# 資通安全法律案例彙編

## 第 14 輯

行政院國家資通安全會報技術服務中心

中華民國 106 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。

# 目次

壹、資訊保護（Security）.....1

勒索病毒目的似乎不在贖金 Petya 比想像更複雜.....2

離職前以他人名義於系統複製客戶檔案，房仲業務員遭起訴.....5

智慧支付平臺遭爆恐洩個資　政府機關坦言有疏失.....10

哥哥個資全 PO 網 弟討債反挨罰 9 萬.....14

擔心個資外洩 第三類謄本更安全.....17

國家機密保護法擬修正，涉密人員退職後至少出境管制 3 年.....21

「數位通訊傳播法草案」針對煩人的商業電子訊息加以規範.....25

英商惡搞合約 2 萬人同意 1 千小時社區服務換免費 WIFI.....30

因應 APCN-2 海纜斷線，有關機關督促業者辦理頻寬調度並儘速排除障礙.....33

中繼站轉接、竄改來電號碼　半年騙上千萬.....38

波音誤洩 3.6 萬員工個資，自家 DLP 資料保護軟體未發揮效用.....41

美國政府下令禁用俄跨國公司卡巴斯基實驗室之軟體.....45

不滿遭攔查 警方：依法行使職權.....49

惡男密錄散布性愛影片 遭判刑 3 月.....53

證券商遭網路攻擊 金融主管機關要求加強資安防範.....56

中國網軍 轉攻擊我關鍵基礎設施.....60

整形診所洩密　數百女性豐胸裸照曝光.....63

Windows 10「默默蒐集」個資 遭怒控侵犯隱私.....67

App 浮濫蒐集個資 消保主管機關將進行整頓 ..... 72
旅行社個資外洩 民眾遭詐騙近 20 萬元 ..... 78
人為疏失 Verizon 六百萬客戶資訊被披露 ..... 81
盜拷布袋戲上網分享 檢察官透過谷歌抓到大學生 ..... 85
駭客入侵出國登錄系統 外交機關公開致歉 ..... 89
被炒抓狂 研發副處長刪光公司 5 千筆檔案 ..... 93
立委提案 患者有愛滋病須主動告知救護人員 ..... 96
採購案洩密 警政機關承辦人員判處 2 月有期徒刑 ..... 100
英國新法令 上色情網站必須驗證年齡 ..... 103
指紋捺印建檔 可協助走失者快速辨識身分與提供家屬聯絡資訊 ..... 107
搜尋結果頻現「假球」 職棒老闆告 Google 求移除敗訴 ..... 111
貳、資訊公開（Disclosure） ..... 115
公布戴奧辛蛋來自特定蛋雞場，立委疑衛福部未審先判 ..... 116
健康風險評估不給看 環團怒向市府提訴願 ..... 119
全國 9 萬補教師學經歷公開 歡迎各界來找砸 ..... 123
參、資訊監察（Monitors） ..... 127
監看電郵惹議 美國安局宣布停止 ..... 128
澳洲防恐 逼臉書等交加密訊息 ..... 133
查私菸偷裝 GPS 不起訴 法官打臉：加重判刑 ..... 137
兒孫燒炭亡 嬤控警延誤害命 ..... 141

肆、資訊應用（Application）.....145
未來無人機使用者 可能須先註冊方得操作.....146
無人小巴 凌晨試行台北街頭.....150
開放網路申辦月租型門號 可用數位簽章方式申辦.....153
跨國資訊交換 台灣準備好了.....157
自我評量.....161
是非題.....162
選擇題.....173

# 壹、資訊保護（Security）

類別：資訊保護【案號：S10601】

## 勒索病毒目的似乎不在贖金 Petya比想像更複雜

### 【焦點話題】

勒索病毒 WannaCry 肆虐全球，造成許多人的重要檔案遭到加密並遭勒索贖金，其後又出現新型勒索病毒 Petya，先於烏克蘭爆發，接連影響歐、美等國家，不同於 WannaCry，Petya 入侵電腦後，會修改電腦硬碟設定，並建立排程工作於一小時內重新開機，一旦受影響電腦重開機後其螢幕將直接跳出勒索訊息，且無法進行其他操作。而該病毒主要攻擊政府與企業等組織，不僅烏克蘭總理電腦受害，超市與 ATM 電腦也遭殃，嚴重影響民生運作，導致龐大損失。對此大規模的攻擊，烏克蘭警方表示，Petya 病毒案件影響包含個人與企業已至少 1,500 件。

【參考資料來源：ithome，106/6/22】

### 【重點摘要】

1. 使用惡意軟體將使用者電腦加密上鎖或加密其硬碟上檔案之行為，均屬「變更」使用者電腦或其相關設備之電磁紀錄。
2. 為降低資安事件發生之風險，組織應定期進行資安訓練，宣導資訊安全事件對組織之影響，以及預防、因應之方式等資訊。

### 【法律觀點】

首先，有關侵入他人電腦，進行檔案加密、變更電磁紀錄之部分，刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」，而本案之 Petya 病毒，即屬行為人透過「變更」使用者電腦或其相關設備之電磁紀錄，以達到癱瘓使用者電腦、設備之效果，造成使用者無法正常使用，而造成使用者之損失，行為人可能構成妨害電腦使用罪，而有相對罰則。

其次，若駭客除侵入電腦之行為外，另要求被害人給付價金，方解除加密狀態者，按刑法第 346 條第 1 項之規定：「意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付者，處六月以上五年以下有期徒刑，得併科一千元以下罰金。」亦可能構成恐嚇取財罪，而有相對罰則。

綜上，非法侵入他人電腦並要求價金者，應以妨害電腦使用罪、恐嚇取財罪，數罪併罰之。

## 【管理 Tips】

使用資訊科技已經成為現代社會活動的必要方式，但在運用新興科技提供商業服務時，組織必須將網路安全列為重要事項。例如 WannaCry 事件即係來自網路攻擊，所有企業或政府機關都有可能成為被攻擊對象，如何強化網路管控措施是所有組織都需面對之議題。除了平日應定期做員工教育訓練，宣導資訊安全事件對組織的影響、拒絕下載來路不明的盜版軟體、注意社交工程郵件以及重要資料時常備份外，組織亦可透過諸如定期檢查「安全性更新」或限制員工使用網際網路等主動之網路控制措施，均可有效降低侵害發生。

## 【相關標準】

ISO 27001：2013（CNS 27001）

●A.7.2.2　資訊安全認知、教育及訓練

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

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

●A.12.2.1　防範惡意軟體之控制措施

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

(2)適用說明： 新興之惡意軟體攻擊日益頻繁，組織平時即應針對相關惡意攻擊軟體進行相關預防性工作，且熟捻遭攻擊後之因應措施，本案中，如組織善盡對於作業系統修補程式之更新作業，即可有效避免系統遭受侵害。

●A.12.3.1 資訊備份

(1)標準內容： 應依議定之備份政策，定期取得資訊、軟體及系統的影像備份複本，並測試之。

(2)適用說明： 為避免無法預期之資料毀損或侵害，以降低損失風險，定期進行相關資料之有效備份具必要性，本案中，若組織善盡對於相關資訊之備份，於電腦遭受攻擊後，相關資訊仍得以保存，而可有效降低組織之損失。

●A.13.1.1 網路控制措施

(1)標準內容： 應管理及控制網路，以保護資訊系統及應用。

(2)適用說明： 現今網路空間之陷阱層出不窮，若得以適當將部分有問題之網域限制聯網，亦可降低惡意程式由網頁攻擊之風險，本案中，如組織如對員工連網採取限制或是根本性的禁止非必要連網活動，對於電腦、設備遭植入惡意軟體等造成系統受侵害之可能性可有效降低。

