務機關係包括關鍵基礎設施者、公營事業及政府捐助之財團法人。**【資訊保護 S10711】**

解析：依照資通安全管理法第 3 條第 6 款規定：「特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」故答案為正確。

12. (O) 公務機關透過有效的資通安全演練作業，可降低災害發生時所造成的損害程度，而其演練作業項目可能包括社交工程演練、資安事件通報及應變、網路攻防演練、情境演練等。。**【資訊保護 S10712】**

解析：依照資通安全事件通報及應變辦法第 18 條規定：「公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：一、社交工程演練。二、資通安全事件報及應變演練。三、網路攻防演練。四、情境演練。五、其他必要之演練」故答案為正確。

13. (X) 金管會為提升銀行業者對於資訊安全之重視，明定台灣所有銀行業者應設立獨立法

遵及資安單位，並將資訊安全執行情形做成資訊安全整體執行情形聲明書提報董事會。**【資訊保護 S10713】**

解析：依照金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條第 2 項規定：「銀行業前一年度經會計師查核簽證之資產總額達新臺幣一兆元以上者，應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管。」及同條第 3 項：「銀行業資訊安全專責單位負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，由資訊安全專責單位主管與董（理）事長（主席）、總經理、總稽核聯名出具資訊安全整體執行情形聲明書（附表二），並於會計年度終了後三個月內提報董（理）事會。」綜上可知，僅規範資產總額達新臺幣一兆元以上者的銀行業者，故答案為錯誤。

14. (X) 依我國現行法規定，所有性侵害或性剝削加害人基於公共利益及社會安全，政府皆須公布其姓名及照片。**【資訊公開 D10714】**

解析：依我國性侵害犯罪防治法第 9 條規定，中央主管機關針對性侵害事件須建立檔案資料，原則上應予保密，惟依同法第 23 條第 4 項之規定，在特定情形下，為維護公共利益及社會安全之目的得供特定人員查閱。故本題所稱所有性侵害或性剝削加害人基於公共利益及社會安全，地方政府皆須公布其姓名及照片，有誤。

15. (X) 在我國，為保障人民之隱私權，司法院裁判書不能公開。**【資訊公開 D10715】**

解析：法院組織法第 83 條第 1 項：「各級法院及分院應定期出版公報或以其他適當方式，公開裁判書。但其他法律另有規定者，依其規定。」故答案為錯誤。

16. (X) 為增進人民對公共事務之瞭解、信賴及監督並促進民主參與，政府資訊應當全部公開之，不得有例外。**【資訊公開 D10716】**

解析：依政府資訊公開法第 18 條規定：政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。……九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。」綜上所述，政府公開資訊因應各種情況得限制公開或不予公開，故答案為錯誤。

17. (O) 隨著政治檔案條例草案通過，未來政黨、附隨組織及黨營機構所持有的政治檔案，皆應將收回國有。**【資訊公開 D10717】**

解析：依政治檔案條例草案第 6 條第 1 項：「政黨、附隨組織及黨營機構持有政治檔案，經促進轉型正義委員會審定為國家檔案者，應於該會指定期限內移歸檔案局管理，並由該

會、檔案局及持有檔案之政黨、附隨組織及黨營機構依審定清冊作成紀錄。」故答案為正確。

18. (X) 民眾參與環保署環境影響評估會議並於討論過程中錄音錄影，該影音資料係屬政府資訊。**【資訊公開 D10718】**

解析：依政府資訊法第 3 條規定：「本法所稱政府資訊，指政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。」綜上所述，政府資訊應為政府機關於職權範圍內而作成，故答案為錯誤。

19. (X) 為避免民眾恐慌，公私場所具有經中央主管機關指定公告之固定污染源，如有設置或變更等，皆不得公開相關資訊。**【資訊公開 D10719】**

解析：依照空氣污染防治法第 24 條第 1 項規定：「公私場所具有經中央主管機關指定公告之固定污染源，應於設置或變更前，檢具空氣污染防制計畫，向直轄市、縣(市)主管機關或中央主管機關委託之機關申請及取得設置許可證，並依許可證內容進行設置或變更。前項固定污染源設置或變更後，應檢具符合本法相關規定之證明文件，向直轄市、縣(市)主管機關或經中央主管機關委託之機關申請及取得操作許可證，並依核發之許可證內容進行操作。　直轄市、縣(市)主管機關或經中央主管機關委託之機關，應於前二項許可證核發前，將申請資料登載於公開網站，供民眾查詢並表示意見，作為核發許可證之參考。固定污染源設置與操作許可證之申請、審查程序、審查原則、公開內容、核發、撤銷、廢止、中央主管機關委託或終止委託及其他應遵行事項之辦法，由中央主管機關定之。」，顯見具經中央主管機關指定公告之固定污染源者，於設置或變更應具許可證，而相關發政機關應於發證前將相關資料公開，故答案為錯誤。

