資通安全法律案例彙編

第 16 輯

行政院國家資通安全會報技術服務中心

中華民國 108 年 11 月

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

「英國首次針對歐盟境外之資料控制者採取 GDPR 執法行動」 ---------- 3

「半導體業者重營業秘密保護 積體電路電路布局申請下滑」 ---------- 7

新加坡通過「反假資訊法」 違者最高處 10 年有期徒刑及巨額罰款---------- 12

智慧監視器被駭發假警報 苦主以為飛彈來襲---------- 16

華盛頓州修正通過個人資料外洩通知法案---------- 20

官網被駭 市府：民眾個資未外洩 ---------- 24

遠端遙控軟體被用來攻擊政府單位---------- 30

通訊軟體遇「國家級網絡攻擊」 與示威同時發生---------- 35

監視器對準鄰居家門口 老師判賠萬元---------- 38

因應國家機密保護法修法 調整涉密人員出境管制期間---------- 42

保險電銷 客戶不想聽須立刻停止行銷---------- 46

藉承攬國軍工程刺探軍事機密 2 包商涉共諜案起訴 ---------- 50

電信管理法三讀 5G 開放共網共頻共建---------- 54

政委：難辨電信設備廠商私營或國營 台灣 5 年前已禁用---------- 59

私密照勒索 女總裁判刑---------- 64

買太多吃不完 轉賣商品附「圖」吃官司 ---------- 68

貳、資訊公開(DISCLOSURE) ----------71

3 家托嬰中心未裝監視器 市長要求強制裝設 ---------- 72

開拓資料想像力 建立開放資料應用典範 ---------- 77

政府採購公布評選委員學經歷 ---------- 81

脫產近 4000 萬、遷 7 次戶口 肉羹大戶欠稅追到了---------- 85

中火 6 天 2 職災 3 死 全面停工體檢 ---------- 89

參、資訊監察(MONITORS) ----------94

「沃爾瑪專利的音檔監控工具可以監聽員工與客戶的對話」---------- 95

舊金山成為美國首例禁止臉部辨識軟體的城市---------- 99

德國政府擬要求數位服務公司提供用戶個資 ----------103

調查冒名檢舉案查 IP 憲兵逕向電信公司調資料挨告----------107

肆、資訊應用(APPLICATION)---------- 112

電子支付再鬆綁 銀行超商可繳水電費----------113

用區塊鏈確保投票真實性 南韓「自由韓國黨」3 月開跑 ----------117

「信用小白」利多！用手機門號就能向銀行辦貸款 ----------120

收養、監護等 6 項法院判決 今起可線上辦理登記----------125

經濟部中小企業處修正融資服務平台介接電子資料使用管理規範 ----------129

伍、自我評量---------- 136

是非題----------137

選擇題----------146

壹、資訊保護（Security）

類別：資訊保護【案號：S10801】

「英國首次針對歐盟境外之資料控制者採取 GDPR 執法行動」

【焦點話題】

加拿大 Aggregate IQ Data Services Limited (AIQ)公司因其代表英國政治組織處理英國公民個人資料，進而利用姓名、電子郵件等個人資料，於社群媒體上針對特定當事人，進行個人化政治性廣告，遭英國隱私專員辦公室(Information commissioner’ s Office, ICO)以其未透明告知當事人資料如何使用，廣告推送也未經當事人同意，認定違反歐盟一般資料保護規則(General Data Protection Regulation, GDPR)及英國資料保護法(Data Protection Act, DPA)。ICO 之執法行動以執法通知(Enforcement Notice)的形式送達，要求 AIQ 在通知送達後 30 日內，停止處理從英國政府組織或其他方式獲得之英國公民個人資料，否則 AIQ 恐面臨高達 20 億歐元或 AIQ 全球收益 4%的罰款。

【參考資料來源：Lexology，107/11/6】

【重點摘要】

1. 歐盟一般資料保護規則第 3 條規定適用 GDPR 的領域範圍包括「設立在歐盟境內」的資料控管者(controller)或處理者(processor)，以及「設立於歐盟境外」之資料控管者或處理者如有下述條件：(1)基於提供商品或服務所需，針對歐盟境內之資料主體進行個資處理行為；(2)基於「監控」歐盟境內自然人行為所需，對資料主體進行個資處理行為；(3)資料控管者雖非設立於歐盟境內，但所設立之處依據國際公法適用歐盟會員國法律，亦適用 GDPR。

2. 有些業者認為 GDPR 不會對較小的海外公司採取執法行動，被稱為距離迷思(distance myth)；部分業者則認為，其所蒐集之資料類型與性質存在違規門檻，被稱為門檻迷思(threshold myth)，但目前 ICO 對 AIQ 所提出的執法通知顯然已打破上開二種迷思。

【法律觀點】

在全球化的時代，透過網際網路運作的跨境貿易盛行，例如跨境電商活動，僅需網際網路即可進行交易，使得各國人民的個人資料被蒐集的機會大為提高。因此，歐盟於 2018 年 5 月提出一般資料保護規則(General Data Protection Regulation, GDPR)對此進行規範。

對企業而言，GDPR 保護對象為歐盟境內的資料主體，因此，當控管者[1](controller)或處理者[2](processor)於歐盟境內進行個資處理活動，即適用 GDPR[3]。然而，當控管者或處理者非設立於歐盟境內時，如符合下列情形亦適用 GDPR：(1)基於提供商品或服務所需，針對歐盟境內之資料主體進行個資處理行為[4]；(2)基於「監控」歐盟境內自然人行為所需，對資料主體進行個資處理行為[5]；(3)資料控管者雖非設立於歐盟境內，但所設立之處依據國際公法適用歐盟會員國法律[6]。

依據英國隱私專員辦公室(Information commissioner’s Office, ICO)所發出之執法通知[7]，設立於加拿大的公司 Aggregate IQ Data Services Ltd(AIQ)屬於 GDPR 所規範的控管者，ICO 發現 AIQ 將商業行為廣告的技術應用於政治競選活動以及脫歐公投，此應用並非資料主體所得知悉，且亦與資料原始蒐集目的不符，在 AIQ 不具備其他合法處理依據下，ICO 因而認定 AIQ 未遵守 GDPR 第 5 條(a)-(c)合法公平透明原則；目的限制原則；資料最小化原則，以及第 6 條資料合法處理規定此外，AIQ 亦未能遵守 GDPR 第 14 條個資間接蒐集公平透明要求，，其並未向資料主體提供第 14 條第 1 項和第 2 項的資訊，也不符合第 14 條第 5 項所列免告知情形。是以，即便 AIQ 未實體設立於歐盟地區， ICO 仍得對其提出具強制執行力之執法通知，當 AIQ 未履行時，ICO 即有可能依據英國資料保護法(Data Protection Act, DPA)對其進行裁罰。

---

[1] General Data Protection Regulation, art. 4(7)
[2] General Data Protection Regulation, art. 4(8)
[3] General Data Protection Regulation, art. 3(1)
[4] General Data Protection Regulation, art. 3(2)(a)
[5] General Data Protection Regulation, art. 3(2)(b)
[6] General Data Protection Regulation, art. 3(3)
[7] ENFORCEMENT NOTICE THE DATA PROTECTION ACT 2018 PART 6, SECTION 149. https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf

同時，AIQ 一案也可窺見個人資料的數據分析，涉及西方民主政治時，可能會是歐洲個人資料監管機關的關注重點。

【管理 Tips】

透過網際網路資訊傳遞無遠弗屆，而歐盟通過 GDPR 後亦慢慢展現其跨境效力，在 ICO 對 AIQ 提出執法通知前，世界各地公司行號不停臆測其執法行動與罰款評估，有些業者認為 GDPR 不會對較小的海外公司採取執法行動，被稱為距離迷思(distance myth)，而其他部分業者則認為其所蒐集之資料類型與性質存在違規門檻，被稱為門檻迷思(threshold myth)，然因目前 ICO 對 AIQ 所提之執法通知顯然已打破上開二種迷思，故設立歐盟境外的企業如有蒐集處理歐盟地區人民之個人資料，應遵守其相關規範，以免觸法。

然而，根據 GDPR 規範要求，對於我國電子商務產業及經營對外貿易企業而言，勢必提升其法規遵循成本，甚可能形成貿易障礙。是以，除考慮企業本身是否適用 GDPR 相關規定，企業應先遵守我國之個人資料保護法，更甚者得建置個人資料保護與管理系統。我國亦已成立個人資料保護專案辦公室因應 GDPR 相關事宜，向歐盟申請適足性認定工作，並配合檢討個人資料保護法，協調整合及加強各部會落實執行個資法之一致性。

【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：　依照 GDPR 規定，係指已識別或可識別自然人之相關資訊（資料主體）；可識別之自然人係可以直接或間接識別的個人，諸如姓名，識別碼，位置資料，線上識別資料或一

個或多個特定於物理，生理，自然人的遺傳，心理，經濟，文化或社會認同等。

ISO 29100：2011（CNS29100）

- 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：　依照 GDPR 規定係指蒐集處理個人資料應具備適當性、關聯性以及與處理資料目的時的必要性。

類別：資訊保護【案號：S10802】

「半導體業者重營業秘密保護 積體電路電路布局申請下滑」

【焦點話題】

據經濟部智財局統計，我國積體電路電路布局申請件數於民國 104 年至 105 年間皆破百件，於 106 年則下滑至 58 件，係因近三年主要申請者為美國某半導體業者，該業者申請占比超過九成，其於 106 年申請量驟減以致影響該年總申請件數。就比例而言，國內業者於積體電路電路布局相對較少，係因我國業者多以營業秘密、專利申請保護其研發技術與成果。

智財局表示，業者若有研發技術與成果想要保護，可依照需求抉擇申請專利、營業秘密，或積體電路電路布局等三道機制。

【參考資料來源：自由電子報，107/10/21】

【重點摘要】

1. 營業祕密法第 2 條規定，營業祕密係指方法、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，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。

2. 積體電路電路布局法第 10 條第 2 項規定，申請電路布局登記時，如果圖式、照片或積體電路成品，涉及積體電路製造方法之秘密者，得以書面敘明理由，而以其他資料代替為申請，此時組織能透過「祕密性」、「經濟價值」以及「保密措施」等要件，使積體電路電路布局成為營業祕密，既可避免因公開所帶來的風險，亦可做到一定程度的保護，同時，如積體電路電路布局同時符合專利法上「產業利用性」、「新穎性」及「進步性」等要素，亦可透過申請發明專利為保護，不過其亦有因公開所帶來的弊害，組織亦應加以考量。

【法律觀點】

積體電路電路布局保護法第 2 條[1]規定，積體電路指將電晶體、電容器、電阻器或其他電子元件及其間之連接線路，而積體電路布局則為在積體電路上之電子元件及接續此元件之導線的平面或立體設計，集積在半導體材料上或材料中，而具有電子電路功能之成品或半成品，亦即積體電路布局為積體電路之平面或立體設計之結果[2]。

而積體電路電路布局保護法明定受保護的電路布局權應具備由於創作人之智慧努力而非抄襲之設計與創作時就積體電路產業及電路布局設計者而言非屬平凡、普通或習知者[3]，亦即需具備原創性及非普遍性兩個要件。而原創性之概念源自於著作權法，而非普遍性之概念則類似於專利法之非顯而易見性[4]，由此可知，積體電路電路布局同時兼具著作權與專利的性質。

但電路布局權亦和其他權利不盡相同，積體電路電路布局必須在申請登記後始得主張電路布局權[5]，不需要實質審查[6]，且必須於商業利用後二年內申請登記，逾期則不受積體電路電路布局保護法保護[7]。而就營業祕密而言，根據營業祕密法第 2 條[8]規定，營業祕密應具備「祕密性」、「經濟價值」及「保密措施」。由此可

---

[1] 積體電路電路布局保護法第 2 條第 1、2 項：「本法用詞定義如左：一、積體電路：將電晶體、電容器、電阻器或其他電子元件及其間之連接線路，集積在半導體材料上或材料中，而具有電子電路功能之成品或半成品 。二、電路布局：指在積體電路上之電子元件及接續此元件之導線的平面或立體設計。」

[2] 一般而言，積體電路可主張之權利為「發明專利權」、「營業祕密」; 積體電路電路布局可主張之權利則包括「發明專利權」、「積體電路電路布局權」、「著作權」及「營業祕密」。其理由在於，就積體電路本身之特性，除非經由逆向工程方能得知其連接線路之特殊性，因此實務上對於積體電路之發明保護，除申請專利外，反而常見以積體電路與週邊電路所組成之電路布局為保護客體，故本文亦以積體電路電路布局為討論核心。

[3] 積體電路電路布局保護法第 16 條第 1 項。

[4] 積體電路電路布局保護法第 16 條立法理由三前段。

[5] 積體電路電路布局保護法第 15 條第 1 項。

[6] 積體電路電路布局保護法第 16 條立法理由二前段。

[7] 積體電路電路布局保護法第 13 條。另，專利權的取得，以發明專利而言，其需要申請登記以為實體審查，通過後方取得專利權，而著作權則以著作人於著作完成時即享有著作權，二者與積體電路電路布局保護法均略有不同。

[8] 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、因其審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。」

知，營業祕密、積體電路布局權及專利權最大不同在於是否具備「祕密性」，亦即積體電路布局權與專利權因其必須登記，如要登記則須先行公開，而營業祕密的重點在於「祕密性」，當積體電路布局公開時，所公開的部份將不再是營業祕密[9]。

而二者在權利保護上也略有差異，著作權法關於著作物之保護，除民事侵權行為損害賠償以外，當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的營業秘密，即構成營業祕密法第 13-1 條[10]侵害營業秘密罪。而積體電路電路布局保護法並無刑事責任，僅有民事侵權損害賠償等相關權利，因此於選擇時，仍應考量適合自身之方式。

【管理 Tips】

針對積體電路電路布局保護，有數種權利得以選擇主張，分別為「發明專利權」、「積體電路布局權」、「營業祕密」[11]。

以發明專利權[12]來看，其保護期間為二十年，較積體電路布局權的十年為久，惟

---

[9] 積體電路電路布局保護法第 10 條第 2 項：「前項圖式、照片或積體電路成品，涉及積體電路製造方法之秘密者，申請人得以書面敘明理由，向電路布局專責機關申請以其他資料代之。」因此仍有保留申請人以其他資料申請而維持布局營業秘密之彈性空間，惟當申請人選擇公開時，即喪失營業祕密所稱之祕密性，此應由申請人加以考量。

[10] 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。」

[11] 因積體電路電路布局圖屬於著作權法中的圖形著作（所謂圖形著作者，係指以思想、感情表現圖形之形狀或模樣之著作，其包括地圖、圖表、科技或工程設計圖及其他之圖形著作。科技或工程圖形著作，係指器械結構或分解圖、電路圖或其他科技或工程設計圖形及其圖集著作，智慧財產法院 102 年民著上字第 26 號民事判決參照），著作權在著作人於著作完成時即享有著作權，故積體電路布局的著作權在其完成時就已經由著作人取得而得享有權利，而不受是否公開或有無保護之影響，故在此不另與討論。

[12] 另，專利法第 22 條第 1 項規定：「可供產業上利用之發明，無下列情事之一，得依本法申請取得發明專

其申請必須實質審查，因此需完整揭露資訊，容易遭仿冒，而積體電路布局申請僅有形式審查，且涉及積體電路製造方法之秘密者，申請人得以其他資料代替，因此其遭仿冒之可能性則較申請發明專利為低。

其次，是否為營業祕密則有其要件，包括「祕密性」、「經濟價值」及「保密措施」，如組織能明確定義營業祕密並建立清單，以要求組織人員負有保密約定，申請積體電路電路布局或發明專利即非必要。

因此，在管理程序上應先應就技術價值、產品生命週期等因素為綜合評估，決定是否為取得發明專利而公開技術，再者，申請積體電路電路布局權時，因涉及積體電路製造方法之秘密，此時可不將圖式予以公開，而以其他資料代替為申請，此時組織能透過「祕密性」、「經濟價值」以及「保密措施」等要件，使積體電路電路布局成為營業祕密，既可避免因公開所帶來的風險，亦可做到一定程度的保護。

【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：　組織在決定如何選擇適用法規時，應瞭解各法規之目的並依循其應適用之法令。以本案例而言，組織決定以發明專利、積體電路電路布局或以營業祕密的方式保護，必須先就實際需求及法規之保障程度分析，再加以決

利：一、申請前已見於刊物者。二、申請前已公開實施者。三、申請前已為公眾所知悉者。」亦即透過「產業利用性」、「新穎性」及「進步性」等三要素，對專利申請為限縮，此與積體電路電路布局保護所重者「原創性」及「非普遍性」亦有所不同，故如積體電路電路布局具備發明專利之要件時，亦未嘗不可以申請發明專利予以保護，惟仍應考量後述之實質審查及營業祕密保持可能性。

定。

- A.18.1.2　智慧財產權

(1) 標準內容：　應實作切適程序，以確保遵循與智慧財產權及專屬軟體產品使用相關之法律、法令、法規及契約的要求事項。

(2) 適用說明：　組織應建立適當程序，使組織得以依循，以積體電路電路布局而言，組織如決定不申請專利或電路布局，則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，以確保事故發生時的權利保障。

類別：資訊保護【案號：S10803】

新加坡通過「反假資訊法」　違者最高處 10 年有期徒刑及巨額罰款

【焦點話題】

新加坡國會於民國 108 年 5 月 8 日通過防止網路假訊息與網路操縱法(Protection from Online Falsehoods and Manipulation Act)[1]，新加坡內政兼司法高層指出，少數新興媒體透過假帳號、數位廣告、機器人程式等手段，致使不實資訊迅速散播，導致人們對真實訊息及政府產生不信任感，更甚者恐引發煽動騷亂、公共衛生危機等，後果難以想像，因此，該法明確規定禁止於網路發布任何針對國家的偏見言論等，執法部門有權要求刪除此類內容。觸法者最高恐處以 10 年徒刑及巨額罰款，且內閣各部長有評斷資訊真偽、要求更正、刪除不實資訊，甚或是屏蔽網站之權力，惟此規範亦引起部分民眾質疑新法賦予政府過大權力，且將限制言論自由。

【參考資料來源：ETtoday，108/5/9】

【重點摘要】

1. 新加坡防止網路假訊息與網路操縱法第 7 條規定，禁止人民在新加坡境內或境外散播虛假資訊，而該傳播不利於新加坡的國家安全；公共衛生、社會安全，公共安寧或公共財政；不利於新加坡與其他國家的友好關係；影響總統與議員選舉；煽動敵意的，仇恨或芥蒂；或是打擊人民對政府履行職責的信心，違者可處以 5 年以下有期徒刑，或科或併科 5 萬元新幣，同時如果是以虛假帳戶或是自動化程式散布或加速散布虛假事實時更加重其刑。

2. 我國目前為防杜散播假訊息造成危害，現有法規主要以社會秩序維護法第 63 條第 1 項第 5 款規定「散佈謠言，足以影響公共之安寧」而得處 3 日以

[1] Government of Singapore, Protection from Online Falsehoods and Manipulation Act 2019，網址：https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625#pr7-（最後瀏覽日：108 年 7 月 3 日）

下拘留或新臺幣 3 萬元以下罰鍰。

【法律觀點】

新加坡議會於 2019 年 5 月通過「防止網路虛假與操弄法案」(Protection from Online Falsehoods and Manipulation Act, POFMA)，使政府得採取適當措施以杜絕人民以電子通訊等方式傳播不實資訊、以假帳號進行通訊和資訊處理之行為，並提昇線上政治廣告之透明度[2]。

POFMA 首先禁止人民在新加坡境內或境外散播不實資訊，而若傳播具相當理由判斷應屬不實資訊而涉及不利於新加坡國家安全；公共衛生、社會安全，公共安寧、財政；不利於新加坡與其他國家友好關係；影響總統與議員選舉；煽動敵對、仇恨或芥蒂；或是打擊人民對政府履行職責的信心等，亦在禁止之列[3]，違反者，如為個人最高可處 5 萬元新幣或 5 年以下有期徒刑或二者併處，而在其他情況下，最高可處 50 萬元新幣[4]，上述行為若以假帳號、自動化程式加速散布不實資訊者，可加重其刑[5]。

其次，實際執行，或意圖執行自動化程式於新加坡傳播不實資訊者，個人最高可處 6 萬元新幣或 6 年以下有期徒刑或二者併處[6]。再者，當行為人知悉並請求、接受或同意接受任何財務或物質利益提供散布不實資訊，亦屬於犯罪[7]。

另外，依據 POFMA，政府亦被賦予權力，任何部會首長可要求不實資訊提供者更正並停止傳播該不實資訊[8]，甚至得請資訊通信媒體發展管理局(Info-communications Media Development Authority, IMDA)下令網際網路通訊服務商封鎖該資訊位址，而網際網路通訊服務商如不遵守該命令，將可處每日最高

[2] POFMA art 5
[3] POFMA art 7 §1
[4] POFMA art 7 §2
[5] POFMA art 7 §3
[6] POFMA art 8
[7] POFMA art 9 §1&2
[8] POFMA art 10~12

2 萬元新幣之處罰，並得按日連續罰之，最高可處共計 50 萬元[9]。並可勒令網際網路中介服務者如 Facebook、Google 等公司，針對經政府判斷之不實資訊予以更正[10]或下架[11]。

而我國目前為防杜散播假訊息造成危害，現有法規主要以社會秩序維護法第 63 條第 1 項第 5 款規定「散佈謠言，足以影響公共之安寧」而得處 3 日以下拘留或新臺幣 3 萬元以下罰鍰，並另於 107 年 12 月之行政院院會通過修正包括「災害防救法」等六個法案[12]，在法案中納入禁止散播假新聞之規範及其罰則，內容多以故意散播不實訊息或謠言而影響秩序或生損害為要件，亦即以「故意」、「非真實」以及「危害」為要件，以降低打擊假消息而形成「言論箝制」的可能。

【管理 Tips】

不實資訊之散布方式不斷更新，網際網路即係被濫用以傳播謊言和不實資訊之最新手段。不實資訊所造成之危害可就下列面向觀之：首先，不實資訊係於社群媒體興起後，操作者藉由網際網路之便利而以各國主流社群媒體為平臺散播不實資訊，進而造成各式不利益之影響。其次，不實資訊對於組織而言，可能連帶造成傳播惡意軟體傳播而造成組織巨大損失。

而因應不實資訊之方式，就外部而言，國家勢必有一定程度之介入，以釐清事實，並建立有效澄清之管道，使民眾得以接觸事實。就組織內部而言，則可由四個方法共同構成防護：

1. 建立用戶意識：假新聞等不實資訊傳播係因為民眾希望與其社交網路分享資

[9] POFMA art 16

[10] POFMA art 21

[11] POFMA art 22

[12] 政院：不可傷害言論自由　三重機制防制「惡、假、害」不實訊息，網址：https://www.ey.gov.tw/Page/9277F759E41CCD91/a87eb5ee-9466-438a-a6fe-a8570db6ab1a（最後瀏覽日：108 年 5 月 15 日）

訊，因此，民眾在分享資訊前應先查看連結及其內容之真偽，即可初步防止不實資訊不必要的傳播。

2. 利用分析服務：透過分析服務，監控網際網路中可能的目標、網頁劫持或假域名，透過分析服務可以判斷訊息來源之可信度。

3. 保護和監控網路：確保組織具有適當之能量以保護網路並確保組織資訊安全。安裝最新版本之端點安全解決方案，並持續進行更新，藉此降低惡意軟體感染設備之風險。此外，透過網路監控以儘早發現異常流量，降低資料外洩風險。

4. 保持機器學習與自動化：當假新聞等不實資訊網站被識別出，即可迅速將其列入黑名單，並將更新策略自動推送到組織內部所有設備，以確保組織內部人員知曉相關內容及保護相關設備。

【相關標準】

ISO27001：2013（CNS27001）

- 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：　組織應對網路進行控管，藉此保護和監控網路，以確保組織的網路服務具有適當的安全性，以保護網路並確保組織資訊安全。

- 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：　組織可透過機器的自動化學習及推送，當假訊息等網站之資訊被識別出來後，以黑名單方式自動推送至組織內所有設備，以避免受到威脅，並可透過使用者認知建立用戶意識，降低假訊息所帶來的威脅。

類別：資訊保護【案號：S10804】

智慧監視器被駭發假警報 苦主以為飛彈來襲

【焦點話題】

美國舊金山灣區發生一起家庭監視攝影機謊稱北韓以三枚洲際彈道導彈攻美之假警報案件，經該家庭監視攝影機製造商調查過去三個月之案件發現，主因係該設備之使用者密碼遭駭客於該製造商外之其他網站漏洞盜取，從而取得該設備之控制權，強烈建議使用者應採用加強版之驗證技術(例如除帳號密碼外，同時透過手機簡訊驗證之方式)。

【參考資料來源：中央社，108/1/22】

【重點摘要】

1. 駭客非法入侵電腦或其相關設備並對被害人予以竊聽侵害他人隱私甚鉅，恐將同時構成刑法第 358 條「入侵電腦或其相關設備罪」、同法第 315 條之 1「妨害秘密罪」及通訊保障及監察法第 24 條「違法監察他人罪」。
2. 影像監控系統資安標準依據影像監控系統之不同安全構面分別訂定安全要求分項，包括：實體埠之安全管控、實體異常行為警示、實體防護、安全啟動、作業系統與網路服務安全、網路服務連接埠安全、更新安全、敏感性資料儲存安全、網頁管理界面安全、操控程式之應用程式安全、日誌檔與警示、敏感性資料傳輸安全、通訊協定與設置安全、Wi-Fi 通訊安全、鑑別機制安全、通行碼鑑別機制、權限控管、隱私資料的存取保護、隱私資料的傳輸保護等項目，通過測試後，依照所測試等級，方得稱通過該安全等級之安全要求分項等級，以符合一定不同程度之資安要求。

【法律觀點】

我國刑法妨害電腦使用罪章第 358 條「入侵電腦或其相關設備罪」，規定無故入

侵他人之電腦或其相關設備者，最高可處三年以下有期徒刑[1]。其立法理由明確表示：「鑒於對無故入侵他人電腦之行為採刑事處罰已是世界立法之趨勢，且電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性，此種行為之危害性應已達科以刑事責任之程度，為保護電腦系統之安全性，爰增訂本條。」除無故入侵他人電腦行為會受到處罰外，如製作專供犯妨害電腦使用罪章之電腦程式，而供自己或他人犯該章之罪，依同法第 362 條之規定，最高可處五年以下有期徒刑[2]。而同法第 315 條之 1「妨害秘密罪」，則是以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為要件，而得處 3 年以下有期徒刑[3]，其立法理由在於「目前社會使用照相、錄音、錄影、望遠鏡及各種電子、光學設備者，已甚普遍。惟以之為工具，用以窺視、竊聽、竊錄他人隱私活動、言論或談話者，已危害社會善良風氣及個人隱私，實有處罰之必要」。

此外，我國通訊保障及監察法（以下簡稱通保法）為保障人民秘密通訊自由及隱私權不受非法侵害，該法第 24 條第 1 項即對違法監察他人通訊者定有刑責，最重可處五年以下有期徒刑[4]。

本案如發生在我國，因駭客係運用其他網路管道取得密碼，故以其他手法取得被害人之登入帳號，而入侵被害人之電腦相關的網路攝影機，因此適用刑法第 358 條，而駭客如又有利用被害人的網路攝影機以監視被害人之生活情形，則同時觸犯同法第 315 條之 1 之妨害秘密罪。又，家庭係為私人生活不可侵犯之

[1] 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。」

[2] 刑法第 362 條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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。」

[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 24 條：「違法監察他人通訊者，處五年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。」

核心領域，因此被害人於家中遭監視、監聽，駭客係又涉犯通保法第 24 條第 1 項違法監察罪，綜上所述，駭客非法入侵電腦或其相關設備並對被害人予以竊視、竊聽，侵害他人隱私甚鉅，將同時違反刑法第 358 條、第 315 條之 1 與通保法第 24 條之規定，不可不慎。

【管理 Tips】

近年來物聯網 (IoT) 技術發展迅速，物聯網相關產品亦相近推出，也因而造成日常用品逐漸朝向數位化邁進，影像監控設備也是其中之一。

惟於享受科技帶來便利之同時，相關風險亦伴隨而生，諸如藉由網路攝影機為跳板進行各式網路攻擊等，有鑒於此，參照國際物聯網相關資安標準，我國經濟部、國家通訊傳播委員會與臺灣資通產業標準協會針對影像監控系統資安標準推出多部規範及測試標準[5]，冀以促進國內產業整體優質化及產品競爭力，並提升影像監控裝置之資安等級。

業者若恪守上開規範及測試標準，可確保所產出之影像監控裝置達一定程度之資安等級。該規範將安全等級參考資安風險高低及技術實現複雜度等因素綜合考量，分為 1 級、2 級、3 級等三個等級[6]，並依實體安全、系統安全、通訊安全、身分鑑別與授權機制安全以及隱私保護等五個安全購面[7]，考量不同構面所面臨之資安風險各有不同，分別以安全構面對應安全要求項目[8]，包括實體埠之安全管控、實體異常行為警示、實體防護、安全啟動、作業系統與網路服務安全、網路服務連接埠安全、更新安全、敏感性資料儲存安全、網頁管理界面安全、操控程式之應用程式安全、日誌檔與警示、敏感性資料傳輸安全、通訊協定與設置安全、Wi-Fi 通訊安全、鑑別機制安全、通行碼鑑別機制、權限控管、隱私資料的存取保護、隱私資料的傳輸保護等項目。相關業者宜於開發過程中依上開文件之要求，妥善

[5] 目前除「影像監控系統資安標準—第一部：一般要求」外，臺灣資通產業標準協會也針對網路攝影機、影像錄影機、網路儲存裝置提出更細部的資安標準以及測試規範。

[6] 影像監控系統資安標準—第一部：一般要求 4.1.3

[7] 影像監控系統資安標準—第一部：一般要求 4.1.1

[8] 影像監控系統資安標準—第一部：一般要求 4.1.2

注意各構面之安全要求項目，並配合其測試規範之測試方法進行測試，以使影像監控裝置符合現階段資安之要求。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.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：　物聯網蓬勃發展，諸多結合感測技術、通訊技術、數據分析等技術之連網服務，使民眾生活更為便利，也為資安帶來更大的威脅，而製造商因開發連網設備時，建議依據主管機關所提供之相關資安規範，建立軟體及系統開發規則，降低設備所帶來的資安風險。

ISO 27001：2013(CNS 27001)

- 24.1.1　資訊安全要求事項分析及規格

(1) 標準內容：　資訊安全相關要求事項，應納入新資訊系統或既有資訊系統之強化的要求事項中。

(2) 適用說明：　主管機關所提供之相關資安規範，廠商應時時注意，如有新要求，則應進行分析並納入所開發的系統中，以確保符合業界合理水準的資訊安全。

類別：資訊保護【案號：S10805】

華盛頓州修正通過個人資料外洩通知法案

【焦點話題】

美國華盛頓州於 2019 年 5 月 7 日通過 HB 1071 法案，主要修正州法(Revised Code of Washington, RCW) 第 19.255 章「個人資料—外洩通知 (Personal information-Notice of security breaches)」，該法案將於 2020 年 3 月 1 日正式生效。未經授權獲取資料，危及該居民個人資訊的安全性、機密性或完整性，因此華盛頓州要求個人、企業和公共機構於個人資料外洩時，通知任何有可能受到損害的華盛頓居民，修法重點主要為：(1)擴大個人資料之定義；(2)增訂線上帳戶之安全管理；(3)通知時間及內容管理規範等。原個人資料之定義為姓名結合個人社會安全碼、金融帳號或信用卡等，而目前 HB 1071 法案將新增出生日期、私人密鑰、學生證、護照識別碼、健康保險識別碼等資料。另外，針對發現違規行為之通知時間要求，一般而言通知必須於最有利時間完成，而新規定將原本不得超過 45 個日曆天之要求，縮短至 30 個日曆天，而通知總檢察長之門檻仍為受影響之華盛頓居民逾 500 名。

【參考資料來源：JD Supra，108/5/10】

【重點摘要】

1. 華盛頓州修正 HB 1071 法案第 5 條規定，當受違規行為影響者超過 500 人時必須通知總檢察長，而通知內容包括受違規行為影響的人數或估計人數；違規行為所涉及的個人資訊類型清單；曝險的時間範圍；遏制違規行為的步驟摘要；以及不包括任何個人身份資訊的安全漏洞通知的樣本。

2. 我國個人資料保護法第 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。而個資法施行細則第 22 條第 2 項則要求通知之內容應包括個人資料被侵害之事實及已採取之因應措施。

【法律觀點】

美國華盛頓州於本次修法重點其一為外洩通知時間，除特定情形外，組織須於發現違規行為後 30 日內通知受影響者，必要時得延長 14 日，其通知內容包括增加暴露之時間範圍，發生日期及發現日期等[1]，而當外洩事件涉及帳戶或密碼，可透過電子郵件發出通知，且必須告知當事人立即更改登錄憑證或採取其他適當措施保護帳戶，而若外洩事件涉及對本身提供之電子郵件帳戶的消費者登錄憑據時，則不能以該受損電子郵件帳戶通知消費者[2]。另外，受影響者超過 500 人時，則須通知總檢察長(the Attorney General)[3]，其通知內容包含：受影響人數、所涉及之個人資訊類型清單、發生日期及發現日期、採取之應變措施等[4]，且必須持續更新通知予總檢察長。