類別：資訊保護【案號：S10602】

## 離職前以他人名義於系統複製客戶檔案，房仲業務員遭起訴

### 【焦點話題】

林女曾於房仲公司服務，離職前夕利用主管名義登入電腦系統，意圖複製其曾經手之業務檔案，由於林女於進行時即遭發現，雖其表示複製檔案僅為留念並無他意，惟房仲公司仍懷疑，林女係為因帶槍投靠他公司才複製檔案，並對林女提出妨害營業秘密、背信及偽造文書等告訴。其後，檢方調查認為，林女於複製檔案時即被發現，且該等檔案尚未移出為他用，故妨害營業秘密、背信部分為不起訴，而冒用主管名義登入電腦系統複製業務檔案部分，則依偽造文書罪嫌起訴。

【參考資料來源：中時電子報，106/6/6】

### 【重點摘要】

1. 無故以他人名義進入電腦系統、設備、取得相關電磁紀錄等行為，可能觸犯刑法妨害電腦使用罪章，負有相關刑責。此外，因電磁紀錄足以表示意思證明者，屬準文書，則未經他人同意即使用其帳號、密碼者，亦可能觸犯刑法偽造文書罪章，同樣負有相關刑責。
2. 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。
3. 員工離職時如私自攜出營業祕密等組織機密資料，將觸犯妨害營業祕密法且負有刑責。

### 【法律觀點】

無故輸入他人帳號以登入電腦系統並複製資料之行為，為刑法第 358 條[1]、第

[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

359 條[2]之構成要件，且為善盡對於各類資料之保護，刑法將足以為意思表示證明之電磁紀錄擬制為準文書[3]，故偽造他人帳號登錄之行為，可能同時觸犯妨害電腦使用罪及偽造文書罪。

其次，營業祕密法於 85 年訂定時規定違反營業祕密法者僅負有民事責任，當時關於刑事責任僅能依靠刑法相關條文規範，例如刑法第 317 條洩漏工商祕密罪加以處罰，然該條文刑度僅為 1 年以下有期徒刑，並無法產生足夠的遏止作用。因此，經濟部為了加強保障組織所持有之營業秘密，維護競爭秩序，從 101 年開始就著手修正營業秘密法，並於 102 年 1 月通過增加第 13-1 條至第 13-4 條關於侵害營業秘密的刑事責任，就是希望能對各企業的營業成果提供更完整的保護。

就營業祕密法第 2 條[4]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。由上可知，營業祕密應具備下列要件：

●祕密性：非一般涉及該類資訊之人所知者。例如非屬該公司內員工，雖亦是為相同類型工作，但並不會知悉者。

●經濟性：因其秘密性而具有實際或潛在之經濟價值者。亦即該經濟性並不需已經實現，而是將來有可能因之獲利亦屬之。

●保密措施：有人已採取合理之保密措施者。例如有加密、上鎖或組織有限制

---

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 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」。

[3] 刑法第 220 條：「在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。　　錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」。

[4] 營業祕密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」。

一定人員方得閱覽之情形。

本案離職人員係遭檢察機關依偽造私文書等罪嫌起訴，惟其如有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；或是未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密；又或是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；又或是明知他人知悉或持有之營業秘密有前述情形，而取得、使用或洩漏，依營業祕密法第 13-1 條[5]，將遭處 5 年以下有期徒刑或拘役，得併科新臺幣 100 萬元以上 1000 萬元以下罰金。此外，如果因為侵害營業秘密而獲得利益，且該利益超過罰金最多額，量刑時還能夠在不法所得利益之三倍範圍內酌量加重。此外，營業祕密法中除有刑事責任外，於第 11、12 與 13 條[6]亦有民事侵害排除請求權、損害賠償請求權以及惡意侵害懲罰性賠償，最重可請求到損害額之三倍。

**【管理 Tips】**

[5] 營業祕密法第 13-1 條：「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。　　前項之未遂犯罰之。　　科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之三倍範圍內酌量加重。」。

[6] 營業祕密法第 11 條「營業秘密受侵害時，被害人得請求排除之，有侵害之虞者，得請求防止之。被害人為前項請求時，對於侵害行為作成之物或專供侵害所用之物，得請求銷燬或為其他必要之處置。」；營業祕密法第 12 條「因故意或過失不法侵害他人之營業秘密者，負損害賠償責任。數人共同不法侵害者，連帶負賠償責任。前項之損害賠償請求權，自請求權人知有行為及賠償義務人時起，二年間不行使而消滅；自行為時起，逾十年者亦同。」；營業祕密法第 13 條「依前條請求損害賠償時，被害人得依左列各款規定擇一請求：一、依民法第二百十六條之規定請求。但被害人不能證明其損害時，得以其使用時依通常情形可得預期之利益，減除被侵害後使用同一營業秘密所得利益之差額，為其所受損害。二、請求侵害人因侵害行為所得之利益。但侵害人不能證明其成本或必要費用時，以其侵害行為所得之全部收入，為其所得利益。依前項規定，侵害行為如屬故意，法院得因被害人之請求，依侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之三倍。」。

針對營業秘密保護，美國聯邦調查局提出了一系列參考方法[7]：

●瞭解風險(recognize the threat.)；

●辨別與評估營業秘密(Identify and value trade secrets.)；

●實施維護營業秘密的明確計畫(Implement a definable plan for safeguarding trade secrets.)；

●保護實體營業秘密及限制存取營業秘密(Secure physical trade secrets and linit access to trade secrets.)；

●為員工提供持續不斷的安全教育訓練(Provide ongoing security training to employees.)；

●制訂內部風險控制計畫(Develop an insider threat program. )；

●發現可疑事件時，主動向檢調通報，以避免造成營業秘密所有人之專有資訊無法挽回之損害(Proactively report suspicious incidents to the FBI before your proprietary information is irreversibly compromised.)。

大多數資訊外洩為人員故意或過失所造成，因此，資訊安全除技術面外，更應首重於人員管理面。人員管理乃管理制度中重要之一環，為建立正確之資訊安全管理規範，組織應定期進行教育訓練及宣導，並且要求全員參與，依不同業務性質之單位，講解如何落實日常作業管理。如有違反資訊安全規範者，應有適當之方法要求改善或予以合理之懲處，方能使全體同仁建立一致之資訊安全觀念。此外，事件發生後，為避免影響當事人之權益，亦應於事件查明後儘速通知當事人，以提醒其防範。

**【相關標準】**

ISO 27001：2013（CNS 27001）

[7] Federal Bureau of Investigation, Economic Espionage FBI Launches Nationwide Awareness Campaign, 網址：https://www.fbi.gov/news/stories/economic-espionage

●A.7.2.2　資訊安全認知、教育及訓練

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

(2)適用說明：　如平時有對人員進行教育訓練，使人員瞭解資安之重要性，可降低如本案般，因人員故意行為將客戶檔案攜走情形發生。

●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，以對違反資訊安全之員工採取行動。

(2)適用說明：　對於違反資安之人員進行懲處，或於契約中訂定損害賠償責任，可提醒人員所負有之責任，而本案林女可能就會顧及賠償責任，而不為此等違法行為。

BS 10012：2017

●5.4　將個人資料保護嵌入組織文化

(1)標準內容：　透過認知育教育訓練確保組織成員對於個人資料保護的意識，並藉此將個人資料保護的使命深入組織文化。

(2)適用說明：　透過教育訓練，使組織內的每個人均可瞭解資料保護重要性，可降低如本案般，因人員故意行為將客戶檔案攜走情形發生。

類別：資訊保護【案號：S10603】

## 智慧支付平臺遭爆恐洩個資　政府機關坦言有疏失

### 【焦點話題】

某機關所推出之智慧支付平臺，因該平臺之個人資料均使用明碼傳輸，個人資料外洩之風險將大幅提高，而遭網友告誡民眾千萬不要使用。該機關坦言，因平臺係作為支付業者及各機關之服務中介，本身不處理金流，使用者所輸入之資料僅用於身分確認，亦不會儲存會員之個人資料，故第一版智慧支付平臺之傳輸協定係採超文本傳輸協定(HyperText Transfer Protocol, http)，而非較安全之超文本傳輸安全協定(Hypertext Transfer Protocol Secure, https)，其帳號、密碼皆採明碼傳輸，確有資料外洩之風險，具備一定技術的人員（如駭客）可能得以透過監控軟體拆看資訊傳輸封包，而造成個人資料外洩。此外，廠商之設計未依招標規範規定採用安全傳輸方式，而相關局處於系統上線時，也未能及早發現疏失，將深切檢討，除重新修訂、強化相關標準作業程序外，並將嚴格要求廠商全面檢視程式之安全性，而讓民眾使用得更安心。