20. (X) 公司為保障商業秘密外洩，得安裝監控軟體預防外洩風險。**【資訊監察 M10720】**

解析：依刑法第 315-1 條規定：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」及通訊保障及監察法第 24 條第 1 項規定：「違法監察他人通訊者，處五年以下有期徒刑。」綜上述而言，即便為保護商業機密而安裝監控軟體，仍會側錄他人通訊紀錄，有侵害隱私之虞，屬非法監察之範疇，故答案為錯誤。

21. (O) 按我國現行法規，檢察官如欲聲請調取票必須符合重罪原則及必要性。**【資訊監察 M10721】**

解析：依通訊保障及監察法第 11-1 條第 1 項規定：「檢察官偵查最重本刑三年以上有期徒刑之罪，有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性時，除有急迫情形不及事先聲請者外，應以書面聲請該管法院核發調取票。聲請書之應記載事項，準用前條第一項之規定。」故答案為正確。

22. (X) 檢察官偵查重大案件需要掌握嫌疑犯之位置資訊，係因位置資訊並未受到通保法規範，故得逕行調取之。**【資訊監察 M10722】**

解析：依通訊保障及監察法第 3-1 條第 1 項規定：「本法所稱通信紀錄者，謂電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。」故答案為錯誤。

23. (X) 在我國，通訊監察之方法係以截收監聽、錄音、錄影、攝影、開拆、檢查、影印等，必要時得聲請於私人住宅裝設監視器等監察設備。**【資訊監察 M10723】**

解析：依照通訊保障及監察法第 13 條第 1 項規定：「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」故答案為錯誤。

24. (X) 奧克蘭於 2013 成立區域警示中心，建立多重感測監控系統，為利執法機關提高效率，執法單位得向隱私諮詢委員會登記後，始得獲取個人隱私之資訊。**【資訊監察 M10724】**

解析：奧克蘭市成立隱私諮詢委員會，由各市議會區的自願專員組成，其職責包括提供針對監察設備購買時的諮詢與技術援助、為隱私與資訊保護相關立法起草、對現有與規劃中的監察設備提交年度策略報告、提供其他地區隱私立法與資訊、召開公聽會、就區域警示中心的功能及政策進行審查，執法機關亦需要經過隱私諮詢委員會同意後，方取得個人隱私之資訊。

25. (X) 太陽花社區管委會為保障住戶安全，於大門及中庭各處架設監視器，管委會此舉則違反個人資料保護法規定。**【資訊應用 A10725】**

解析：依個人資料保護法第 51 條規定：「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。」綜上而言，利用監視器以影音資料的方式蒐集個人資料，但不與其他個人資料結合，此不受個人資料保護法之規範。

26. (O) 遙控無人機是目前資安熱議話題，未來所有無人機玩家無須經過測驗合格取得操作

證，仍得操作。**【資訊應用 A10726】**

解析：依民用航空法第 99-10 條第 2 項規定：「下列遙控無人機之操作人應經測驗合格，由民航局發給操作證後，始得操作：一、政府機關（構）、學校或法人所有之遙控無人機。二、最大起飛重量達一定重量以上之遙控無人機。三、其他經民航局公告者。」故答案為有誤。

27. (O) 電子票證使用於網際網路交易越來越普及，加強消費者與平台間的身分驗證機制，可有效強化資訊安全之控款。**【資訊應用 A10727】**

解析：因消費者的金流或資訊流皆掌握於電子票制發行機構者中，因此電子票證發行機構將面臨許多資訊安全的隱憂，而金管會於 107 年 3 月修正電子票證應用安全強度準則，其目的除為提升使用之便利性外，更在於整合因應電子支付機構與電子票證發行機構之安全性控管，例如加強消費者之身分驗證機制等。故答案為正確。