然而，我國個人資料保護法（下稱個資法）第 12 條規定，組織違反規定，導致個人資料被竊取、洩漏等其他侵害者，應查明後以適當方式通知當事人。通知方法則按個資法施行細則第 22 條第 2 項要求，其通知內容應包括個人資料被侵害之事實及已採取之因應措施。另外，目前各目的事業主管機關針對轄下特許事業多訂有個人資料檔案安全維護計畫及處理辦法，如外洩事件屬重大事故時，須通報目的事業主管機關並通知當事人被侵害之事實、已採取的因應措施[5]及諮詢服務專線[6]等，惟該通報並非法定義務，亦不得依此裁罰[7]。

---

[1] Washington State SUBSTITUTE HOUSE BILL 1071 art 5(8)

[2] Washington State SUBSTITUTE HOUSE BILL 1071 art 2(5)(d)(ii)

[3] Washington State SUBSTITUTE HOUSE BILL 1071 art 5(7)

[4] Washington State SUBSTITUTE HOUSE BILL 1071 art 5(7)(a)

[5] 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。」

[6] 例如：不動產經紀業個人資料檔案安全維護管理辦法第 17 條：「經紀業應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事故時，迅速處理以保護當事人之權益。　前項應變機制，應包括下列事項：一、採取適當之措施以控制事故對當事人造成損害。二、查明事故發生原因及損害狀況，並以適當方式通知當事人事故事實、因應措施及諮詢服務專線等。三、研議改進措施，避免類似事故再度發生。四、發生重大個人資料事故者，應即以書面通報直轄市、縣（市）主管機關。　前項第四款所稱重大個人資料事故，指個人資料被竊取、洩漏、竄改或其他侵害事故，致危及大量當事人權益之情形。」

[7] 法務部法律字第 10403503590 號函釋說明二(二)：「次按中央目的事業主管機關訂定安全維護標準辦法如規

【管理 Tips】

就管理而言，如我國組織發生個資事故時，應遵守個資法及各目的事業主管機關相關規範。根據我國個資法第 12 條規定個資事故事件應於查明後通知當事人，而應查明事項為事故發生原因及損害狀況，查明時間個資法及法務部函釋均未規定時限，亦恐發生組織查明時間過長，不願公布或通知，將有損當事人權益。因此，目前法規顯有不足之處，未來可於修法之際參考援引外國立法例，加強目的事業主管機關之地位，甚可統整單一單位接受個資事件通報，以符合國際潮流而與之接軌。

【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、法規及契約的要求事項。

(2) 適用說明：　就發生事故是否需通報主管機關，組織應瞭解其所適用之規範，以我國目前法規而言，未通報主管機關為非處罰要件，惟若適用 GDPR 等具有跨境效力之規範時，組織未予通報或通報有瑕疵時，將有相對應之罰則，不可不慎。

ISO 27001：2013(CNS 27001)

- A.16.1.2　通報資訊安全事件

定非公務機關就個人資料外洩應予通報，因該通報並非法定義務，非公務機關如發生個人資料外洩事件時，其目的事業主管機關仍應就該非公務機關有無違反個人資料保護法（以下簡稱個資法）第 27 條第 1 項或未依第 27 條第 2 項訂定安全維護計畫或處理方法，依個案具體情形審酌是否符合個資法第 48 條第 4 款之處罰構成要件，目的事業主管機關不得僅因非公務機關未依安全維護標準辦法所定通報機制向目的事業主管機關為通報，即逕予裁罰。」

(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： 無論資安事故是否需通報主管機關，依法仍需於查明後以適當方式通知當事人，而該通知多非第一線人員可自行決策，因此在通知或通報前，內部仍必須將事件層層通報，使決策者知悉並進行後續處理。

類別：資訊保護【案號：S10806】

官網被駭 市府：民眾個資未外洩

【焦點話題】

108 年 5 月 4 日一民眾發現我國某市政府之全球資訊網無法連線，隨即以 1999 市民專線向該市府反映，經該市府初步調查其全球資訊網係因不明病毒攻擊，而導致服務中斷，隨即依資通安全管理法及相關應變程序之規定，啟動相關因應機制，諸如：請系統維護及資安維護廠商進行緊急處理、進行資通安全事件之通報，並協請行政院國家資通安全會報技術服務中心派員支援及釐清事發原因。

經針對病毒碼之初步鑑識，受影響範圍主要係市府內部之行政公文系統及職員入口網，目前改採紙本作業，且無民眾個資外洩之情況。

【參考資料來源：聯合新聞網，108/5/7】

【重點摘要】

1. 資通安全事件通報及應變辦法第 2 條將資通安全事件區分為四級。其區分係以標的是否涉及核心業務、公務機密、敏感資訊、國家機密、以關鍵基礎設施為基礎，再以所涉及者之嚴重程度加以判斷，而數字愈高者愈嚴重。
2. 資通安全事件通報及應變辦法第 4 條與第 11 條要求，公務機關或是特定非公務機關在知悉資通安全事件後，就應於一小時內依規定對主管機關或是目的事業主管機關進行資通安全事件通報，如嗣後發現等級需為變更，則應續行變更。如因故無法依規定方式通報者，應於規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由，當無法通報之事由解除後，應依指定方式補行通報。

【法律觀點】

為使各受規範對象得妥適辦理資通安全事件之通報及應變，以降低資通安全事件之發生機率，或於發生資通安全事件時可迅速妥適因應，有效降低損害，資

通安全管理法第 14 條第 4 項[1]及第 18 條第 4 項[2]針對公務機關及特定非公務機關明定辦法，規範資通安全事件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[3]。

該辦法第 2 條規定將資通安全事件區分為四級。其區分係以標的是否涉及核心業務、公務機密、敏感資訊、國家機密、以關鍵基礎設施為基礎，再以所涉及者之嚴重程度加以判斷，而數字愈高者愈嚴重[4]。舉例而言，當資通安全事件發生，其涉及遭嚴重竄改之部分非屬單位之核心業務系統，屬第二級資通安全事件。然而，當資安事件發生時，公務機關或特定非公務機關應於知悉後一小時內依照規定向主管機關或目的事業主管機關進行通報，如嗣後發現等級需為變更，則應續行變更，其通報之內容包括發生機關、發生或知悉時間、狀況之描

[1] 資通安全管理法第 14 條第 4 項：「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。」

[2] 資通安全管理法第 18 條第 4 項：「前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由主管機關定之。」

[3] 資通安全事件通報及應變辦法總說明。

[4] 資通安全事件通報及應變辦法第 2 條：「資通安全事件分為四級。公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：一、非核心業務資訊遭輕微洩漏。二、非核心業務資訊或非核心資通系統遭輕微竄改。三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。　各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件：一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。」

述、等級之評估、因應事件所採取之措施、外部支援需求評估以及其他相關事項[5]等基本通報項目。如因故無法依照規定方式通報者，應於規定之時間內依照其他適當方式通報，並註記無法依規定方式通報之事由，當無法通報之事由解除後，應依指定方式補行通報[6]。

再者，當公務機關或特定非公務機關完成資通安全事件之通報後，必須在規定時間完成損害控制或復原作業，依照主管機關指定之方式及對象辦理通知事宜，並於完成後一個月內送交調查、處理及改善報告[7]。

依本案例而言，該市政府之上級機關為行政院，故市府應將資通安全事件之發

---

[5] 資通安全事件通報及應變辦法第 3 條

[6] 資通安全事件通報及應變辦法第 4 條：「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。　前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。」資通安全事件通報及應變辦法第 11 條：「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。　前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。」

[7] 資通安全事件通報及應變辦法第 6 條：「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事宜：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。公務機關依前項規定完成損害控制或復原作業後，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。　前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。上級、監督機關或主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。」資通安全事件通報及應變辦法第 13 條：「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事宜：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。特定非公務機關依前項規定完成損害控制或復原作業後，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。　前項調查、處理及改善報告送交之時限，得經中央目的事業主管機關同意後延長之。中央目的事業主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應於審查後送交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。」

生機關、發生或知悉時間、狀況之描述、等級之評估、因應事件所採取之措施、外部支援需求評估以及其他相關事項，依案情輕重透過指定方式向行政院為通報[8]，而此次受損情形為市政府全球資訊網無法連線，應屬業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運，而為核心資通系統[9]。因此，當核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作，則屬第三級資通安全事件，該市政府應於知悉事件後 36 小時內完成損害控制或復原作業[10]，依主管機關指定之方式及對象辦理通知，並在完成損害控制或復原作業後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。

---

[8] 按行政院於 105 年 8 月 1 日正式成立資通安全處(以下簡稱資安處)，由行政院層級統整國家資通安全機制，以專責、專業、專人之方式，推動國家整體資安工作，並由資安處直接指揮及督導「國家資通安全技術服務中心」(以下簡稱技服中心)相關資安業務及工作。技服中心依據第五期發展方案與「國家資通安全戰略報告」，主要業務範圍如下：一、研議資安法規、規範及指引；研析我國整體資安威脅情勢，掌握資安風險與防護現況，完備國家資安基礎環境。二、建立政府資安治理成熟度模式；建構巨量資料分析能量，強化政府機關(構)資安聯防監控。三、規劃及推動政府機關(構)資安整體防護，建立全方位資安防禦縱深機制。四、推動國家層級資安聯防體系，建立資安情資分享機制，維運資安資訊分享與分析中心(National-Information Sharing and Analysis Center, N-ISAC)及電腦緊急應變中心(National-Computer Emergency Response Team, N-CERT)及資安聯防監控中心(National-Security Operation Center, N-SOC)等。五、協助政府機關(構)處理資安事件，加強緊急應變及處理復原能力；辦理網路攻防演練，輔以資安稽核與技術檢測，提升政府機關(構)之資安防護、監控、預警、管理及通報應變能力。六、推動關鍵基礎設施之資安防護，建立國家層級資安風險評估機制。七、規劃政府資安職能發展藍圖，辦理職能評量，持續培育資安專業人才，推廣全民資安意識。八、推動資安學研合作，促進國際交流合作與經驗分享。九、其他與資通安全相關之業務。

[9] 資通安全事件通報及應變辦法第 2 條說明 2：「所定核心業務，依資通安全管理法施行細則第七條第一項之規定認定；所定核心資通系統，依該細則第七條第二項之規定認定，併予敘明。」而資通安全管理法施行細則第 7 條：「前條第一項第一款所定核心業務，其範圍如下：一、公務機關依其組織法規，足認該業務為機關核心權責所在。二、公營事業及政府捐助之財團法人之主要服務或功能。三、各機關維運、提供關鍵基礎設施所必要之業務。四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第四款涉及之業務。前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。」故按該條第 1 項第 4 款而指涉依資通安全責任等級分級辦法第 5 條第 2 款：「業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。」故市政府全球資訊網，應屬業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運，而為核心資通系統。

[10] 資通安全事件通報及應變辦法第 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事宜：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。」

【管理 Tips】

資通安全事件發生時，公務機關及特定非公務機關負有通報義務，然而，通報雖是義務，但平時若無演練，如遇資通安全事件發生時亦容易反應不急，因此，資通安全事件通報及應變辦法亦要求公務機關及特定非公務機關訂定資通安全事件通報及應變之作業規範。

就一般組織而言，可參考資通安全事件應變作業規範之要求，建立資通安全事件作業規定，作為事件發生時的處理參考，其包括應變小組之組織、事件發生前之演練作業、事件發生時之損害控制機制、事件發生後之復原、鑑識、調查及改善機制、事件相關紀錄之保全及其他資通安全事件應變相關事項，以作為於知悉資通安全事件後，得迅速確實進行資通安全事件應變之依據。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.16.1.1　責任及程序

(1) 標準內容：　應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。

(2) 適用說明：　就資通安全事故而言，組織應建立自身之應變程序，並將之文件化，以確保資通安全事故發生時，組織人員能依循該文件之程序進行後續處理。

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：　公務機關與特定非公務機關於資通安全事件發生時，負有通報主管機關或目的事業主管機關之義務，且該通報應依

照資通安全事件通報及應變辦法之相關規定加以處理。

類別：資訊保護【案號：S10807】

遠端遙控軟體被用來攻擊政府單位

【焦點話題】

遠端遙控軟體是企業經常使用的合法軟體，其功能在於連線遠端電腦，提供遠端支援及共享桌面。亦因如此，遠端遙控軟體成為網路攻擊者及詐騙者用於獲得系統的欺詐性存取。然而，研究人員表示近來發現遠端遙控軟體武器化之惡意軟體，主要以歐洲及其他地區的政府和金融資訊為目標。

其感染媒介則以典型網路釣魚電子郵件開啟，郵件包含聲稱係來自美國「機密」檔案的惡意附件，且為取信於人，該附件甚至使用美國國務院標誌，當使用者打開附件後將自動開啟遠端遙控軟體，進而竊取使用者電腦之資訊。

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

【重點摘要】

1. 為因應現時外國、大陸地區、香港、澳門之威脅，以有效確保國家安全及利益，因此增加如洩漏、交付、刺探或收集國家機密或報請核定之國家機密的對象為外國、大陸地區、香港、澳門或其派遣之人者，按新修正之國家機密保護法第 32 條至第 34 條規定，不論其犯罪類型或管道，均較單純洩漏、交付、刺探或收集時更為加重刑度之規定。

2. 國家機密保護法第 11 條與第 12 條規定，當核定為國家機密後，原則上應至保密期限期滿或解除機密之條件成就後，方得解密，而涉及國家安全情報來源或管道之國家機密，更應永久保密。

【法律觀點】

國家機密保護法訂於民國 92 年，以保護攸關國家安全或國家利益之國家機密為主，及確保國家安全利益，而不包括其他一般公務機密或純屬私人利益之隱私

或營業秘密事項[1]。國家機密之定義兼採實質與形式要件，除實質上須為確保國家安全或利益而有保密之必要外，亦應由國家機密保護法規定核定其機密等級者，始足當之，並以政府機關持有或保管之資訊為限[2]。而國家機密保護法將機密等級區分為「絕對機密」、「極機密」以及「機密」[3]，各機關之人員於其職掌或業務範圍內，有應屬國家機密之事項時，應按其機密程度擬訂等級，先行採取保密措施，並即報請核定；有核定權責人員，應於接獲報請後三十日內核定[4]，當核定為國家機密後，原則上應至保密期限期滿或解除機密之條件成就後，方得解密[5]，而涉及國家安全情報來源或管道之國家機密，更應永久保密[6]。

原本國家機密保護法僅針對洩漏、交付、刺探或收集經依國家機密保護法核定或報請核定之國家機密者，課以刑事責任[7]。然因應現時外國、大陸地區、香

---

[1] 國家機密保護法第 1 條立法理由。

[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] 國家機密保護法第 6 條。

[5] 國家機密保護法 11 條：「核定國家機密等級時，應併予核定其保密期限或解除機密之條件。　前項保密期限之核定，於絕對機密，不得逾三十年；於極機密，不得逾二十年；於機密，不得逾十年。其期限自核定之日起算。　國家機密依前條變更機密等級者，其保密期限仍自原核定日起算。　國家機密核定解除機密之條件而未核定保密期限者，其解除機密之條件逾第二項最長期限未成就時，視為於期限屆滿時已成就。　保密期限或解除機密之條件有延長或變更之必要時，應由原核定機關報請其上級機關有核定權責人員為之。延長之期限不得逾原核定期限，並以二次為限。國家機密至遲應於三十年內開放應用，其有特殊情形者，得經立法院同意延長其開放應用期限。　前項之延長或變更，應通知有關機關。」

[6] 國家機密保護法第 12 條第 1 項：「涉及國家安全情報來源或管道之國家機密，應永久保密，不適用前條及檔案法第二十二條之規定。」

[7] 108 年 5 月修正前之國家機密保護法第 32 條：「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。　因過失犯前項之罪者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。　第一項之未遂犯罰之。」108 年 5 月修正前之國家機密保護法第 33 條：「洩漏或交付依第六條規定報請核定國家機密之事項者，處五年以下有期徒刑。　因過失犯前項之罪者，處一年以下有期徒刑、拘役或科或併科新臺幣十萬元以下罰金。　第一項之未遂犯罰之。」108 年 5 月修正前之國家機密保護法第 34 條：「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。　刺探或收集依第六條規定報請核定國家機密之事項者，處三年以下有期徒刑。　前二項之未遂犯罰之。」

港、澳門之威脅，以有效確保國家安全及利益，因而增加洩漏、交付、刺探或收集國家機密或報請核定之國家機密的對象為外國、大陸地區、香港、澳門或其派遣之人者，不論其犯罪類型或管道，更為加重刑度之規定[8]，且為更有效之防範，並增訂預備犯及陰謀犯之處罰規定[9]。另外，考量洩漏或交付絕對機密者，足以使國家安全或利益遭受非常重大之損害，故增訂當所洩漏、交付、刺探或收集者屬於絕對機密或擬訂等級為絕對機密時，加重其刑至二分之一的規定[10]。

然而，如本案例發生於我國，首先應先確認被刺探或收集者是否屬於政府機關持有或保管之資訊，如否，則不適用國家機密保護法；如是，則應判斷被刺探或收集之客體是否屬於經核定的國家機密或報請核定國家機密者，如否，則因其係無故透過社交工程方式入侵他人之電腦，行為人恐構成刑法妨害電腦使用罪。如被刺探或蒐集者屬於經核定的國家機密或報請核定國家機密時，則需要再行判斷刺探或收集者是否具有特殊性，意即是否為外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人，如屬上開人等，則依法可處一年以上七年以下有期徒刑，且如所刺探或收集屬絕對機密或其擬訂等級屬絕對機密之事項時，最重可處十年六個月的有期徒刑。

【管理 Tips】

犯罪集團透過網路攻擊政府或特定單位之新聞時有耳聞，如美國巴爾的摩市府於

---

[8] 國家機密保護法第 32 條第 2 項：「洩漏或交付前項之國家機密於外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人者，處三年以上十年以下有期徒刑。」、同法第 33 條第 2 項：「洩漏或交付依第六條規定報請核定國家機密之事項於外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人者，處一年以上七年以下有期徒刑。」、同法第 34 條第 2 項：「為外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人刺探或收集經依本法核定之國家機密或依第六條規定報請核定國家機密之事項者，處一年以上七年以下有期徒刑。」

[9] 國家機密保護法第 32 條第 5 項：「預備或陰謀犯第一項或第二項之罪者，處二年以下有期徒刑。」、同法第 33 條第 5 項：「預備或陰謀犯第一項或第二項之罪者，處一年以下有期徒刑。」、及同法第 34 條第 2 項：「預備或陰謀犯第一項、第二項或第三項之罪者，處一年以下有期徒刑。」

[10] 國家機密保護法第 32 條第 6 項：「犯前五項之罪，所洩漏或交付屬絕對機密者，加重其刑至二分之一。」、同法第 33 條第 6 項：「犯前五項之罪，所洩漏或交付屬擬訂等級為絕對機密之事項者，加重其刑至二分之一。」、同法第 34 條第 6 項：「犯前五項之罪，所刺探或收集屬絕對機密或其擬訂等級屬絕對機密之事項者，加重其刑至二分之一。」

2019 年受駭客使用名為 RobbinHood 的勒索軟體感染大約 1 萬台市府電腦，並要求支付比特幣[11]。其犯罪手法多以社交工程[12]方式，導致缺乏警覺性的使用者十分容易掉入陷阱。

面對社交工程之因應可分由兩種角度，第一，就組織角度而言，組織應對於權限加以分級控管，非屬各單位執掌之事務，不應掌握帳號、密碼等特殊權限；安裝防毒軟體，設定個人防火牆，並定期更新病毒碼；針對電腦系統及應用程式隨時更新修補程式；強制設定安全密碼；判定資料等級並予以加密。第二，就個人角度而言，應隨時具備危機意識，對於不明來源之可疑電子郵件不予開啟；不隨意點擊電子郵件之附件檔與超連結；如有疑似社交工程之行為，應立即回報相關管理單位，並進行事件記錄。

畢竟社交工程係利用人性弱點加以攻擊，而「人」又是組織內最難以掌握的一環，因此透過組織與個人之角度雙管齊下，方能將組織所面臨到的風險降至最低。

【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：　組織應對其員工或相關之約用人員能進行有效之教育訓練，使組織成員能了解到社交工程的重要性，以及應如何

[11] https://gizmodo.com/hackers-are-holding-baltimores-government-computers-hos-1834948639 (瀏覽日期：2019 年 6 月 10 日)

[12] 社交工程(Social Engineering)係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。https://nicst.ey.gov.tw/Page/16FFA138E66A0905/6aececb4-50ec-4c3e-b331-d8e0ddfc4586 (瀏覽日期：2019 年 6 月 10 日)

避免受到其攻擊，應能有效降低組織據此所面臨到的風險。

ISO 27001：2013(CNS 27001)

- A.9.2.2　使用者存取權限之配置

(1) 標準內容：　應實作正式之使用者存取權限配置程序，已對所有形式之使用者針對所有系統及服務，指派或撤銷存取權限。

(2) 適用說明：　組織應對權限建立分級控管，非屬個人分內事宜，不應掌握帳號、密碼等特殊權限，如不幸發生事故時，亦可降低產生的損害。

類別：資訊保護【案號：S10808】

通訊軟體遇「國家級網絡攻擊」 與示威同時發生

【焦點話題】

香港人民由於反對修訂《逃犯條例》走上街頭示威，抗議民眾廣泛使用於互相溝通及交換資訊的通訊軟體遭到來自中國的分散式阻斷服務攻擊（Distributed Denial of Service, DDoS），該通訊軟體官方回應駭客係利用「殭屍網路」發動攻擊，其利用預先埋入其他電腦的惡意程式，於同時間向單一目標發動攻擊，致使美國及部分其他國家的用戶出現網路連接問題。而該次攻擊事件被認為是國家級駭客攻擊，皆是因為其攻擊時間與香港示威抗議活動同時發生，並非個別事件。

【參考資料來源：明報，108/6/13】

【重點摘要】

1. 透過分散式阻斷服務攻擊「干擾」使用者電腦或其相關設備，以達到癱瘓使用者之電腦或其相關設備之效果，造成使用者無法正常使用電腦或其相關設備，將觸犯刑法第 360 條之干擾電腦或其相關設備罪。
2. 限制點對點加密傳輸軟體於組織內使用可透過閘道防火牆、入侵預防系統、用戶端防火牆以及資安政策等方式，避免組織成員不當使用點對點加密傳輸軟體，造成組織損失。

【法律觀點】

阻斷服務攻擊（Denial-of-Service Attack，簡稱 DoS 攻擊）又稱洪水攻擊，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」（意即傀儡機或肉機），組織成數個命令與控制節點傳送偽造包或垃圾封包，向特定的目標發動阻斷服務式攻擊，使預定攻擊目標癱瘓，稱為「分散式阻斷服務攻擊」（Distributed Denial-of-Service Attack，簡稱 DDoS 攻擊）

[1]，亦稱為「殭屍網路」（Botnets）[2]。

而本案如發生於我國，屬行為人透過「干擾」使用者電腦或其相關設備，以達到癱瘓之效果，造成使用者電腦等設備無法正常運作致生損害，恐遭處以三年以下有期徒刑、拘役或科或併科十萬元以下罰金3。另外，如有製造專供妨害電腦使用等設備之電腦程式，且有利用並造成損害之事情，恐處以五年以下有期徒刑、拘役或科或併科二十萬元以下罰金4。因此，無故妨害他人電腦及製造妨害電腦之使用程式皆會構成犯罪，應小心謹慎，以免誤滔法網。

【管理 Tips】

本案中之通訊軟體係支援雙重認證（two-step verification）及點對點加密傳訊，甚至可以設定訊息「閱後刪除」或「定時刪除」，確保訊息不留痕跡，因此受到重視隱私者之喜愛。而其中最受重視隱私使用者重視的則是「點對點加密傳訊」功能，係因於一般狀況，通訊軟體通常採用「裝置對伺服器及伺服器對裝置」的加密資料傳輸模式，而「點對點」加密資料傳輸模式，係透過去中心化的網路傳輸，使資料僅存放於使用者端，並未透過伺服器為中介，因此伺服器端並無法取得使用者所傳輸之資訊，以保障使用者隱私。

然而，亦因「點對點」加密傳輸軟體的保密效果，以致外界無法取得使用者傳輸內容，故被認為是駭客與病毒溫床。因此，目前針對如何防堵「點對點」加密傳輸軟體帶來的潛在威脅，亦是各組織須進一步解決的問題。

首先，透過閘道防火牆設定規則阻擋已知的軟體通訊埠，意即「擋 Port」之作法，但目前大多數之點對點加密傳輸軟體多支援使用亂數通訊埠，發現其通訊埠受阻擋時，會跳用至其他通訊埠，故透過閘道防火牆的效果較弱；第二，透過入侵預防系統（Intrusion Prevention System, IPS）廠商所提供之入侵偵測特徵，利用

---

[1] https://zh.wikipedia.org/wiki/阻斷服務攻擊 最後瀏覽日：108 年 6 月 17 日。

[2] https://zh.wikipedia.org/wiki/殭屍網絡 最後瀏覽日：108 年 6 月 17 日。

[3] 刑法第 360 條規定：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[4] 刑法第 362 條規定：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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。」

封包特徵擋下通訊，此方法係利用個別軟體發出的封包於表頭檔均有個別特徵，而入侵預防系統則可透過該特徵，阻擋點對資料傳輸，不過目前亦已有軟體會進行「表頭加密」，使入侵預防系統無法得知；第三，透過用戶端防火牆，直接限制未許可的軟體對外連線，此方法係為最簡潔的方法；第四，以資安政策要求組織成員，明確規範使用規則，以技術手段外之政策規範成員，使組織成員有所遵循。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.12.6.2　對軟體安裝之限制

  (1) 標準內容：　應建立並實作使用者安裝軟體之管控規則。

  (2) 適用說明：　以資安政策要求組織成員，明確規範使用規則，限制成員安裝非受允許之軟體，尤其是具有對外連線可能之通訊軟體，避免組織遭受到損害。

- A.13.2.1　網路傳送政策及程序

  (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形式通訊設施之資訊傳送。

  (2) 適用說明：　使用網路傳送包括文字或檔案等資訊時，組織應具有政策對所傳送的程序及手段加以規範，避免非允許之狀態下傳送資訊，如此方可降低不當的資訊傳輸，甚至是外部惡意軟體的攻擊。

類別：資訊保護【案號：S10809】

監視器對準鄰居家門口 老師判賠萬元

【焦點話題】

朱男不滿認為邱姓鄰居於自家窗戶架設雲端監視器，將鏡頭對準朱男家門口，長期監視朱男及其家人生活作息，且寄予存證信函以要求改善，惟邱姓鄰居僅拆除監視器線路，嗣後才將監視器拆除。朱男認為邱姓鄰居 24 小時監控，已逾比例原則，侵害其隱私權、人格權請求移除侵害及要求賠償。而邱姓鄰居則認為監視器所設範圍係於自家花園及被告門口前，未拍攝其房屋內部，且未想侵害朱男隱私，無故意之意。他收到鄰居朱男的存證信函，立即拆除監視器線路，爾後亦自行拆除監視器。然而，法官認為邱姓鄰居雖非故意侵害，但已造成隱私權侵害無誤，審酌邱姓鄰居裝設監視器至自動拆除，僅約 4 個月，朱男請求賠償金額過高，最後判處賠償 1 萬元。

【參考資料來源：聯合報，107/3/28；臺灣高等法院臺中分院 107 年上易字第 208 號民事判決】

【重點摘要】

1. 我國法院（如臺灣高等法院 106 年上字第 651 號民事判決、臺灣桃園地方法院 107 年訴字第 2382 號民事判決）多認定公寓大廈當層之電梯間通道樓板等俗稱為「小公」之共有部分，可得特定出入人士為當層住戶及其訪客，乃為可得特定之人，並非眾人均得自由通行、使用之公共區域，各當層住戶當得保有其生活之隱私具備合理隱私期待。

2. 臺北市錄影監視系統設置管理自治條例第 5、8、11 及 13 條規定，架設公有監視器前需申請並經由警察局准駁，而資料應予保密且除有必要外一年內應銷毀。

【法律觀點】

科技日益進步，監視器研發不斷創新，相較於過去監視器之解析度及拍攝範圍皆大有進步，造成的糾紛更勝以往。監視器可拍攝範圍其判斷標準亦成為眾人

所關注的重點，而我國法院係以「合理隱私期待」為準，判斷是否侵害隱私，有論者[1]參酌法院判決後，提出可由「侵害場所」、「侵害手段」及「資訊性質」加以觀察。

首先，就侵害場所而言，若涉及住家時，通常會給予高度保障，係因此為私人不可侵害領域，包含通訊保障及監察法亦禁止私人住宅之通訊監察[2]。當侵害場所屬於住家以外之場所，則應檢視場所性質是否類同於住家，若該場所屬公共場所，則應進一步檢視侵害手段及資訊性質。然就侵害手段而言，物理侵入通常可認為是一種侵略性較高的手段，但如以常見普遍之科技工具侵入，且係一般人可明確意識之情形，愈可能降低合理隱私期待。再者，就資訊性質而言，所蒐集的資訊愈足以揭示個人的私生活或具高度私密性時，亦有更高可能主張具有合理隱私期待。

以私人監視器架設為例，應先檢視侵害場所是否涉及住家，我國法院認定公寓大廈進出該層樓電梯及走道等公共空間，可得特定出入人士為當層住戶及其訪客，應具備合理隱私期待[3]，且其性質屬私領域空間，應受保護。

本案例並非上開所述之電梯及走道等公共空間，屬於住家以外之場所，但亦非純然的公共場所。事實上，法院對於社區公共空間是否具有合理隱私期待素有爭議，部分法院判決認為社區中庭及大門口非屬私人空間，應不具備合理隱私期待[4]，相反地，亦有部分法院判決認為社區中庭僅有社區住戶及經住戶允許之人方得進入，屬於私領域空間[5]，故具有隱私合理期待。

---

[1] 李明勳，合理隱私期待之研究—以定位科技為例，國立政治大學法律學研究所碩士論文，中華民國 102 年 7 月，頁 183-186。

[2] 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。」

[3] 臺灣新北地方法院 105 年訴字第 144 號民事判決。

[4] 臺灣桃園地方法院 107 年訴字第 2382 號民事判決：「而系爭社區中庭及大門口非屬私人空間，亦非如公寓大廈當層之電梯間通道樓板等俗稱為「小公」之共有部分（可得特定出入人士為當層住戶及其訪客，具備合理隱私期待），而係任何經過之人得隨時看見、並無任何隱密性可言之公共空間，是住戶或訪客於中庭活動均應有予不特定人知悉之認知。」。

[5] 臺灣高等法院臺中分院 107 年上易字第 208 號民事判決：「兩造房屋位於設有管理委員會、有門禁管制之社區，被上訴人住家大門前方固直接銜接社區中庭，然亦僅有社區住戶及經住戶允許之人員得進入該區域，並

然而，本案例爭點在於邱姓鄰居所裝設監視器之拍攝範圍，其一鏡頭對準於朱男家大門口且非僅有花圃範圍，而監視器所拍攝之影像內容，足以知悉朱男之生活作息動態、親友到訪、人際交往狀況等私人資訊。就資訊性質而言，當所蒐集之資訊足以揭示個人私生活，屬私人活動領域內應受保護之權利，即應受隱私權保護之範疇，但因邱姓鄰居已自行移除監視器，且侵害範圍與時間之情節不大，故判賠非財產上損害一萬元。

【管理 Tips】

近年來，資訊設備普及與平價化，民眾對於環境安全亦高度重視，除政府所架設置之公有監視器[6]外，民眾亦自行架設監視器，以作為事前預防或事後提供證據保護自己的手段。

就組織之角度而言，無論架設監視器之理由係為提升人身或財產安全，皆應建立有效之管理程序，並進行事前評估以降低違法風險。以台北市政府為例，架設公有監視器需申請並經由警察局准駁[7]，資料應予保密[8]且除有必要外一年內應銷毀[9]。而上述步驟套用至組織於架設監視器時，其應先經內部獨立單位進行評估，資料應存放於安全無虞之處，如有利用監視器資料之需求應進行申請，且資料應於一定時間內銷毀，藉以降低違法之風險。

【相關標準】

非一般不特定之公眾均能自由出入之場所，故被上訴人就其於住家大門前方之區域，仍存有隱私之合理期待，應屬被上訴人之私領域空間。」

[6] 以台北市為例，按臺北市錄影監視系統設置管理自治條例第 4 條第 2 項規定：「錄影監視系統之主要攝影方向，應以公共場所為主，不得針對特定私人處所設置。」因此，針對公有監視器而言，政府係已考量到不得據此侵犯個人隱私。