【參考資料來源：自由電子報，106/6/25】

### 【重點摘要】

1. 資料於網路傳輸時，若透過未經加密之傳輸協定，資料會採以明碼之方式傳輸，即可能造成包含帳號、密碼等所傳輸資料之外洩風險將大幅提升。
2. 基於資訊安全之考量，電子支付機構所建置之支付平臺、機制，於受理使用者註冊時、使用者登入電子支付平臺時、進行電子交易時，均應符合電子支付機構資訊系統標準及安全控管作業基準辦法之規定。
3. 各機關進行資訊業務委外服務時，為確保委外服務之績效與資通安全，各機關應落實相關之監督、稽核並管控服務水準。

### 【法律觀點】

近年來行動支付工具逐步興盛，政府機關亦已嘗試進行推廣。惟現行針對電子支付訂定之規範，包括「電子支付機構管理條例」、「電子支付機構使用者身分確認機制及交易限額管理辦法」、「電子支付機構資訊系統標準及安全控管作業基準辦法」及「電子支付機構業務管理規則」等管理法令，均以民間的電子支付機構[1]為規範對象；而有關政府機關電子支付作業之規定，中央政府各級機關部分，例如「國庫集中支付作業要點」，地方政府則應按其自治規範辦理。除上述直接與電子支付相關之規範外，其他與資訊或資通系統安全相關之法令規定，如亦適用於電子支付相關事項者，各機關亦應遵循。

因電子支付所涉及之資料包括個人身分證明資料以及財務資料，如果產生外洩等情事，將對使用者產生嚴重影響，因此金融監督管理委員會要求電子支付機構於在進行電子支付交易時，需符合電子支付機構資訊系統標準及安全控管作業基準辦法[2]之安全規定，包括電子支付機構於受理使用者註冊時應有身分確認程序之安全設計[3]；使用者登入電子支付平臺時應進行身分確認，並得以帳號及固定密碼登入，針對帳號及固定密碼應有安全設計[4]；進行電子交易時對於不同交易類型，應依其不同交易限額，採用不同的交易安全設計[5]；且對個人資料之保護更需符合一定的要求[6]。故如為一般企業作為電子支付機構，應依電子支付機構管理條例所授權之電子支付機構資訊系統標準及安全控管作業基準辦法進行資訊系統安全控管。

有關電子支付機構管理條例之適用對象為股份有限公司，而政府機關非屬之，因此無論該平臺是否處理金流，又或是僅作為支付業者及各機關的服務中介，

[1] 電子支付機構管理條例第 3 條本文：「本條例所稱電子支付機構，指經主管機關許可，以網路或電子支付平臺為中介，接受使用者註冊及開立記錄資金移轉與儲值情形之帳戶 ( 以下簡稱電子支付帳戶 )，並利用電子設備以連線方式傳遞收付訊息，於付款方及收款方間經營下列業務之公司。」。

[2] 電子支付機構資訊系統標準及安全控管作業基準辦法第 2 條：「電子支付機構辦理電子支付機構業務之資訊系統及安全控管作業，應依本辦法規定辦理。」。

[3] 電子支付機構資訊系統標準及安全控管作業基準辦法第 4 條。

[4] 電子支付機構資訊系統標準及安全控管作業基準辦法第 5 條。

[5] 電子支付機構資訊系統標準及安全控管作業基準辦法第 6 條。

[6] 電子支付機構資訊系統標準及安全控管作業基準辦法第 13 條。

均不適用電子支付機構管理條例，惟參照政府機關之電子支付相關規範，以國庫集中支付作業要點為例，若機關自行辦理電子支付作業時，仍有諸如憑證管理、系統管理等規定[7]，且若政府機關係委託外部廠商為支付平臺之設計、建置，於委託契約中，應得要求該廠商所設計、建置之支付平臺，符合諸如電子支付機構資訊系統標準及安全控管作業基準辦法所規定之相關標準，其次，若因相關機關之故意或過失，導致使用者之個人資料外洩，按個人資料保護法或其他法律，造成個人資料外洩之機關負損害賠償責任。

**【管理 Tips】**

確保交易過程中之資料安全無虞，乃電子支付平臺消費體驗中重要的環節，惟有確保電子支付機構之交易資訊安全，以避免因資訊系統運作、傳輸或處理之錯誤，進而影響客戶交易之穩定、資料安全才能使民眾用得安心。

組織開發之平臺或系統，應於產品設計、開發與測試等過程中，將資訊安全與資料保護列為重點項目之一，並且制訂標準作業程序於上線前全面檢測程式、APP 之安全性，以強化及改善消費者體驗，使民眾願意使用電子支付。

組織若有系統、平臺之需求，而委外進行開發、建置時，為確保產品之可用性、績效，並避免觸犯相關規定，應對委外廠商為監督之義務。

**【相關標準】**

ISO 27001：2013（CNS 27001）

●A. 14.1　資訊系統之安全要求事項

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

[7] 國庫集中支付作業要點第 106 點：「各機關應積極改善作業環境，實施電子支付作業。實施電子支付作業之機關，應先向憑證管理中心申請憑證 IC 卡後，再向本署提出申請安裝電子支付作業系統。電子支付作業系統軟體，由本署提供，並協助安裝、測試後實施。」。

(2)適用說明： 資訊系統之安全，應於系統開發時，即納入考量，如本案中，若委外廠商於平臺建置、開發時，即善為考量相關應符合之資訊等安全標準，即可避免後續諸如個人資料洩漏風險等缺失之產生。

●14.2.7 委外開發

(1)標準內容： 組織應監督及監視委外系統開發活動。

(2)適用說明： 資訊系統、平臺之委外開發等作業，委託者本於委託契約之關係，即得對該系統、平臺之建置、開發進行監督，一方面得確保系統、平臺之可用性，一方面亦得監督相關作業之合法性。如本案，該機關若於建置時妥善進行監督，即可有效避免發生相關系統疏失。

BS 10012：2017

●6.1.7 隱私設計與預設

(1)標準內容： 應確保所提供之系統、產品或服務對於個人資料的處理的風險，並透過設計以確保隱私控制之適切性。

(2)適用說明： 組織對於所建置之系統，應確保使用者及相關資訊之隱私具備一定程度之有效保護，本案中，若於平臺建置、設計時，妥善納入對於系統登錄人員其隱私保護之控制措施，則可避免後續諸如個人資料洩漏風險等缺失之產生。

類別：資訊保護【案號：S10604】

## 哥哥個資全PO網 弟討債反挨罰9萬

### 【焦點話題】

林姓男子不滿其兄避不出面處理債務糾紛，去年 4 月將載有其兄姓名、出生年月日、身分證字號、住處之土地謄本、本票強制執行狀、家事起訴狀、假扣押狀等具有個人資料之資料，全部張貼於其臉書上，其兄得知後報警處理，林男被檢方依違反個人資料保護法起訴。法院認為，林男明知土地登記謄本等文件載有其兄之個人資料，仍於臉書上張貼其兄之個人資料，使不特定人士只要瀏覽其臉書就可得知，依「非法利用個人資料罪」處以 3 個月有期徒刑，得易科 9 萬元罰金[1]。