28. (O) 近年來各式無人載具科技與相關創新應用蓬勃發展，未來台灣業者進行自駕車或無人機之創新實驗時，得部分排除相關監理規範之適用。**【資訊應用 A10728】**

解析：行政院於 107 年 5 月 17 日通過經濟部擬具的「無人載具科技創新實驗條例」草案，將送請立法院審議。對於針對創新實驗之申請，規定主管機關應確認屬於依現行法規無法取得目的事業主管機關許可或核准之範疇，及為進行創新實驗而應排除適用之法律、法規命令或行政規則。

29. (O) 金融科技發展與創新實驗條例之立法目的係參考國外的監理沙盒制度，為我國建立安全之金融科技創新實驗環境，賦予業者在風險規模可控的環境內，測試其金融創新產品、業務、商業模式及供應機制，且不受一般法規之限制，更能進一步推動金融科技發展。**【資訊應用 A10729】**

解析：監理沙盒措施可提供產業與政府間溝通對話機制、法規調適機制、扶植金融創新及加速創新商轉等功能，是以台灣為利金融科技發展，遂於 107 年初立法並公布《金融科技發展與創新實驗條例》，並於同年陸續施行子法。

30. (X) 電子簽章係指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽，然數位簽章係使用個人生物特徵達到簽章目的，故數位簽章非屬電子簽章之範疇。**【資訊應用 S10730】**

解析：依照立法院公報第 90 卷第 38 期委員會紀錄第 177 頁，數位簽章與電子簽章兩者指涉的內容並不一樣，數位簽章係專指以「非對稱型密碼技術」所製作之電子簽章，電子簽章之意義則較廣泛，例如可以個人的生物特徵如指紋、眼紋及聲紋來達到簽章之目的，

故答案為錯誤。

選擇題

1. (3) 對於資訊安全之防護，請問下列何者錯誤?(1)組織之員工應定期接受其工作職能之相關訓練。(2)應實作防範惡意軟體之偵測、預防及復原控制措施。(3)應定期關閉防毒軟體。(4)應管理及控制網路。**【資訊保護 S10701】**

   解析：選項(3)應為 ISO 27001 資訊備份 A.12.3.1 :「應議定之備份政策，定期取得資訊、軟體及系統的影像備份複本，並測試之。」

2. (1) 我國個人資料法規定組織應於蒐集個人資料時，必須對當事人進行告知事項。請問下列關於告知事項內容何者有誤?(1)組織應告知個人資料的儲存方式。(2)組織應告知個人資料利用的期間。(3)組織應告知當事人權利行使方式。(4)組織應告知蒐集的目的。**【資訊保護 S10702】**

   解析：依個人資料保護法第 8 條規定：「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。」，故選項(1)並非法律規定的範疇。

3. (4) 根據我國電信法要求，我國販售的電信終端設備應通過技術規範。請問，關於訂定技術規範下列何者為非? (1)電氣安全，防止網路操作人員或使用者受到傷害。(2)第一類電信事業設置之電信機線設備與使用者連接之終端設備，應有明確之責任分界。(3)不得損害第一類電信事業之電信機線設備或對其機能造成障礙。(4)電磁相異。**【資訊保護 S10703】**

   解析：依電信法第 42 條第 3 項規定：「第一項技術規範之訂定，應確保下列事項：一、不得損害第一類電信事業之電信機線設備或對其機能造成障礙。二、不對第一類電信事業之電信機線設備之其他使用者造成妨害。三、第一類電信事業設置之電信機線設備與使用者連接之終端設備，應有明確之責任分界。四、電磁相容及與其他頻率和諧有效共用。五、電氣安全，防止網路操作人員或使用者受到傷害。」故選項(4)應為電磁相容。

4. (4) 依照個人資料保護法規定，當個資外洩事故發生時，組織應查明後通知當事人，請問組織可採取何種方式進行「通知」?(1)傳真。(2)電子郵件。(3)簡訊。(4)以上皆可能。**【資訊保護 S10704】**

   解析：按個人資料保護法施行細則第 22 條第 1 項規定：「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。」故應選選項(4)以上皆可能。