[7] 臺北市錄影監視系統設置管理自治條例第 5 條第 1 項：「市政府所屬各機關設置錄影監視系統，應向警察局提出申請並經核准後始得設置。」及同條例第 8 條第 1 項：「警察局應於受理申請後三十日內，以書面通知設置許可之准駁結果。」

[8] 臺北市錄影監視系統設置管理自治條例第 11 條：「錄影監視系統影音資料應予保密，非依法定程序，不得處理及利用。」

[9] 臺北市錄影監視系統設置管理自治條例第 13 條：「錄影監視系統影音資料，除其他法律另有規定或因調查犯罪及其他違法行為，有繼續保存之必要者外，至遲應於一年內銷毀之。」

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： 就監視器設置所拍得之影像，如可識別特定個人時，就已屬於個人資料，此時依法應對該資料進行有效的控管以及保護，避免因資安事故造成組織及當事人之損害。

類別：資訊保護【案號：S10810】

因應國家機密保護法修法　調整涉密人員出境管制期間

【焦點話題】

《國家機密保護法》民國 108 年 5 月 10 日修正通過後，自 108 年 5 月 12 日起施行，重點為之一為：刪除涉密人員退離職後可縮短出境管制期限規定，並明定管制時間最長可達六年。是以，總統府於研議後，正式發函予卸任總統、副總統等卸任涉密人員，調整管制期限。係因《國家機密保護法》及《臺灣地區與大陸地區人民關係條例》規定，對於卸任涉密人員之出境或赴陸管制是否延長，總統府作為原服務機關有責任審酌當事人涉密程度，站在國家安全與利益做適當的處置。並考量國家機密公文最低保密期限為十年，對於涉密程度極高的重要人員如卸任總統、副總統等予以適度延長，符合法律規範及比例原則。

【參考資料來源：自由時報，108/5/17】

【重點摘要】

1. 國家機密保護法第 26 條第 1 項規定，國家機密核定人員、辦理國家機密事項業務人員，以及前二者之退、離職或移交國家機密未滿三年之人員，如欲出境應經其 (原) 服務機關或委託機關首長或其授權之人核准，審酌其守密程度等相關事由後據以准駁。

2. 按國家機密保護法第 26 條及第 12 條規定，因應現時面臨之外境威脅及嚇阻不法洩漏國家機密事件發生，退離職或移交業務涉密人員之出境管制，國家機密核定機關得視情形延長管制期間，而其延長原則上僅以一次為限，且不得逾三年但如有應永久保密的涉及國家安全情報來源或管道之國家機密時，可不限次數的延長。

【法律觀點】

國家機密保護法自 92 年 10 月 1 日施行迄今，已逾 15 年，其立法目的乃係為

建立國家機密保護制度，以確保國家安全與利益[1]。而國家機密攸關國家安全及利益，當涉及國家機密之退離職人員得任意出境，在外恐易發生洩漏國家機密之情事，將造成國家安全及利益之重大損害。因此，國家機密保護法規定，國家機密核定人員、辦理國家機密事項業務人員及前二者之退、離職或移交國家機密未滿三年之人員，如欲出境應經其 (原) 服務機關、委託機關首長或其授權之人核准，審酌其守密程度等相關事由後據以准駁，如其涉密不深或無發生洩密之虞，亦自應予准許[2]。

再者，為因應現時面臨之外境威脅及嚇阻不法洩漏國家機密事件發生，本次修法將原本退離職或移交業務涉密人員之出境管制期間國家機密核定機關得視情形延長或縮短，改為僅得延長，延長原則僅以一次為限，且不得逾三年，意即最多不可超過六年，惟如涉及國家安全情報來源或管道之國家機密，應予以永久保密[3]。

【管理 Tips】

國家機密是為國家生存之本，如由掌有國家機密人員任意資敵，將使國家蒙受嚴重傷害。因此，我國實務上針對涉密人員之出境，可區分為事前列冊及事中准駁，事前要求機關必須繕具辦理或核定國家機密現職退離職或移交人員建檔名冊，函送內政部移民署限制出境[4]。而當名冊內之人員有出境需求時，應於出境前檢具出境行程、所到國家或地區、從事活動及會晤之人員等書面資料，向

---

[1] 國家機密保護法第 1 條。

[2] 國家機密保護法第 26 條第 1 項：「下列人員出境，應經其（原）服務機關或委託機關首長或其授權之人核准：一、國家機密核定人員。二、辦理國家機密事項業務人員。三、前二款退離職或移交國家機密未滿三年之人員。」

[3] 國家機密保護法第 12 條第 1 項：「涉及國家安全情報來源或管道之國家機密，應永久保密，不適用前條及檔案法第二十二條之規定。」

[4] 辦理或核定國家機密現職退離職或移交人員出境作業規定第 3 條：「涉及國家機密人員依本法第二十六條第一項規定，應經核准始得出境；其（原）服務機關或委託機關（以下簡稱限制機關），應繕具辦理或核定國家機密現職退離職或移交人員建檔名冊（格式如附件一），函送內政部移民署（以下簡稱移民署）限制出境，並通知當事人。有異動時，並應於異動後七日內，通知移民署及當事人。但限制機關另有出境管制規定者，依其規定。」

機關提出申請[5]，並經機關准許後方得出境。

不過，一般民間組織並無如政府一般具有強大的公權力，惟仍須以其他方式限制現離職人員之保密責任。首先，組織應於員工到職時，要求簽署保密承諾書，使其瞭解相關規範以確實遵循。其次，組織應依員工之業務需求，給予適當之權限，以保護組織重要機密。最末，組織亦應建立離職程序，確認離職員工所掌握之資料不為私人攜出，以避免後續紛爭產生。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.7.1.2　聘僱條款與條件

  (1) 標準內容：　組織與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。

  (2) 適用說明：　在聘僱員工時，組織即應於聘僱契約敘明保密義務等資訊安全相關條款，要求員工於現退離職時，均對組織機密負有保密責任，避免因機密外洩導致組織受到嚴重傷害。

- A.9.2.2　使用者存取權限之配置

  (1) 標準內容：　應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。

  (2) 適用說明：　組織於系統使用時應建立名冊，對使用者進行紀錄，並依其需求與層級賦予相對應的存取權限，且應定期檢視使用者存取權限之必要性，如使用者無需求目的時，即應撤銷

[5] 國家機密保護法施行細則第 32 條第 2 項：「本法第二十六條第一項各款所定人員出境，應於出境二十日前檢具出境行程、所到國家或地區、從事活動及會晤之人員等書面資料，向（原）服務機關或委託機關提出申請，由該機關審酌申請人之涉密、守密程度等相關事由後據以准駁，並將審核結果於申請人提出申請後十日內以書面通知之。但申請人為機關首長，或現任職原服務機關或委託機關之上級機關者，其申請應向上級機關提出，並由該上級機關首長或其授權人員予以准駁。」

其存取權限，以降低不當存取發生之可能性。

類別：資訊保護【案號：S10811】

保險電銷 客戶不想聽須立刻停止行銷

【焦點話題】

金融管理機關早於 106 年針對銀行業者訂有銀行業電話行銷應遵循原則，明確規範銀行業者從事電話行銷行為時，消費者表明不願接收行銷電話後，即不得再以電話行銷之方式推廣其金融商品或服務。惟針對保險業之電話行銷則無特別規定，以致消費者往往有電話掛不斷等擾民情形，引發反感。

因此，金融管理機關於 108 年 2 月公布最新保險業、保險經紀及代理人電話行銷業務應注意事項，其中增訂消費者如於電話線上表達拒絕接受行銷時，電話行銷人員應立即停止行銷，以尊重消費者拒絕接受行銷之權利，不得用任何方式繼續陳述、強迫消費者聆聽。未來如有消費者陳情保險業者之電銷人員有違反規定之情形，調閱錄音確定屬實，主管機關將依保險法規定發罰。

【參考資料來源：中時電子報，108/2/13】

【重點摘要】

1. 保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 5 點第 2 項規定保險業者之電話行銷人員，在消費者於電話線上表達拒絕接受行銷時，電話行銷人員應立即停止行銷。
2. 個人資料保護法第 20 條第 2 項對於利用個人資料為行銷時，如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，且該法第 48 條亦規定違反停止行銷規定時，主管機關得按次處新臺幣 2 萬元以上 20 萬元以下罰鍰。

【法律觀點】

現今通訊數位科技發達，透過各式數位科技管道用以行銷產品或服務，而電話行銷乃為最常見之方式。由於電話行銷的便捷性，廣受各大業者使用，尤以保

險業及金融業最為廣泛，其中電話行銷人員易於行銷過程造成消費者困擾，且個人資料保護法於 104 年修正公布，對於利用個人資料為行銷時，如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，如違反規定者，主管機關得按次處新臺幣 2 萬元以上 20 萬元以下罰鍰[1]。是以，主管機關為此於 108 年 2 月修正《保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項》（下稱保險業電話行銷注意事項規定），針對保險業、保險代理人公司及保險經紀人公司以電話行銷方式招攬保險之行為進行規範，以保障消費大眾權益，以維護其專業形象。

依照保險業電話行銷注意事項規定，保險業、保險代理人公司及保險經紀人公司所屬電話行銷人員應向消費者說明告知個人資料來源[2]，並表明保險電話行銷目的、確認要保人之身分，並將電話行銷人員之姓名、登錄字號、所屬公司名稱、服務電話及保險契約重要內容完整告知要保人[3]。如消費者於電話線上表達拒絕接受行銷時，電話行銷人員應立即停止行銷[4]。

另外，針對保險業、保險代理人公司及保險經紀人公司處理電話行銷業務，應將該注意事項內容納入內部控制及業務招攬作業程序[5]，而未建立或未確實執行內部控制、稽核制度、招攬處理制度或程序時，應依保險法規定應限期改正，

---

[1] 個人資料保護法第 20 條第 2 項、第 3 項「非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。」

[2] 保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 5 點說明三「第二項有關保險業、保險代理人公司及保險經紀人公司所屬電話行銷人員應向消費者說明之內容包括行銷目的及告知個人資料來源。」

[3] 保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 6 點第 2 項。

[4] 保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 5 點第 2 項。

[5] 保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 13 點：「保險業應將本注意事項內容依保險業招攬及核保理賠辦法第六條第一項第四款規定納入內部之業務招攬處理制度及程序。　保險代理人公司及保險經紀人公司應將本注意事項內容依保險代理人公司保險經紀人公司內部控制稽核制度及招攬處理制度實施辦法第六條第一項規定納入內部之業務招攬處理制度及程序。　保險業、保險代理人公司及保險經紀人公司應遵循保險業、保險代理人公司或保險經紀人公司電話行銷作業流程（附件）辦理本項業務，並應訂定電話行銷管理辦法或內部作業程序，分別函報所屬公會備查，修正時亦同。」

或併處新臺幣 10 萬元以上 300 萬元以下罰鍰[6]。

且因保險代理人公司係代理保險業經營業務[7]，故保險代理人公司違反該項規定時，保險業亦得對其暫停代理或終止代理[8]。

綜上所述，無論是個人資料保護法或保險法相關規定，對於個人資料之行銷利用，均需使當事人知悉所應瞭解之事項，並予以其停止利用個人資料行銷之機會。

【管理 Tips】

無視當事人意願之電話行銷造成消費者困擾及虛耗組織資源，同時影響消費者對於行銷業者及商品之反感。因此，組織於電話行銷時，除注意電話行銷流程是否符合法律規範，避免觸法情形發生外。同時，組織亦須建立電話行銷作業流程：（一）透過事前教育訓練協助電話行銷人員熟悉其應遵循之規範；（二）透過電話錄音，在發生爭議時可查核電話行銷人員是否違反相關規定；（三）透過事後獎懲，針對保險業、保險代理人公司及保險經紀人公司進行管控，以達事前、事中及事後的全面性管理，並落實於組織作業流程中。

【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。

---

[6] 保險法第 167-3 條：「違反第一百六十五條第三項或第一百六十三條第五項準用上開規定，未建立或未確實執行內部控制、稽核制度、招攬處理制度或程序者，應限期改正，或併處新臺幣十萬元以上三百萬元以下罰鍰。」

[7] 保險法第 8 條：「本法所稱保險代理人，指根據代理契約或授權書，向保險人收取費用，並代理經營業務之人。」

[8] 保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 14 點：「保險業與保險代理人公司之代理契約，除應約定保險代理人公司應依本注意事項規定辦理外，並應約定保險代理人公司如有違反本注意事項之情事，保險業得依情節輕重，對保險代理人公司予以限期改善、暫停代理或終止代理等處理。」

(2) 適用說明：　組織應辨識出個人資料以及相關流程，使當事人依保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項或個人資料保護法請求拒絕行銷，組織方得依法為之。

ISO 27001：2013（CNS 27001）

- A.7.2.3　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：　組織在建立電話行銷作業流程時，應對電話行銷人員及其直屬主管應接受專業訓練，其應備資格、條件、教育訓練、管理及獎懲，透過教育訓練增進相關人等對電話行銷作業的知識、技術和核心能力，進而提昇員工與組織的績效水準，並降低錯誤發生的可能。

類別：資訊保護【案號：S10812】

藉承攬國軍工程刺探軍事機密 2 包商涉共諜案起訴

【焦點話題】

新北市中和區某工程公司張姓負責人及林姓合夥人疑被中國大陸吸收，收受中國大陸資金，涉嫌藉承攬國軍工程，欲刺探軍事機密及在外發展共諜組織，經臺灣高檢署調查發現，張姓、林姓包商在設立公司前，曾多次前往大陸，疑在大陸受中國大陸軍情人員吸收，並收受不明資金後返台，自 2016 年 6 月設立工程公司後，積極鎖定軍事營區、各縣市政府公共工程、捷運局及學校標案進行投標，其承攬範圍涵蓋國防部、陸軍司令部及海軍司令部等，得標「忠信營區阻絕設施整修工程」、「官兵體能訓練室整修工程」、「東澳嶺營區避雷針基座工程」、「石門營區營門設施整修工程」、「岳崙營區 P 庫浪板架設工程」等多項軍方標案，總得標金額達 6,796 餘萬元，並趁承攬軍方工程的機會，協助中國大陸刺探我國國軍電子、資訊及網路作戰等國防軍事秘密，經偵監多時後，於本年度 6 月中旬收網。

【參考資料來源：自由時報，108/9/2】

【重點摘要】

依國家安全法第 2-1 條、第 5-1 條及第 5-2 條規定，洩漏、交付或傳遞、刺探或收集關於公務上應祕密之文書與大陸地區者，依法最重得處 7 年以下有期徒刑，並得併科新臺幣 1,000 萬元以下罰金，且可能喪失請領退休給與之權利，已支領者並應追繳之。

【法律觀點】

近年屢傳中國大陸情報、政治作戰機關透過不肖人士接觸我國現役及退除役軍官，企圖蒐集、刺探我國國家機敏情報，或從事間諜行為，其中極少數我國國軍現役或退除役同仁因不堪利誘而出賣上述機敏情報予中國大陸情報、政治作戰機關、嚴重影響我國國家安全及其他盡忠職孚之國軍同仁

備戰任務、生命安全[1]，因此於 108 年 7 月施行之國家安全法，目的即在於補強現階段不足之處。

按新修正國家安全法規定，人民不得為外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人為發起、資助、主持、操縱、指揮或發展組織；洩漏、交付或傳遞、刺探或收集關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄[2]。其中洩漏、交付或傳遞、刺探或收集關於公務上應祕密之文書，而該公務上應祕密之文書係指對國家政務或事務上具有利害關係，且人民或相關法人無權要求政府提供之資訊而應保守之秘密始能維持國家政務或事務之推行者而言，非以有明文規定為唯一標準[3]。因此，只要符合上開要求，並非僅限於經依國家機密保護法[4]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、禁止公開者方屬於公務上應祕密之文書[5]，其他非國家機密保護法所規範應秘密之範圍，但屬公務上不得

---

[1] 立法院第 9 屆第 7 會期第 1 次臨時會第 1 次會議紀錄委員劉世芳提案要旨（一）。

[2] 國家安全法第 2-1 條：「人民不得為外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人為下列行為：一、發起、資助、主持、操縱、指揮或發展組織。二、洩漏、交付或傳遞關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄。三、刺探或收集關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄。」

[3] 參臺灣高等法院高雄分院 106 年度軍上訴字第 2 號刑事判決。

[4] 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。」因此，適用國家機密保護法者，首應依法核定該特定事項為國家機密，在未有核定的前提下，仍應適用國家安全法。

[5] 政府資訊公開法第 18 條第 1 項：「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

任意提供特定人以外非相關人員知悉之資訊者，亦可能成為「公務上應祕密之文書」[6]。

本案因當事人疑似向中國大陸情報人員刺探我國國軍電子、資訊及網路作戰等國防軍事秘密[7]，如提供之資料屬政府內部文件屬公務上應祕密之文書時，其行為係符合人民為大陸地區或其派遣之人，洩漏、交付或傳遞公務上應祕密之文書等資訊，依法最重得處 7 年以下有期徒刑，並得併科新臺幣 1000 萬元以下罰金[8]。其次，如該員為退休公務人員，按新修正同法第 5-2 條規定，將喪失請領退休給與之權利，已支領者並應追繳之[9]。

【管理 Tips】

組織應依照法律要求、價值、重要性及對未經授權揭露或修改之機敏性分級，透過資訊分級，可將資源有效集中於值得保護之資產上。

因此，如同組織於建立資訊安全管理措施時，應考量對分享資訊或限制資訊之效益及影響，以及法定事項，將資訊依其機密性、完整性及可用性，以及其他要求，作為資訊分級的依據，並對所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。

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。」

[6] 如行為人所刺探、收集、洩漏或交付依國家機密保護法所核定之國家機密時，則依國家機密保護法之相關規定予以處罰，最重可處 15 年以下有期徒刑。

[7] 國家安全法第 5-1 條第 2 項：「違反第二條之一第二款規定者，處一年以上七年以下有期徒刑，得併科新臺幣一千萬元以下罰金。」

[8] 另，刑法第 132 條第 2 項規定「非公務員因職務或業務知悉或持有第 1 項（即中華民國國防以外應秘密）之文書、圖畫、消息或物品，而洩漏或交付之者，處 1 年以下有期徒刑、拘役或 3 百元以下罰金」，則刑法第 132 條第 2 項之罰則顯較國家安全法第 5- 1 條規定為輕，且公務秘密與中華民國國防以外應秘密亦有重疊之情形，則行為人所為如同時該當於上開構成要件時，因保護之法益相同，應依法規競合之理論，適用國家安全法第 5-1 條規定論罪科刑。

[9] 國家安全法第 5-2 條：「軍公教及公營機關（構）人員，於現職（役）或退休（職、伍）後，有下列情形之一者，喪失其請領退休（職、伍）給與之權利；其已支領者，應追繳之：一、犯內亂、外患罪，經判刑確定。二、犯前條之罪、或陸海空軍刑法違反效忠國家職責罪章、國家機密保護法第三十二條至第三十四條、國家情報工作法第三十條至第三十一條之罪，經判處有期徒刑以上之刑確定。前項應追繳者，應以實行犯罪時開始計算。」

實作面若均具備相關程序可供參照，可使人員能清楚瞭解操作方式，避免不當存取，而明示人員責任及相對應的懲處，有助於人員認知及履行相關責任，透過契約義務反應資安政策並於其違反時給予懲處，均屬員工於建立資訊分級時，所不可缺漏的事項。

【相關標準】

ISO 27001：2013（CNS 27001）

- A. 8.2.1　資訊之分級

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

(2) 適用說明：　因組織資源有限，無法將組織內所有資訊均予以最高保密程度，且如所有資訊均予以最高等級保護，將使組織運作窒礙難行，故資訊分級為保護資訊的首要階段，透過資訊分級，能將揭露不致造成傷害或衝擊性低的資訊予以低程度的保護，而將精力置於揭露對組生存產生風險之資訊。

ISO 27001：2013（CNS 27001）

- A.7.1.2　聘用條款及條件

(1) 標準內容：　組織與員工及約用人員簽訂之契約化協議書，宜敘明雙方對資訊安全的責任。

(2) 適用說明：　透過員工的契約義務，反映組織資訊安全政策，並簽訂保密協定，使員工在違反法規或組織要求時，能先一步地進行必要處置。

類別：資訊保護【案號：S10813】

電信管理法三讀 5G 開放共網共頻共建

【焦點話題】

國家通訊傳播委員會預計於 108 年底啟動 5G 頻譜拍賣競標，因應釋照在即，加上電信法 1996 年修正後再無重大結構性修正，立法院會於今年 5 月三讀通過「電信管理法」，開放電信業者共用網路、共用頻譜、共同建設網路，以加速 5G 推展與市場參進。同時，為確保整體網路使用之安全，對公眾電信網路之設置及電信服務之提供訂有防護義務。

針對防務義務，明定主管機關得定期、不定期檢驗公眾電信網路，如涉及國安事項時，得限制採購及使用特定電信相關設備。條文亦明確規範申設公眾電信網路的資格、申請程序，並應符合國安、資通安全及通訊監察等功能需求。此外，為降低災害造成網路中斷無法服務之風險、提升公眾電信網路運作可靠度，主管機關有權界定「關鍵電信基礎設施」之範圍。

【參考資料來源：自由時報，108/5/31】

【重點摘要】

1. 電信管理法確立了共頻、共網及共建三大原則，讓企業得以設置符合其營運需求之電信網路，降低市場進入門檻同時訂有防護義務。不論申請使用電信資源之公眾電信網路者，或申請非使用電信資源之公眾電信網路者均應提出網路設置計畫，計畫內容應包括使用符合有關機關國家安全考量之電信設備、網路之資通安全偵測及防護規劃、使用符合主管機關公告之資通安全標準設備等 (電信管理法第 37 條及第 38 條)。

2. 組織在進行資通安全管理機制時，首應針對資產進行盤點，再就所盤點得出之資產進行風險評鑑以評估資通安全等級，進而對不同等級之風險進行不同程度的管理機制，並以之作為後續資源投入的依據。

【法律觀點】

立法院於 108 年 5 月三讀通過電信管理法，並於同年 6 月 26 日公布。本次修法精神係「健全匯流產業發展、鼓勵創新服務、促進市場公平競爭」、「促進頻率號碼等電信稀有資源和諧、有效、公平彈性運用」、以及「增進匯流基礎網路增設、維護效率與網路安全」[1]。

就電信事業管理方面，為確保國家資通安全防護，完善民眾隱私保護，要求設置使用電信資源之公眾電信網路之電信事業或其他經主管機關公告之電信事業，應訂定資通安全維護計畫。其中資通安全維護計畫內容應包括資通安全管理範圍及分級處理方式、符合資通安全管理驗證措施；資通安全維護計畫執行方式、資通安全事件聯防應變措施以及其他經主管機關指定有助於資通安全之管理措施[2]，未訂定資通安全維護計畫或未按計畫實施者最高得處新臺幣 100 萬元罰鍰，未改善者得連續罰[3]。

另外，關於使用公眾電信網路方面，除傳統利用電信資源包括頻率及電信號碼所設置的公眾電信網路外，基於網際網路相連之特性，無論是否使用電信資源之公眾電信網路，一律視為公眾電信網路，藉由課予一致性資安標準，以確保整體網路使用之安全[4]。而申請使用電信資源之公眾電信網路者應檢具申請書、營運計畫及網路設置計畫，向主管機關申請許可。且鑑於我國國際處境特殊，公眾電信服務之安全穩固與國計民生息息相關，故網路設置計畫須要求使用符合有關機關國家安全考量之電信設備、網路之資通安全偵測及防護規劃、使用符合主管機關公告之資通安全標準設備[5]，

---

[1] 參立法總說明。

[2] 電信管理法第 15 條第 1、2 項。

[3] 電信管理法第 79 條第 1 項第 13 款。

[4] 電信管理法第 36 條第 1 項：「公眾電信網路分類如下：一、使用電信資源之公眾電信網路。二、未使用電信資源之公眾電信網路。」

[5] 電信管理法第 37 條第 1 項第 5 至 7 款：「申請設置使用電信資源之公眾電信網路者應檢具申請書、營運計畫及網路設置計畫，向主管機關申請許可。經主管機關許可，始得營運及設置；其電信網路增設或變更者，亦同。...五、使用符合有關機關國家安全考量之電信設備。六、網路之資通安全偵測及防

違反相關規定者，最高可處 500 萬元罰鍰，並通知停止使用[6]。同時，設置公眾電信網路提供電信服務時，使用之電信設備應符合有關機關之國家安全考量，以及具有足以確保資通安全之偵測及防護功能，在公眾電信網路者未遵守於提供電信服務期間應遵守之義務時，主管機關應限期改正，未改正者，最重主管機關得命其終止使用[7]，且同時得處 100 萬元以下罰鍰。

另，為提升公眾電信網路持續運作之可靠度，以確保國家安全及消費者權益，明定主管機關基於公共利益之考量得指定公眾電信網路之全部或一部為關鍵電信基礎設施，且關鍵電信基礎設施設置者，亦必須訂定關鍵電信基礎設施防護計畫，經主管機關評定後實施[8]。

【管理 Tips】

在使用公眾電信網路時，無論是否使用電信資源，均有一定程度的資安風險，因此本次電信管理法修法亦以此為重點加以管理。而電信管理法相關子法尚未完成訂定的同時，目的事業主管機關仍須依據主管機關組織法之

護規劃。七、使用符合主管機關公告之資通安全標準設備。...」

同法第 38 條則規定未使用電信資源之公眾電信網路者，亦需檢具申請書及網路設置計畫，向主管機關申請許可。經主管機關許可，始得設置，且計畫中亦應有使用符合有關機關國家安全考量之電信設備、網路之資通安全偵測及防護規劃，以及使用符合主管機關公告之資通安全標準設備。

[6] 電信管理法第 74 條第 1、2 項：「違反第三十七條第一項規定，未經許可擅自設置使用電信資源之公眾電信網路者，處新臺幣五十萬元以上五百萬元以下罰鍰，並通知停止使用。　違反第三十八條第一項規定，未經許可擅自設置未使用電信資源之公眾電信網路者，經主管機關命其停止使用並限期改善；屆期未改善仍繼續使用者，處新臺幣五十萬元以上五百萬元以下罰鍰，並通知停止使用。」

[7] 電信管理法第 40 條第 1 項第 4、5 款，第 2 項第 4、5 款，第 3 項：「設置使用電信資源之公眾電信網路提供電信服務時，應符合下列規定：...四、使用之電信設備應符合有關機關之國家安全考量。五、具有足以確保資通安全之偵測及防護功能。...設置未使用電信資源之公眾電信網路提供電信服務時，應符合下列規定：四、使用之電信設備應符合有關機關之國家安全考量。五、具有足以確保資通安全之防護功能。網路架構及性能應符合前二項規定或其網路設置計畫。　不符合者，設置公眾電信網路者應依主管機關之通知，限期改正或限制使用；其情節重大者，主管機關得命其終止使用。」

[8] 資通安全管理法第 16 條亦有中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者之相關規定。

規定，已訂定之相關辦法作為管理依據[9]。現行相關辦法包括針對電信事業訂定之「電信事業資通安全管理手冊」，依據該手冊，電信事業管理作業包含資通安全之管理標準、等級評估、管理機制、教育訓練、應變通報以及實施評鑑[10]。

以資通安全等級評估為例，手冊要求評估資通安全等級，以定義資通安全範圍與邊界，確定資通安全需求水準，作為後續訂定風險處理優先順序之參考，而步驟則為 1. 調查營運所需之資產群組；2. 依據每一資產群組失效後之「衝擊影響程度」，評估資通安全等級，決定資通安全管理機制改善之優先順序，並每年定期更新。而評估資通安全等級則是將營運所需之資產群組全部納入後，針對個別資產群組依「影響業務運作」、「資料保護受到損害」、及「法律規章之遵循」等之影響構面，分別評定各影響構面之資產安全等級，區分為 A、B、C 三級，而個別資產群組中如有任一影響構面為高者，則取最高者為其資通安全等級，再依據不同等級給予不同的風險管理作為[11]。

而各組織在執行資通安全管理時，本亦應針對資產進行盤點，再就所盤點得出之資產進行風險評鑑，依照不同之資產安全等級，進行個別的風險管理作法，作為後續資源投入的依據。

【相關標準】

ISO 27001：2013（CNS 27001）

---

[9] 國家通訊傳播委員會組織法第 3 條第 8 款：「本會掌理下列事項：...八、資通安全之技術規範及管制。...」

[10] 電信事業資通安全管理作業要點第 2 點：「為執行電信事業資通安全管理作業，應製作電信事業資通安全管理手冊。　本手冊應符合保障通信安全及維護使用者權益之原則。其內容應包含下列各款事項：(一)資通安全管理標準。(二)資通安全等級評估。(三)資通安全管理機制。(四)資通安全教育訓練。(五)資通安全應變通報。(六)資通安全實施評鑑。　本手冊之研訂，應邀集相關業者、專家或機構共同討論，並視實施情況檢討修正。　本手冊訂定或修正完成，應循文書作業程序簽核並於本會網站公告。」

[11] 電信事業資通安全管理手冊 三、要項說明 (二)資通安全等級評估。

- 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：　對資產進行盤點之目的，在於確保資訊安全，一旦資產出現遺失或損毀的狀況，可能導致公司資料消失或洩漏，且資產盤點為風險評鑑之前階段，透過資產清冊的建立，知悉資訊資產之狀況，方可評估個別資產資通安全等級，決定資源投入之優先順序。

- A. 8.2.1　資訊之分級

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

(2) 適用說明：　透過適當的資訊分級，可使該組織最關鍵且需受到保護的資訊系統將會被優先提出與實作，可使組織資源為有效分配，避免資源的浪費。

類別：資訊保護【案號：S10814】

政委：難辨電信設備廠商私營或國營 台灣 5 年前已禁用

【焦點話題】

行政院數位政務委員表示，台灣早於建置 4G 基礎設施時，即針對電信設備進行系統新風險評估，考量中國電信設備廠商無法判斷私營或國營，故已全面禁用來自中國製造的電信產品，其中係因中國有一定規模以上之公司，皆必須於公司內設立共產黨之部，因此企業無法清楚劃清國營、私營之界線。而目前歐美國家因中美貿易戰跟進暫停合作，亦因為台灣及早這麼做，因此在國際上有一定的資安話語權，可供國際借鏡相關經驗。

【參考資料來源：世界日報，108/5/30】

【重點摘要】

1. 機關辦理資訊、電訊或通訊設備有關採購，因兩岸尚未締結與政府採購法第 17 條第 1 項有關之條約或協定，得依個案特性及實際需要於招標文件中限制大陸地區之財物或勞務參與。如認廠商所供應之財物或勞務之原產地為大陸地區，有影響國安(含資安)或機敏資訊外洩之疑慮者，可於招標文件中明定廠商所提供之財物或勞務之原產地不得為大陸地區。

2. 陸資廠商包括大陸地區廠商、第三地區含陸資成分廠商，以及在臺陸資廠商，在屬於「具敏感性或國安(含資安)疑慮之業務範疇」時，任一類型經公告之陸資廠商均不得參與，惟為避免違反世界貿易組織(WTO)、臺紐經濟合作協定(ANZTEC)及臺星經濟夥伴協定(ASTEP)等國際協定，其所適用之規定略有不同。

【法律觀點】

近來物聯網之安全防護問題備受質疑，以及第五代行動通訊技術的發展日

趨成熟，並預計於 2019 年 12 月進行競價釋照[1]，因此，資通訊產品的安全性受到更多的重視。

政府機關辦理資訊、電訊或通訊設備有關採購，應依照政府採購法規定執行，且為達到採購之效果，政府機關辦理時應依實際需要，設定投標廠商之基本資格，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[2]，藉以確保採購品質。

為達到資通訊安全的保障，而機關辦理資訊、電訊或通訊設備有關採購，應判斷採購案件是否屬「具敏感性或國安(含資安)疑慮之業務範疇之資訊服務採購」或「影響國家安全採購」，依採購案件之特性及實際需要，就標的及履約能力等事項訂定投標廠商基本資格，並載明於招標文件。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」，為免發生國安或資安疑慮，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 款規定，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廠商參與[3]。

承上所述，所謂陸資廠商，包含大陸地區廠商、第三地區含陸資成分廠商，及在臺陸資廠商。機關辦理資訊、電訊或通訊設備有關採購時，應依陸資廠商之分類訂定採購標的之原產地及投標廠商資格[4]：一、大陸地區廠商：兩岸未簽署相互開放政府採購市場之條約協定，於招標文件載明不允

---

[1] 5G 開跑，NCC 針對釋照及後續監理修正相關法規，國家通訊傳播委員會，108 年 6 月 19 日，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&cate=0&keyword=&is_history=0&pages=0&sn_f=41563 （最後瀏覽日：2019 年 8 月 5 日）。