【參考資料來源：自由時報，106/3/12】

### 【重點摘要】

1. 姓名、出生年月日、身分證字號、住處的土地謄本、本票強制執行狀、家事起訴狀、假扣押狀等，只要是能夠直接或間接識別個人之資料均屬個人資料。

2. 於臉書發表貼文若包含個人資料時，即屬使用他人個人資料之情形，需符合法定使用要件方可使用。

### 【法律觀點】

土地謄本、本票強制執行狀、家事起訴狀、假扣押狀等文件，所載姓名、出生年月日、身分證字號、住處等，均屬個人資料，受到個人資料保護法之保護，必須符合法定要件方可蒐集、處理，且原則不得為特定目的外之利用。

個人資料保護法對於未遵守該法應盡義務或違反該法之規範，訂有罰則[2]，本

[1] 臺灣基隆地方法院 106 年基簡字第 21 號刑事判決。

[2] 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。」

案當事人因欲要求對方還款，即張貼他人個人資料於臉書，而對於個人資料之使用，如前所屬須符合法定要件，本案當事人對於該個人資料之使用顯非出於合法或正當之目的，亦已超出必要範圍[3]，按個人資料保護法之規定，即可能受諸如有期徒刑、罰金等刑事責任追究( 本案即遭處以 3 個月有期徒刑，得易科 9 萬元罰金 ) ，其次，除了刑事責任外，依個人資料保護法第 29 條規定，亦可能遭到權利受侵害人請求損害賠償。

**【管理 Tips】**

個人資料於網路應用時，應注意以下兩點：一、資料之利用應與蒐集時應與原始目的相符。本案林男將記載有其兄之個人資料之文件隨意張貼並公開於網路上，已與原始蒐集之目的不相符，已違反個人資料保護法關於個人資料應於目的內利用之規定。二、個人資料之公開除個人資料保護法外，仍應注意是否觸犯其他相關法規或法令的規定。

如為組織經營粉絲團或其他社群媒體，前開事項亦應相同注意，組織於管理時，應制定正確之個人資料保護規範 ( 如訂定個人資料檔案安全維護計畫 ) ，而除定期做員工教育訓練與資訊安全政策宣導外，應將個人資料蒐集時之特定目的予以盤點，使員工於處理及利用時能知悉其可應用之範圍，避免發生合理範圍外之使用。

**【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：　本案中，土地謄本、本票強制執行狀、家事起訴狀、假扣押狀等文件所包含之姓名、出生年月日、身分證字號、住

[3] 同註 1，判決理由書。

處等均屬個人資料，應確保利用時係依法為之。

ISO 29100：2011（CNS29100）

●5.3　目的適法性及規定

(1)標準內容：　個人可識別資訊之使用與處理時，相關目的應以遵從適用之法律為基礎。

(2)適用說明：　利用個資時應符合蒐集目的所適用之法令為依歸，本案即係當事人未考量蒐集目的而違法利用之情形。

類別：資訊保護【案號：S10605】

## 擔心個資外洩 第三類謄本更安全

### 【焦點話題】

過去許多民眾都因舊制謄本揭露資訊過分詳細、開放任何人申請，導致土地開發業者或仲介業者據此登門叨擾。內政機關已修正「土地登記規則」第 24-1 條條文，自 2015 年 2 月 2 日起，原規定任何人皆能申請的第二類土地登記謄本，改以去識別化方式，僅公開所有權人的姓氏、部分國民身分證統一編號，但仍保留完整住址資料，以促進土地利用及整合開發需要，假如民眾有疑慮，可請求隱匿部分地址資料，並新增利害關係人才能申請的第三類土地登記謄本，增加謄本分級，保護個資安全。此外，新制三類謄本亦依照申請人資格不同，將謄本分為三類：第一類謄本，顯示登記名義人全部資料，限登記名義人或其代理人才可申請；第二類謄本，隱匿登記名義人的出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿資料，任何人都能申請；第三類謄本，隱匿登記名義人的統一編號、出生日期，限利害關係人才可申請。

【參考資料來源：自由電子報，106/6/25】

### 【重點摘要】

1. 土地謄本區分為三類，第一類：顯示登記名義人全部登記資料；第二類：隱匿登記名義人之出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿之資料。；第三類：隱匿登記名義人之統一編號、出生日期之資料。
2. 姓名或其他個人資訊如以編號顯示，僅公開未涉隱私部分，且以匿名化或去識別化處理，此種情形無從識別特定個人而無侵害隱私權之虞。

### 【法律觀點】

地籍謄本舊制時，任何人皆可申請之第二類謄本（包含登記名義人完整之姓

名與地址），而蒐集第二類謄本多為房仲業者，透過自地政機關合法取得之謄本資料，知悉登記名義人姓名、地址，藉此發信請求委託出賣房屋，多造成住戶困擾。亦因此促成土地登記規則之修正，依修正後土地登記規則第 24-1 條[1]規定，土地謄本區分為三類，第一類：顯示登記名義人全部登記資料，僅登記名義人或其他依法令得申請者方得申請；第二類：隱匿登記名義人之出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿之資料。但限制登記、非自然人之姓名及統一編號，不在此限，此類謄本任何人均得申請；第三類：隱匿登記名義人之統一編號、出生日期之資料，此類則係登記名義人、具有法律上通知義務或權利義務得喪變更關係之利害關係人得申請。

法務部法律字第 10100253980 號函[2]明示，針對姓名或其他個人資訊如以編號顯示，僅公開其餘未涉隱私部分，且匿名化或去識別化處理，此種情形無從識別特定個人而無侵害隱私權之虞。亦即應將「公開個人資料欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間予以比較衡量判斷後，方得決定是否應將資料予以公開。因此，為保障個人隱私權，同時兼顧不動產交易安全，主管機關修訂土地登記規則，將第二類謄本之登記名義人之出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿之資料予以部分隱匿，且如登記名義人為自然人時，得依登記名義人之請求，提供申請住址隱匿服務[3]，以避免登記名義人之個人資料

[1] 土地登記規則第 24-1 條第 1 項：「申請提供土地登記及地價資料，其資料分類及內容如下：一、第一類：顯示登記名義人全部登記資料。二、第二類：隱匿登記名義人之出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿之資料。但限制登記、非自然人之姓名及統一編號，不在此限。三、第三類：隱匿登記名義人之統一編號、出生日期之資料。」。

[2] 法務部法律字第 10100253980 號函釋要旨：「個人資料保護法第 5 條、政府資訊公開法第 18 條等規定參照，公務機關將個人資料提供民意代表作為審查公務機關預算使用時，如資料就姓名部分以編號顯示，亦以編號對應個別優惠存款額度，似係就「公開個人資料欲增進之公共利益」與「不公開個人資料所保護之隱私權益」間比較衡量判斷，而依上述規定，僅公開其餘未涉隱私部分，且匿名化或去識別化處理，已無從識別特定個人而無侵害隱私權之虞。」。

[3] 土地登記規則第 24-1 條第 2 項：「前項第二款資料，得依登記名義人之請求，隱匿部分住址資料。但為權利人之管理人及非自然人，不適用之。」。

受到過度揭露。

**【管理 Tips】**

資料分級控管一直在資訊管理中具備一定的重要性，且分類亦應與時俱進，就如同土地登記規則將原本的二種謄本再劃分為三種，即是在因應個人資料保護法等新規定，為提升對於當事人保障所增加的新制，藉由使用目的與對象之不同，分別標示所需之資料，以強化防護。

雖然一般組織並沒有強制規定要將資訊進行分類分級，但藉由分級制度區分各類文件的管控方式，有助於提升組織內部風險控管效率，且文件上清楚標示機密等級，亦能協助企業員工瞭解文件重要性，並依規定處理，建立重要資料防護機制。