5. (4) 我國政府機關於辦理資訊及通訊安全相關採購案，針對廠商之資訊安全責任何者錯誤？(1)應遵守機關資訊安全管理及保密規定。(2)廠商提供之軟體進行版本管理。(3)廠商交付之軟體，應先行檢查是否內藏惡意程式。(4)若發生資安事件，廠商自行處理，得不需要通報機關。**【資訊保護 S10705】**

解析：依照行政院公共工程委員會所訂定之資訊服務採購契約範本第 16 條第 19 項第 5 款規定：「廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。」故選項(4)為錯誤。

6. (3) 政府機關辦理採購，請問下列何者錯誤?(1)招標文件於公告前應予保密。(2)底價於開標後至決標前，仍應保密。(3)機關對於廠商投標文件，原則於決標後得公開之。(4)不得於開標前洩漏底價。**【資訊保護 S10706】**

解析：依政府採購法第 34 條規定：「機關辦理採購，其招標文件於公告前應予保密。但須公開說明或藉以公開徵求廠商提供參考資料者，不在此限。機關辦理招標，不得於開標前洩漏底價，領標、投標廠商之名稱與家數及其他足以造成限制競爭或不公平競爭之相關資料。底價於開標後至決標前，仍應保密，決標後除有特殊情形外，應予公開。但機關依實際需要，得於招標文件中公告底價。機關對於廠商投標文件，除供公務上使用或法令另有規定外，應保守秘密。」故選項(3)除特定規定外，政府機關應對廠商投標文件保密。

7. (1) 社交工程係指利用人性弱點來騙取機敏資料再行詐騙，請問下列何者方式並非降低受社交工程攻擊風險之方式?(1)大量下載非法軟體。(2)不隨意下載郵件附件檔。(3)不隨意點擊郵件內夾帶的超連結。(4)不下載非法軟體及檔案。**【資訊保護 S10707】**

解析：社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，不未經確認即提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害。

8. (4) 請問下列何者非屬營業秘密法所稱之營業秘密?(1)該營業秘密因其秘密性而具有實際或潛在之經濟價值者。(2)該營業秘密之所有人已採取合理之保密措施者。(3)該營業秘密非一般涉及該類資訊之人所知者。(4)該營業秘密係針對個人資料保護加以限制。**【資訊保護 S10708】**

解析：依營業秘密法第 2 條規定：「本法所稱營業秘密，係指方法、技術、製程、配方、

程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」故選項(4)為錯誤。

9. (3) 為確保國家安全及利益，遂將國家機密等級區分為絕對機密、極機密以及機密，請問下列何者為區分等級之標準？(1)其洩漏後對執政黨影響程度。(2)其洩漏後對國家名譽損失程度。(3)其洩漏後對國家安全或利益造成之傷害程度。(4)其洩漏後對事件之當事人影響程度。**【資訊保護 S10709】**

解析：依照國家機密保護法第 4 條規定：「國家機密等級區分如下：一、絕對機密　適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。二、極機密　適用於洩漏後足以使國家安全或利益遭受重大損害之事項。三、機密　適用於洩漏後足以使國家安全或利益遭受損害之事項。」故選項(3)為正確。

10. (4) 請問下列何者屬於一般資料保護規範(GDPR)的適用範圍?(1)在台美籍外語老師。(2)松江小吃店老闆。(3)大安國小學生。(4)法國營業服飾業者。**【資訊保護 S10710】**

解析：依照一般資料保護規範(GDPR)第 3 條適用範圍之規定，無論個人資料的處理活動是否發生於歐盟境內，只要個人資料的控管者（controller）與處理者（processor）的分支機構設置在歐盟領域內，即適用。再者，對歐盟成員國的人民提供服務並處理其個人資料，亦適用。

11. (2) 我國於 107 年 6 月公布資通安全管理法，並針對公務機關及特定非公務機關加以規範，請問下列何者屬於資通安全管理法所納管之特定非公務機關？(1)關鍵基礎設施提供者。(2)公營事業。(3)政府捐助之財團法人。(4)以上皆是。**【資訊保護 S10711】**

解析：依照資通安全管理法第 3 條第 6 款規定：「六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」故應選選項(4)以上皆是。

12. (3) 請問下列關於個資事故發生時的應變措施，何者錯誤？(1)應於事件查明後，通知當事人。(2)組織可利用電子郵件之方式通知當事人。(3)僅須通知當事人其個資被侵害之事實。(4)如通知當事人之費用過鉅，組織則可利用網際網路等方式通知。**【資訊保護 S10712】**