[2] 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。」

[3] 行政院公共工程委員會 104 年 1 月 27 日工程企字第 10400024613 號函。

[4] 行政院公共工程委員會 107 年 12 月 20 日工程企字第 1070050131 號函。

許大陸地區廠商參與；二、第三地區含陸資成分廠商：我國已簽署世界貿易組織(WTO)政府採購協定(GPA)、臺紐經濟合作協定(ANZTEC)及臺星經濟夥伴協定(ASTEP)，對於適用上開協定採購，得基於國家安全理由排除該等協定之適用，並於招標文件中載明不允許第三地區含陸資成分廠商參與；三、在臺陸資廠商：屬影響國家安全之採購，包括但不限於經濟部投資審議委員會(下稱投審會)公告之「具敏感性或國安(含資安)疑慮之業務範疇」之採購，得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 款規定於招標文件載明不允許投審會公告之在臺陸資廠商(含陸資資訊服務業者)參與。

而屬經濟部投資審議委員會網站公告之「具敏感性或國安(含資安)疑慮之業務範疇」[5]目前主部門包括能源、水資源、通訊傳播、交通、金融與銀行、緊急救援與醫院、中央政府與地方機關及科技園區與工業區等八大領域之重要資通訊系統。綜上可知，目前我國政府機關進行資訊、電訊或通訊設備有關採購時，首先須判斷所採購項目是否有影響國安（含資安）或機敏資訊外洩等疑慮，並於招標文件妥為訂定採購標的之原產地及投標廠商資格。

【管理 Tips】

組織於建構資訊相關系統時，多會委託外部單位協助辦理，但業務委外勢必有風險存在，因此，排除潛在風險係為組織於業務委外時必須處理之事項。關於投標廠商資格，首先，應建立選商標準，並於必要時透過相關背景調查，根據廠商之專業能力、技術經驗及財務能力，再加以評核廠商能力；再者，組織得透過契約與廠商議定雙方之責任義務，並於契約內明訂資訊安全注意事項，及相對應之罰則與賠償責任，降低雙方風險。

[5] 具敏感性或國安(含資安)疑慮之業務範疇，http://web.moi.gov.tw/psu/files/news/201523932551I3-01%E5%85%B7%E6%95%8F%E6%84%9F%E6%80%A7%E6%88%96%E5%9C%8B%E5%AE%89(%E5%90%AB%E8%B3%87%E5%AE%89)%E7%96%91%E6%85%AE%E4%B9%8B%E6%A5%AD%E5%8B%99%E7%AF%84%E7%96%87.pdf

根據行政院公共工程委員會滾動調整之資訊服務採購契約範本[6]，其關於資通安全責任之內容可供一般業者參考。

1、廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。此外機關保有對廠商以派員稽核或其他適當方式執行相關查核的權利。。

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)，提出安全性檢測證明，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。廠商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或移交之，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，如違反資通安全相關法令或知悉發生資安事件時，必須立即通報機關，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通安全的要求。

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，並就機關所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。

【相關標準】

ISO 27001：2013（CNS 27001）

● A.7.1　聘用前

[6] 資訊服務採購契約範本第 16 條第 17 目。

(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：　委外提供資訊服務或採購資訊設備，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：S10815】

私密照勒索 女總裁判刑

【焦點話題】

江姓總裁於 2001 年創立徵信公司，該公司周姓業務執行總監於 2011 年間接受林姓委託人委託查詢某女子之個人素行，並於隔年 5 月竊錄該女子與不詳男子於臥室內之非公開活動及身體隱私部位，並將照片寄送至女子信箱，且指派另名員工持續打電話至女子辦公室恐嚇、脅迫女子離職。

一審判決認為：江姓總裁為公司負責人及執行長，長期投身徵信業，具足夠知識、經驗及能力協助彰顯社會正義，保障人民權利，應警覺徵信業給人的偏見，卻長期默視並容許公司職員違法牟利，東窗事發後推諉卸責，顯現只想享受營利，處 1 年有期徒刑，二審則加重為 2 年有期徒刑。

【參考資料來源：聯合報，108/7/31；臺灣高等法院 105 年上訴字第 3057 號刑事判決】

【重點摘要】

1. 個人隱私近年來已普遍受到國人的重視，無故以工具，用以窺視、竊聽、竊錄他人隱私活動、言論或談話或身體隱私部位者，已危害社會善良風氣及個人隱私，實有處罰之必要，因此刑法第 315-1 條規定，凡以工具為上開情形時，可處 3 年以下有期徒刑、拘役或 30 萬元以下罰金，而未以工具為之時，則以社會秩序維護法[1]之規定，以秩序罰處罰之。
2. 組織負責人意圖營利供給設備，便利其組織成員執行違法行為，組織負責人亦屬於共同正犯，而不得以未參予或非親自執行業務等語，而為免責。

【法律觀點】

[1] 社會秩序維護法第 83 條第 1 款：「有左列各款行為之一者，處新臺幣六千元以下罰鍰：一、故意窺視他人臥室、浴室、廁所、更衣室，足以妨害其隱私者。…」

現代徵信公司普遍利用多種高科技電子設備進行業務活動，包括針孔攝影機、GPS 追蹤器或隔牆聽音器等，其設備本身並未違法，惟須注意使用者是否以合法手段利用該類設備。而利用電子設備所作成之資訊，多以電磁紀錄形式保存，以電磁紀錄之特性而言，係可透過電腦設備予以編輯、處理、傳輸、顯示或儲存，本質上具備一定的可再現性，且因電腦科技日益創新與進步，在重複讀取、傳輸電磁紀錄的過程中，原有電磁紀錄的檔案內容，可隨時複製而不致減損，屬電磁紀錄與一般動產的差異所在[2]，可見透過電磁紀錄的形式存取資料，將導致資料可無限制增加，此時透過高科技電子設備所完成之電磁紀錄，將對於當事人之權益侵害風險更形擴大。

亦因現今高科技電子設備設計愈來愈精密，可使一般人不易察覺其設備之存在，且於不知不覺遭竊錄、竊聽，導致眾多糾紛發生。然而，如未取得他人之同意，並利用高科技電子設備以偷拍、竊錄的方式任意取得他人非公開之活動，已嚴重侵害個人隱私權，故依刑法第 315-1 條第 2 款[3]規定，無故以錄影竊錄他人非公開之活動、言論、談話或身體隱私部位，處 3 年以下有期徒刑、拘役或 30 萬元以下罰金。

本案例周姓總監以公司名義承接案件，並使用公司所購置之針孔等現有設備及工具，以錄影、照相等方式竊錄他人非公開活動與隱私部位，並進行剪輯、複製，交付委託客戶，已觸犯竊錄非公開活動內容罪；且其將偷拍照片寄送到女子信箱，並指派員工接續打電話至女子辦公室騷擾，亦觸犯刑法第 305 條[4]的恐嚇危安罪，而負責人江姓總裁雖並無直接參與個別業務承接之細節，亦不親自執行與參與偷拍等細節，但不容否認其偷拍所裝設之針孔等攝影器材，以及剪輯畫面所使用之電腦等設備，均屬其所經營之徵信公司所

[2] 最高法院 107 年台上字第 1096 號刑事判決。

[3] 刑法第 315-1 條第 2 款：「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：…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] 刑法第 305 條：「以加害生命、身體、自由、名譽、財產之事，恐嚇他人致生危害於安全者，處二年以下有期徒刑、拘役或三百元以下罰金。」

有。因此，江姓女總裁身為公司負責人為公司經營目的，提供攝影器材、針孔、電腦等工具、設備予公司之外務人員執行竊錄等行為，亦構成刑法第315-2 條[5]意圖營利供給設備竊錄非公開活動內容罪規定，而最終法院定應執行刑為周姓總監有期徒刑 1 年 7 個月，江姓女總裁有期徒刑 2 年[6]。

【管理 Tips】

本案例可就二層面加以觀察，首先係執行者之責任，各行各業皆有需實際執行業務事項，對於執行業務者，組織應透過聘用條款，使其瞭解資訊安全之責任，並透過教育訓練確實佈達組織內部相關規範及外部法律責任等，使執行業務者能清楚知悉組織運作準則，避免觸犯內部規定或法律。以本案為例，如業務執行者有足夠的法律認知意識，瞭解其行為可能面臨的法律風險與責任，進而確認其攝錄及後續作為的合法性，當可避免侵害他人隱私。

再者係為監督者之責任，即一般所稱之「員工闖禍，老闆負責」的概念，當組織成員因故意過失侵害他人權利時，負有監督義務者，即必須對其未盡適當監督負起責任。因此，分層管理係為管理的重要事項，透過有效監督，可降低組織中執行者違法風險。以本案為例，如監督者針對屬於徵信公司之攝影器材以及電腦等設備，進行適當管理，例如：執行業務者借用設備時，能確實確認其使用目的及範圍，則可避免其之不當利用，亦可避免後續法律責任。

【相關標準】

ISO 27001：2013（CNS 27001）

---

[5] 刑法第 315-2 條第 3 項：「意圖營利供給場所、工具或設備，便利他人為前條第一項之行為者，處五年以下有期徒刑、拘役或科或併科五萬元以下罰金。...製造、散布、播送或販賣前二項或前條第二款竊錄之內容者，依第一項之規定處斷。」

[6] 江某之應執行刑為有期徒刑 2 年，尚包括同案涉犯貪污治罪條例之行賄罪，而非僅意圖營利供給設備竊錄非公開活動內容罪。

- A.7.1.2　聘用條款及條件

(1) 標準內容：　組織與員工及約用人員簽訂之契約化協議書，應敘明雙方對資訊安全的責任。

(2) 適用說明：　組織在聘用員工前，應與其簽訂契約化協議書，透過聘用條款及條件，使其知悉如有違反相關規定時，所應負擔的責任，降低員工違法的可能性。

- A.11.2.5　資產之攜出

(1) 標準內容：　未經事前授權，不得將設備、資訊或軟體帶出場域外。

(2) 適用說明：　組織應建立設備之使用規範，要求組織成員應依規定使用設備，避免不當存取，且應有適當授權方得將資產攜出，並考量場域外之風險，以作為是否得攜出之判斷依據。

類別：資訊保護【案號：S10816】

買太多吃不完 轉賣商品附「圖」吃官司

【焦點話題】

張女於購物台購入纖體產品，後因購買數量太多吃不完，便將部分產品透過網路轉賣，並從購物台網站下載產品圖片使用，事後購物台發現提告其違反著作權法。張女辯稱，當初覺得購買大組的纖體產品比較划算，雖然自己吃不完，但可找人一起體驗分售，收到產品後便將部分上網拍賣，並順手到該購物台下載產品圖片，放在網頁當作說明，認為產品本就是在購物台購買，並不知道下載產品圖片使用會觸法。

而法官指出，就算張女從購物台購入纖體產品，亦不代表其擁有產品圖片使用權，否則豈謂在書店購得有著作權之書籍後，即可任意影印拷貝，此為至明之理，張女不得諉為不知，審結以擅自以重製之方法侵害他人著作財產權，判處張女拘役 20 天。

【參考資料來源：自由時報，108/6/27；臺灣桃園地方法院 108 年桃智簡字第 1 號刑事判決】

【重點摘要】

1. 著作權法第 91 條第 1 項規定，擅自以重製之方法侵害他人之著作財產權者負有刑事責任，在沒有獲得任何授權時，不得將該商品所刊載之他人享有著作權之照片、文字或其他具著作權之物件任意轉載。
2. 著作權法第 91 條第 2 項，加重重製罪係以意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權，因此如所銷售或出租者不是重製物，重製物僅係恰好附合於銷售或出租者時，則與加重重製罪無關。

【法律觀點】

由於網際網路的發展，各式拍賣平台興起，部分民眾經常透過網路出售多餘不需的物品，並於產品附上圖文，使他人容易瞭解物品之規格、現況及相關注意事項，然而網路文字、圖片及影像易於重製，無論係為詳細呈現

物品內容或單純避免麻煩，將產品於官網的文字、圖片或影像，直接複製至銷售頁面，藉以吸引購買者目光，此即有違反著作權法的風險。

按著作權法第 91 條規定：「擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。」本案當事人表示，其係於電視購物購買商品，故由電視購物網站複製產品圖片刊載於拍賣網站。而法院認為縱使當事人係由購物台購得有刊載照片之商品，但並無獲得任何授權，因此不得將該商品所刊載之他人享有著作權之照片任意轉載於自身之拍賣網站頁面，並以「否則豈謂在書店購得有著作權之書籍後，即可任意影印拷貝」，作為說明。

而同法第 92 條[1]規定之非法公開傳輸亦有刑事處罰，惟非法公開傳輸之低度行為應為非法重製之高度行為所吸收，因前者之行為情節較重，應論以擅自以重製之方法侵害他人之著作財產權罪，故不另論罪。

【管理 Tips】

本案例係個人於拍賣二手物品時，盜取官方網站之行銷圖片作為己用，進而引發廠商提告，指其侵犯著作權，最終法院認其為非法重製圖片，但非據此營利，故僅處拘役 20 日。

從組織管理而言，組織應理解到智慧財產權管理的重要性，並非僅奠基於不使組織內的智慧財產權外洩來看，亦是希望能降低觸法風險。因此，組織應建立法令遵循管理流程，定期對業務過程評估其觸法風險，找出應控制未控制之風險，採取適當措施設計或修改控管機制；組織亦應定期就可能觸法之風險予以排序，而優先處理高風險事項；針對法令遵循管理流程應發展後續改善計畫，藉以評估整體的影響及法遵計畫的有效性。

【相關標準】

[1] 著作權法第 92 條：「擅自以公開口述、公開播送、公開上映、公開演出、公開傳輸、公開展示、改作、編輯、出租之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。」

ISO 27001：2013（CNS 27001）

- A.18.1.2　智慧財產權

(1) 標準內容：　應實作適切程序，以確保遵循與智慧財產權及專屬軟體產品使用相關之法律、法令、法規及契約的要求事項。

(2) 適用說明：　組織應建立包括智慧財產權的法令遵循管理流程，除避免智慧財產權外洩外，亦要防止侵害他人的智慧財產權，降低觸法風險，以本案為例，如當事人能知悉著作權法相關規定，則不會任意轉載圖片於拍賣網站自己之帳號網頁內。

貳、資訊公開(Disclosure)

類別：資訊公開【案號：D10817】

3 家托嬰中心未裝監視器　市長要求強制裝設

【焦點話題】

托嬰中心虐嬰事件頻傳，中市府社會局報告，目前中市立案托嬰中心共 152 家，其中公設民營托嬰中心 5 家，占總數 3%；私立托嬰中心 147 家，占總數 97%。社會機構表示，稽查托嬰中心作業主要有建築物安全管理、消防安全設備與托育服務運作情形等，稽查頻率由社會機構會同都市發展機構、消防機構等單位，每週排定 2 次公安聯合稽查班次。

然而，針對裝設監視器方面，社會機構表示目前仍有 3 家托嬰中心未裝設，由於兒童及少年福利與權益保障法已修正通過須全面加裝，相關施行辦法中央機關仍討論中，並根據中部市府首長指示發文要求 3 家業者裝設。

【參考資料來源：中央社，108/5/6】

【重點摘要】

1. 依兒童及少年福利與權益保障法第 49 條規定，為促進兒童及少年身心健全發展，以保護兒童及少年，當任何人對於兒童或少年有遺棄、身心虐待等等的行為，經直轄市、縣（市）主管機關依兒少權法裁罰後，主管機關必須建立裁罰資料庫，而該資料庫的用途在於供政府機關（構）及其他經中央主管機關同意之機構、法人或團體查詢
2. 為保護嬰兒安全與發生兒虐案件時得查知相關事實並確保證據之保存，以利責任歸屬，保障當事人家長及托嬰中心雙方權益，兒童及少年福利與權益保障法第 77-1 條強制要求托嬰中心應裝設監視錄影設備。

【法律觀點】

兒虐事件頻傳引發外界對於兒童及少年福利與權益保障法（下稱兒少權法）修法之重視，為杜絕兒虐案及狼師事件，立法院於 108 年度修法，其中修法重點

包括「司法及早介入兒少保護案件調查程序」、「建立兒少保護加害人裁罰紀錄資料庫」、「建立兒童死因回溯分析機制」、「加重對兒少為不當行為的處罰」以及「兒少權益相關策略」。

然而，為促進及保護兒童與少年身心健全發展，當任何人對於兒童或少年有遺棄、身心虐待等行為[1]，經直轄市、縣（市）主管機關依照兒少權法裁罰後，主管機關必須建立裁罰資料庫，而該資料庫之用途在於提供政府機關（構）及其他經中央主管機關同意之機構、法人或團體查詢[2]，其目的在於以確實有效防止不適任專業人員於兒童及少年相關服務單位任職[3]，是以，性侵害犯罪、情節重大性騷擾或性霸凌等，經教育主管機關認定屬實者，縱使並非有罪判刑確定，亦不得擔任兒童及少年福利機構、兒童課後照顧服務班及中心之負責人或工作人員，如已聘任，經認定亦應停止聘用[4]。

---

[1] 兒童及少年福利與權益保障法第 49 條第 1 項：「任何人對於兒童及少年不得有下列行為：一、遺棄。二、身心虐待。三、利用兒童及少年從事有害健康等危害性活動或欺騙之行為。四、利用身心障礙或特殊形體兒童及少年供人參觀。五、利用兒童及少年行乞。六、剝奪或妨礙兒童及少年接受國民教育之機會。七、強迫兒童及少年婚嫁。八、拐騙、綁架、買賣、質押兒童及少年。九、強迫、引誘、容留或媒介兒童及少年為猥褻行為或性交。十、供應兒童及少年刀械、槍砲、彈藥或其他危險物品。十一、利用兒童及少年拍攝或錄製暴力、血腥、色情、猥褻、性交或其他有害兒童及少年身心健康之出版品、圖畫、錄影節目帶、影片、光碟、磁片、電子訊號、遊戲軟體、網際網路內容或其他物品。十二、迫使或誘使兒童及少年處於對其生命、身體易發生立即危險或傷害之環境。十三、帶領或誘使兒童及少年進入有礙其身心健康之場所。十四、強迫、引誘、容留或媒介兒童及少年為自殺行為。十五、其他對兒童及少年或利用兒童及少年犯罪或為不正當之行為。」同條第 2 項：「前項行為經直轄市、縣（市）主管機關依第九十七條規定裁罰者，中央主管機關應建立裁罰資料，供政府機關（構）及其他經中央主管機關同意之機構、法人或團體查詢。」本項本次亦略修正，為使實務運用更為明確，修正第一項第十一款，增列「性交」二字，明定禁止利用兒童及少年拍攝或錄製性交等有害兒童及少年身心健康之出版品、圖畫、錄影節目帶、影片、光碟、磁片、電子訊號、遊戲軟體、網際網路內容或其他物品。

[2] 兒童及少年福利與權益保障法第 49 條第 2 項：「前項行為經直轄市、縣（市）主管機關依第九十七條規定裁罰者，中央主管機關應建立裁罰資料，供政府機關（構）及其他經中央主管機關同意之機構、法人或團體查詢。」本項本次亦略修正，為使實務運用更為明確，修正第一項第十一款，增列「性交」二字，明定禁止利用兒童及少年拍攝或錄製性交等有害兒童及少年身心健康之出版品、圖畫、錄影節目帶、影片、光碟、磁片、電子訊號、遊戲軟體、網際網路內容或其他物品。

[3] 兒童及少年福利與權益保障法第 49 條 108 年立法理由二。

[4] 兒童及少年福利與權益保障法第 81 條第 5 項：「主管機關應主動查證兒童及少年福利機構負責人是否有第一項各款情事；兒童及少年福利機構聘僱工作人員之前，亦應主動查詢，受請求查詢機關應協助查復。」、同法

且兒童及少年福利機構、兒童課後照顧服務班及中心在聘僱工作人員之前，必須檢具名冊，並檢附資格證明文件影本、切結書、健康檢查表影本、近三個月內核發之警察刑事紀錄證明書，意即一般所稱之良民證及其他相關文件，報請教育主管機關核准[5]。另外，為加強對兒童及少年之保護，前次修法通過對於兒童或少年有遺棄、身心虐待等行為者，得公布其姓名或名稱之規定，於本次修正提高罰鍰金額上限至新台幣 60 萬元，以達嚇阻之效[6]。

此外，為保障兒童安全與兒虐案件發生時，得查知相關事實並證據保存，以利責任歸屬，保障家長及托嬰中心雙方權益，因此，本次修法另一個重點在於強制要求托嬰中心裝設監視錄影設備，並授權中央主管機關訂定托嬰中心裝設監視器之管理規範，讓家長安心送托並兼顧孩子隱私權[7]。

【管理 Tips】

就政府角度而言，資料蒐集時應判斷其必要性及合理性。然而，將蒐集資料、建立資料庫，並開放資料庫，伴隨而來的風險大於單純蒐集資料。同時，強制設置監視器亦已侵害被監視者之隱私權，其中當被監視者屬無行為能力之嬰幼兒，其並無資訊自我決定之能力。因此，無論是資料庫開放或監視器裝置，政府應透過訂定法令方得予以規範，在隱私保護及公共利益間取得平衡。

然而，就一般組織而言，若組織之資料庫等敏感或重要資產時，遭竊取或洩漏等

第 81-1 條第 5 項：「教育主管機關應主動查證兒童課後照顧服務班及中心負責人是否有第一項各款情事；兒童課後照顧服務班及中心聘僱工作人員之前，亦應主動查詢，受請求查詢機關應協助查復。」、同法第 81-1 條第 1 項：「有下列情事之一者，不得擔任兒童課後照顧服務班及中心之負責人或工作人員：一、曾犯性侵害犯罪防治法第二條第一項之罪、性騷擾防治法第二十五條之罪、兒童及少年性交易防制條例之罪、兒童及少年性剝削防制條例之罪，經緩起訴處分或有罪判決確定。但未滿十八歲之人，犯刑法第二百二十七條之罪者，不在此限。二、有性侵害行為，或有情節重大之性騷擾、性霸凌、第四十九條第一項各款所定行為之一，經教育主管機關查證屬實。三、有非屬情節重大之性騷擾、性霸凌、第四十九條第一項各款所定行為之一，教育主管機關認定有必要予以解聘或解僱，並審酌案件情節，認定一年至四年不得聘用或僱用。四、有客觀事實認有傷害兒童少年之虞，經教育主管機關認定不能執行職務。」

[5] 兒童及少年福利與權益保障法第 81 條第 6 項。

[6] 兒童及少年福利與權益保障法第 97 條：「違反第四十九條第一項各款規定之一者，處新臺幣六萬元以上六十萬元以下罰鍰，並得公布其姓名或名稱。」

[7] 兒童及少年福利與權益保障法第 77-1 條。

事故發生時，組織將造成重大損失，因此組織於內部設置監視器以確保自身環境安全，並非不得為之[8]。尤其組織內有必要之資訊保護時，對於實體及環境本即應保全區域內的安全，並防止資產遺失或損害等情形發生，此時甚至應設置監視器以避免外部惡意攻擊或是內部人員的違法亂紀，以期事件發生時能掌握證據瞭解事件真相，惟仍應注意相關法令規範，避免因蒐集資料而違法之情形。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.9.2.2　使用者存取權限之配置

(1) 標準內容：　應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。

(2) 適用說明：　依照兒童及少年福利與權益保障法規定任何人對於兒童或少年有遺棄、身心虐待等行為，經直轄市、縣（市）主管機關依兒少權法裁罰後，主管機關必須建立裁罰資料庫，但可查詢該資料庫之人員則仍應以政府機關（構）及其他經中央主管機關同意之機構、法人或團體為限，故主管機關對於可存取資料庫者，必須建立程序以對使用者加以控管。

[8] 臺灣高等法院 94 年度勞上易字第 46 號民事判決「雇主在其有使用權之場所裝設監視錄影機，本為其利用其有使用權之財產；且雇主為保護其財產，自可採取相當之保護措施；再員工本負有遵守公司工作規則及於勤務時間對雇主應負專心業務之義務，不論勞雇間是否另有具體工作規則之制定，雇主為維持其企業秩序，解釋上自有權利對勞工提供勞務之情況加以監督權限。雇主在其工作場所裝設監視錄影機，雖可能影響員工之個人隱私權，然此部分牽涉之隱私權，僅限於勞工工作時間內之身體外觀動作，此部分隱私權尚非屬隱私權最核心部分如肖像、前科、指紋等，且未牽涉公共利益或善良風俗，應可要求員工忍受。惟雇主欲貫徹其保護財產及對員工上開要求，因此所為之執行方法必須合理不得濫用，故雇主在工作場所裝設監視錄影機監督勞工之工作狀況，應符合 1、目的之必要性-基於合法之業務目的；2、方法之妥當性 - 讓接觸、使用及揭露資訊限制在足以達成目標之目的範圍內；3、利益之比較衡量 - 使用最小之侵害手段達成業務上目標。」

ISO 27001：2013(CNS 27001)

- A.11.1.1　實體安全周界

(1) 標準內容：　應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。

(2) 適用說明：　當組織內部具有敏感或重要資訊時，該類資產如遭竊取或洩漏等事故時，將造成組織重大損失，故應防止其遭未經授權之實體存取、損害及干擾，而進出管控是針對於實體安全週界控管之主要方法，而以門禁管控時，通常會以監視系統作為輔助，於錯誤發生時能有證據加以確保事件真相。

類別：資訊公開【案號：D10718】

開拓資料想像力 建立開放資料應用典範

【焦點話題】

107 年 11 月資料開放高峰會由國發會、行政院、Open Data 聯盟及 opendata.tw 計畫聯合舉辦。現今社會企業面臨數位轉型，公部門的轉型也須檢視開放資料的「可被利用性」，關照使用者導向的資料觀點，藉由恰當的收集、處理以及利用，讓資料從開放起初就能顧及系統的通透性與使用者的便利性，因此資料能如何充份依規範結構化，以供系統存取，是為一大重點。然而，就民間角度而言，目前政府資料開放數量雖多，但多為報告形式，民眾並無法實際使用。是以，政府無疑是重要資料之供應者，而政府如何提供高品質資料且鼓勵發展應用，是為政府推動資料開放之重要工作。

【參考資料來源：自由時報，108/5/31】

【重點摘要】

1. 政府資料開放係以政府資訊公開法可得公開之資料為本，亦即包括法規命令或預算及決算書等政府資訊公開法第 7 條之政府資訊，且無依同法第 18 條規定限制公開或不予提供之情形時，方會進入到政府資料開放作業原則適用的範圍。
2. 依政府資料開放作業原則第 11 條規定，開放格式應符合下列規定：(一)可直接取得；(二)易於處理；(三)易於理解；(四)確保資料品質；(五)利於資料間串聯運用。

【法律觀點】

政府資訊公開之目的係為保障人民知的權利，與人民共享及公平利用政府之資訊，增加人民對公共事務之了解、信賴及監督，並促進民主參與[1]。因此，欲利

[1] 政府資訊公開法第 1 條。

用開放資料達到提升生活品質、滿足產業需求及各級政府或部會間之決策品質，其資料應具有便利性。行政院將 108 年訂為台灣地方創生元年，希望可透過整合中央政府、地方政府與民間各類統計資料及地圖資訊，以掌握與追蹤台灣各地人口流動、經濟發展及地方建設狀況，希望透過不同資料尺度的視野轉換，以鄉鎮視角為新起點，提供推動地方創生所需相關資訊[2]。

因此，為極大化開放政府資料，其以政府資訊公開法為基礎，推動政府資料以開放格式、機器可讀且具一定品質方式提供外界使用，結合民間資源及創意，達成施政便民及公開透明之目的，以落實推動政府資料開放新政策[3]，行政院於 108 年 1 月 17 日以院授發資字第 1081500073 號函修正行政院及所屬各級機關政府資料開放作業原則。

首先，明定政府資料開放之範圍[4]，政府資料開放係以政府資訊公開法可得公開之資料為本，意即含法規命令、預算及決算書等，及其他依照政府資訊公開法第 7 條[5]規範之政府資訊，且無同法第 18 條[6]規定限制公開或不予提供之情事，

---

[2] https://www.thenewslens.com/article/118763 台灣第一個地方創生資料庫「TESAS」誕生了！（最後瀏覽日：108 年 6 月 12 日）

[3] 行政院及所屬各級機關政府資料開放作業原則修正總說明。

[4] 行政院及所屬各級機關政府資料開放作業原則修正第 2 條：「政府資料開放之範圍，指各機關於職權範圍內取得或作成，且依政府資訊公開法得公開之各類電子資料，包含文字、數據、圖片、影像、聲音、詮釋資料（metadata)等。」

[5] 政府資訊公開法第 7 條第 1 項：「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。」

[6] 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

原則上即為政府資料開放作業原則之適用範圍。

其次，開放之政府資料為提昇其可用性，以利直接取用，並得混合加值應用發展各式服務，因此政府資料開放作業原則要求其開放格式應符合下列規定[7]：(一)可直接取得：無需人為操作即可透過連結直接獲取資料；(二)易於處理：優先提供結構化資料[8]；(三)易於理解：應於詮釋資料描述其欄位說明及編碼意義等；(四)確保資料品質：不得任意分割，以確保其完整性，並力求資料之正確性及時效性；(五)利於資料間串聯運用：提供之資料欄位格式定義應與政府資料標準[9]相符。是以，透過機器對機器識別讀取及利用，以達到政府資料開放之正確性及時效性。

【管理 Tips】

依照政府資料品質提升機制運作指引之要求，判斷開放政府資料之品質相關標準，係以資料使用流程為出發點，分為資料可直接取得、資料易於處理、資料易於理解三個面向，透過連結有效性、資料資源能否直接下載、是否屬結構化檔案類型、詮釋資料編碼描述與資料相符、詮釋資料欄位描述與資料相符以及資料更新時效

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。」

[7] 行政院及所屬各級機關政府資料開放作業原則第 11 條。

[8] 所謂固定欄位結構化資料是指資料可以被呈現在資料庫欄位，且具有固定欄位、固定格式以及固定順序的資料。而非結構化資料則是指形式自由且不遵循標準的格式規範，一團沒有組織的數據，例如一般文字、圖檔、音樂、影片、電子郵件或網頁等資料，至於非固定欄位結構化資料則是介於固定欄位結構資料庫與非結構資料庫之間，具備欄位但欄位不具備一致性，例如在一個資料表中可能只有部份資料列含有生日欄位，同時只有部份資料列含有電話訊息。結構化資料的優點在於因為規則已經被明定，因此資料很容易的就可以被後續程式取用分析，因此透過結構化資料能夠提昇開放資料可用性，非結構化資料並不易透過機器直接辨識，會造成使用者在取得資料時的困難，而非固定欄位結構化資料的好處是容易收納變數極多或難以預測的資料集，並依然保有可查找性，但缺點則是效能會低於固定欄位結構化資料。

[9] 目前政府建有政府資料標準平臺，透過統一標準格式，讓政府資料可以易於處理，並在資料間串聯運用。https://schema.gov.tw/employ （最後瀏覽日：108 年 6 月 12 日）

性等指標，用以判斷資料品質是否良好[10]。

另外，政府資料品質提升機制運作指引亦針對資料品質提昇提出通則性作法，並對於 API、固定欄位結構化資料、非固定欄位結構化資料及非結構化資料等不同資料類型，提出建議資料格式，以利資料取用者能輕易使用[11]。

總體而言，政府資訊公開已不再以量取勝，資料如不能被利用就不是資料，因此，透過政府資料的標準化，政府資訊公開才能「質量兼備」。

【相關標準】

ISO 27001：2013(CNS 27001)

- 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：　開始進行資料開放前，必須將所有資料予以盤點，進行妥適之分類、分級等管理措施，並對於其所持有之其應予以分類並製表列冊，以確認政府資料是否得以公開。

[10] 政府資料品質提升機制運作指引 貳、資料品質提昇流程介紹。

[11] 政府資料品質提升機制運作指引 參、資料品質提升作法說明。

類別：資訊公開【案號：D10819】

政府採購公布評選委員學經歷

【焦點話題】

行政院公共工程委員會為協助各機關遴選採購評選委員，特建置「專家學者建議名單資料庫」，其專業領域包含工學類等 16 類別，並下分景觀設計等 250 個科別專長，一共 4 千餘名專家學者。並於 108 年 7 月 1 日起政府電子採購網增加公開評選委員學經歷欄位，供各機關公開評選委員名單時一併登載，以利各界檢視其與採購標的之關聯性。部分機關設定專業類科別及專長條件後，就符合條件者採隨機遴選，其目的是防弊，避免請託關說或受個人喜好偏見影響。而機關肩負評選成敗責任，一般用資料庫挑選與評選項目有關專長的專家學者，會再從其中審慎選擇較合適者簽報機關首長或其授權人員核定。

【參考資料來源：工商時報，108/6/27】

【重點摘要】

1. 為求達到採購品質，避免產生採購評選委員會所聘之專家學者，得否獨立公正評選之疑慮，政府採購法第 94 條要求，專家學者不得為政府機關之現職人員。
2. 為達評選委員資訊公開透明之目的，避免外界質疑黑箱作業及委員名單外洩之爭議，採購評選委員會組織準則第 6 條明定委員名單應予公開於主管機關指定之資訊網站，而目前則公開於政府電子採購網供民眾查詢。