**【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、重要性及對未經授權揭露或修改之敏感性分級。

(2)適用說明：　以本案例而言，透過地籍謄本分級可將無揭露必要之資訊過濾後再予適度公開，達到資訊流通與資訊安全之平衡。

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，在合法目的下揭露必要之資料。

(2)適用說明：　因不同權利人所得知悉、需要之資料並不盡相同，故本案之地籍謄本亦須同此概念，予以區分不同對象，以不同類

別之地籍謄本分別揭露必要之資訊。

類別：資訊保護【案號：S10606】

## 國家機密保護法擬修正，涉密人員退職後至少出境管制3年

### 【焦點話題】

主管機關考量國家機密攸關整體國家安全或利益，為強化涉密人員之管理機制，爰進行國家機密保護法之修正，相關草案已經行政院院會通過，並送請立法院審議。修正後將刪除涉密之退離職或移交國家機密人員之「管制期間縮短」規定。且為因應目前面臨之境外威脅，並為嚇阻不法洩漏國家機密事件發生，草案亦新增、另列關於洩漏、交付、刺探經核定之國家機密或報請核定國家機密之事項予外國、大陸地區、香港、澳門或其派遣之人者之規定，並增訂預備或陰謀犯之處罰；而當前述違法事項所涉國家機密屬於絕對機密者，更有加重其刑至二分之一等相關規定。

【參考資料來源：中時電子報，106/7/6】

### 【重點摘要】

1. 為強化涉密人員及退離職或移交業務人員之出境管理機制，修正退離職或移交業務涉密人員之出境管理期間雖得調整延長，但不得縮短。
2. 為因應與更有效防範目前外國、大陸地區、香港、澳門之威脅，國家機密保護法修正草案，修正另列關於洩漏、交付、刺探或收集經核定之國家機密或報請核定國家機密之事項予外國、大陸地區、香港、澳門或其派遣之人者之處罰規定。

### 【法律觀點】

政府資訊公開與否，應以原則公開、例外禁止公開之模式為之[1、2]，而公開政

[1] 政府資訊公開法第 6 條。

[2] 政府資訊公開法第 7 條。

府資訊之目的，在於便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與[3]。如資料涉及國防、軍事及外交政策等，且如其公開或揭露，可能危及國家生存或安全時，即有限制或禁止公開之可能；國外立法例上亦有類似之規定。

國家機密保護法之立法目的，在於建立國家機密保護制度，並確保國家安全及利益[4]；而為因應境外威脅及減少不法洩漏國家機密事件發生之風險，並考量國家機密係攸關國家安全、利益，故該法本即定有涉密等人員之出境管制規定。而為避免實務運作時，各機關寬認該法關於縮短出境管制期間之規定，以致保護強度降低，並為因應及更有效防範來自境外之威脅，行政院於 106 年 7 月通過法務部擬具之國家機密保護法修正草案，並送請立法院審議。該草案刪除出境管制期間縮短之規定[5]、調整將與國家機密相關事項(包含已受核定、報請核定中之事項)洩漏或交付予境外區域或其人員，或為其刺探、收集國家機密相關事項者之處罰[6、7、8]。

---

[3] 政府資訊公開法第 1 條。

[4] 國家機密保護法第 1 條。

[5] 國家機密保護法第 26 條修正草案：「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。前項第三款之期間，國家機密核定機關得視情形延長之。」。

[6] 國家機密保護法第 32 條修正草案：「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。洩漏或交付前項之國家機密於外國、大陸地區、香港、澳門或其派遣之人者，處三年以上十年以下有期徒刑。因過失犯前二項之罪者，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、第二項之未遂犯罰之。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。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。」。

[7] 國家機密保護法第 33 條修正草案：「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。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、澳門或其派遣之人者，處一年以上七年以下有期徒刑。因過失犯前二項之罪者，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、第二項之未遂犯罰之。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。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。」。

[8] 國家機密保護法第 34 條修正草案：「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。為外國、大陸地區、香港、澳門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。前三項之未遂犯罰之。預備或陰謀犯第一項、第二項或第三項之罪者，處一年以下

## 【管理 Tips】

國家機密為國家生存之本，對於組織而言亦同，對於現正管理或持有國家機密，或曾持有或管理者，均應有適當程度之規管。

組織成員除依相關法令對所掌握之機密資料負有保密義務外，組織於員工就職時即應開始進行管理，除簽訂保密條款等必要事項，尚須防範日常執勤時的資料外洩，並建立完善離職程序，確認離職前其所掌握之機敏資料不被攜出，以避免日後紛爭。

## 【相關標準】

ISO 27001：2013（CNS 27001）

●A.7.2.2　資訊安全認知、教育及訓練

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

(2)適用說明：　組織應對相關員工進行教育訓練，以使其知悉法規內容，並使人員瞭解資安之重要性，以降低因人員故意或過失導致組織機密外洩之風險。本案中所提到之法律及其修正草案即包含關於洩漏、交付、刺探或收集國家機密相關事項之禁止規定與相關罰則，組織應使人員知悉上開規定及罰則之內容，以降低非法情事之發生與致生損害之可能。

●A.7.3.1　聘用責任之終止或變更

(1)標準內容：　應對員工及承包者定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。

---

有期徒刑。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。」。

(2)適用說明： 組織之人員其因業務所知悉之資訊，如有應保密者，不僅因其職務中止或變更，即解除保密義務。本案中，依國家機密保護法規定，持有機密之人員在退離職、業務移交後，仍負有保密義務，且如因故意或過失造成機密洩漏者均有相關罰則，組織應確實傳達此規範內容，期能有效警惕離職之涉密人員，避免機密資料外洩。

類別：資訊保護【案號：S10607】

## 「數位通訊傳播法草案」針對煩人的商業電子訊息加以規範

### 【焦點話題】

通訊傳播主管機關公布數位通訊傳播法草案 具體內容，而許多民眾深受其擾的商業電子訊息，亦在該草案之規範範圍內。依數位通訊傳播法草案規定，商業電子訊息的發送方必須在訊息中提供當事人可選擇「拒絕接收」之免費回傳機制和聯絡方式。發送方於接獲當事人拒絕其發送之通知時，應立即停止發送同類商業電子訊息。該條草案之立法說明中則指出，違反該規定者，其發送即為不法之發送，且發送方應負民事損害賠償責任。

【參考資料來源：ETNEWS，106/1/4】

### 【重點摘要】

1. 電子郵件信箱或通訊軟體帳號等資訊，如蒐集者能將之與其他資料對照、組合、連結而得識別特定個人時，即屬個人資料保護法（下稱個資法）所保護之範疇，使用該等資料須符合法定要件；且利用該等資料進行行銷時，亦須符合個資法諸如行為人須提供當事人表示拒絕之方式等規定，若違反者，並有對應之罰則規定。
2. 縱然未利用個人資料，依數位通訊傳播法草案之規定，行為人於發送商業電子訊息時，應提供接收之當事人得免費表示拒絕繼續接收之機制，且應標示為商業訊息並提供接收人關於發送方之聯繫資訊。

### 【法律觀點】

目前業者常以發送商業電子訊息之方式，進行商品或服務之行銷，而其所利用之電子郵件等聯絡方式，如依具體情形，堪認屬個資法所指個人資料時[1]，

[1] 電話號碼或電子郵件等聯絡方式，個人資料保護法規定，如得直接或間接方式識別該個人之資料即為個人資料，惟如何判斷能否識別，仍應從蒐集者角度加以觀察，如蒐集者能將電話號碼或電子郵件與其他資料

則受到個資法之保護，必須符合法定要件方可蒐集、處理，且原則不得為特定目的外之利用[2]。且個資法對於利用個人資料於行銷者，亦有相關要求，例如應於首次行銷時提供免費之拒絕方式，而當事人拒絕時，應停止利用該個人資料為行銷等[3]；而違反相關規定者，亦有對應之罰則。

在數位經濟時代中，為保障資訊自主選擇與不受他人干擾之權利，並兼顧數位經濟之發展，縱然未涉及個人資料之利用，建立與商業電子訊息相關之行為守則[4]仍有其必要性。按數位通訊傳播法草案規定，商業電子訊息之發送方於發送時，應提供收受方之當事人得拒絕接收(opt-out)之適當方式；且發送方於接獲拒絕接受訊息之通知時，應立即停止其發送行為[5]。而為使當事人於開啟商業電子訊息前，即有辨識及過濾商業電子訊息之可能，發送方於發送時應清楚標明聯繫資訊，並於內容之適當位置，標註商業識別資訊。此外，為維護當事人之權益，數位傳輸傳播法草案，亦明定發送方不得隱匿或變造信首資訊及足資識別為商業訊息之資訊[6]。如發生私權爭議時，當事人則可向法院依民事訴訟法規定聲請定暫時狀態處分[7]，以茲救濟。