解析：依個人資料保護法施行細則第 22 條第 2 款規定：「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。」故選項(3)為錯誤。

13. (1) 金管會依法要求資產兆元以上銀行業者應設置資訊安全單位，下列何者錯誤?(1)銀行業者之資通安全單位皆得兼辦銀行其他業務。(2)資訊安全單位人員應受資訊安全專業課程訓練或職能訓練。(3)資安單位主管須與其他高階主管共同提出資通安全整體執行情

形聲明書，並提報董事會。(4)銀行業者無分公營或民營，皆須依法遵守資安相關工作。**【資訊保護 S10713】**

解析：依照金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條第 1 項規定：「銀行業應設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。但主管機關對信用合作社及票券金融公司另有規定者，依其規定。」故選項(1)為錯誤。

14. (2) 下列何者情形不得對性侵害或性剝削者公開其身分資訊(1)強迫少年性交者。(2)公然猥褻者。(3)當應接受身心治療或輔導教育之加害人。(4)強迫兒童為猥褻者。**【資訊保護 D10714】**

解析：依性侵害防治法第 23-1 條前段規定：「第二十一條第二項之被告或判決有罪確定之加害人逃亡或藏匿經通緝者，該管警察機關得將其身分資訊登載於報紙或以其他方法公告之」另按，兒童及少年福利與權益保障第 97 條：「違反第四十九條各款規定之一者，處新臺幣六萬元以上三十萬元以下罰鍰，並得公布其姓名或名稱。」是以，拒絕接受身心治療或輔導教育之加害人及強迫、引誘、容留或媒介兒童及少年為猥褻行為或性交者，得公布其姓名或名稱，故選項(2)為錯誤。

15. (1) 保障個人生活私密領域免於他人侵擾，下列何者為裁判書應隱蔽部分?(1)身分證字號。(2)犯罪事實。(3)姓名。(4)所犯法條。**【資訊公開 D10715】**

解析：依照法院組織法第 83 條第 2 項規定：「前項公開，除自然人之姓名外，得不含自然人之身分證統一編號及其他足資識別該個人之資料。」故選項(1)為正確。

16. (1) 請問下列何者政府資訊得限制公開或不予公開？(1)軍事作戰計畫等國家機密資訊。(2)全國環境輻射偵測。(3)高中職以上學校學生就學貸款統計。(4)臺北市政府公共債務情形。**【資訊公開 D10716】**

解析：依政府資訊公開法第 18 條規定：政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。……九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。」故選項(1)應屬國家機密，不得公開之。

17. (1) 隨著政治檔案條例草案通過，未來各類政治檔案即將解密公開，請問下列關於「政治檔案條例」草案相關內容何者有誤？(1)政治檔案為私人團體所持有，經促進轉型正義委員會審定，即可強制徵收。(2)政治檔案當事人之繼承人表示不予公開之私人文書，得

不提供閱覽。(3)依法核定為機密檔案之資料，不得提供閱覽、抄錄或複製。(4)經審定為政治檔案之資料，由政黨持有者，應於指定期限內移歸檔案局管理。**【資訊公開 D10717】**

解析：依政治檔案條例草案第 3 條立法理由後段：「至政黨以外之私人團體所持有之政治檔案，基於尊重人民財產權，不強制徵集，而應依現行『私人或團體捐贈珍貴文書獎勵辦法』、『國家發展委員會檔案管理局受託保管及收購私人或團體珍貴文書要點』以捐贈、收購或受託保管等方式納為國家檔案典藏。」故選項(1)應不得強制徵收之。

18. (3) 請問下列何者不屬於政府資訊應主動公開之資訊?(1)行政指導有關文書。(2)預算及決算書。(3)涉及國家機密之軍事採購合約。(4)合議制機關之會議紀錄。**【資訊公開 D10718】**

解析：依照政府資訊公開法第 7 條第 1 項規定：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：一、條約、對外關係文書、法律、緊急命令、中央法規標準法所定之命令、法規命令及地方自治法規。二、政府機關為協助下級機關或屬官統一解釋法令、認定事實、及行使裁　　量權，而訂頒之解釋性規定及裁量基準。三、政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號。四、行政指導有關文書。五、施政計畫、業務統計及研究報告。六、預算及決算書。七、請願之處理結果及訴願之決定。八、書面之公共工程及採購契約。九、支付或接受之補助。十、合議制機關之會議紀錄。」次按同法第 18 條第 1 項第 1 款規定：「一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。」選項(3)係符合國家機密，故答案為錯誤。