【法律觀點】

政府採購法之立法目的在於建立一套兼具提升採購效率與功能及確保採購品質之公平、公開採購程序[1]，而需要公開客觀評選的限制性招標[2]，及合於招標文件

[1] 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。」

[2] 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

規定之最有利標[3]等類的政府採購案中，因其未有最低價格標的固定標準，故必須透過評選的方式，選出合乎資格的得標廠商，此時，即需成立採購評選委員會，作為評選單位[4]。

為求達到採購品質，採購評選委員會之成員必須是專家學者，然而為避免衍生所聘專家學者得否獨立公正評選之疑慮，於 108 年度修法增訂專家學者不得為政府機關之現職人員之規定[5]。而評選委員會原則應於招標前成立，並於完成評選事宜且無待處理事項後解散，僅有例外時方得於開標前成立[6]。

此外，為達評選委員資訊公開透明之目的，避免外界質疑黑箱作業及委員名單外洩之爭議，採購評選委員會組織準則明定委員名單應公開於主管機關指定之資訊網站。又考量評選委員名單公開後，評選委員如有辭職或解聘之情形，致評選前評選委員名單有修正者，機關亦應將修正後之委員名單予以公開，而僅在機關衡酌個案特性及實際需要，認有不予公開之必要者，方不公開[7]。

政府電子採購網為前述主管機關指定之資訊網站，且為利各界檢視採購評選委

招標：…九、委託專業服務、技術服務、資訊服務或社會福利服務，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。…」

[3] 政府採購法第 56 條第 1 項：「決標依第五十二條第一項第三款規定辦理者，應依招標文件所規定之評審標準，就廠商投標標的之技術、品質、功能、商業條款或價格等項目，作序位或計數之綜合評選，評定最有利標。…」同法第 52 條第 1 項第 3 款：「機關辦理採購之決標，應依下列原則之一辦理，並應載明於招標文件中：…三、以合於招標文件規定之最有利標為得標廠商。…」

[4] 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。」

[5] 政府採購法第 94 條第 1 項：「機關辦理評選，應成立五人以上之評選委員會，專家學者人數不得少於三分之一，其名單由主管機關會同教育部、考選部及其他相關機關建議之。前項所稱專家學者，不得為政府機關之現職人員。評選委員會組織準則及審議規則，由主管機關定之」

[6] 採購評選委員會組織準則第 3 條：「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。前項第一款之評選項目、評審標準及評定方式有前例或條件簡單者，得由機關自行訂定或審定，免於招標前成立本委員會為之。但本委員會仍應於開標前成立。」

[7] 採購評選委員會組織準則第 6 條：「本委員會成立後，其委員名單應即公開於主管機關指定之資訊網站；委員名單有變更或補充者，亦同。但經機關衡酌個案特性及實際需要，有不予公開之必要者，不在此限。機關公開委員名單者，公開前應予保密；未公開者，於開始評選前應予保密。」

員之專業性與採購標的之關聯性，所公開者除原有採購評選委員姓名及職業資訊外，還包括評選委員學經歷[8]，俾使評選委員之專業資訊更為透明。

【管理 Tips】

政府採購的公平性與其資訊公開的程度息息相關，透過真正的專家學者參與，方對國家整體有所幫助，而專家學者的職業與學經歷公開，將可使各界更能檢視政府機關對於專案的管控是否到位。在公開個案評選委員之姓名、職業及學經歷前，需先蒐集評選委員之個人資料，目前係以專家學者建議名單資料庫建置及除名作業要點，作為資料庫建置依據，而所蒐集的資料包括姓名、性別、行動電話等十多項個人資料[9]，而蒐集大量個人資料的同時，應避免侵害個人隱私，仍然必須對公開範圍加以限制，應僅得公開必要資料且降低涉及會影響結果之資訊，以期符合資訊公開之意義。

以組織而言，亦可能有蒐集大量個資之情形，然並非組織之所有人員均有瞭解所有資訊之必要，故組織應適時檢視組織資訊，適當標註其重要性，並檢視權限，以透過權限劃分，避免非必要人員取得相關資訊。

【相關標準】

ISO 27001：2013（CNS 27001）

- A. 8.2.1 資訊之分級

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

(2) 適用說明： 組織應建立適當的資訊分級措施，以本案為例，如因所蒐集的專家學者資料廣且深，並建立資料庫，對於各類資訊

[8] 個案採購評選委員之學經歷資訊，可至政府電子採購網（https://web.pcc.gov.tw）/常用查詢/採購評選委員名單項下查詢。

[9] 政府採購專家學者建議名單資料庫申請審查表，而得蒐集之法定要件則以經當事人同意而蒐集、處理及利用個人資料。

予以劃分，依據不同的敏感性劃給不同的等級。

- A. 9.2.2 使用者存取權限之配置

(1) 標準內容： 應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。

(2) 適用說明： 組織應針對使用者存取進行管理，確保獲得授權者之存取，以及防止未經授權之存取，以本案為例，因非組織內所有使用者，均需取得專家學者資訊，因此應僅給予必要者其系統存取權限。

類別：資訊公開【案號：D10820】

脫產近 4000 萬、遷 7 次戶口 肉羹大戶欠稅追到了

【焦點話題】

北區國稅局表示，中和一名肉羹大盤商，自 1998 年 7 月至 2002 年 6 月期間，未依規定申請稅籍登記，批售自製肉羹，漏報銷售額新臺幣(下同)1.6 億元，經北區國稅局查獲後，核定補徵營業稅及營利事業所得稅並裁處罰鍰，合計 2121 萬多元。但該名大盤商繳款 841 萬元營業稅本稅後，其餘營業稅罰鍰及營利事業所得稅合計 1280 萬元，皆不願繳納，並申請復查、提起訴願及行政訴訟，且於行政救濟期間出售名下位於台北市萬華的三戶房屋、加油站股份、出脫債券及將銀行存款提領一空，總計脫產 3917 萬元。除脫產以外，肉羹大盤商還七度遷移戶籍，以為執行文件無法送達就可以逃避責任，因此執行分署認定肉羹大盤商「顯有逃匿之虞」及「就應供強制執行之財產有隱匿或處分」的情況，向新北地方法院聲請管收獲准，管收九天後，家人代繳清 1259 萬多元稅款及滯納金、滯納利息，才獲釋結案。

北區國稅局提醒，常有民眾誤以為欠繳稅捐，只要處於「無資力」的狀態，國家公權力便無從介入。事實上，欠繳稅捐前的財產移轉行為，足以證明有隱匿財產之情事，各執行分署可依法採取相關之強制措施，千萬不要心存僥倖進行脫產，以免陷管收窘境，之後仍須繳清稅款。

【參考資料來源：聯合新聞網，108/8/22】

【重點摘要】

1. 政府資訊公開法第 18 條第 6 款及第 7 款規定，對有害個人隱私或營業祕密等事項，為保護當事人之權益，該類資訊原則禁止公開，僅在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時，才得例外公開。

2. 稅捐稽徵法第 34 條規定，對重大欠稅案件或重大逃漏稅捐案件經確定後，得公告其欠稅人或逃漏稅捐人之（一）納稅義務人姓名或名稱；納稅義務人

為營利事業者，應一併公告其負責人姓名及地址。（二）稅目別。（三）欠稅年度。（四）欠稅或罰鍰金額【含滯納金、利息及滯（怠）報金】。（五）公告內容屬自然人地址者，其門牌號碼可予簡略，僅公告至街道或村里名稱。

【法律觀點】

憲法第 19 條明文規定人民有依法納稅之義務，而稅收則為政府所得主要來源，且用以維持政府運作，因此對於政府而言能夠有效、確實地收取稅收乃是政府的一大課題。

然而，個人財產、所得、營業、納稅等事項，應屬個人重視之隱私，稅捐稽徵人員處理納稅義務人相關資料時，必然會經手其財務隱私，因此稅捐稽徵法特別規定，稅捐稽徵人員對於納稅義務人之財產、所得、營業、納稅等資料，除特定人員及機關外，應絕對保守秘密[1]。再者，就政府資訊公開法第 18 條第 6 款及第 7 款規定，對有害個人隱私或營業祕密等事項，為保護當事人之權益，該類資訊原則禁止公開[2]。是以，政府及公務人員對納稅義務人之稅務細節，皆負有保密義務。

不過，近年納稅義務人積欠及逃漏稅款相形嚴重，為有效防止納稅義務人逃漏稅捐，稅捐稽徵法針對重大欠稅、逃漏稅捐案件經確定者，得公告其欠稅或逃漏稅捐人之姓名與內容[3]。而所謂重大欠稅案件，係指納稅義務人個人累計欠稅

---

[1] 稅捐稽徵法第 33 條第 1 項：「稅捐稽徵人員對於納稅義務人之財產、所得、營業、納稅等資料，除對下列人員及機關外，應絕對保守秘密：一、納稅義務人本人或其繼承人。二、納稅義務人授權代理人或辯護人。三、稅捐稽徵機關。四、監察機關。五、受理有關稅務訴願、訴訟機關。六、依法從事調查稅務案件之機關。七、經財政部核定之機關與人員。八、債權人已取得民事確定判決或其他執行名義者。」

[2] 政府資訊公開法第 18 條第 6、7 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。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。」

[3] 稅捐稽徵法第 34 條第 1 項：「財政部或經其指定之稅捐稽徵機關，對重大欠稅案件或重大逃漏稅捐案件經確定後，得公告其欠稅人或逃漏稅捐人姓名或名稱與內容，不受前條第一項限制。」

逾 1,000 萬元或營利事業累計逾 5,000 萬元，且符合稅捐稽徵法規定之確定案件[4]。因此，主管機關即可公告之納稅義務人之姓名、稅目別、欠稅年度、欠稅或罰鍰金額及自然人之地址，惟僅得公告至街道或村里名稱，而納稅義務人為營利事業者，應一併公告其負責人姓名及地址[5]。且納稅義務人欠稅達一定金額者，得函請相關機關限制其出境[6]，對於有能力卻故意拖延欠稅者，則可透過執行機關向法院聲請准予拘提、管收之手段，促使欠稅人履行納稅義務[7]。

綜上所述，本案肉羹大盤商涉嫌逃漏營業稅、營利事業所得稅共 2030 萬，屬重大欠稅者，然而該名盤商繳納部分稅款後，利用脫產、遷移戶籍等方式逃避責任，因此執行分署認定其顯有逃匿之虞及就應供強制執行之財產有隱匿或處分之情況，向新北地方法院聲請管收獲准，予以管收。

【管理 Tips】

針對納稅義務人個人累計欠稅逾 1,000 萬元及營利事業累計欠稅逾 5,000 萬元者，民眾可於各主管機關網站查詢上述重大欠稅人名單。同時，主管機關應考量該類資料之機密性、完整性及可用，納入適當之安全作業程序及控制措施。且因個人的財產、所得、營業、納稅，屬法律要求予以確實保密之重要資料，須明確區分欠稅人或逃漏稅捐人之身分，確保公開予大眾之資訊均為正確且未有非授權

---

[4] 稅捐稽徵法第 34 條第 3 項：「第一項所稱確定，係指左列各種情形：一、經稅捐稽徵機關核定之案件，納稅義務人未依法申請復查者。二、經復查決定，納稅義務人未依法提起訴願者。三、經訴願決定，納稅義務人未依法提起再訴願者。四、經再訴願決定，納稅義務人未依法提起行政訴訟者。五、經行政訴訟判決者。」

[5] 財政部台財稅字第 09904504190 號函說明三。

[6] 稅捐稽徵法第 24 條第 3 項本文：「在中華民國境內居住之個人或在中華民國境內之營利事業，其已確定之應納稅捐逾法定繳納期限尚未繳納完畢，所欠繳稅款及已確定之罰鍰單計或合計，個人在新臺幣一百萬元以上，營利事業在新臺幣二百萬元以上者；其在行政救濟程序終結前，個人在新臺幣一百五十萬元以上，營利事業在新臺幣三百萬元以上，得由財政部函請內政部移民署限制其出境；其為營利事業者，得限制其負責人出境。」

[7] 行政執行法第 17 條第 5 項：「行政執行官訊問義務人後，認有下列各款情形之一，而有管收必要者，行政執行處應自拘提時起二十四小時內，聲請法院裁定管收之：一、顯有履行義務之可能，故不履行。二、顯有逃匿之虞。三、就應供強制執行之財產有隱匿或處分之情事。四、已發見之義務人財產不足清償其所負義務，於審酌義務人整體收入、財產狀況及工作能力，認有履行義務之可能，別無其他執行方法，而拒絕報告其財產狀況或為虛偽之報告。」

的修改。而資料既依法對外公開，即必須確保資訊可供予一般民眾瀏覽。

【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：　依法應辨識出個人資料以及相關流程，並區分可公開與不應公開之資料，避免資料不當外洩。

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：　組織應針對所適用法規有所瞭解，以稅捐稽徵法為例，無論是個人或是營利事業均有納稅義務，因此組織必須瞭解稅法上之作為流程，以及違法時所可能遭遇之風險，例如限制出境或管收等可能性，並建立適法作為之管理流程，以供組織成員作為之依據。

類別：資訊公開【案號：D10821】

中火 6 天 2 職災 3 死 全面停工體檢

【焦點話題】

台電台中火力發電廠近期進行年度整修養護工程接連發生職業災害，遭職業安全衛生署列為高風險稽查對象。先是 107 年 10 月於二號機器大修工程中，二名負責移除止水塊的外包潛水員作業時溺斃，同年 11 月八號機大修工程，再傳工安意外。另外，台電林口火力發電廠於 9 月 28 日亦有工人進行潛水作業不慎死亡。

台中港務消防隊於 11 月初獲報，六十五歲鄭姓清灰工人遭八號機空氣預熱器夾傷受困，消防員獲報到場，發現受困者安全繩遭拉扯進機器內，已明顯死亡。職業安全衛生署派員到場檢查，勒令現場停工，除追究工作場所負責人涉嫌觸犯業務過失致死責任，同時把負責人姓名刊登在職災地圖網頁，要求中火確實檢討災害原因、研提改善對策。

【參考資料來源：聯合報，107/11/1】

【重點摘要】

1. 依據政府資訊公開法第 6 條，以及勞動部公布重大職業災害案件作業要點規定，當發生重大職業災害時，主管機關得將事業單位名稱、發生重大職業災害之地址、日期、罹災人數、災害類型、原事業單位行業別、轄區勞動檢查機構名稱、工程名稱、場所，以及業主名稱予以公開。
2. 無論是職業安全管理或是資訊安全管理，在管理制度中賞罰併濟是管理者提昇組織效率的重要作法，對於未依照管理制度作為造成組織損害者，予以適當的懲處，對於優良表現者，亦應給予適當的獎勵，透過有效的績效考核，達到去蕪存菁的效果。

【法律觀點】

職業災害的發生，除造成當事人身心與社會功能受創外，往往容易造成整個家

庭經濟陷入困境。因此，為防止職業災害，保障工作者安全及健康，我國於民國 63 年制定勞工安全衛生法，並於 102 年大幅修正並更名為職業安全衛生法，且為藉助社會及媒體之監督力量，督促不良之事業單位、雇主等改善、提升服務品質，於 102 年修法[1]時規定，如事業單位勞動場所發生死亡災害、罹災人數在 3 人以上、發生災害之罹災人數在 1 人以上，且需住院治療等情形[2]，得公布其事業單位、雇主等服務機構之名稱及負責人姓名[3]。

主管機關除依照職業安全衛生法對事業單位進行公告外，為維護工作者安全與健康，強化業主及事業單位落實職業安全衛生設施，並建立重大職業災害案件之資訊公開機制，增進民眾對於職場安全維護及監督之瞭解[4]，主管機關於 106 年 12 月依據政府資訊公開法第 6 條[5]，以及勞動部公布重大職業災害案件作業要點，推出重大職業災害公開網(https://pacs.osha.gov.tw)，其中將發生重大職業災害資訊，包括事業單位名稱、發生重大職業災害之地址、發生重大職業災害之日期、罹災人數、災害類型、發生重大職業災害之業主名稱等資訊[6]加以

---

[1] 職業安全衛生法第 37 條第 2 項：「事業單位勞動場所發生下列職業災害之一者，雇主應於八小時內通報勞動檢查機構：一、發生死亡災害。二、發生災害之罹災人數在三人以上。三、發生災害之罹災人數在一人以上，且需住院治療。四、其他經中央主管機關指定公告之災害。」

[2] 行政院勞工委員會（81）台勞安三字第 32211 號：「依勞工安全衛生法第二十八條第二項第三款規定，公告指定雇主應於二十四小時內報告檢查機構之職業災害如左：氨、氯、氟化氫、光氣、硫化氫、二氧化硫等化學物質之洩漏，發生勞工罹災需住院治療在一人以上之災害。」

[3] 職業安全衛生法第 49 條：「有下列情形之一者，得公布其事業單位、雇主、代行檢查機構、驗證機構、監測機構、醫療機構、訓練單位或顧問服務機構之名稱、負責人姓名：一、發生第三十七條第二項之災害。二、有第四十條至第四十五條、第四十七條或第四十八條之情形。三、發生職業病。」

[4] 勞動部公布重大職業災害案件作業要點第 1 點。

[5] 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。」

[6] 勞動部公布重大職業災害案件作業要點第 4 點：「四、 本部建置重大職業災害資料庫網頁，提供民眾查詢、瀏覽，並公布重大職業災害資訊（如附表）: (一)事業單位名稱。但承攬人、再承攬人名稱不予公布。(二)發生重大職業災害之地址。但屬道路、河川、隧道、管道、山坡地或景觀等工程，得不予公布地址。(三)發生重大職業災害之日期。(四)罹災人數。(五)災害類型。(六)原事業單位行業別（無原事業單位時，以承攬工作獨立施作而未轉包或分包之事業單位行業別載述）。(七)轄區勞動檢查機構名稱。 營繕工程除揭露前項第一款至第七款之資訊外，並得公布下列資訊：(一)發生重大職業災害之工程名稱。(二)發生重大職業災害之場所。(三)發生重大職業災害之業主名稱。」

公開。亦因此類資訊公開之母法依據為政府資訊公開法，故其公告之內容除非受政府資訊公開法第 18 條[7]之限制，否則其並無特殊之範圍限制，並可大於職業安全衛生法所得公布之事項。而職業安全衛生法與勞動部公布重大職業災害案件作業要點於發生死亡災害[8]之情形下，二者會重合，其餘部份之非死亡案件情形，則依職業安全衛生法第 49 條公布。

此外，為提升職業安全衛生管理水準，鼓勵事業單位、主辦機關等廠商維護工作者安全，並建立職業安全衛生優良案件之資訊公開機制，保障民眾知的權利，增進人民對公共事務之瞭解[9]，主管機關亦將績優案件或良好案件公告於職安卓越網[10]，藉此對業者加以鼓勵。

本案受裁罰單位發生職業安全衛生法第 37 條第 2 項第 1 款規定之死亡職業災害，主管機關除得依職業安全衛生法第 49 條第 1 款規定公布事業單位名稱外，尚得依政府資訊公開法第 6 條與勞動部公布重大職業災害案件作業要點第 4 點公布事業單位名稱、發生重大職業災害之地址等事項，並刊登於職災地圖網頁。

---

[7] 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。」

[8] 勞動部公布重大職業災害案件作業要點第 2 點第 1 項：「二、本要點用詞，定義如下： (一) 重大職業災害，指下列職業災害之一：1、工作場所發生職業安全衛生法第三十七條第二項第一款規定之職業災害。2、勞動場所發生自營作業者死亡之職業災害。」

[9] 勞動部公布職業安全衛生優良案件作業要點第 1 點。

[10] 網址同職災公開網，均為 https://pacs.osha.gov.tw。

【管理 Tips】

政府資訊公開法之立法目的在於便利人民公平利用政府依職權所作成或取得之資訊，除增進一般民眾對公共事務之瞭解、信賴及監督外，更能促進民主之參與[11]。因此，政府機關於判斷是否進行政府資訊公開時，首先，應確認其是否屬於政府資訊公開法第 3 條[12]之政府資訊；再者，如屬於政府資訊，是否應依同法第 6 條主動適時公開；且注意是否屬於同法第 18 條之限制公開事由，以及有無例外得公開之情形；最末，縱為限制公開事項，可否將資訊分離後，而就得公開之部份予以公開或提供。

此外，由本案例可延伸得知，無論是職業安全管理或是資訊安全管理，在管理制度中，除對於未依照管理制度作為造成組織損害者，可以予以適當的懲處外，對於優良表現者，亦應給予適當的獎勵，以作為鼓勵。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.7.2.3 懲處過程

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

  (2) 適用說明： 組織應針對所應用的管理制度，建立有效之獎懲標準，並據之對違反規定者進行相對應的懲處。本案即係組織違反法令致發生職災而有死傷，因此必須進行懲處以及公告。

- A.18.1.1 適用之法規及契約的要求事項之識別

[11] 政府資訊公開法第 1 條立法理由。

[12] 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。」

(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，組織針對相關職業安全法規之遵循應可更加小心，避免造成此類損害。

參、資訊監察(Monitors)

類別：資訊監察【案號：M10822】

「沃爾瑪專利的音檔監控工具可以監聽員工與客戶的對話」

【焦點話題】

全球最大零售商沃爾瑪提出新的監控技術專利，該專利描述在其購物商場中需要「聲音傳感器」(sounds sensors)和「傾聽前端」(listening to the frontend)技術，沃爾瑪將使用感應器接收員工和顧客間互動及收銀檯周圍所產出的聲音，例如掃描器的嗶嗶聲，裝袋等產生的聲音，進而分析音檔內容並計算績效指標。而該績效指標係包括員工是否與客戶進行聊天、查看員工是否使用特定問候語或依照公司的標準作業流程執行。

而該項專利申請之最終目的希冀提昇員工效率與績效，並有效降低商場的運作成本及提高客戶滿意度。不過如同大部分的專利一般，目前沃爾瑪尚未將該項技術現實化，並聲明表示其不斷考慮新的概念和方法，有助於進一步改善加強客戶服務的方式。

【參考資料來源：Dailymail，107/7/12】

【重點摘要】

1. 通訊保障及監察法第 3 條所稱之通訊有三種，分別為：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，因此只要涉及到與上開定義有關之內容，均受其保障。

2. 當蒐集的音檔可以用直接或間接方式識別特定個人，甚或是該個人的社會活動時，因已符合個人資料保護法第 2 條之個人資料之定義，故應存在同法第 19 條規定符合法律明文規定等特定情形，並對資料主體履行告知義務。

【法律觀點】

我國通訊保障及監察法（下稱通保法）所稱之通訊有三種，分別為：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[1]。無論是政府機關或一般民眾，只要涉及上開定義有關之內容，均受到通保法之保障，但該保障必須係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[2]。惟是否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，仍必須就客觀事實加以認定[3]。

而以刑法判斷是否具有隱密性之期待時，通常以是否為公開或非公開為基本的判斷要素，「非公開活動」則指活動者主觀上具有隱密性之期待，且在客觀上已利用相當環境或採取適當設備，足資確保其活動之隱密性，使一般人均能藉以確認活動者主觀上具有隱密性期待，而無誤認之虞者，始足當之[4]。因此，即便當事人主觀上認為屬於非公開之談話，但如果活動於客觀上評價時，一般人會認為並未選擇適當之談話處所以保護言論內容不被他人知悉，則該談話在客觀上並不是非公開行為，並不具有隱密性存在。

就沃爾瑪案例而言，因其裝置設置於購物商場中，而購物商場是多數或不特定人有可能看見或聽見的環境，且客觀上並無活動隱密性之可能。因此，縱然我國廠商效法沃爾瑪在其商場內裝設得捕捉商場內的聲音，雖未觸犯通保法相關規定，惟仍有違反其他法律之虞[5]。

按照個人資料保護法（下稱個資法）規定，所謂個人資料包含自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財

---

[1] 通訊保障及監察法第 3 條第 1 項。

[2] 通訊保障及監察法第 3 條第 2 項。

[3] 通訊保障及監察法施行細則第 2 條第 4 項。

[4] 最高法院 101 年度台上字第 6343 號刑事判決參照。

[5] 另，企業如非法進行通訊監察，即可能觸犯刑法第 315-1 條之無故竊錄罪，及通保法第 24 條第 1 項之非法監察罪，惟刑法之無故竊錄罪係以非公開活動為限，而通保法之非法監察係奠基於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，本案中因裝置係設置於購物商場中，屬於開放空間，較難認定當事人之作為屬於非公開活動或對通訊內容有隱私或祕密之合理期待，在此併予說明。

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[6]。因此，如蒐集之音檔得以直接或間接方式識別特定個人，甚或是該個人的社會活動時，則適用個資法相關規定。而蒐集個人資料除須有特定目的外，亦須符合八種法定情形之一[7]，否則恐遭由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正[8]，且如違法蒐集是意圖為自己或第三人不法之利益或損害他人之利益，而足生損害於他人時，還可能遭處 5 年以下有期徒刑[9]。因此，如本案發生於我國時，仍應考量個資法規定以合法蒐集個人資料。

【管理 Tips】

「聲音傳感器」和「傾聽前端」等裝置係為環境監控裝置，其目的在於蒐集環境聲音以檢視作業環境及流程是否須要改善，惟該環境監控裝置係有收錄員工及客戶之聲音，此涉有個資法之可能，故組織進行相關資料蒐集時，仍應依循一定程序。

首先，該項專利係利用公共場所蒐集環境音並加以分析，被蒐集者並無隱私期待可能性，故排除通保法之適用。但如以個資法之角度觀察，其針對所蒐集之資料加以分析，故必須確認所蒐集之資料於分析後是否為個人資料。再者，如屬個人

---

[6] 個人資料保護法第 2 條第 1 款。

[7] 個人資料保護法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

[8] 個人資料保護法第 47 條：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：一、違反第六條第一項規定。二、違反第十九條規定。三、違反第二十條第一項規定。四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。」

[9] 個人資料保護法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

資料，其蒐集之個人資料行為已具備特定目的[10]，故必須符合個資法之法定情形。是以，如具備特定目的與法定情形時，則應對個人資料主體進行告知，以避免爭議發生。

然而，組織蒐集資料時仍應考量人格權與個人資料合理利用之平衡，以誠信原則為依歸，訂定資料蒐集準則及有效之管理措施，並對蒐集資料之相關紀錄予以留存，得於未來訴訟發生時，用以提出舉證責任。

【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。本案如為我國組織於前台裝設收音檔監控設備，組織應先分析所適用之法規，且因恐涉及個資法，故應符合個資法要求於蒐集資料時之具備特定目的、法定情形及對資料主體為告知之要件，並做好資料保存，以免後續訟爭敗訴風險。

[10] 目的在於提昇員工效率與績效，並有降低購物商場的運作成本以及提高客戶滿意度。

類別：資訊監察【案號：M10823】

舊金山成為美國首例禁止臉部辨識軟體的城市

【焦點話題】

舊金山將成為美國首例禁止臉部辨識(Facial-Recognition)技術的城市。舊金山監事會(San Francisco Board of Supervisors)於 108 年 5 月通過《停止祕密監視條例》(Stop Secret Surveillance Ordinance)。

該立法決議內容指出，監視技術恐威脅或壓迫某些種族、宗教、性取向等特定族群的隱私。臉部辨識技術對於公民權利和自由的危害，遠超過其帶來的好處，該技術將加劇種族歧視且威脅人民不受政府持續監視的權利。因此，臉部辨識技術於執法過程當中應審慎應用，只有在法律強而有力的監督、問責措施下，輔以制度透明要求，才能在應用同時保障公民權利及自由。此外，臉部辨識技術及其衍生數據，亦只有在符合公民意旨且具應用實益的情況下，才能尋求技術的資助、獲取、使用及數據的共享。

【參考資料來源：中央廣播電台，108/5/15】

【重點摘要】

1. 《停止秘密監視條例》施行後，舊金山政府機關如有應用臉部辨識技術[1]的需求，原則上應經過監事會核准，否則將可能違反條例。
2. 《停止秘密監視條例》第 19B.2(a)條要求，舊金山政府機關為下列行為時，應報請監事會核准：監視技術所需費用、新技術獲取或租用、條例列舉情況外之監視技術利用、與非政府機關有契約關係，而取得，共享或以其他方式使用

[1] 監視技術「包括但不限於以下內容：國際移動用戶辨識碼（IMSI）捕捉器和其他蜂巢式網路模擬器；自動車牌辨識器；電動收費讀卡器；閉路電視攝影機；槍擊檢測硬體和服務；影像以及聲頻監控或記錄技術，如監控攝影機，廣角攝影機和可穿戴式人體攝影機；移動 DNA 捕獲技術；生物識別軟體或技術，包括面部，語音，虹膜和步態識別軟體和數據庫；旨在監控社交媒體服務的軟體；X 光車；旨在預測犯罪活動或犯罪行為的軟體；無線電頻率 ID（RFID）掃描儀；和包括軟體和硬體在內之工具，監視範圍則包含未經授權訪問電腦，電腦服務或電腦網路」。

監察技術或；與非政府機關有契約關係，取得其監視技術衍生數據[2]。

3. 為降低政府侵害個人隱私的風險，舊金山《停止秘密監視條例》第 19B.2(d)條原則上禁止政府機關取得、保存或使用任何臉部辨識技術，同時亦限制該技術衍生數據之使用[3]。甚至代表政府進行民事、行政訴訟之律師，亦不得使用臉部辨識技術及技術衍生數據[4]。

【法律觀點】

臉部辨識技術目前廣泛使用於各國政府公共生活中，例如：中國大陸於新疆維吾爾族自治區採用臉部辨識技術，開始自動化種族主義[5]的新時代。在美國，臉部辨識技術使用無處不在，執法機構亦越來越廣泛使用。目前，美國目前各地已有數十個當地警察部門使用該項技術將駕駛執照及大頭照與犯罪資料庫相匹配，同時亦使用於監視人群，例如：抗議、購物中心或音樂會等，以即時識別潛在犯罪嫌疑人。

該條例之通過，代表警方將無法利用公共場所之攝影機與影像處理技術及犯罪照片資料庫加以連結比對。此外，該條例規範範圍未及於聯邦層級，因此聯邦機關如舊金山國際機場等機關已布建的臉部識別系統、生物辨識掃描儀，因而不受影響。當然，此規範僅限於舊金山政府機關，因此非政府機關如使用臉部辨識系統作為紀錄考勤之民間公司，仍不受影響。

---

[2] San Francisco CITY BOARD FILE NO. 190110　SECTION 19B.2(a).