## 【管理Tips】

濫發電子商業訊息可能造成網路容量壅塞及系統資源虛耗，除可能影響民眾使用網路服務之意願，在利用民眾個人資料進行電子商業訊息發送之情形，除非符合特定目的及其他個資法相關規定，否則亦有違法之可能。因此，組織於使用電子商業訊息為行銷時，應注意是否符合法律規定，諸如相關資料

---

對照、組合、連結而得識別特定個人，即屬個人資料，但仍需從蒐集者本身綜觀各種情況與事證加以判斷，無法僅依單一資料類型，即認定是否為個資法所稱之個人資料，參法務部 102 年 5 月 15 日法律字第 10203502260 號函釋、法務部 103 年 6 月 18 日字第 10303506790 號函釋。

[2] 個人資料保護法第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」。

[3] 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。」

[4] 數位通訊傳播法草案第 23 條，立法理由二。

[5] 數位通訊傳播法草案第 23 條第 2 項。

[6] 數位通訊傳播法草案第 23 條，立法理由三、四。

[7] 數位通訊傳播法草案第 19 條，立法理由。

是否經合法取得與使用、有無清楚表明為商業行銷、是否提供當事人得拒絕接收之機會與適當方式，以及是否設有機制，以利在當事人拒絕接受時，即停止電子商業訊息之發送。

同時，為避免觸法情形發生，組織應對發送電子郵件之行銷作業流程予以掌握，避免發生人員在不符合法要件之情形下，對外執行發送商業電子郵件等行銷行為；並應確實建立起相關之資訊安全管理機制，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。

(2)適用說明：　組織應辨識出個人資料以及相關法定要求，以利當事人依數位通訊傳播法（如獲通過）或個資法請求拒絕行銷時，組織得即時依法因應。

ISO 29100：2011（CNS 29100）

●5.2　同意及選擇

(1)標準內容：　堅持同意原則，意指下列事項。

- 向個人可識別資訊(personally identifiable information, PII)當事人表明，以選擇是否允許處理其 PII，除非 PII 當事人無不同意之自由，或所適用法律允許無須該自然人同意即可處理 PII。PII 當事人之選擇必須是自由提供、特定且基於充分理解。

- 取得 PII 當事人選擇加入之同意以蒐集或其他方法處理敏感 PII，除非適用之法律允許無須該自然人同意下處理敏感之 PII。

- 於取得同意前，通知 PII 當事人關於其在個人參與及存取原則下之權利。

- 於取得同意前，向 PII 當事人提供以公開、透明及告知原則所表明之資訊。

- 向 PII 當事人解釋給予或不予同意之涵義。

宜制定條款，提供機會讓 PII 當事人選擇如何處置其 PII，及允許 PII 當事人方便且免費撤回同意。此要求宜依隱私權政策辦理。即便撤回同意，PII 控制者可能需持有某些 PII 一段時間，以便遵循法律或契約義務 ( 例：資料持有、可歸責性 ) 。無須同意，即可依法處理 PII 時，宜儘可能告知 PII 當事人。當 PII 當事人有撤回同意之能力並選擇撤回時，除非法律強制，不宜為任何目的處理該 PII。

對 PII 控制者而言，堅持選取原則，意指下列事項。

- 對 PII 當事人就有關其 PII 處理在蒐集、初次利用或爾後適用時，儘快提供清楚、明確、易懂、可取得及可負擔之機制，以便其行使選擇及給予同意。

- 實作 PII 當事人於其同意中表達之取捨。

此外，可定義於同意以外 ( 例：合約績效，PII 當事人及其重要之利益、或法律之遵循 )處理 PII 之額外條款。某些實例中，適用之法律規定 PII 當事人之同意並不構成得以處理 PII 之充分法律基礎 ( 例：未成年者在無父、母或監護人許可下，所給

之同意）。此外，PII 之國際傳輸需考量額外之要求事項。於處理或傳輸資料前，遵循上述額外條款係 PII 控制者之責任。

(2)適用說明：組織於處理個人可識別資訊時，其程序、機制應可被檢驗且透明，並使該資訊之權利人知悉蒐集、使用之目的、處理及保存方式等。如此可使相關權利人對組織產生信任，亦可幫助避免濫為蒐集、處理或利用權利人資料行為之發生。依數位通訊傳播法草案或個資法之要求，組織利用個人資料為行銷時，該資訊之取得、處理及利用除應符合法律規定外，於當事人拒絕行銷時，組織亦應依其要求停止發送商業電子訊息。

類別：資訊保護【案號：S10608】

## 英商惡搞合約 2萬人同意1千小時社區服務換免費WIFI

### 【焦點話題】

許多人於消費時均未對所同意之契約條款進行瞭解，而英國某 WIFI 供應商為使消費者認知到謹慎審視契約條款之重要性，日前將「要求消費者須提供一 1 千小時之社區服務」條款加入 WIFI 服務契約中；約 2 萬人疑未審視條款內容即簽署契約。該公司表示，其無意要求消費者履行該條款，此舉係為提醒消費者，若未瞭解相關契約條款，可能在不知情的情況下同意不需要的加價服務或有違己願之契約條件；例如消費者可能因此授權業者取得與契約履行無關的私人資訊如網路瀏覽數據等。而在此之前，另一英國網路安全公司亦曾於 2014 年於倫敦進行了類似的實驗，該實驗中消費者可使用免費 WIFI，惟須拿小孩做為交換；實驗亦發現許多消費者同意該契約條件。

【參考資料來源：自由電子報，106/7/16】

### 【重點摘要】

1. 契約條款如係企業經營者為與多數消費者訂立同類契約之用，而預先擬定並提出者，其即屬於定型化契約，此類契約係由企業單方擬定，消費者應仔細確認內容，以避免不必要之糾紛。
2. 依民法、消費者保護法（下稱消保法）與定型化契約相關規定之意旨，此類契約之條款應符合平等互惠原則、誠信原則，且不得有違公共秩序、善良風俗，違反者無效。
3. 若契約約定蒐集之資料屬個人資料者，則有個人資料保護法之適用，相關資料必須符合法定要件方可蒐集、處理，且原則不得為特定目的外之利用。

### 【法律觀點】

網路服務業者若於其服務契約之條款中，加入諸如需蒐集使用者資訊等要求，而該等資訊若屬個人資料保護法所稱之個人資料者，應受個人資料保護法之規範，須符合法定要件方可蒐集、處理，且原則並應在符合特定目的之前提下方能利用。

服務提供者如為企業經營者[1]時，其服務條款因係企業經營者為與多數消費者訂立同類契約，所預先擬定，故屬於定型化契約條款[2]，應適用消保法之相關規定。亦即，此類條款之內容，應本於平等互惠之原則，且若有違反誠信原則、對消費者顯失公平者，無效[3]。此外，民法有關法律行為之規範，亦有明定不得違反公共秩序或善良風俗，違反者無效之規定[4]。因此有關定型化契約條款是否有效，應檢視其內容是否符合平等互惠原則、誠信原則，以及有無牴觸公共秩序或善良風俗者而顯失公平或不當，加以判斷。

綜上所述，本案中 WIFI 供應商所訂定服務契約之條款，如有蒐集消費者資料並予以利用或要求消費者提供相關服務時，應注意該等資料是否屬個人資料，若是，必須符合法定要件方可蒐集、處理，且原則不得為特定目的外之利用。又該契約係與多數消費者訂立之同類契約，而所提出預先擬定之契約條款，應屬於定型化契約，契約內容要求使用服務者提供 1 千小時社區服務，斟酌契約之性質、締約目的、全部條款內容、交易習慣及其他情事，並比較同類契約情事，此種約定內容似非正常合理，因此，要求服務使用者應進行 1 千小時社區服務之條款，若於我國發生，按消保法之規定，可能會被認定為違反誠信原則，對消費者顯失公平而無效。