19. (4) 為落實資訊公開，空氣污染防制法規定應公開公私場所固定污染源之相關資料，請問下列何者有誤?(1)固定污染源應於設置或變更前，向主管機關申請取得設置許可證。(2)如有設置或變更，應提供空氣污染防治計畫予主管機關。(3)民眾得查詢申請資料並表示其意見。(4)許可證核發前，不得預將資料登載於公開網站。**【資訊公開 D10719】**

解析：依照空氣污染防治法第 24 條第 3 項：「直轄市、縣（市）主管機關或經中央主管機關委託之機關，應於前二項許可證核發前，將申請資料登載於公開網站，供民眾查詢並表示意見，作為核發許可證之參考。」是以，許可證核發前，申請資料應公開登載於公開網站，故選項(4)為錯誤。

20. (1) 下列關於通訊保障及監察法之相關規定何者錯誤?(1)偵查機關未經法院聲請監聽票而監聽之，該證據得視情節利用。(2)通訊保障及監察法立法目的在於保障人民秘密通訊自由。(3)公務機關進行通訊監察任務時，應符合比例原則。(4)私人不法取證是否具有證據能力應視法官依照比例原則判斷而定。**【資訊監察 M10720】**

解析：依通訊保障及監察法第 18-1 條第 3 項規定：「違反第五條、第六條或第七條規定

進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據或其他用途，並依第十七條第二項規定予以銷燬。」綜上可知，偵查機關若無監聽票的非法監聽，所取得之內容或衍生的證據，均不得採為證據，故選項(1)錯誤。

21. (3) 檢察官依通訊保障及監察法聲請調取票，須符合下列何者要件? (1)事中監督。(2)補償性原則。(3)重罪原則。(4)事後通知。**【資訊監察 M10721】**

解析：依照通訊保障及監察法第 11-1 條第 1 項規定：「檢察官偵查最重本刑三年以上有期徒刑之罪，有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性時，除有急迫情形不及事先聲請者外，應以書面聲請該管法院核發調取票。聲請書之應記載事項，準用前條第一項之規定。」最輕本刑三年以上有期徒刑之罪為重罪範圍，故選項(3)為正確。

22. (2) 請問下列組織何者於法律上負有協助執行通訊監察之義務?(1)Line 台灣連線。(2)中華電信。(3)Facebook 臉書。(4)WeChat 微信。**【資訊監察 M10722】**

解析：依通訊保障及監察法施行細則第 26 條規定：「本法第十四條第二項所稱協助執行通訊監察之義務，指電信事業及郵政事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備及本施行細則所定之其他配合事項。」是以，選項(1)(3)(4)係為社群軟體並非電信業者，故答案為選項(2)。

23. (1) 請問下列何者符合通訊保障及監察法保障之「通訊」?(1)社交軟體對話紀錄。(2)通聯記錄。(3)Google 定位。(4)電腦 IP 位址。**【資訊監察 M10723】**

解析：依照通訊保障及監察法第 3 條第 1 項規定：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。」社交軟體符合利用電信設備發送、儲存、傳輸信息，故選項(1)為正確。

24. (2) 奧克蘭市於 2016 年 1 月成立隱私諮詢委員會，請問下列關於隱私諮詢委員會之職責何者有誤?(1)為隱私與資訊保護相關立法起草。(2)分析監聽技術並發展之。(3)召開公聽會。(4)審查區域警示中心(DAC)之功能及政策。**【資訊監察 M10724】**

解析：依照 OAKLAND CITY COUNCIL ORDINANCE NO. 13349 C.M.S. SECTION 2.規定：「隱私諮詢委員會(PAC)之職責包括：提供針對監察設備購買時的諮詢與技術援助、為隱私與資訊保護相關立法起草、對現有與規劃的監察設備提交年度策略報告、提供其他隱私立法與資訊、召開公聽會、就區域警示中心(DAC)的功能及政策進行審查」是以，選項