[3] San Francisco CITY BOARD FILE NO. 190110　SECTION 19B.2(d)

[4] San Francisco CITY BOARD FILE NO. 190110　SECTION 19B.2(h)

[5] 自動化種族主義(automated racism)是紐約時報記者 Paul Mozur 於" One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority" 報導所提出，其提到「臉部辨識技術融入了中國快速發展的監控攝影機網路中，專門針對維吾爾人的外觀，並記錄他們的來往和搜索與審查的記錄。這種做法使中國成為應用下一代技術觀察其人才的先驅，可能開啟自動化種族主義的新時代。」(The facial recognition technology, which is integrated into China' s rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review. The practice makes China a pioneer in applying next-generation technology to watch its people, potentially ushering in a new era of automated racism.)用以形容中國大陸在新疆以自動化的監控方式，進行種族判定是為自動化種族主義。https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html， (最後瀏覽日：108 年 5 月 22 日)

事實上，透過臉部辨識技術監控時常是弊大於利，於 2018 年由美國公民自由聯盟以名為「Rekognition」的臉部辨識工具的測試中，該軟體將 28 位黑人國會成員誤認為是罪犯[6]。目前我國並未直接規範臉部辨識技術應用，關於新興監視科技應用所涉及之隱私議題，主要規範於個人資料保護法（下稱個資法），是以，居於智慧城市的我們，亦可思考如何在維持公共安全、社會秩序，以及犯罪偵防同時保障民眾權益，藉以降低政府侵害個人隱私的風險。

【管理 Tips】

根據我國個資法之規定，臉部辨識之特徵，非屬於病歷、醫療、基因、性生活、健康檢查及犯罪前科等特種個人資料[7]，故僅能歸類於一般個人資料，與姓名、地址等其他個人資料[8]。

從管理之角度而言，我國個資法僅需保護一般個人資料亦已足夠，意即遵守蒐集要件、具備特定目的並輔以告知義務之履行即可，而不需如特種個人資料一般的原則禁止蒐集。而政府單位如以街頭監視器作為一般交通違規取締之工具，即必須注意是否符合該監視器裝設時之特定目的，如目的為犯罪偵防，原則上必須排除作為交通違規取締之用途[9]。因此，政府單位使用臉部辨識技術時，雖僅以一般個人資料處理，仍需注意法規之要求。

【相關標準】

---

[6] Jacob Snow, *Amazon´s Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (JULY 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (最後瀏覽日：108 年 5 月 22 日)

[7] 個人資料保護法第 6 條第 1 項：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」

[8] 個人資料保護法第 2 條第 1 款：「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。」

[9] 以臺北市錄影監視系統設置管理自治條例為例，該條例第 4 條規定錄影監視系統之設置，應以維護公共安全、社會秩序、犯罪預防及偵查為目的，而同條例第 11 條則規定，錄影監視系統影音資料應予保密，非依法定程序，不得處理及利用。因此，除依法定程序外，排除非維護公共安全、社會秩序、犯罪預防及偵查之目的外利用。

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、法規及契約的要求事項。

(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事項。本案中，舊金山市訂定嚴格的監控管理條例，則市府即應遵守此條例，對於臉部辨識技術應予以排除而不再使用。

類別：資訊監察【案號：M10824】

德國政府擬要求數位服務公司提供用戶個資

【焦點話題】

德國政府提出「透明數據」計畫，要求販售數位助理的公司必須開放用戶數據予政府，以便「防範駭客攻擊」，這項法令範圍包含亞馬遜智慧音箱 Echo、谷歌 Home 乃至蘋果語音助理 Siri 等數位助理，此舉也讓外界擔心，對於德國人民的隱私、人權造成嚴重侵犯。

然而，針對德國政府而言，數位足跡變得越來越重要，家庭數位助理、智能設備及語音控制設備等可存儲大量資料，例如使用時間、對話錄音等更複雜及敏感之資訊，獲取該類資訊能有效幫助執法機構打擊犯罪，國家與聯邦政府需要權限獲取個人數位裝置產生之資料。但蒐集及儲存此類資訊亦可能對用戶隱私產生嚴重影響。

【參考資料來源：聯合報，108/6/11】

【重點摘要】

1. 亞馬遜、谷歌或蘋果等智慧裝置製造及服務業者，非屬通訊監察及保障法第 14 條所稱之電信事業，故無配合通訊監察之義務。
2. 智慧裝置屬「物」，其所儲存之通訊內容屬「電磁紀錄」，如該智慧裝置可作為證據時，司法機關可透過刑事訴訟法第 122 條及第 133 條之規定，以搜索、扣押的方式取得「過去已結束」之通訊內容。

【法律觀點】

目前民眾於家庭環境內使用網路麥克風、居家攝影機等智慧裝置之情形已相當普遍，提供便利性的同時亦引起社會大眾對於隱私影響之關注。然而，民眾使用其裝置時，應同時思考部分隱私將提供予智慧裝置之私人公司，甚至恐有政府取得之風險。

以智慧型手機為例，其具有通話及通訊功能，政府為有效打擊犯罪係有許多手段可資運用，而通訊監察即為其一。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。然因通保法之規定，如具有足夠的事實認定犯罪嫌疑人涉犯特定重罪，且有相當理由可信其通訊內容與案件相關，並難以由其他方式進行調查時，得聲請核發通訊監察書進行監察[1]。

另按通保法規定[2]，電信事業有協助執行通訊監察之義務，該義務包含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，並協助執法機關執行通訊監察[3]。然而，行政院主計總處定義電信業屬於 J 大類 61 中類，其定義為「從事有線電信、無線電信及其他電信相關服務之行業；提供網際網路接取服務（IASP），以及透過提供有線電信傳輸服務，將電視頻道節目有系統地整合並傳送至收視戶亦歸入本類。」其與本案私人公司業者業別屬性並不相同。且按通保法施行細則第 26 條[4]規定，協助執行通訊監察義務應屬第一

[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] 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

類電信事業業者範疇，而第一類電信事業係屬特許行業，故通訊傳播委員會定期公告之經營者名單與行政院總主計處定義之電信業相符。因此，本案提及亞馬遜、谷歌或蘋果等資訊服務業者，於我國非屬電信事業，故無配合通訊監察之義務。

然而，即便資訊服務業者無配合通訊監察義務，亦不代表嗣後政府無法取得資料。事實上，智慧裝置屬於「物」，其中儲存之通訊內容屬於「電磁紀錄」，因此，當特定之智慧裝置作為證據，而司法機關已明確知悉所欲搜索、扣押之範圍時，即可以透過搜索、扣押的方式取得通訊內容[5]。

【管理 Tips】

法律上，資訊服務業者並沒有配合通訊監察之義務，惟資訊服務業者傳遞訊息，仍須透過電信業者之服務，而世界各地執法機構因加密技術，導致查緝犯罪和恐怖分子[6]更為困難。因此，國際間各政府目前正積極想方設法限制加密服務之使用，以便提供更多監控機會。

綜上，組織應特別注意資訊保護與資訊（通訊）監察間取得平衡，各業者應時刻注意法規動向，尤其是電信業者，然目前部份國家傾向修法以擴大政府對於電信業者的強制解密和技術援助獲取資料的能力，甚至要求組織根據要求向警方提供

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。」

[5] 刑事訴訟法第 133 條第 1 項：「可為證據或得沒收之物，得扣押之。」

[6] 例如，美國聯邦調查局在 2015 年為調查參與聖貝納迪諾大規模槍擊事件的個人的 iPhone 內容時，蘋果公司的加密技術使聯邦調查局在沒有攻擊者密碼的情況下無法取得手機的資料，原本聯邦調查局試圖要求蘋果公司開發新的軟體使之能夠取得手機上的資訊，不過最終是以聯邦調查局找到第三方以協助解鎖 iPhone 收場。

加密資訊，並建立繞過加密的後門。

【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：　執法機關與電信業者均應瞭解所涉法律及應用範圍，以進行相關業務之執行，避免觸法。我國法目前並未賦予非電信業者的通訊監察配合義務，亦因此政府無法要求智慧裝置製造及服務業者在設備中預設後門等方式為通訊監察之準備，而必須應向法院聲請核發扣押裁定，檢察機關應瞭解適用法規以依法行政。

類別：資訊監察【案號：M10825】

調查冒名檢舉案查 IP 憲兵逕向電信公司調資料挨告

【焦點話題】

徐姓民眾於 107 年 10 月因不滿楊姓憲兵隊調查官未報請檢察官許可，向法院聲請核發調取票，逕行發文向中華電信調取其於 107 年 8 月使用國防部民意信箱之電腦 IP 等資料，有違法監察他人通訊之嫌，向該憲兵調查官提告。

然而，該憲兵調查官表示，因有民眾報案指稱遭人冒名寄件至國防部部長信箱，並要求調查冒名者資料，因冒名者涉嫌違反個資法，因 IP 申登人資料屬於通訊使用者資料，才向國防部政務辦公室函調國防部部長信箱之寄件檢舉人 IP 位置，而依照通訊保障及監察法規定係可依職權調取。

綜上所述，檢方認為通訊保障及監察法關於調取「通信使用者資料」部分，其相關權責規範係檢察官，而非司法警察官，因此實務上衍生出司法警察官能否依職權調取通信使用者資料之疑義，惟通訊保障及監察法係保障「現時或未來發生」之通訊內容，檢舉信屬「過去已結束」之通訊內容，已非秘密通訊自由保護客體，因此，該憲兵調查官為不起訴處分。

【參考資料來源：自由時報，108/7/3】

【重點摘要】

1. 智慧財產法院 106 年度刑智上易字第 65 號刑事判決表示，涉及通信紀錄之調取票，在輕罪時應係檢察官聲請由法院核准，而重罪時，則由檢察官依職權調取，無論輕重罪，司法警察官均不得自為調取。

2. 按最高法院 106 年台非字第 259 號刑事判決所定，調取票所能調取之客體乃「通信紀錄」或「通信使用者資料」，通訊監察書所監察之客體係「現時或未來發生」之「通訊內容」，針對「過去已結束」之「通訊內容」，則應適用刑事訴訟法，依刑事訴訟法搜索、扣押相關規定進行辦理。

【法律觀點】

通訊保障及監察法（下稱通保法）係政府機關進行通訊監察之依據，其目的在於保障國家侵害人民祕密通訊自由及隱私權，在兼及國家安全的前提下，而對通訊監察予以限制[1]。而民國 103 年修法時，除將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，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]外，亦增加當偵查最重本刑三年以上有期徒刑之罪時，如果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，則檢察官可以以書面向法院聲請核發調取票，而調取的內容包括通信紀錄及使用者資料，於相同情形下，司法警察官則應報請檢察官許可後，向該管法院聲請核發調取票。而當涉及特定重罪時，則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[3]。惟該新增條文對於司法警察官可否獨立調取通信紀錄並沒有說明，意即司法警察官能否逕行向電信公司調取通信紀錄並無確切規範其法定程序。

對此，智慧財產法院 106 年度刑智上易字第 65 號刑事判決表示：「國家為偵查

---

[1] 通訊監察及保障法第 1 條：「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。」

[2] 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。…」。

[3] 通訊保障及監察法第 11-1 條：「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。　司法警察官因調查犯罪嫌疑人犯罪情形及蒐集證據，認有調取通信紀錄之必要時，得依前項規定，報請檢察官許可後，向該管法院聲請核發調取票。檢察官、司法警察官為偵辦最輕本刑十年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪防制條例等罪，而有需要時，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，不受前二項之限制。第一項之急迫原因消滅後，應向法院補行聲請調取票。　調取票，應記載下列事項：一、案由。二、應調取之通信紀錄或使用者資料。三、有效期間，逾期不得執行調取及調取後應將調取票交回之意旨。　第一項、第二項及第四項之聲請經法院駁回者，不得聲明不服。　核發調取票之程序，不公開之。　有調取第七條之監察對象通信紀錄及通訊使用者資料必要者，由綜理國家情報工作機關向電信或郵政事業調取，不受前七項之限制。」

犯罪，而有查看人民通信紀錄，以及瞭解通信使用者資料時，已非毫無法律限制，且已經立法者列為法官保留及令狀原則之適用範圍。其中關於通信使用者資料部分，雖然表面上只對檢察官有所規定，而未規定司法警察官在取得通信記錄時之法定程序，但檢察官在我國刑事偵查法制上，為唯一之偵查主體，司法警察官依其層級僅分別有協助檢察官偵查犯罪之職權，或受檢察官之指揮，偵查犯罪（刑事訴訟法第 229、230 條參照），依照法律之體系解釋，實在難以認為協助或接受指揮之司法警察官可以不受審查、自主取得人民之通信使用者資料，但作為偵查主體之檢察官卻反而要受法官保留及令狀原則之拘束。」據上可知，法院認為無論重罪與否，可發動調取通信紀錄主體應為檢察官，只是輕罪時，需由檢察官發動再由法院核准，而重罪時，僅需由檢察官依職權調取即可，司法警察官僅為協助檢察官偵查犯罪或受檢察官之指揮偵查犯罪，並沒有獨立調取通信紀錄的權力。

本案中，檢方認為通保法關於「通信使用者資料」部分，係規範檢察官而非司法警察官，且通保法保障的是「現時或未來發生」的通訊內容，檢舉信屬「過去已結束」通訊內容，已非秘密通訊自由保護客體，因此將其不起訴。

惟分析智慧財產法院之判決，通保法關於通信使用者資料部份，雖僅規範檢察官，但其係因檢察官為偵查主體故加以規範，而司法警察官僅有協助等權責，舉重以明輕，不應認為未規範者反可任意調取。其次，如檢方所調取者為電腦 IP 申登人資料，則屬於「通信使用者資料」，仍屬於前開應以調取票調取之對象。再者，檢方認為檢舉信屬過去已結束通訊內容，故非屬秘密通訊自由保護客體，但按最高法院 106 年台非字第 259 號刑事判決[4]意旨，如屬於「過去已結束通訊內容」者，應回歸適用刑事訴訟法，依刑事訴訟法搜索、扣押相關規定，而非得任意以調取之名義規避搜索、扣押之義務。據此，該不起訴處分仍

[4] 最高法院 106 年台非字第 259 號刑事判決：「貳、本院按…通保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，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，依刑事訴訟法搜索扣押相關規定為之。…」

有討論空間。

【管理 Tips】

實施管理制度時，可發現任何規定皆有其所欲規範的主客體，惟未列入規範條文者，並非必然屬於無規範狀態，仍應就其條文意旨加以判斷，未於條文清楚規定者，而可能透過解釋而受到限制。

又，本案涉及到「通信紀錄」、「通信使用者資料」與「通訊內容」等個人可識別資訊，意即個別項目均涉及到不同程度的隱私，而法規亦對此為不同程度的取用規則。例如，通信紀錄與通信使用者資料所受到的保護，明顯低於通訊內容所受到的保護程度。據此，組織可針對不同項目予以不同程度之保護，在取用個人可識別資訊時，針對涉及個人隱私程度高低，定義出層級化的保護準則，在涉及個人隱私程度高者，則要求較多取用關卡，而涉及個人隱私程度低者，則可給予較低度的限制。

【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。本案中警方調取者，涉及「通訊之實質內容」，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之函調方式取得，此次雖獲得檢察官不起訴處分，但警方應對於適用之法規仍應更加瞭解，避免此類案件重複發生。

- 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： 本案涉及到「通信紀錄」、「通信使用者資料」與「通訊內容」等個人可識別資訊，而組織可針對不同項目予以不同程度之保護，在取用個人可識別資訊時，針對涉及個人隱私程度高低，定義出層級化的保護準則。

肆、資訊應用(Application)

類別：資訊應用【案號：A10826】

電子支付再鬆綁 銀行超商可繳水電費

【焦點話題】

「電子支付」簡稱電支，其功能包含代收代付、帳戶儲值及帳戶資金移轉，我國總使用人數約 526 萬人。為兼顧民眾支付便利性，金融主管機關於 108 年 7 月修正「電子支付機構業務管理規則」部分條文，宣布開放電子支付多項使用方式與範圍，包含開放金融機構、便利商店業及超級市場業代收稅捐、水電費、停車費或罰款；開放電支機構發行電子支付帳戶專用儲值卡；放寬交易業務必須再確認之規定門檻；開放電支機構得為使用者支付大眾運輸或停車場業者之款項，進行單次墊款；及開放電支機構提供使用者間訊息傳遞服務等。因此，本次修正部分條文其目的在於，提升電子支付機構服務之完整性及方便性，增加消費者使用電子之付機會，推動電子之付之業務需求。

【參考資料來源：自由時報，108/7/4】

【重點摘要】

1. 為因應實務交易需求，電子支付機構業務管理規則第 20-1 條開放電子支付機構得利用行動電話等電子設備以網路方式，例如簡訊、語音、社群訊息等，針對使用者間之相互訊息通知需求。
2. 因應民眾重視個人資料維護之要求，並滿足實務上不同交易型態之支付服務需求，電子支付機構業務管理規則第 7 條規定支付指示應記載事項，要求對於個人使用者之「姓名」部分，應予部分遮蔽處理，並得以「與電子支付機構約定足資識別身分之資訊」方式記載。

【法律觀點】

電子支付機構業務管理規則係於 104 年 4 月 27 日訂定發布，並自 104 年 5 月 3 日施行，於 108 年進行第四次修正，同年 7 月公布施行。本次修法重點係為

因應電子支付機構推動業務需求，提升電子支付機構服務之完整性及使用者儲值電子支付帳戶之方便性，並強化電子支付機構收款使用者之風險控管[1]。

此次修正係因應實務交易需求，其修正重點如後：（一）開放電子支付機構利用電子設備以網路方式，提供使用者間通知訊息服務，如使用簡訊、語音、社群訊息等[2]，通知使用者物流配送情形或交易進行狀況等。（二）為提升使用者儲值便利性，增加電子支付機構收受儲值款項管道，開放電子支付機構得發行電子支付帳戶專用儲值卡，提供未有信用卡或簽帳金融卡之民眾多一種消費方式選擇，有助於擴大使用[3]。（三）兼顧民眾支付便利性，開放金融機構、便利商店及超級市場代收規費、稅捐與罰鍰、服務費及其他相關服務費用等款項[4]。（四）考量使用者支付大眾運輸事業或停車場款項，如有餘額不足之情形，開

---

[1] 電子支付機構業務管理規則部分條文修正總說明前言（108.07.02 修正）。

[2] 電子支付機構業務管理規則第 20-1 條：「電子支付機構提供收款使用者收付訊息整合傳遞或使用者間訊息傳遞服務，應符合下列規定： 一、與使用者或其他機構簽訂契約，約定雙方之權利、義務及責任。 二、對於所提供之服務，採取適當防護及控管措施，避免訊息遭洩漏、竄改或傳遞不法訊息。 三、所取得及儲存之收付訊息，以提供服務所必要者為限。四、對於執行業務所知悉之相關資訊，除法令另有規定、經簽訂契約或書面明示同意者外，不得為執行業務目的外之利用。」

[3] 電子支付機構業務管理規則第 12-1 條：「電子支付機構發行電子支付帳戶專用儲值卡應符合下列規定：一、電子支付帳戶專用儲值卡之儲存金錢價值方式，應採拋棄式，不得記載使用期限，並以新臺幣為限。二、電子支付帳戶專用儲值卡如有滅失、遺失或被竊等情形時，不得掛失止付。三、單張電子支付帳戶專用儲值卡之金額上限為新臺幣五千元，並以新臺幣百元倍數為發行單位。單次購買電子支付帳戶專用儲值卡之金額不得超過新臺幣五萬元，且不得以信用卡購買。四、電子支付帳戶專用儲值卡之正面或背面明顯處應記載電子支付機構之聯絡資訊及可供查詢持卡人權利義務訊息之管道，並載明下列事項；儲值卡版面難以完整呈現應記載事項者時，應以書面或其他合理方式告知持卡人應記載事項內容：(一)電子支付帳戶專用儲值卡之面額。(二)電子支付帳戶專用儲值卡之序號或其他足資證明交易之資訊。(三)電子支付帳戶專用儲值卡之使用須知。(四)攸關持卡人權利義務之事項。(五)其他經主管機關規定之事項。五、發行電子支付帳戶專用儲值卡收取之款項，視為本條例第六條第二款規定之儲值款項。六、應訂定安全控管計畫並建立防偽盜冒及帳務核對機制，於販售電子支付帳戶專用儲值卡時，即時傳遞、確認及核對販售訊息，並保存明細資料交易紀錄至少五年；明細資料應充分揭露販售日期、卡號、金額及幣別等項目。」

[4] 電子支付機構業務管理規則第 10 條第 2 項：「收款使用者應為代理收付實質交易款項之最終收款方。但收款使用者為金融機構、便利商店業及超級市場業，並有下列情形之一者，不在此限： 一、受各級政府委託代徵收之規費、稅捐與罰鍰。 二、受公用事業委託代收之服務費。 三、受大眾運輸事業委託代收之票價及其他相關服務費用。 四、其他經主管機關核定之款項。」

放電子支付機構得進行單次墊款[5]。（五）為強化電子支付機構對收款使用者之審查機制，電子支付機構如接受非個人收款使用者申請註冊及代理收付實質交易款項最近六個月平均交易額達新臺幣八萬元之個人收款使用者，應向聯徵中心查詢相關簽約及解約資料[6]。（六）因應民眾重視個人資料維護之要求，並滿足實務上不同交易型態之支付服務需求，規定支付指示應記載事項，對於個人使用者之姓名部分，應予部分遮蔽處理，並得以「與電子支付機構約定足資識別身分之資訊」方式記載[7]。

【管理 Tips】

近年來，主管機關對電子支付法規不斷鬆綁，促使民眾提升使用意願，並加強電子支付之推廣。然而，放寬法規限制的同時，亦必須對電子支付機構進行相對應的風險管理。例如：要求建立電子支付機構與收款使用者往來情形資料庫，以供各電子支付機構查詢。用以針對電子支付機構對收款使用者之風險控管。

以電子支付機構對於收款使用者而言，其應建立風險控管措施，包括建立徵信審核機制、風險評等機制及調查、評估實地訪視機制等，且明定調查及評估內容應包括交易異常狀況、電子支付機構報送之收款使用者簽訂及終止契約資料，及信用卡業務機構報送之特約商店簽訂及終止契約資料等資料，其目的即在於落實風

---

[5] 電子支付機構業務管理規則第 15 條：「電子支付機構不得對使用者提供電子支付帳戶透支及放款等授信或信用額度，或於使用者支付指示之金額逾電子支付帳戶餘額時，為使用者代墊款項。但為單次墊款且使用於大眾運輸事業或停車場業，不在此限。」

[6] 電子支付機構業務管理規則第 5-1 條：「電子支付機構與收款使用者簽訂及終止契約時，應通報財團法人金融聯合徵信中心(以下簡稱聯徵中心)。 電子支付機構接受非個人收款使用者註冊申請時及對於代理收付實質交易款項最近六個月平均交易額達新臺幣八萬元之個人收款使用者，應向聯徵中心查詢下列資料，並留存相關紀錄備查： 一、電子支付機構報送之收款使用者簽訂及終止契約資料。 二、信用卡業務機構報送之特約商店簽訂及終止契約資料。 三、其他經主管機關規定之資料。 電子支付機構未符合前二項規定者，應於中華民國一百零八年十二月三十一日前調整符合規定。」

[7] 電子支付機構業務管理規則第 7 條第 2 項：「使用者支付指示應記載下列事項：一、付款方姓名、名稱或與電子支付機構約定其他足資識別身分之資訊及電子支付帳戶帳號；其中個人使用者之姓名，應予部分遮蔽。二、收款方姓名、名稱或與電子支付機構約定其他足資識別身分之資訊及電子支付帳戶帳號；其中個人使用者之姓名，應予部分遮蔽。三、支付款項之確定金額及幣別。四、支付款項如非立即移轉，其移轉條件、期間或付款方指示方式。五、其他主管機關規定之事項。」

險控管的要求。

就組織而言，尋找合作對象時應建立選商標準，亦可同電子支付機構業務管理規則，以事前的徵信機制，剔除具有疑慮之合作對象，並有眾多合作對象時，以風險評等機制對風險等級較高之收款使用者，應採取一定避險措施，並建立調查、評估或實地訪視機制，確保合作對象是否有異常情形。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.15.2.1 供應者服務之監視及審查

(1) 標準內容： 組織應定期監視、審查及稽核供應者服務交付。

(2) 適用說明： 組織在進行供應服務者管理時，應建立調查、評估或實地訪視機制，確保合作對象是否有異常情形，避免供應者所提供之服務不符組織需求。

類別：資訊應用【案號：A10827】

用區塊鏈確保投票真實性 南韓「自由韓國黨」3 月開跑

【焦點話題】

南韓最大在野黨「自由韓國黨」昨宣佈，將與台灣新創團隊 ioeX 跨國合作，採用 ioeX 區塊鏈解決方案推動區塊鏈投票系統，預計今年 3 月將正式用於黨內選舉。韓國自由黨黨代表羅卿媛(Na Kyung Won)特別說明，區塊鏈的可追溯性、與不可篡改特性，可協助投票選舉更有效率。

而 ioeX 創辦人暨執行長洪啓淵指出，這次為自由韓國黨打造的客製化平台，讓黨內的各項投票，皆可藉由平台直接進行、並留存區塊鏈記錄。此外，為方便傾聽民意，平台也打造請願功能，並設置議員活動紀錄，民眾可藉平台獲得最新議員動態資訊。

洪啓淵表示，希望透過區塊鏈的落地應用，讓更多人瞭解區塊鏈實際使用的功能，投票系統只是一個開端，後續將會不斷地擴大 ioeX 組網和雙區塊鏈系統的落地應用。

【參考資料來源：自由時報，108/2/1】

【重點摘要】

1. 憲法第 129 條規定：「本憲法所規定之各種選舉，除本憲法別有規定外，以普通、平等、直接及無記名投票之方法行之。」
2. 我國目前選舉之普通原則，凡達公民年齡的國民，不分貧富、地域、宗教、黨派、性別、種族等都有投票權，惟數位落差之差異亦恐與我國現行之選舉制度有相悖之處。

【法律觀點】

區塊鏈（blockchain）一般被稱為分散式帳本技術，具有去中心化[1]、開放性[2]、獨立性[3]及安全性[4]等優點，又因具有可回溯性及不可竄改性之特性，進而被廣泛討論至可否利用於區塊鏈投票系統。

按我國憲法第 129 條規定：「本憲法所規定之各種選舉，除本憲法別有規定外，以普通、平等、直接及無記名投票之方法行之。」由此可知，憲法所定之選舉，即必須符合上開「普通」、「平等」、「直接」及「無記名」等四個要件。

首先，因選舉必須採無記名投票方式，而區塊鏈技術係以私鑰(Private Key)之方式確認使用者，並透過公鑰及私鑰比對確認身分後方得以投票，因此政府應留意公鑰與私鑰之對應關係，否則投票者真實身分可能被掌握。其次，因我國目前選舉之普通原則，凡達公民年齡的國民，不分貧富、地域、宗教、 黨派、性別、種族等都有投票權，利用線上系統投票須先克服數位落差[5]之疑慮。最末，對於是否為本人進行投票行為，更是現行難以利用區塊鏈技術進行選舉投票的因素之一，因使用區塊鏈投票時所進行的身分驗證，應係由政府所核發之身分證明文件，而其於投票時是否為本人所持有，多以驗證碼之方式進行核對，因此難以對投票者的身份進行驗證，不能保證投票者沒有被收買，進而提高賄選之可能性。

在現行的法規下，我國並未對以區塊鏈進行投票為規範，因此，如將來預以塊鏈技術進行選舉投票，仍應針對普通、平等、直接及無記名等四個要件進行評估，以避免造成選舉不公之情形。

【管理 Tips】

近年來，區塊鏈應用成為全球新興議題之一，其中區塊鏈投票系統廣受討論，

---

[1] 去中心化係指區塊鏈技術本身不需依賴第三方管理機構控管，沒有中心機制，本身可通過分散式核算和存儲，以及各個節點實現自我驗證、傳遞和管理。

[2] 開放性係指除被加密之資料外，任何人皆可透過公開介面查詢區塊鏈數據，其系統訊息開放且高度透明。

[3] 獨立性係指基於協商一致的規範和協議，區塊鏈系統不依賴第三方，所有節點能在系統內自動安全的驗證、交換數據，不需要任何人為的干預。

[4] 安全性係指整個區塊鏈中的每一個節點皆存有數據或資料，如無法掌握區塊鏈中的 51%的節點，即無法操控或修改區塊鏈中的數據或資料。

[5] 係指社會上不同性別、種族、經濟、居住環境、階級背景的人，接近使用數位產品的機會與能力上的差異。

係因區塊鏈投票可以解決重複投票及竄改投票結果之風險，惟伴隨而來的網路安全相關問題卻是一大挑戰，例如：網路、網站及載具的安全性，或利用釣魚電子郵件攻擊誘騙民眾提供投票憑據等。

因此，如我國欲採區塊鏈系統投票，仍應從安全性、透明度以及隱私保護加以著手，就安全性而言，投票所使用的裝置、網路、伺服器都有安全風險，愈多的節點將產生愈多的風險，如何解決安全性的問題，應透過專業團隊進行規劃及建置系統之開發規則，並針對網路、網站、載具之安全性及利用釣魚式攻擊進行測試，並詳實記載測試過程及應對方法。就透明度而言，因區塊鏈本身特性為去中心化且具備開放性，是由投票系統的每個用戶共同維護和管理系統的資訊，因此網路透明也就是以區塊鏈系統投票的優勢。但就隱私保護部份而言，因為身分驗證與隱私保護常處於衝突情形，例如，在確認本人之情形下要如何確保選票不會與投票者聯繫起來，又或是他人代替本人進行遠程投票，這些都是在採取區塊鏈技術投票前，所必須要考量的部份。

【相關標準】

ISO27001：2013（CNS27001）

- A.14.2.8 系統安全測試

  (1)標準內容： 於開發中，應實施安全功能性之測試。

  (2)適用說明： 組織應於開發中進行安全測試並留存紀錄，進而從測試結果中發現問題並改善之。

- 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。

  (2)適用說明： 組織針對惡意軟體應建立管理機制，並進行必要的事前預防及保護措施。

類別：資訊應用【案號：A10828】

「信用小白」利多！用手機門號就能向銀行辦貸款

【焦點話題】

金融監督管理委員會（下稱金管會）之「金融科技發展與創新實驗條例」(俗稱金融監理沙盒)於 107 年 1 月 31 日正式上路，此創新實驗機制提供業者一個試行創新商品、服務或商業模式之實驗場所，實驗期間業者可暫時排除法令適用，金管會將審酌創新實驗結果，主動檢討相關金融法規，並提供轉介輔導。國內首件監理沙盒實驗係由銀行業者與電信業者合作提出之「實踐普惠金融，首創電信行動身分認證」，實驗內容主要是藉由電信帳單及手機號碼驗證，讓「金融小白」辦理信用貸款，這項計畫原本預計自 107 年 12 月 5 日開始實驗一年，4 千名參與者，曝險金額上限 2 億元。對此，金管會綜合規劃處處長表示，上述實驗經過 8 個月後，已完成參與者實驗且達到零違約，提前實驗成功。金管會收到銀行報告書後將召開評估會議，判定有無達到當初計畫目的，之後才會出具意見書給銀行，但不保證一定會完成修法。

【參考資料來源：自由時報，108/8/15】

【重點摘要】

1. 金融科技創新實驗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，但創新實驗內容涉及應修正法律時，可再額外延長，全程實驗期間不得逾三年。創新實驗結束後，金管會應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。

2. 多重要素驗證係指用戶要通過兩種以上的認證機制之後，才能得到授權，使用電腦資源。例如，於網頁登入時，除透過第一層密碼驗證外，另外以手機簡訊、手機 APP 等方式，傳送認證碼或超連結與使用者，透過第二甚至第三手段，做身分驗證。

【法律觀點】

金融科技為金融服務帶來新樣貌，也讓金融市場面臨新的法遵、監理挑戰。為因應無現金社會的到來，我國於 107 年初完成立法並公布「金融科技發展與創新實驗條例」，相關子法亦於 107 年 4 月底陸續施行，而建立金融監理沙盒機制，除了扶植新創金融科技產業，更是監管科技（Regulation Technology, RegTech）發展的起跑點。

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[1]。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，但若當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行為，全程實驗期間不得逾三年[2]。且為排除法規障礙，條例亦於實驗期間排除相關法規之處罰規定[3]，以打造友善法規環境。而主管機關在受理申請創新實驗外，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，如認有修正必要時，即必須於創新實驗屆滿後三個月內提交修正草案報院審查[4]。

---

[1] 金融科技發展與創新實驗條例第 3 條。

[2] 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。」

[3] 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。」

[4] 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

本次創新實驗係係透過手機號碼辦理行動身分識別（Mobile ID），同時驗證個人資料及 SIM 卡，比對該名客戶以雙證件於電信業者臨櫃申辦門號時所提供之資料，以確保實為客戶本人[5]，讓參與實驗之客戶可於線上申請信用卡與小額信貸，而 Mobile ID 的身分識別亦讓實名認證行動化，不需要電腦、讀卡機等設備，即可識別使用者的身分。不過，目前相關規定尚未允許金融業者使用 Mobile ID 作為身分認證辦理開戶等事宜，故仍應進行風險分析並據以調整有關規範，可望創新實驗之結果能盡快落實。

【管理 Tips】

過去電腦計算能力大幅成長，暴力破解密碼技術已是稀鬆平常，僅透過密碼強度作為資安保護已屬不足，而多重要素驗證(Multi-factor Authentication, MFA)則是作為補足單一驗證的不足。所謂多重要素驗證係為一種電腦存取控制的方法，用戶要通過兩種以上的認證機制，即能得到授權使用電腦資源[6]。例如，透過使用者的手機簡訊、電話通知和行動應用程式等不同的驗證選項，當使用者登入設備或網站時，除了第一道密碼驗證之外，多重要素驗證會結合前述的手機簡訊、電話通知或行動應用程式，做第二道即時性的身份驗證。而 Mobile ID 行動身分識別是指，用戶透過載有 SIM 卡的行動裝置，連線至行動通信網路發出確認請求，並在應用系統中輸入手機門號及身分證字號，透過 TWID 身分識別中心向所屬電信業者詢問身分識別的結果[7]，而透過 Mobile ID

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。　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。」

[5] 凱基銀與中華電信攜手 手機身分認證服務率先啟動 首件金融創新實驗計畫 12 月 5 日正式上線，https://www.kgibank.com/about_us/L06/L0601/L0601_0232.html （最後瀏覽日：108 年 8 月 23 日）

[6] 多重要素驗證，https://zh.wikipedia.org/wiki/%E5%A4%9A%E9%87%8D%E8%A6%81%E7%B4%A0%E9%A9%97%E8%AD%89 （最後瀏覽日：108 年 8 月 23 日）

[7] 五大電信共同站台，Mobile ID 行動識別服務最快明年上線，https://technews.tw/2018/11/28/mobile-id-with-support-from-five-telecom-companies-launches-in-taiwan/ （最後瀏覽日：108 年 8 月 23 日）

加上其他驗證方式，達到多重要素驗證的方式。

不過，使用 Mobile ID 作為多重要素驗證的一環時，所會遇到的問題在於手機門號的使用者是否為門號申請人。以目前現況而言，個人多重門號已為常態，其中包含一人申請並使用多門號，亦可能為一人申請多門號予多人使用，如屬後者，則透過連結回電信業者確認身分時，所確認之身分亦不一定為門號的真實使用者，例如，父母於小孩未成年時所辦之門號，於小孩成年後持續使用，此時如小孩使用父母之身份證件及 Mobile ID 為多重要素驗證，可能會使銀行方誤判而予以貸款。