## 【管理 Tips】

[1] 消費者保護法第 2 條第 2 款：「二、企業經營者：指以設計、生產、製造、輸入、經銷商品或提供服務為營業者。」。

[2] 消費者保護法第 2 條第 7 款：「七、定型化契約條款：指企業經營者為與多數消費者訂立同類契約之用，所提出預先擬定之契約條款。定型化契約條款不限於書面，其以放映字幕、張貼、牌示、網際網路、或其他方法表示者，亦屬之。」。

[3] 詳見消費者保護法第 11 條、第 12 條之規定。

[4] 民法第 72 條：「法律行為，有背於公共秩序或善良風俗者，無效。」。

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

組織如欲使用定型化契約進行蒐集個人資料等業務時，除需先訂定完整蒐集、處理及利用個資之程序外，尚需善盡告知當事人之義務，且應注意避免於契約條款中加入不當條文，如斟酌契約之性質、締約目的、全部條款內容、交易習慣及同類契約內容，相關條款非屬正常合理時，即應考量調修，以免導致契約條款無效，甚至受到當事人求償。而消費者在簽訂定型化契約時，仍應仔細確認契約條款，避免對自己造成不必要之困擾，甚至受到實質損害。

**【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： 組織應知悉所適用之相關法規並依法行事。本案中，WIFI供應商之本意僅在測試消費者是否注意契約條款，並非真要在條款中加入不當之內容；但在一般狀況下，組織於訂定契約條款時，應妥善知悉、瞭解個人資料保護及其他相關法規規範，從而訂定符合法律規定及相關原則之契約條款。

類別：資訊保護【案號：S10609】

## 因應APCN-2海纜斷線，有關機關督促業者辦理頻寬調度並儘速排除障礙

### 【焦點話題】

通傳主管機關指出，近來固網業者因國際海纜(亞太 2 號海底電纜，Asia Pacific Cable Network-2, APCN-2)斷訊，造成上網阻塞、中斷等對用戶之不利影響，顯示出業者之備援計畫及應變能力尚須強化。該機關已督促業者於海纜斷訊障礙排除前，積極向其他國際海纜業者調度可用海纜頻寬，以紓解對美國等之網際網路壅塞現象。

此外，為提升電信事業之網域名稱伺服器(Domain Name Server, DNS)之資通安全防護能力，該機關擇選具 DNS 主要設施之 10 家電信業者，於年中辦理 DNS 實兵攻防演練及情境演練，以驗證其 DNS 安全防護機制及通報、應變處置程序，並督促電信事業加強 DNS 設施安全防護能量，確保服務提供及持續營運。未來亦將持續督導電信事業並配合有關機關辦理關鍵基礎設施防護(Critical Infrastructure Protection, CIP)及關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)之年度訪評及演練，並參與跨領域資安演練，以進一步提升電信事業跨領域資安防護與應變能力。

【參考資料來源：自由電子報，106/5/1】

### 【重點摘要】

1. 國家關鍵基礎設施安全防護指導綱要針對關鍵基礎設施之分類，其主部門包含能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八類。

2. 資通安全管理法草案亦規範，非公務機關若經指定為關鍵基礎設施提供者，除應訂定、修正、實施資通安全維護計畫，並繳交年度資通安全維護計畫實施情形外，亦應辦理資安事件之通報應變，及執行機關所屬資通安全責任等級所要求之應辦事項。

3. 業者依契約內容提供服務者，應確保其服務穩定供給，若生服務中斷等情事，除契約中已合法約定免責條款外，應對契約相對人為適當補償，而若因此致生損害者，權益受損者亦得向業者提起債務不履行損害賠償訴訟，以資救濟。

**【法律觀點】**

現代科技日新月異，而人民需求雖依時間可能有所不同，但維持基本生活仍為最低要求，依據國家關鍵基礎設施安全防護指導綱要，關鍵基礎設施範圍之主部門分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八類，其下並各分為數項次領域及重要元件設施[1]。

而現於立法院審議之資通安全管理法草案，所規範之關鍵基礎設施係指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，並經行政院公告者[2]。而關鍵基礎設施提供者則指經行政院核定之維運或提供關鍵基礎設施之非公務機關[3]。

綜合以上規定可知，待資通安全管理法草案通過後，如非公務機關維運或提供國家關鍵基礎設施安全防護指導綱要所定領域之關鍵基礎設施，且經行政院核定為關鍵基礎設施提供者時，其即應受資通安全管理法之約束；除應符合其所屬資通安全責任等級之要求外，亦須訂定、修正及實施資通安全維護計畫、向主管機關提出資通安全維護計畫實施情形，遇資安事件則應進行事件之通報與應變，且於其資通安全管理有缺失或待改善情形時，亦須提出相

[1] 行政院，103 年 12 月 23 日，國家關鍵基礎設施防護指導綱要。

[2] 資通安全管理法草案第 2 條第 1 項第 6 款：「關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，並經行政院公告者。」。

[3] 資通安全管理法草案第 2 條第 1 項第 7 款：「關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，依第十五條第一項規定經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行政院核定之非公務機關。」。

應之改善報告[4]。

除了上述法令要求外，針對業者與消費者間之服務提供，應屬契約關係，業者應提供穩定且合適之服務予消費者，若生服務中斷等情事，除於契約內具合法之免責條款約定外，應以諸如退費等方式為適度之補償，而若致使消費者產生損失，業者面臨消費者所提債務不履行之訴時，亦可能有損害賠償之責任。

綜合上述，如認海底電纜屬國家關鍵基礎設施安全防護指導綱要中所定之通訊傳播類別之關鍵基礎設施，雖然現行之國家關鍵基礎設施安全防護指導綱要之規範範圍僅為行政院及所屬各級機關（構）、行政法人、國營事業、地方政府，尚未含括國營事業以外之一般民間業者[5]；但於資通安全管理法通過後，民間業者倘經核定為關鍵基礎設施提供者時，即負有訂定資通安全維護計畫，並於事故發生時依法進行通報及應變之義務，且須於事件因應之階段性任務完成後，向主管機關提出調查、處理及改善報告等。此外，考量業者與消費者間之消費、服務契約關係，業者應負有維持其服務正常、穩定之義務，若產生服務中斷等情事，應有諸如退費等相關因應之機制，且若因而致生消費者之損失時，可能須負損害賠償責任。

**【管理 Tips】**

資通安全管理法草案對於關鍵基礎設施提供者，於第 2 條第 1 項第 7 款係有

[4]資通安全管理法草案第 15 條：「中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。　　關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。　　關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形。　　中央目的事業主管機關或直轄市、縣（市）政府應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。　　關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關或直轄市、縣（市）政府。　　第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。」。

[5] 國家關鍵基礎設施安全防護指導綱要第參點實施對象與目的，「本指導綱要所定義關鍵基礎設施之掌(監)理者包括：行政院及所屬各機關、機構、行政法人、國營事業、地方政府。」。

定義，而有高度要求之原因，在於其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響，故於第 15 條要求關鍵基礎設施提供者平時即應備有資通安全維護計畫，以進行資通安全之管理。

而在資通安全管理法草案尚未提出前，國家通訊傳播委員會已針對電信事業之資訊通訊安全管理作業訂定電信事業資訊通訊安全管理作業要點[6]，並據以公告電信事業資通安全管理手冊，其主要架構為建立（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。

前述要點及手冊之規定，以及審議中之相關資通安全管理法草案及其子法，應均會就資通安全維護計畫之必要事項、實施情形之提出方法及事件之通報、應變等內容為規定，其項目與內容即可作為一般組織於進行資通安全管理時之參考。為強化組織面對資通安全事件時的應變能力，組織針對重要設施之管理，尤應備有資通安全管理機制，並定期演練緊急應變計畫，以提升內部人員之應變能力，並確保組織具備持續提供服務與營運之能力。