(1)、(3) 、(4)皆符合上述，故選項(2)為錯誤。

25. (2) 下列何者係屬我國個人資料保護法的保障範圍?(1)公司的交易紀錄。(2)小安的年度健檢報告。(3)大光銀行的監視器紀錄。(4)小花自行出版的自傳。**【資訊應用 A10725】**

解析：依個人資料保護法第 2 條第 1 款規定：「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。」故選項(2)為自然人之健康檢查資料，則受個人資料保護法保障之。

26. (4) 遙控無人機是目前資安熱議話題，請問下列我國對於遙控無人機之要求何者有誤?(1)重量 250 克以上的無人機須辦理註冊。(2)部分遙控無人機操作人應經測驗合格。(3)操作人於限航區操作，最重得處 150 萬罰鍰。(4)如欲於禁航區飛行，經登記使得操作。**【資訊應用 A10726】**

解析：依民用航空法第 99-10 條規定：「自然人所有之最大起飛重量二百五十公克以上之遙控無人機及政府機關（構）、學校或法人所有之遙控無人機，應辦理註冊，並將註冊號碼標明於遙控無人機上顯著之處，且一定重量以上遙控無人機飛航應具射頻識別功能。下列遙控無人機之操作人應經測驗合格，由民航局發給操作證後，始得操作：一、政府機關（構）、學校或法人所有之遙控無人機。二、最大起飛重量達一定重量以上之遙控無人機。三、其他經民航局公告者。」及同法第 99-13 條第 1 項規定：「禁航區、限航區及航空站或飛行場四周之一定距離範圍內，禁止從事遙控無人機飛航活動；航空站或飛行場四周之一定距離範圍由民航局公告之。」故選項(4)為錯誤。

27. (2) 請問下列關於「線上即時交易」何者正確?(1)交易時，透過郵局寄信之方式以傳遞資訊。(2)電子票證餘額及交易紀錄儲存於發行機構端。(3)交易時，不需發行機構即時連線。(4)電子票證餘額及交易紀錄儲存於電子票證端。**【資訊應用 A10727】**

解析：依照電子票證應用安全強度準則第 4 條第 2 款規定：「線上即時交易：係指透過各種網路型態，經由特約機構、加值機構或直接與發行機構即時連線進行交易，並將電子票證餘額及交易紀錄即時儲存於發行機構端者，包含特約機構與發行機構間、加值機構與發行機構間、加值機構或特約機構與其所屬之端末設備間之即時訊息傳輸」故選項(2)為正確。

28. (4) 請問下列關於無人載具實驗條例草案何者有誤?(1)創新實驗須由經濟部召開審查會議。(2)創新實驗需具有創新性。(3)申請創新實驗期間原則為一年，必要時可延長一年。(4)創新實驗期間不得排除現行法律之適用。**【資訊應用 A10728】**

解析：依照無人載具實驗條例草案第 22 條第 1 項規定：「申請人於創新實驗期間，於主管機關核准創新實驗之範圍內辦理創新實驗者，其創新實驗行為不適用核准決定載明排除適用之法律、法規命令或行政規則規定。但不包括洗錢防制法、資恐防制法及相關法規命令或行政規則。」故選項(4)為錯誤。

29. (3) 監理沙盒措施可以提供產業與政府間的溝通對話機制、法規調適機制並扶植金融創新及加入創新商轉等功能，請問下列何者選項為全球首部成文法推動監理沙盒之國家?(1)英國。(2)美國。(3)台灣。(4)新加坡。**【資訊應用 A10729】**

解析：台灣於 107 年初完成立法並公布「金融科技發展與創新實驗條例」，其子法亦於同年 4 月底陸續施行。則選項(1)(2)(4)雖皆有計劃實施，惟仍未設立專法，故選項(3)為正確。

30. (4) 請問下列關於電子簽章法之規範何者有誤?(1)電子簽章亦包含數位簽章。(2)法令規定應簽名或蓋章者，經相對人同意得以電子簽章為之。(3)電子簽章與電子文件得取代傳統簽名、蓋章與書面，且具法律效力。(4)目前數位簽章得簽署任何電子文件，並無法規限制。**【資訊應用 S10730】**

解析：依照電子簽章法第 10 條規定：「以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第一項之效力：一、使用經第十一條核定或第十五條許可之憑證機構依法簽發之憑證。二、憑證尚屬有效並未逾使用範圍。」故選項(4)為錯誤。