本次監理沙盒實驗使用 Mobile ID 完成身份認證 4 千件係已達標，但相對於該電信業者所有之 1,058.7 萬個手機用戶[8]，佔比有限，之後是否修改辦理電子銀行業務安控基準，開放 Mobile ID 取得與自然人憑證相同的安全認證資格，為後續所應探討之事。一旦金管會判定可行，未來有望透過銀行公會自律規範等規範修正，讓其它銀行跟進一體適用。

【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。目前金融科技發展與創新實驗條例已經施行，相關配套辦法亦已上路，金融業者在進行創新

[8] 2019 年第 1 季行動通訊市場統計資訊，https://www.ncc.gov.tw/chinese/files/19070/3773_41619_190703_1.pdf （最後瀏覽日：108 年 8 月 22 日）

實驗時，應針對目前是否有法規限制，如何申請及進行創新實驗，並於結束創新實驗後，針對申請案所涉及之管制法令進行檢討研修，如認有修正必要時並提出修正建議。

類別：資訊應用【案號：A10829】

收養、監護等 6 項法院判決 今起可線上辦理登記

【焦點話題】

內政部自 107 年 7 月 16 日起開放法院判決（含調解、和解）離婚登記、死亡登記等戶籍登記的線上申辦服務，而 108 年 6 月 1 日起更進一步新增收養登記、終止收養登記、監護登記、輔助登記、未成年子女權利義務行使負擔登記及出境遷出登記等 6 項線上申辦服務。

內政部表示，過去民眾收到法院裁判文件或戶政事務所寄發的出境滿 2 年通知書後，即必須跑一趟戶政事務所辦理登記，而現在民眾只要符合申辦資格，即可上網以自然人憑證提出申請，除了收養登記須另行掃描養子女姓氏約定書外，其他各項登記則不須再掃描或上傳證明文件，戶政事務所受理後就會進行查證審核並辦理登記，並於完成後以電子郵件通知，屆時民眾再到任一戶政事務所換發證件即可。

【參考資料來源：自由時報，108/7/3】

【重點摘要】

1. 主管機關為確認申請人為具備資格之當事人，係以電子簽章法第 2 條第 6 款所稱「載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明」之憑證以確認當事人身分，惟使民眾使用戶政網路登記作業系統產製具有電子簽章之電子文件作為通信及交易之基礎，取代傳統公私領域之書面文件及簽名、蓋章確定之相關法律責任，仍應由申請人同意以使用之。

2. 自然人憑證的功能係在網路上作資料交換時，作為辨識雙方身分之用，透過自然人憑證之資料來源辨識（Authentication）以及不可否認性（Non-repudiation），確保係申請人本人所操作，目前自然人憑證使用的網路應用服務包括戶政網路登記作業、網路報稅、勞保年資及個人退休金專戶查詢

等多項便民服務[1]。

【法律觀點】

內政部戶政司已建置戶政網路登記作業，以推動戶籍申辦服務作業流程化及便利化。目前線上申辦戶籍登記作業包括離婚登記、死亡登記、出生地登記、監護登記、輔助登記、未成年子女權利義務行使登記、收養登記、終止收養及回復本姓登記，以及出境遷出登記等項目。目前必須由民眾以自然人憑證登入系統，線上填載申請資料，例如線上申辦終止收養及回復本姓登記，其需填具被收養者國民身分證統一編號、證明文件作成機關、政府機關證明文件案號，以及是否同意回復本姓等申請資料，方依據申請人戶籍所在地戶政事務所進行派送，俟戶政事務所接獲通報，查證後，始完成登記。

而內政部戶政司分別於 107 年 7 月 16 日[2]以及 108 年 6 月 1 日[3]依據戶籍法第 27 條第 2 項[4]規定，將前述戶籍登記項目新增於線上申辦的範疇。惟因線上申辦係無法與當事人面對面確認其身分，故內政部為確認申請人為具備資格之當事人，使用自然人憑證以確認當事人身分，此係由於自然人憑證，係電子簽章法第 2 條第 6 款所稱「載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明」之憑證，因此透過網路環境，民眾持自然人憑證登入系統，已足以表彰個人真實身分。

而民眾使用戶政網路登記作業系統產製具有電子簽章之電子文件作為通信及交易之基礎，取代傳統公私領域之書面文件及簽名、蓋章確定之相關法律責任，

---

[1] 內政部憑證管理中心應用系統網站連結，http://moica.nat.gov.tw/link_1.html （最後瀏覽日：108 年 9 月 2 日）

[2] 內政部台內戶字第 1071202244 號函釋。

[3] 內政部台內戶字第 1080241959 號函釋。

[4] 戶籍法第 27 條：「登記之申請，由申請人以書面、言詞或網路向戶政事務所為之。　依前項規定以網路申請登記之項目，由中央主管機關公告，並刊登政府公報。」

仍應依電子簽章法第 4 條第 1 項[5]以及第 9 條第 1 項[6]規定，經相對人同意者後方得為之，由申請人本人同意使用。

【管理 Tips】

本案例可分為兩部分進行探討：

首先，針對主管機關(服務提供者)：可從機密性（Confidentiality）、完整性（Integrity）以及可用性(Availability)加以考量，就機密性而言，應有適當之控制措施，保護資訊系統網頁與後端資料庫間之網路傳遞資料，例如傳遞資料採取加密機制等，以確保民眾上傳資料的機密性，避免非授權人員存取、使用或竄改；就完整性而言，服務提供者應對於資訊系統網頁資訊的完整性加以保護，確保公開予大眾之資訊，在服務提供者內部與外部均為一致；就可用性而言，服務提供者確保資訊與系統能夠持續營運、正常使用，當服務使用者要求使用資訊系統時，使用者均可以在適當的時間內獲得回應，並獲得所需服務。

其次，對民眾(服務使用者)：自然人憑證可以在網路上作資料交換時，可作為網路身分證以辨識雙方身分，就如同上述服務提供者所希望達成之目標，機密性、完整性、可用性外，透過資料來源辨識(Authentication)以及不可否認性(Non-repudiation)，確保係申請人本人所操作，故自然人憑證之重要性可想而知，使用者應妥善保管其自然人憑證、PIN 碼（卡片密碼）與用戶代碼[7]，以降低身分被冒用與資料外洩之可能性。

【相關標準】

ISO 27001：2013（CNS 27001）

- A.14.1.3　保護應用服務交易

---

[5] 電子簽章法第 4 條第 1 項：「經相對人同意者，得以電子文件為表示方法。」

[6] 電子簽章法第 9 條第 1 項：「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。」

[7] PIN 碼卡片密碼預設為持卡人民國出生**年**月**日共六碼，因此於使用前會請申請者先至內政部憑證管理中心專屬網站進行密碼變更，而用戶代碼則為使用者自設之 6~10 位代碼，可混合設定英文、數字或特殊符號，其用途為當 PIN 碼（卡片密碼）遭鎖卡時，可使用用戶代碼於專屬網站進行鎖卡解碼。亦可使用此用戶代碼於專屬網站進行卡片停（復）用。

(1)標準內容： 應保護應用服務交易中涉及之資訊，以防止不完整傳輸、誤選路(mis-routing)、未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。

(2)適用說明： 組織在使用公共網路上傳送的應用服務時，應確保資訊傳用時的安全性，避免未經授權者得介入修改，以符合其機密性、完整性以及可用性，且如發生未經授權者得介入之情形，亦會將資料來源辨識以及不可否認性一併推翻。

- A.9.4.2 保全登入程序

(1)標準內容： 當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。

(2)適用說明： 服務提供者應該選擇合適的鑑別技術，以證實使用者所宣稱的身分，以本案為例，即係使用自然人憑證作為嚴謹的鑑別及身分查證方式，藉此避免非授權者之存取。

類別：資訊應用【案號：A10830】

經濟部中小企業處修正融資服務平台介接電子資料使用管理規範

【焦點話題】

為鼓勵創業及支持中小企業不斷創新轉型發展，政府運用中小企業信用保證基金，以各項政策性貸款支持中小企業取得生命週期各階段發展所需資金，協助企業於競爭激烈的環境下永續發展。據此，經濟部中小企業處於 108 年 9 月 3 日修正「經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範」，配合財政部同意企業得採電子授權方式進行資料介接，增訂電子授權相關規定，使企業代表、負責人除臨櫃以書面或電子手寫裝置簽章外，同時可透過網際網路連線至介接資料使用單位之資訊系統，利用電子憑證授權。且為確保為有權限者的介接，因此增訂介接資料使用單位應確實審核企業、其負責人之身分與授權資訊，並對授權書之驗證結果及授權書之真實性負責等強化資通安全之控管規定。

【參考資料來源：中企財字第 10809003310 號令，108/9/3】

【重點摘要】

1. 為提升金融機構查詢效率及降低查詢成本，本次修正「經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範」時，新增企業得採電子授權方式，透過網際網路連線至介接資料使用單位之資訊系統，利用電子憑證授權，同意介接資料使用單位蒐集、處理及使用其相關資料。

2. 「財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務機關電子資料使用管理辦法」要求介接資料使用單位應訂定「信用資訊查詢作業控管要點」其內容至少應包括介接資料使用單位營業單位主管之職責、受指定查詢人員應注意事項、查詢作業之內部管理與控制、查詢資格要件、信用資訊之利用及保密、及介接資料使用單位內部對資訊使用及保密相關作

業應定期查核，並將查核報告副本送聯徵中心。

【法律觀點】

鑑於我國中小企業的特性，常受限於營運周轉金不足而無力爭取辦理更多或更高金額之業務，為協助業者能更順利取得所需融資，以利擴大業務，進一步帶動我國中小企業蓬勃發展及轉型，因此為協助中小企業順利取得銀行融資，經濟部中小企業處與銀行公會及財團法人金融聯合徵信中心（下稱聯徵中心）共同建置中小企業融資服務平台，由聯徵中心作為查調介接管道，提供更透明之企業營運資訊予銀行作為貸款評估之參考，以提升銀行對中小企業放款之意願。

當進行融資授信時，因涉及查調企業、其負責人相關介接資料，因此必須分別取得企業及其負責人之授權，及蒐集個人資料告知事項暨個人資料提供同意書[1]，授權包括金融機構等介接資料使用單位[2]透過中小企業處及聯徵中心[3]，向提供介接資料之公務及非公務機關（以下簡稱介接機關）發查資料，而所得查詢的介接資料包括稅務、公司登記、工廠登記等，及其他同意中小企業處介接資料之公務機關及非公務機關所提供之資料[4]。而介接機關於接受發查後，將查詢結果轉由中小

[1] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 3 點第 1 項：「介接資料使用單位為融資授信目的，查調企業、其負責人相關介接資料時，應分別取得企業、其負責人之書面授權或電子授權，及蒐集個人資料告知事項暨個人資料提供同意書（企業授權書如附件 A、企業負責人授權書如附件 B、蒐集個人資料告知事項暨個人資料提供同意書如附件 C；其流程如附件 D - 企業、其負責人授權書審核流程圖）。」

[2] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 2 點第 2 項第 1 款：「介接資料使用單位為經本處授權之聯徵中心會員金融機構、及財團法人中小企業信用保證基金，及其他經介接機關同意使用介接資料之介接資料使用單位。」

[3] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 2 點第 1 項第 1 款：「本處及本處授權之財團法人金融聯合徵信中心（以下簡稱聯徵中心）為介接資料管理單位，經提供介接資料之公務及非公務機關（以下簡稱介接機關）同意，本處得授權介接資料使用單位使用介接資料，其介接資料使用單位名單應副知聯徵中心及介接機關備查。」

[4] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 4 點第 3 項：「中小企業融資服務平台提供之介接資料如下：1、 依財政部財政資訊中心九十八年二月二十七日台財稅字第〇九八〇四〇〇一六一〇號函核定之各項經加值運算之財務比率五十項及比對發票驗證結果，及一百零六年十二

企業處與聯徵中心交給介接資料使用單位。

而為提升金融機構查詢效率及降低查詢成本，中小企業處於本次修正規範時，新增企業得採電子授權方式，意即除原本需由企業代表、負責人填寫書面授權書，同意介接資料使用單位蒐集、處理及使用其相關資料外[5]，亦可透過網際網路連線至介接資料使用單位之資訊系統，利用電子憑證授權，同意介接資料使用單位蒐集、處理及使用其相關資料，惟介接資料使用單位應確保該授權資訊不被竄改，及具備不可否認性，且其授權資訊可完整呈現並於日後取出查驗，並應對授權書之驗證結果及授權書之真實性負責[6]。

因涉及多項重要資料，故該使用管理規範亦針對介接資料之使用及系統介接方式、介接資料使用單位資料使用者之管理、介接資料之保密、保護義務[7]以及介

月七日資國字第一〇六〇〇〇三六三七號函核定之查調項目。 2、經濟部商業司核定之公司登記相關資料。 3、經濟部工業局核定之工廠登記相關資料。 4、台灣電力股份有限公司提供之企業用電及欠費等相關資料。 5、台灣自來水股份有限公司、臺北自來水事業處提供之企業用水及欠費等相關資料。 6、勞動部勞工保險局核定之投保人數及欠費等相關資料。 7、其他同意本處介接資料之公務機關及非公務機關所提供之資料。」

[5] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 3 點第 2 項：「1.書面授權分為以下兩種： (1)企業代表、負責人填寫書面授權書，同意介接資料使用單位蒐集、處理及使用其相關資料。(2)企業代表、負責人臨櫃申請融資時，介接資料使用單位得提供授權書電子檔，由企業代表、負責人於電子手寫裝置簽章，取得企業、其負責人之授權，同意介接資料使用單位蒐集、處理及使用其相關資料。 2.介接資料使用單位應確實審核企業、負責人之身分，及其授權資訊，並於取得企業、負責人之書面授權後，始可將授權書傳真，或將授權書電子檔傳送至聯徵中心備查。 3.介接資料使用單位應對授權書之驗證結果及授權書之真實性負責。」

[6] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 3 點第 3 項：「電子授權 1.電子授權係指企業代表、負責人透過網際網路連線至介接資料使用單位之資訊系統，並於該系統內之資料使用授權書頁面，利用電子憑證授權，同意介接資料使用單位蒐集、處理及使用其相關資料。 2.介接資料使用單位應確實審核企業、其負責人之身分與授權資訊，並於取得企業、其負責人之電子授權後，始可將授權資訊透過金融機構資訊系統傳送至聯徵中心備查。 3.介接資料使用單位應確保該授權資訊不被竄改，及具備不可否認性，且其授權資訊可完整呈現並於日後取出查驗，並應對授權書之驗證結果及授權書之真實性負責。」

[7] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 6 點：「六、介接資料之保密、保護義務 (一) 本處應遵循「資通安全管理法」等相關規定辦理。 (二) 聯徵中心應遵循「銀行間徵信資料處理交換服務事業許可及管理辦法」及本使用管理規範等相關規定辦理。 (三) 介接資料使用單位，介接公務及非公務機關電子資料，除應遵守法定資訊安全作業規範、各介接機關訂定之系統安全及作業管制

接資料之查核[8]，作出規範要求。

【管理 Tips】

介接資料因涉及資料傳遞，因此對於資料傳遞時其保密、保護義務是所有經手單位所必須共同承擔的，而這也是一般組織於進行資料介接或傳遞時，所應注意之事項。不過介接資料最終使用者係為介接資料使用單位，其除應遵守法定資訊安全作業規範、各介接機關訂定之系統安全及作業管制等資通安全管理規範外，並應遵循「財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務機關電子資料使用管理辦法」。

該使用管理辦法針對介接資料使用單位及其資料使用者之管理提出一定要求，首先，蒐集介接資料時，必須要有企業及其負責人之授權與個資提供同意書[9]，

等資通安全管理規範外，並應遵循「財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務機關電子資料使用管理辦法」等相關規範辦理。 (四) 資料使用者對列印之紙本資料應負保管之責，妥善存放，確保資料不外流，並於使用完畢後，立即銷毀。 (五) 介接資料使用單位應確實保存企業、其負責人之書面或電子授權相關資料、檔案及紀錄，保存期限應至少至貸款期間終止後五年，其介接資料使用單位有更長之保存期限規定者，從其規定。 (六) 介接資料使用單位若發現介接資料外洩、遭竊、遭竄改或遺失等情事，應立即向本處通報。經本處查證屬實者，即通報該介接資料所屬介接機關。 (七) 介接資料使用單位及資料使用者對介接資料之使用，如違反個人資料保護法及稅捐稽徵法規定，致當事人權益受損害者，應負損害賠償責任（個人資料保護法第二十八、二十九條及稅捐稽徵法第三十三條規定）。另涉及刑事責任者，依稅捐稽徵法及個人資料保護法之相關規定，移送司法機關辦理。」

[8] 經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 7 點：「七、介接資料之查核 (一) 本處應對介接資料使用單位之行為與活動加以記錄、監控及稽核，包括使用者查詢件數、啟動發查時間、文件何時列印、資料傳檔時間等資安紀錄（log）。 (二) 本處產製查詢之資安紀錄（log）報表，定期與各介接機關交叉比對查詢筆數是否相符，並每月至介接資料使用單位查核登載之查調筆數及內容是否與資安紀錄（log）報表相符。(三) 介接機關得不定期至本處調閱相關資料進行抽查，另本處及介接機關得不定期派員至介接資料使用單位調閱相關資料進行抽查，介接資料使用單位不得拒絕。 (四) 聯徵中心應定期將介接資料使用單位之各項查核結果彙整提供本處。 (五) 介接資料使用單位如有違法或未依本規範進行查調之情事，本處將立即終止該資料使用單位使用本平台之一切權利，倘有侵害第三人權利，使第三人受有損失時，介接資料使用單位應自負相關法律責任及賠償第三人所蒙受之損失。」

[9] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 3 點第 1 項：「三、 介接資料之蒐集（一）企業透過介接資料使用單位申請融資，查調企業、其負責人相關介接資料時，應分別取得企業、其負責人之書面授權或電子授權，及個人資料提供同意書，同意本中心、中企處及經中企處授權之介接資料使用單位蒐集、處理及使用其相關資料(企業授權書如附件 A、企業負責人授權書如附件 B、蒐集個人資料告知事項暨個人資料提供同意書如附件 C)，並應清楚告知企業、其負責

而使用介接資料時，僅得以融資目的所需之徵審查調為限，查詢所查得之所有資訊應嚴限內部參考，不得對外公開或移轉他人[10]，且限制以晶片卡連線、加密檔案傳輸方式查詢信用資訊[11]。而針對資料使用者之管理，則必須經由介接資料使用單位主管，指定專人負責辦理，嚴禁未經指定者查詢[12]，且使用者之帳號密碼為聯徵中心以密件提供，晶片卡與查詢密碼應分別指定不同人員保管。查詢人員異動或業務需要時，應向聯徵中心申請更換查詢密碼[13]。且為防止查詢資訊洩漏或受不當利用，確保資訊查詢作業安全，介接資料使用單位應訂定「信用資訊查詢作業控管要點」送聯徵中心，內容至少應包括 1、介接資料使用單位營業單位主管之職責；2、受指定查詢人員應注意事項；3、查詢作業之內部管理與控制；4、查詢資格要件； 5、信用資訊之利用及保密；及 6、介接資料使用單位內部對資訊使用及保密相關作業應定期查核，並將查核報告副本送聯徵中心[14]。

人授權書之內容以及個人資料保護法、消費者保護法及金融管理相關法令規定之應告知事項。」

[10] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 4 點第 1 項：「四、 介接資料之使用 （一）介接資料使用單位需徵得個別企業、負責人之授權書後，始得使用介接資料，並以融資目的所需之徵審查調為限，查詢所查得之所有資訊應嚴限內部參考，不得對外公開或移轉他人。」

[11] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 4 點第 2 項：「(二）介接資料使用單位資訊查詢方式如下： 1. 本中心受理介接資料使用單位申請以晶片卡連線、加密檔案傳輸方式查詢信用資訊，並得依協商規格辦理批次查詢。...」

[12] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 5 點第 1 項第 1 款：「五、 資料使用者之管理 （一）資料使用者之指定與登記 1. 使用本中心信用資訊之介接資料使用單位主管，應指定專人負責辦理查詢，未經指定者，應嚴禁擅自進行查詢。...」

[13] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 5 點第 2 項第 1 款：「(二）使用者帳號密碼 1. 晶片卡查詢密碼，由本中心以密件掛號寄交查詢單位主管親收，再密交查詢人員使用，晶片卡與查詢密碼應分別指定不同人員保管。查詢人員異動或業務需要時，應向本中心申請更換查詢密碼。...」

[14] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 7 點第 1 項：「七、 安全控管、查核與稽核 （一）安全控管 為防止查詢本中心所得資訊洩漏或受不當利用，確保資訊查詢作業安全，介接資料使用單位應訂定「信用資訊查詢作業控管要點」送本中心，修正時亦同。 前項要點之規範內容至少應包括下列事項：介接資料使用單位營業單位主管之職責。 受指定查詢人員應注意事項。 ˙查詢作業之內部管理與控制。 ˙查詢資格要件。 ˙信用資訊之利用及保密。˙介接資料使用單位內部對資訊使用及保密相關作業應定期查核，並將查核報告副本送本中心。」

另，介接資料使用單位必須定期進行內部稽核，並得由提供介接資料之公務及非公務機關，以及聯徵中心、中企處及提供介接資料不定期派員至介接資料使用單位進行抽查[15]，透過稽核確保介接資料使用單位係以符合相關規範使用資料。

據上可知，當組織將資料提供予外部單位進行使用時，為避免外部單位之故意或過失造成資料毀損、滅失甚至外洩之情形，組織可採取的作為，從資料出去到最後之確認可包括，確保資料使用者之身分、限制資料使用目的、限制資料傳輸方式、資料使用單位應訂定符合組織要求的控管要點、要求資料使用單位定期進行內部稽核，並配合組織進行外部稽核。

【相關標準】

ISO27001：2013（CNS27001）

- A.9.2.2　使用者存取權限之配置

  (1) 標準內容：　應實作正式之使用者存取權限配置程序，以對所有形式之使用者對所有系統及服務，指派或撤銷存取權限。

  (2) 適用說明：　使用者必須取得資訊系統或服務擁有者之授權，以使用資訊系統或服務。以本案而言，必須經由介接資料使用單位主管，指定專人負責辦理，透過授權方得進行資訊系統或服務的使用。

- 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

[15] 財團法人金融聯合徵信中心及其會員透過中小企業融資服務平台介接公務及非公務機關電子資料使用管理辦法第 7 點第 2、3 項：「(二) 查核與稽核 1.　介接資料使用單位 (1) 內部自行查核：... 2.　介接資料管理單位...。(三) 提供介接資料之公務及非公務機關得不定期派員至本中心調閱相關資料進行抽查，另本中心、中企處及提供介接資料之公務及非公務機關得不定期派員至介接資料使用單位調閱相關資料進行抽查...。」

性。

(2) 適用說明： 管理人員必須以其組織所受到的規範，包括外部要求以及內部所訂定之規範，為有效率的進行定期審查，且如發現任何未遵循事項，並應識別原因，評估是否需採取遵循措施，並再次審查其有效性。以本案為例，介接資料使用單位即必須依循規定進行內部稽核，並配合外部稽核，以達有意義的定期與不定期審查。

伍、自我評量

是非題

1. (O) 依照一般資料保護規則(GDPR)規定，無論企業是否設立於歐盟境內，只要該企業係有處理歐盟地區人民之個人資料，即適用 GDPR。**【資訊保護 S10801】**

   解析：依照一般資料保護規範第 3 條第 1 點規範：「本規則適用於控管者或處理者在歐盟境內之分支機構所為之個人資料處理活動，不問該處理是否發生於歐盟境內。」是以，控管者或處理者在歐盟境內之所為之個人資料處理活動，即適用 GDPR。

2. (O) 在我國，積體電路電路布局保護法明定受保護之電路布局權應具創作人之智慧努力而非抄襲之設計且非屬平凡、普通或習知者，是以電路布局權應具備原創性及非普遍性之要件。**【資訊保護 S10802】**

   解析：依照積體電路電路布局保護法第 16 條第 1 項規定：「本法保護之電路布局權，應具備左列各款要件：一、由於創作人之智慧努力而非抄襲之設計。二、在創作時就積體電路產業及電路布局設計者而言非屬平凡、普通或習知者。」故答案為正確。

3. (X) 在我國，如有人民透過社群平台散佈不實資訊，導致人民對真實訊息及國家產生不信任感，我國行政院長有權要求社群平台刪除不實資訊。**【資訊保護 S10803】**

   解析：我國目前為防杜散播假訊息造成危害，現有法規僅以社會秩序維護法第 63 條第 1 項第 5 款規定：「有左列各款行為之一者，處三日以下拘留或新臺幣三萬元以下罰鍰：一、無正當理由攜帶具有殺傷力之器械、化學製劑或其他危險物品者。二、無正當理由鳴槍者。三、無正當理由，攜帶用於開啟或破壞門、窗、鎖或其他安全設備之工具者。四、放置、投擲或發射有殺傷力之物品而有危害他人身體或財物之虞者。五、散佈謠言，足以影響公共之安寧者。六、蒙面偽裝或以其他方法驚嚇他人有危害安全之虞者。七、關於製造、運輸、販賣、貯存易燃、易爆或其他危險物品之營業，未經主管機關許可；或其營業設備及方法，違反法令規定者。八、製造、運輸、販賣、攜帶或公然陳列經主管機關公告查禁之器械者。」是以，如民眾透過社群平台散佈不實資訊，我國行政院長不得要求社群平台刪除，故答案為錯誤。

4. (O) 阿南入侵花花家的居家監視器並窺視其生活情形，甚利用監視器雙向通話功能發出怪聲音致花花心生畏懼，阿南之行為恐遭處三年以下有期徒刑、拘役或三十萬元以下罰金。**【資訊保護 S10804】**

   解析：阿南之行為依照刑法第 358 條規定：「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。」、同法第 315-1 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。」是以，答案為正確。

5. (O) 依照一般資料保護規則(GDPR)規定，當個人資料侵害事故發生時，控管者應向監管機關進行個人資料侵害之通報，且不得無故遲延。**【資訊保護 S10805】**

解析：依照一般資料保護規範第 33 條第 1 點規範：「於個人資料侵害發生時，控管者即應依第 55 條向監管機關通報，不得無故遲延，且如可能，應於發現後 72 小時內通報，但個人資料侵害無造成對當事人權利及自由之風險時，不在此限。於未於 72 小時內向監管機關通報之情形，通報應附遲延之理由。」是以，個人資料侵害發生時，控管者應向監管機關通報，不得無故遲延，且如可能，應於發現後 72 小時內通報，但個人資料侵害無造成對當事人權利及自由之風險時，不在此限，故答案為正確。

6. (X) 依照我國法規，公務機關及特定非公務機關發生三級以下資通安全事件，不需向主管機關進行通報。**【資訊保護 S10806】**

解析：依照資通安全管理法第 14 條第 2 項規定：「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。」及同法第 18 條第 2 項規定：「特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。。」是以，只要發生資通安全事件，公務機關皆須進行通報，故答案為錯誤。

7. (O) 在我國，涉犯洩漏並交付國家機密予外國、大陸地區、香港、澳門等，皆應加重其刑責。**【資訊保護 S10807】**

解析：依照國家機密保護法第 32 條第 1 項規定：「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。」及同條第 2 項：「洩漏或交付前項之國家機密於外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人者，處三年以上十年以下有期徒刑。」綜上而言，如交付國家機密於外國、大陸地區、香港、澳門等，應加重其刑責，故答案為正確。

8. (O) 分散式阻斷服務攻擊係指駭客透過被攻陷的電腦作為傀儡機傳送偽造包，向目標發動擊，致使預定目標癱瘓。**【資訊保護 S10808】**

解析：阻斷服務攻擊（英語：Denial-of-Service Attack，簡稱 DoS 攻擊）亦稱洪水攻擊，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」，向特定目標發動阻斷服務式攻擊時，稱為分散式阻斷服務攻擊（Distributed Denial-of-

Service Attack，簡稱 DDoS 攻擊)，故選項為正確。

9. (X) 陳檢察官向法院聲請通訊監察獲准，除可透過行動電話監聽中蒐集被告通訊對話，亦可透過於私人住宅內裝置竊聽器及錄影器材，以蒐集被告犯罪證據。**【資訊保護 S10809】**

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。」因此，本題不得以裝置私人住宅竊聽器及錄影器材，取得犯罪證據，故答案為錯誤。

10. (O) 在我國，如有涉及國家安全情報來源或管道之國家機密，應永久保密。**【資訊保護 S10810】**

解析：依照國家機密保護法第 12 條第 1 項規定：「涉及國家安全情報來源或管道之國家機密，應永久保密，不適用前條及檔案法第二十二條之規定。」故答案為正確。

11. (O) 保險代理人公司代理保險公司業務，其電話行銷人員對客戶進行行銷時未遵守告知事項，保險公司有權終止代理。**【資訊保護 S10811】**

解析：依照保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 6 點第 2 項規定：「保險業、保險代理人公司及保險經紀人公司之電話行銷人員進行電話行銷時，應先表明保險電話行銷之目的、確認要保人之身分，並將電話行銷人員之姓名、登錄字號、所屬公司名稱、服務電話以及保險契約重要內容完整告知要保人；另主管人員或稽核人員應定期就以上電話紀錄查核是否有違反本注意事項或其他法令之情形。」及第 14 點規定：「保險業與保險代理人公司之代理契約，除應約定保險代理人公司應依本注意事項規定辦理外，並應約定保險代理人公司如有違反本注意事項之情事，保險業得依情節輕重，對保險代理人公司予以限期改善、暫停代理或終止代理等處理。」故答案為正確。

12. (X) 國家安全法所稱之公務上應秘密之文書，僅得以明文規定為唯一標準，例如：國家機密保護法核定之國家機密或其他法律、法規命令等規定之應秘密事項等。**【資訊保護 S10812】**

解析：依照臺灣高等法院高雄分院 106 年度軍上訴字第 2 號判決載明：「國家安全法所稱公務秘密於立法時立法理由雖未為具體之說明，然由其立法旨趣為在「確保國家安全，維護社會安定」，參以政府資訊公開法之例外限制及禁止公開旨趣，應指對國家政務或事務上具有利害關係，且人民或相關法人無權要求政府提供之資訊而應保守之秘密始能維持國家政務或事務之推行者而言，非以有明文規定為唯一標準」，是以公務上應秘密之文書非

以有明文規定為唯一標準，故答案為錯誤。

13. (O)　在我國，不論申請使用電信資源之公眾電信網路者，或申請非使用電信資源之公眾電信網路者均應提出網路設置計畫，計畫內容應包括使用符合有關機關國家安全考量之電信設備、網路之資通安全偵測及防護規劃、使用符合主管機關公告之資通安全標準設備等。**【資訊保護 S10813】**

解析：依照電信管理法第 37 條第 1 項規定：「申請設置使用電信資源之公眾電信網路者應檢具申請書、營運計畫及網路設置計畫，向主管機關申請核准。經主管機關核准，始得營運及設置；其電信網路增設或變更者，亦同。」及同法第 38 條第 1 項規定：「申請設置未使用電信資源之公眾電信網路者，應檢具申請書及網路設置計畫，向主管機關申請核准。經主管機關核准，始得設置；其有增設或變更者，亦同。」故答案正確。

14. (O)　機關欲辦理資訊採購案，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」，得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。**【資訊保護 S10814】**

解析：依照行政院公共工程委員會工程企字第 10400024613 號函說明：「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」，為免發生國安或資安疑慮，請依「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 款規定，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」，故答案為正確。

15. (X)　當民眾向主管機關登記為徵信業者後，因已經主管機關登記同意，得利用錄音、錄影等手法取得被徵信者之私人資料，故其所作之任意監察行為將無違法之虞。**【資訊保護 S10815】**

解析：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。」因此只要是違法對他人通訊為監察，即已觸犯該法，並無所謂登記同意後即可為任意監察行為，故答案為錯誤。

16. (X)　小花向美好官方網站購買大包裝超值面膜 360 片裝組，後發現來不及於效期前使用完畢，遂於電子商務平台轉賣販售，且為求版面精美、內容詳盡，故於官網轉載商品圖片使用，然因小花係於正式通路購買取得商品，因此於官網取得圖片並使用之行為當屬合法。**【資訊保護 S10816】**

解析：依照著作權法第 91 條規定：「擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。」次按，著作權法第 3 條

第 1 項第 5 款：「重製：指以印刷、複印、錄音、錄影、攝影、筆錄或其他方法直接、間接、永久或暫時之重複製作。於劇本、音樂著作或其他類似著作演出或播送時予以錄音或錄影；依建築設計圖或建築模型建造建築物者，亦屬之。」因此，即便於正式通路購買商品，亦無取得官方圖片之合法授權，故不得以此利用轉載官方圖片，答案為錯誤。

17. (X) 小康曾有涉犯少年強制性交前科，如今服刑期滿改過自新，希望能發揮自身所常故設立英文課補班，依照我國目前法規，小康僅需要提交一份企劃書予法務部審核通過即可營業。**【資訊公開 D10817】**

解析：依照兒童及少年福利與權益保障法第 81-1 條第 1 項規定：「有下列情事之一者，不得擔任兒童課後照顧服務班及中心之負責人或工作人員：一、曾犯性侵害犯罪防治法第二條第一項之罪、性騷擾防治法第二十五條之罪、兒童及少年性交易防制條例之罪、兒童及少年性剝削防制條例之罪，經緩起訴處分或有罪判決確定。但未滿十八歲之人，犯刑法第二百二十七條之罪者，不在此限。二、有性侵害行為，或有情節重大之性騷擾、性霸凌、第四十九條第一項各款所定行為之一，經教育主管機關查證屬實。三、有非屬情節重大之性騷擾、性霸凌、第四十九條第一項各款所定行為之一，教育主管機關認定有必要予以解聘或解僱，並審酌案件情節，認定一年至四年不得聘用或僱用。四、有客觀事實認有傷害兒童少年之虞，經教育主管機關認定不能執行職務。」綜上而言，小康係有少年強制性交前科，不得擔任兒童課後照顧服務班之負責人或工作人，故答案為錯誤。

18. (O) 我國政府開放資料作業格式應符合：可直接取得、易於處理、意於理解、資料品質之正確性及完整性及利於資料間串聯運用等五大要件。**【資訊公開 D10818】**

解析：依照行政院及所屬各級機關政府資料開放作業原則第 11 條規定：「各機關提供之開放格式資料，應符合下列規定：(一)可直接取得：無需人為操作即可透過連結直接獲取資料。(二)易於處理：優先提供結構化資料。(三)易於理解：應於詮釋資料描述其欄位說明及編碼意義等。(四)確保資料品質：不得任意分割，以確保其完整性，並力求資料之正確性及時效性。(五)利於資料間串聯運用：提供之資料欄位格式定義應與政府資料標準相符。」

19. (O) 我國機關辦理委託專業服務、技術服務、資訊服務或社會福利服務等限制性招標採購案，應就各採購案成立採購評選委員會，且原則上應於完成評選事項後解散。**【資訊公開 D10819】**

解析：依照採購評選委員會組織準則第 2 條規定：「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。」及同法第 3 條第 1 項規定：「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。」故答案為正確。

20. (X) 稅捐稽徵人員對於納稅義務人之財產、所得、營業、納稅等資料，負有絕對保密義務，故不得以任何理由揭露或公告納稅義務人之欠稅情形。**【資訊公開 D10820】**

解析：依照稅捐稽徵法第 33 條第 1 項：「稅捐稽徵人員對於納稅義務人之財產、所得、營業、納稅等資料，除對下列人員及機關外，應絕對保守秘密：一、納稅義務人本人或其繼承人。二、納稅義務人授權代理人或辯護人。三、稅捐稽徵機關。四、監察機關。五、受理有關稅務訴願、訴訟機關。六、依法從事調查稅務案件之機關。七、經財政部核定之機關與人員。八、債權人已取得民事確定判決或其他執行名義者。次按同法第 34 條第 1 項：「財政部或經其指定之稅捐稽徵機關，對重大欠稅案件或重大逃漏稅捐案件經確定後，得公告其欠稅人或逃漏稅捐人姓名或名稱與內容，不受前條第一項限制。」是以，稅捐稽徵人員針對納稅義務人之稅務相關資料應負絕對保密義務，惟重大欠稅案件或重大逃漏稅捐案件經確定者得公告之，故答案為錯誤。

21. (O) 如發生重大職業災害時，主管機關得將事業單位名稱、發生重大職業災害之地址、日期、罹災人數、災害類型及業主名稱等公開。**【資訊公開 D10821】**

解析：依照勞動部公布重大職業災害案件作業要點第 4 點規定：「本部建置重大職業災害資料庫網頁，提供民眾查詢、瀏覽，並公布重大職業災害資訊（如附表）：（一）事業單位名稱。但承攬人、再承攬人名稱不予公布。（二）發生重大職業災害之地址。但屬道路、河川、隧道、管道、山坡地或景觀等工程，得不予公布地址。（三）發生重大職業災害之日期。（四）罹災人數。（五）災害類型。（六）原事業單位行業別（無原事業單位時，以承攬工作獨立施作而未轉包或分包之事業單位行業別載述）。（七）轄區勞動檢查機構名稱。營繕工程除揭露前項第一款至第七款之資訊外，並得公布下列資訊：（一）發生重大職業災害之工程名稱。（二）發生重大職業災害之場所。（三）發生重大職業災害之業主名稱。」綜上所述，答案為正確。

22. (X) 大富發賣場為確保收銀員工作效率，於賣場內裝設監視器並利用收銀檯錄音系統確保同仁符合公司規定作業流程，惟錄音裝置於監管同仁之時，亦一併收錄顧客之對話內容，此有違反通訊保障及監察法之規定。**【資訊監察 M10822】**

解析：根據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。」又根據同條第 2 項規定：「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。」是以，賣場是多數人或是不特定人於有可能看見或聽見之環境，且客觀上並無活動隱密性之可能，並無違反通訊保障及監察法之規定，故本題答案為非。

23. (O)　舊金山通過禁止秘密監控條例，當地政府部門皆不得使用任何臉部辨識技術或因該技術而取得之資訊。**【資訊監察 M10823】**

解析：依照《停止秘密監視條例》第 19B.2(d)條要求原則上禁止政府機關取得、保存或使用任何臉部辨識技術，同時亦限制該技術衍生數據之使用，甚至代表政府進行民事、行政訴訟之律師，亦不得使用臉部辨識技術及技術衍生數據，故選項為正確。

24. (X)　在我國，手機通訊軟體業者有配合協助執行通訊監察之義務。**【資訊監察 M10824】**

解析：依照通訊保障及監察法第 14 條第 2 項規定：「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。」且依照中華民國行業標準分類，手機通訊軟體業者係為資訊服務業，故選項為錯誤。

25. (O)　我國檢察官偵辦最重本刑三年以上有期徒刑之罪，如有事實足認通信紀錄及使用者資料於本案有必要關連性時，得向法院聲請核發調取票。**【資訊監察 M10825】**

解析：依照通訊監察及保障法第 11-1 條：「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。

26. (O)　隨著電子支付機構業務管理規則修正通過，未來我國民眾至超商繳納水電費等款項，除使用現金、電子票證、信用卡支付，亦可以使用街口 App、Line Pay、一卡通。**【資訊應用 A10826】**

解析：依照電子支付機構業務管理規則第 10 條第 2 項規定：「收款使用者應為代理收付實質交易款項之最終收款方。但收款使用者為金融機構、便利商店業及超級市場業，並有下列情形之一者，不在此限：一、受各級政府委託代徵收之規費、稅捐與罰鍰。二、受公用事業委託代收之服務費。三、受大眾運輸事業委託代收之票價及其他相關服務費用。四、其他經主管機關核定之款項。」承上所述，水電費係屬公用事業委託代收之服務費，故選項為正確。

27. (O)　在我國，凡達公民年齡之國民，不分貧富、地域、宗教、黨派、性別、種族等皆有投票權。**【資訊應用 A10827】**

解析：依照憲法第 129 條規定：「本憲法所規定之各種選舉，除本憲法別有規定外，以普通、平等、直接及無記名投票之方法行之」，而普通原則係指基於國民主權原理，謂具有國籍之人民，均應享有選舉權，不得以階級、宗教、財產等因素限制人民選舉權。

28. (X) 我國為扶植新創金融科技產業，於 107 年初建立金融監理沙盒機制，開放業者從事金融業務實驗，而業者於實驗期間即可排除所有法令之限制。**【資訊應用 A10828】**

解析：依照金融科技發展與創新實驗條例第 25 條第 1 項：「創新實驗範圍涉及主管機關或其他機關（構）訂定之法規命令或行政規則者，主管機關基於創新實驗進行之必要，得於會商其他機關（構）同意後，核准創新實驗於實驗期間排除該等法規命令或行政規則全部或一部之適用，並免除申請人相關行政責任。但洗錢防制法、資恐防制法及相關法規命令或行政規則不得排除。」是以，業者雖於實驗期間原則上應排除法規命令或行政規則全部或一部之適用，但關於洗錢防制法、資恐防治法等法規，並不得排除，故答案為錯誤。

29. (O) 我國內政部戶政司建置戶政網路登記作業系統，以推動戶籍申辦服務作業流程化及便利化，目前已開放民眾利用線上申辦戶籍登記作業完成離婚登記、死亡登記、出生地登記等項目。**【資訊應用 A10829】**

解析：依照內政部台內戶字第 1071202244 號函釋表示：「一、下列戶籍登記項目，得於事件發生或確定後 30 日內，以自然人憑證於網路申請登記：(一)雙方在國內現有或曾設戶籍者，經我國法院調解、和解離婚成立或裁判離婚確定之離婚登記：以當事人之一方為申請人。(二)在國內死亡，死亡者非為戶長之死亡登記：以死亡者之親屬、配偶或同戶之人為申請人。(三)經我國法院為死亡宣告，受死亡宣告者非為戶長之死亡宣告登記：以聲請死亡宣告者為申請人。(四)在國內現有戶籍者，出生地為空白之出生地登記：以本人為申請人。二、本公告另刊載於本部戶政司全球資訊網（https://www.ris.gov.tw）。」故答案為正確。

30. (X) 關於經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範之介接資料授權方式，僅得使用書面授權，以確保企業及其負責人同意。**【資訊應用 A10830】**

解析：依照經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 3 條第 2 項規定：「(二)書面授權 1.書面授權分為以下兩種：(1)企業代表、負責人填寫書面授權書，同意介接資料使用單位蒐集、處理及使用其相關資料。(2)企業代表、負責人臨櫃申請融資時，介接資料使用單位得提供授權書電子檔，由企業代表、負責人於電子手寫裝置簽章，取得企業、其負責人之授權，同意介接資料使用單位蒐集、處理及使用其相關資料。2.介接資料使用單位應確實審核企業、負責人之身分，及其授權資訊，並

於取得企業、負責人之書面授權後，始可將授權書傳真，或將授權書電子檔傳送至聯徵中心備查。3.介接資料使用單位應對授權書之驗證結果及授權書之真實性負責。」綜上所述，其授權方式分為書面授權及電子授權，故答案為錯誤。

選擇題

1. (3) 依照一般資料保護規則(GDPR)規定，下列何者不適用於 GDPR 之規範？(1)於歐盟地區設立據點的公司。(2)雇用歐盟地區人民。(3)歐盟地區的中國籍旅客。(4)提供服務給歐盟地區人民。**【資訊保護 S10801】**

   解析：依照 General Data Protection Regulation, Art.3：「1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.。2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3.This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.」綜上所述，GDPR 所保護之對象為歐盟境內的資料主體，其中包含 1.基於提供商品或服務所需，針對歐盟境內之資料主體進行個資處理行為；2.基於「監控」歐盟境內自然人行為所需，對資料主體進行個資處理行為；3.資料控管者雖非設立於歐盟境內，但所設立之處依據國際公法適用歐盟會員國法律，是以選項(1)(2)(4)皆為正確，選項(3)為錯誤。

2. (3) 我國積體電路電路布局保護法所保障之電路布局權，應符合下列何者選項?(1)由公司出資進行研究。(2)具有營利價值。(3)於創作人之智慧努力而非抄襲之設計。(4)具有公開性。**【資訊保護 S10802】**

   解析：依照積體電路電路布局保護法第 16 條規定：「本法保護之電路布局權，應具備左列各款要件：一、由於創作人之智慧努力而非抄襲之設計。二、在創作時就積體電路產業及電路布局設計者而言非屬平凡、普通或習知者。」是以，依上開規定選項(3)為正確。

3. (2) 假消息日益猖獗，網際網成為傳播不實資訊的最新手段，我國行政院針對假新聞提出的建議定義，請問下列何者為非？(1)出於惡意。(2)使用網路。(3)虛偽假造。(4)造成危害。**【資訊保護 S10803】**

   解析：行政院於 107 年 12 月表示立法院應針對假訊息議題提出相關法制的因應作為，並

同時提出「惡、假、害」的建議定義，亦即「出於惡意、虛偽假造、造成危害」，始有法律規範問責的必要性，而非毫無限制，故選項(2)為錯誤。

4. (1) 關於影像監控系統資安標準第一部：一般要求規範之安全構面定義，下列何者有誤?(1)數位安全。(2)系統安全。(3)實體安全。(4)隱私保護。**【資訊保護 S10804】**

解析：依關於影像監控系統資安標準第一部：一般要求 4.1.1 安全構面規定：「(a)**實體安全**：產品輕易被拆解與否，或產品資料存儲與測試用連接埠的處置，應視為實體安全要求的標的。(b)**系統安全**：產品之作業系統、網路服務、更新服務及韌體程式設計等，須具備足夠之安全防護。(c)**通訊安全**：敏感性資料之通訊安全，和通訊服務存在未知之資安漏洞與否。(d)**身分鑑別與授權機制安全**：溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，須確保鑑別與授權相關機制。(e)**隱私保護**：影像監控裝置之隱私，包括使用者之影像資料，於存取與傳輸的保護及權限管控等，確保隱私資料不應外洩。」故選項(1)為錯誤。

5. (3) 乖乖不動產經紀公司日前發生個資外洩事故，請問依照我國個人資料保護法之相關規定，下列何者有誤?(1)乖乖公司應通知當事人。(2)乖乖公司應通知當事人其採取之因應措施。(3)乖乖公司應通知行政院院長。(4)乖乖公司應提供諮詢服務專線。**【資訊保護 S10805】**

解析：依照個人資料保護法施行細則第 22 條第 2 項規定：「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」及不動產經紀業個人資料檔案安全維護管理辦法第 17 條地 2 項規定：「前項應變機制，應包括下列事項：一、採取適當之措施以控制事故對當事人造成損害。二、查明事故發生原因及損害狀況，並以適當方式通知當事人事故事實、因應措施及諮詢服務專線等。三、研議改進措施，避免類似事故再度發生。四、發生重大個人資料事故者，應即以書面通報直轄市、縣(市)主管機關。」綜上所言，選項(1)(2)(4)皆為正確，選項(3)為錯誤。

6. (4) 某直轄市政府官網遭不明資訊病毒入侵導致全面停擺，依照資通安全事件通報及應變辦法規定某直轄市政府應向主管機關進行通報，其通報內容應包含何者?(1)發生機關。(2)等級之評估。(3)狀況描述。(4)以上皆是。**【資訊保護 S10806】**

解析：依照資通安全事件通報及應變辦法第 3 條規定：「資通安全事件之通報內容，應包括下列項目：一、發生機關。二、發生或知悉時間。三、狀況之描述。四、等級之評估。五、因應事件所採取之措施。六、外部支援需求評估。七、其他相關事項。」故應選選項(4)。

7. (1) 社交工程主要係利用人性弱點，以簡單的溝通達到欺騙目的，請問下列何者選項得

有效防範攻擊並降低風險?(1)不開啟來路不明的電子郵件。(2)下載朋友推薦的非法軟體。(3)下載國外網站的影片。(4)下載非法網站的網路小遊戲。**【資訊保護 S10807】**

解析：社交工程(Social Engineering)係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。因此，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，即能避免社交工程的攻擊傷害。

8. (3) 請問下列何者並未觸犯我國妨害電腦使用罪章?(1)阿龍攻擊作業系統漏洞入侵小美的電腦執行勒索病毒。(2)阿強匿名散播電腦病毒致校園系統故障。(3)宏宏製作專供入侵電腦之工具程式，以作為網路診斷、監控或其他正當之用途。(4)小明利用網路遊戲外掛程式，使虛擬角色快速升等並強化道具裝備。**【資訊保護 S10808】**

解析：依照刑法第 360 條規定：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」故選項(1)(2)(4)選項為錯誤，再依刑法第 362 條規定：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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。」然因，選項(3)係為正當用途，而非致生損害於他人，故為正確。

9. (4) 請問下列何處裝設監視器，民眾可能具備合理隱私期待?(1)超商。(2)公園。(3)捷運站。(4)公寓大廈內的自家門口。**【資訊保護 S10809】**

解析：依照臺灣新北地方法院 105 年訴字第 144 號民事判決，我國法院認定公寓大廈該層樓電梯及走道等公共空間，可得特定出入人是為當層住戶及其訪客，應具備合理隱私期待，而選項(1)(2)(3)係為公共場合，故選項(4)應具備合理隱私期待。

10. (1) 依照我國國家機密保護法規定，請問下列何者人員出境應經由（原）服務機關或委託機關核准?(1)卸任未滿三年的前總統。(2)承包台北市政府公共工程之廠商負責人。(3)龜山鄉公所秘書。(4)中正區戶政事務所志工。**【資訊保護 S10810】**

解析：依照國家機密保護法第 26 條第 1 項規定：「下列人員出境，應經其（原）服務機關或委託機關首長或其授權之人核准：一、國家機密核定人員。二、辦理國家機密事項業務人員。三、前二款退離職或移交國家機密未滿三年之人員。」次按國家機密保護法第 7 條第 1 項第 1 款：「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。」故選項(1)總統則屬國家機密核定人員，故未離退職滿三年者，

出境應經機關准許。

11. (3)　依照保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項規定，上述所屬電話行銷人員向民眾行銷時，應進行說明告知，請問下列告知內容何者有誤?(1)表明保險電話行銷目的。(2)告知電話行銷人員姓名。(3)確認受益人身分。(4)告知民眾個人資料來源。**【資訊保護 S10811】**

解析：依照保險業保險代理人公司保險經紀人公司辦理電話行銷業務應注意事項第 6 點第 2 項規定：「保險業、保險代理人公司及保險經紀人公司之電話行銷人員進行電話行銷時，應先表明保險電話行銷之目的、確認要保人之身分，並將電話行銷人員之姓名、登錄字號、所屬公司名稱、服務電話以及保險契約重要內容完整告知要保人；另主管人員或稽核人員應定期就以上電話紀錄查核是否有違反本注意事項或其他法令之情形。」故選項(3)為錯誤。

12. (1)　我國人民如向外國、大陸地區、香港、澳門等境外敵對勢力洩漏下列何者選項，即涉犯違反國家安全罪責?(1)我國作戰計畫。(2)我國施政計畫。(3)我國預算及決算書。(4)我國合議制機關之會議紀錄。**【資訊保護 S10812】**

解析：依照國家安全法第 2-1 條規定：「人民不得為外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人為下列行為：一、發起、資助、主持、操縱、指揮或發展組織。二、洩漏、交付或傳遞關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄。三、刺探或收集關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄。」故屬選項(1)為答案，而選項(2)(3)(4)皆屬政府資訊公開法所規之政府應主動公開事項。

13. (4)　根據電信事業資通安全管理手冊規定，請問關於電信事業管理作業所包含內容，下列選項何者正確?(1)資通安全應變通報(2)資通安全管理標準。(3)資通安全等級評估。(4)以上皆是。**【資訊保護 S10813】**

解析：依照電信事業資通安全管理第 2 點規定：「基於保障資通安全 2 及維護使用者權益原則，確保通訊系統設備、資料及網路安全，本手冊包含下列要項：(一)資通安全管理標準。(二)資通安全等級評估。(三)資通安全管理機制。(四)資通安全認知訓練。(五)資通安全應變通報。(六)資通安全實施評鑑。(七)年度提報資料要求」故應選選項(4)。

14. (3)　我國機關辦理資訊服務採購時，為避免國安或資安疑慮，得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，請問下列何者非屬於陸資資訊服務業者?(1)大陸地區廠商。(2)第三地區含陸資成分廠商。(3)與大陸地區交易廠商。(4)在臺陸資廠商。**【資訊保護 S10814】**

解析：依照行政院公共工程委員會工程企字第 10100346580 號函說明：「…三、本會 101 年 4 月 18 日函說明三內容修正如下：依前揭規定，廠商非屬自然人者，則所稱陸資廠商，區分如下：(一)大陸地區廠商：指依大陸地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體。(二)第三地區含陸資成分廠商：非依兩岸之法律設立登記而含陸資之廠商，且符合大陸地區人民來臺投資許可辦法第 3 條第 2 項規定之陸資投資公司，即大陸地區人民、法人、團體、其他機構直接或間接持有該第三地區公司股份或出資總額逾百分之三十或對該第三地區公司具有控制能力。(三)在臺陸資廠商：依我國法律設立登記之公司或事業，且屬大陸地區人民來臺投資許可辦法第 5 條規定之陸資投資事業。」故選項(3)非屬陸資資訊服務業者。

15. (2) 個人隱私近年來普遍受國人重視，如欲以高科技電子產品紀錄他人隱私活動、言談或身體隱私部位等，請問下列何者行為恐有違反刑法妨害祕密罪之虞?(1)阿哲付費邀請小花擔任模特兒拍攝私密寫真集。(2)小光未經女友同意，於女友房間內裝設微型錄影機，紀錄女友在家的活動情形。(3)阿江攝影紀錄家族於熱炒店聚餐之時光。(4)花花參加偶像戶外簽唱會並錄影上傳至臉書分享。**【資訊保護 S10815】**

解析：依照刑法第 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。」(1)已經過小花同意，而(3)與(4)均為公開活動，是以，僅有選項(2)為私人隱私活動且未經允許，故有違法之虞。

16. (4) 請問下列何者恐有觸犯著作權法之疑慮?(1)小珊為一名服裝設計師，畢業後與友人共同創業，並自行設計品牌 Logo 供團隊使用。(2)阿光為一名作家，偶然看見阿Q於北歐攝影的極光圖非常喜歡，遂與阿Q購買其使用權，並印製於阿光的新書封面。(3)樂樂於付費圖庫購買素材加以設計完成，並利用於其賣場 Logo。(4)美美為一名知名部落客，為向其觀眾群介紹及推薦產品，發現小婷於臉書分享的使用前後比照圖片極具說服力，於是未經許可將小婷之照片轉貼至其部落格使用。**【資訊保護 S10816】**

解析：依照著作權法第 91 條第 1 項規定：「擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。　意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處六月以上五年以下有期徒刑，得併科新臺幣二十萬元以上二百萬元以下罰金。　以重製於光碟之方法犯前項之罪者，處六月以上五年以下有期徒刑，得併科新臺幣五十萬元以上五百萬元以下罰金。　著作僅供個人參考或合理使用者，不構成著作權侵害。」是以，僅有選項(4)未獲著作權人之合法授權，故其恐觸犯著作權法。

17. (3) 依照我國目前法規，安心托嬰中心欲招聘照護人員，面試者必須提供下列何者資料?(1)護照。(2)台胞證。(3)近三個月內核發之警察刑事紀錄證明書。(4)信用卡。**【資訊公開 D10817】**

解析：依照兒童及少年福利與權益保障法第 81 條第 6 項規定：「兒童及少年福利機構聘僱工作人員前，應檢具相關名冊、資格證明文件影本、切結書、健康檢查表影本、最近三個月內核發之警察刑事紀錄證明書及其他基本資料，報主管機關核准。主管機關應主動查證並得派員檢查；人員異動時，亦同。」故答案為選項(3)。

18. (2) 請問下列何者不是我國政府資訊公開法所規定之政府資訊?(1)台北市政府施政計畫。(2)國安局作戰計畫。(3)行政院主計總處公布 108 年度直轄市及縣(市)總預算彙編。(4)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。**【資訊公開 D10818】**

解析：依照政府資訊公開法第 7 條第 1 項規定：「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。」綜上所言，選項(1)(3)(4)皆為正確。而次按國家機密保護法施行細則第 2 條：「本法所定國家機密之範圍如下：一、軍事計畫、武器系統或軍事行動。二、外國政府之國防、政治或經濟資訊。三、情報組織及其活動。四、政府通信、資訊之保密技術、設備或設施。五、外交或大陸事務。六、科技或經濟事務。七、其他為確保國家安全或利益而有保密之必要者。」故選項(2)則屬國家機密，不得公開之，故為錯誤。

19. (4) 行政院公共工程委員會為協助各機關遴選採購評選委員，特建置專家學者建議名單資料庫，請問下列公開之資訊何者為錯誤?(1)評選委員姓名。(2)評選委員職業。(3)評選委員學經歷。(4)評選委員年齡。**【資訊公開 D10819】**

解析：依照採購評選委員會組織準則第 6 條第 1 項規定：「本委員會成立後，其委員名單應即公開於主管機關指定之資訊網站；委員名單有變更或補充者，亦同。但經機關衡酌個案特性及實際需要，有不予公開之必要者，不在此限。」而政府電子採購網原僅列出委員之姓名及職業，後於 108 年 7 月 1 日新增公開評選委員學經歷欄位，故選項(4)為錯誤。

20. (1) 我國重大欠稅案件或重大逃漏稅案件經確定者，主管機關得公布下列內容，請問何

者錯誤?(1)納稅義務人之姓名，遮蔽部分姓名。(2)稅目別。(3)欠稅年度。(4)納稅義務人之地址，省略門牌號。**【資訊公開 D10820】**

解析：依照財政部台財稅字第 09904504190 號函說明三公告：「三、本案應公告之內容如下：（一）納稅義務人姓名或名稱；納稅義務人為營利事業者，應一併公告其負責人姓名及地址。（二）稅目別。（三）欠稅年度。（四）欠稅或罰鍰金額【含滯納金、利息及滯（怠）報金】。（五）公告內容屬自然人地址者，其門牌號碼可予簡略，僅公告至街道或村里名稱。」故選項(1)為錯誤。

21. (1) 請問事業單位勞動場所發生下列何者情形，雇主不須於八個小時內通報勞動檢查機構?(1)發生受傷事件，且不須住院治療。(2)發生死亡災害。(3)發生災害的罹災人數在三人以上。(4)發生中央主管機關指定公告之災害。**【資訊公開 D10821】**

解析：依照職業安全衛生法第 37 條第 2 項：「事業單位勞動場所發生下列職業災害之一者，雇主應於八小時內通報勞動檢查機構：一、發生死亡災害。二、發生災害之罹災人數在三人以上。三、發生災害之罹災人數在一人以上，且需住院治療。四、其他經中央主管機關指定公告之災害。」故選項(1)為答案。

22. (4) 下列關於我國通訊保障及監察法所稱之「通訊」，請問何者有誤?(1)Line 的聲音信息。(2)小美的情書。(3)WhatsApp 對話紀錄。(4)德德的臉書公開貼文。**【資訊監察 M10822】**

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。」然而，臉書貼文則屬不特定或多數人可共見共聞之場合，係不符合前法第 3 條第 2 項規定：「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。」是以，選項(4)不符合上開規範，故為錯誤。

23. (4) 請問根據我國目前個人資料保護法相關規定，下列何者有誤?(1)個人資料之蒐集應於特定目的內為之。(2)特種個人資料原則上禁止蒐集。(3)蒐集個人資料時，應履行告知義務。(4)臉部特徵屬特種個資。**【資訊監察 M10823】**

解析：依照個人資料保護法第 6 條第 1 項本文規定：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」然而臉部特徵非屬特種個資，故選項(4)為錯誤。

24. (1) 請問下列何種情形得聲請核發通訊監察書?(1)阿光涉嫌向廠商收取公共工程案回扣，最輕處十年以上有期徒刑。(2)阿清無故輸入花花帳號密碼，並瀏覽其臉書，恐處三年以下有期徒刑、拘役或科或併科十萬元以下罰金(3)阿里涉犯偽造文書，恐處五年以下有期徒

刑。(4)小新變造車票並使用之，恐處以一年以下有期徒刑。**【資訊監察 M10824】**

解析：依照通訊保障及監察法第 5 條第 1 項規定：「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。……」是以，選項(1)即符合最輕本刑為三年以上有期徒刑之罪，故為正確。

25. (3) 我國檢察官偵查最重本刑三年以上有期徒刑之罪，可向法院書面聲請核發調取票，請問調取票所調取之內容屬於下列何者選項?(1)犯罪紀錄。(2)定位紀錄。(3)通信紀錄。(4)出生地記錄。**【資訊監察 M10825】**

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。」故選項(3)為正確。

26. (2) 我國於 108 年開放多項電子支付使用方式與範圍，請問下列何者為錯誤?(1)美牙可以到 7-11 便利商店利用電子支付繳納水電費。(2)小明支付停車場款項，但餘額不足時，電子支付機構得進行三次墊付。(3)HiPay 為電子支付機構，其可計畫發行電子支付帳戶專用儲值卡。(4)花倫為電子支付使用者，電子支付機構可利用簡訊通知其交易進行狀況。**【資訊應用 A10826】**

解析：依照電子支付機構業務管理規則第 15 條規定：「電子支付機構不得對使用者提供電子支付帳戶透支及放款等授信或信用額度，或於使用者支付指示之金額逾電子支付帳戶餘額時，為使用者代墊款項。但為單次墊款且使用於大眾運輸事業或停車場業，不在此限。」是以，選項(2)電子支付機構僅得進行單次墊付，故為錯誤。

27. (3) 區塊鏈應用為全球新興話題，請問下列關於區塊鏈之特點何者有誤?(1)去中心化；其技術毋需依賴第三方管理機構，沒有中心機制。(2)開放性；除被加密資料外，任何人皆可透過公開介面查詢。(3)族群性；區塊鏈系統依賴第三方，故所有節點於系統內驗證、交換數據，皆需經過人為干涉。(4)安全性；除非掌握區塊鏈中的 51%節點，否則無法修改其區塊鏈之數據或資料。**【資訊應用 A10827】**

解析：所謂區塊鏈（blockchain），係指藉由密碼學串接並保護內容的串連交易紀錄又稱區段，每一個區段包含前一個區段的加密雜湊、相應時間戳記以及交易資料，具有去中心化、開放性、獨立性及安全性等優點，又因具有可回溯性及不可竄改性之特性。因此，區塊鏈系統不依賴第三方，所有節點能在系統內自動安全的驗證、交換數據，不需要任何人

為的干預，故選項(3)為錯誤。

28. (3)　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之金融業務實驗，請問下列關於創新實驗之規範何者有誤?(1)申請創新實驗期限原則以一年為限，必要時申請得延長六個月。(2)全程實驗期間不得逾三年。(3)實驗期間排除金融相關法規之全部適用。(4)主管機關如認為創新實驗內容具創新性，能有效提升金融服務效率，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。**【資訊應用 A10828】**

解析：依照金融科技發展與創新實驗條例第 25 條規定：「創新實驗範圍涉及主管機關或其他機關（構）訂定之法規命令或行政規則者，主管機關基於創新實驗進行之必要，得於會商其他機關（構）同意後，核准創新實驗於實驗期間排除該等法規命令或行政規則全部或一部之適用，並免除申請人相關行政責任。但洗錢防制法、資恐防制法及相關法規命令或行政規則不得排除。」綜上所述，實驗期間應排除金融相關法令全部或一部適用，但不得排除洗錢防制法、資恐防制法及相關法規命令等，故選項(3)為錯誤。

29. (1)　請問下列何者選項不得利用戶政網路登記作業辦理，以達到程序便利化之目的?(1)死亡登記且死亡者非戶長。(2)法院裁判離婚。(3)兩願離婚。(4)出生地登記。**【資訊應用 A10829】**

解析：依照內政部台內戶字第 1071202244 號函釋表示：「一、下列戶籍登記項目，得於事件發生或確定後 30 日內，以自然人憑證於網路申請登記：(一)雙方在國內現有或曾設戶籍者，經我國法院調解、和解離婚成立或裁判離婚確定之離婚登記：以當事人之一方為申請人。(二)在國內死亡，死亡者非為戶長之死亡登記：以死亡者之親屬、配偶或同戶之人為申請人。(三)經我國法院為死亡宣告，受死亡宣告者非為戶長之死亡宣告登記：以聲請死亡宣告者為申請人。(四)在國內現有戶籍者，出生地為空白之出生地登記：以本人為申請人。二、本公告另刊載於本部戶政司全球資訊網（https://www.ris.gov.tw）。」故選項(3)為錯誤。

30. (4)　請問下列關於經濟部中小企業處修正融資服務平台介接電子資料使用管理規範何者有誤?(1)該規範係鑑於我國中小企業之特性，常受限於營運週轉金不足而無力爭取更多業務，而政府為協助業者能順利取得融資，以擴大企業，帶動我國經濟發展及轉型，故特訂定此規範。(2)介接資料使用單位為經本處授權之聯徵中心會員金融機構、及財團法人中小企業信用保證基金，及其他經介接機關同意使用介接資料之介接資料使用單位。(3)介接資料則包含稅務、公司登記、工廠登記等。(4)介接資料使用單位為融資授信目的，故查調企業、其負責人相關介接資料時，僅能依書面文件取得企業、及負責人之同意。**【資訊應**

用 A10830】

解析：依照經濟部中小企業處中小企業融資服務平台介接公務及非公務機關電子資料使用管理規範第 3 點第 1 項規定：「介接資料使用單位為融資授信目的，查調企業、其負責人相關介接資料時，應分別取得企業、其負責人之書面授權或電子授權，及蒐集個人資料告知事項暨個人資料提供同意書(企業授權書如附件 A、企業負責人授權書如附件 B、蒐集個人資料告知事項暨個人資料提供同意書如附件 C、其流程如附件 D、企業、其負責人授權書審核流程圖)。」綜上所述，執行查調作業時，應取得企業及負責人之書面授權或電子授權，故選項(4)為錯誤。