**【相關標準】**

ISO 27001：2013（CNS 27001）

●A.16.1　資訊安全事故及改善之管理

(1)標準內容：　確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。

(2)適用說明：　資安事故（資安事件）之處理應建立一致及有效作法，以作為事故改善依據，包含事件之調查、處理以及相關通報。本案中負責海底電纜之關鍵基礎設施提供者，若於資安管理法通過後，除平時應訂定、修正及實施資通安全維護計

[6] 國家通訊傳播委員會 100 年 4 月 6 日通傳技字第 10043006740 號令。

畫，以及按其資安責任等級辦理相關應辦事項外，遇資安事件時亦應妥善進行事件之處理，並為通報，使相關機關知悉該資安事件。

●A.17.2.1　維持資訊處理基礎設施可用性

(1)標準內容：　應對資訊處理措施實施充分之多重備援，以符合可用性要求。

(2)適用說明：　組織應就針對其資訊設施維持多重備援機制，以因應不可預見之事故、侵害發生時，使資訊設施仍得以正常運作，不致影響組織運作。本案中負責海底電纜之關鍵基礎設施提供者，如平時備有相關備援之機制，例如與其他組織合作備援計劃等，應可盡可能降低所受障礙之衝擊。

類別：資訊保護【案號：S10610】

## 中繼站轉接、竄改來電號碼　半年騙上千萬

### 【焦點話題】

林男涉嫌以每個月 4 萬租金，在台灣設立詐欺中繼站，做為詐欺集團的跳板，林嫌先向美國承租伺服器頻寬和群呼群發系統，再轉租給泰國詐欺集團話務機房使用，於泰國撥話時，台灣的中繼站會將該電話號碼，竄改為中國大陸公安單位之號碼，再佯裝中國大陸公安單位進行詐騙。因其等藉由中繼站為跳板，使得中國大陸公安難以追緝，而轉向我國請求協助，我國警方經調查後，一舉破獲於泰國設置機房、我國設置電話中繼站之犯罪手法，共逮捕嫌犯 11 名。

【參考資料來源：TVBS 新聞網，106/3/1】

### 【重點摘要】

1. 跨國詐騙集團分工精細使偵查追緝困難，為有係遏阻相關非法行為，刑法規定，該類案件縱於國外發生者仍適用刑法之處罰規定。
2. 如係組織因故意或過失違反個人資料保護法之規定，導致個人資料外流，而使詐騙集團得以利用，進而造成當事人損失時，流出資料之組織可能需要負擔新台幣 2 億元或相關損害所涉利益之損害賠償責任。

### 【法律觀點】

近年來詐欺案件頻傳，且趨於集團化、組織化，甚至結合網路、電信、通訊科技，準此，刑法第 339-4 條第 3 項[1]訂有詐欺罪之加重事由，將利用廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而為詐欺時，提高刑罰至 1 年以上 7 年以下有期徒刑，得併科 100 萬元以下罰金。此外若

[1] 刑法第 339-4 條略以：「犯第三百三十九條詐欺罪而有下列情形之一者，處一年以上七年以下有期徒刑，得併科一百萬元以下罰金：…三、以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯之。…」。

此類案件涉及跨國情事者，可能造成民眾財產鉅大損害與危害國家形象等情形，為維護我國之國際形象，並對於該類跨境加重詐欺案件，賦予我國司法機關有優先的刑事管轄權，以符合民眾對司法之期待[2]，按刑法第 5 條[3]有關於我國領外犯罪者適用我國刑法之規範項目，亦包含利用廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而為詐欺之加重詐欺罪。

此外，如因組織違反個人資料保護法之規定，因故意或過失導致個人資料外流，而使詐騙集團得以利用而造成當事人損失時[4]，發生資料外流者因此可能需要負擔新台幣 2 億元或相關損害所涉利益之損害賠償責任[5]。

**【管理 Tips】**

如組織因故意或過失違反個人資料保護法之規定，導致個人資料外流，而使詐騙集團得以利用而造成當事人損失時，組織負有損害賠償責任，而是否具有故意或過失，應由組織提出證據主張，因此組織在進行蒐集、處理或利用個人資料時，應建立相關管理制度以合理且有效管理所取得之個人資料，諸如蒐集、處理與利用流程，並針對運用過程為紀錄，其目的在於：一、使成員進行個人資料運用時得據以為之；二、使組織如涉訴訟時得以舉證避免損害賠償之產生。

**【相關標準】**

ISO 27001：2013（CNS 27001）

●A.7.2.2　資訊安全認知、教育及訓練

(1)標準內容：　組織所有員工及相關之承包者，依組織所建立政策及程序施行資訊安全事宜。

[2] 刑法第 5 條，105 年 11 月修正理由。

[3] 刑法第 5 條略以：「本法於凡在中華民國領域外犯下列各罪者，適用之：…十一、第三百三十九條之四之加重詐欺罪。」。

[4] 個人資料保護法第 29 條。

[5] 個人資料保護法第 28 條。

(2)適用說明： 若組織對其員工等平時均舉行包含相關詐騙應注意之事項等之有效教育訓練，應可降低組織成員受詐騙而導致相關損失之風險。

●A.12.4.1 事件存錄

(1)標準內容： 應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。

(2)適用說明： 組織平時對於其內部之文件流程以及異常紀錄等相關資訊、文件，應妥善留存與保管，並定期進行檢核。本案中，如組織留有使用者活動、相關文件流動等之紀錄，於發生資訊外洩遭詐騙集團使用時，即可作為相關責任釐清之佐證。

●A.18.1.3 紀錄之保護

(1)標準內容： 應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。

(2)適用說明： 依照個人資料保護法規定，組織對於個人資料檔案，採取適當安全措施，防止遭竊取、竄改、毀損、滅失或洩漏。本案中，組織對於其所持有或保管之個人資料等資訊，宜將相關文件流動等紀錄完整保存，未來若面臨訴訟時，可為相關責任釐清之佐證。

類別：資訊保護【案號：S10611】

## 波音誤洩3.6萬員工個資，自家DLP資料保護軟體未發揮效用

### 【焦點話題】

全球航太大廠波音公司(Boeing)發現有員工將含有 3.6 萬名員工個資之試算表檔案，郵寄給其非 Boeing 員工之配偶。Boeing 隱私長於提交予華盛頓州檢察總長之信件中表示，該名員工並不知道該文件中包含相關機敏個資，因為這些機敏個資都被以隱藏欄位之方式處理，而 Boeing 已針對該名員工與其配偶之電腦進行檢查，亦採取必要措施以確保相關個資未遭他人取得。有關資料外洩防護(Data Loss Prevention, DLP)部分，儘管 Boeing 的確在公司內部大量部署 DLP 軟體─Categorize, Identify and Programmatically extract Hidden Entities and Resolve(CIPHER)，卻僅針對保密層級高之產品相關資料強制執行 DLP 政策，而未成功防堵員工個資流出。

【參考資料來源：iThome，106/2/23】

### 【重點摘要】

1. 按個人資料保護法（下稱個資法）之規定，組織保有個資檔案者，應採行適當之安全措施，防止個資被竊取、竄改、毀損、滅失或洩漏。
2. 按勞動基準法之規定，雇主僱用勞工人數在 30 人以上時，組織必須訂立包括員工所應遵守紀律之工作規則並報主管機關核備。
3. 除非當事人有反對之意思表示，否則不論勞工是否知悉工作規則之存在及其內容，工作規則當然成為僱傭契約內容之一部，如因未遵守工作規則導致組織損失，員工對組織負有損害賠償責任。

### 【法律觀點】

按個資法第 2 條規定，得以直接或間接識別該個人之資料均屬於個資[1]，對於

[1] 個人資料保護法第 2 條第 1 款：「一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、

個資之蒐集、處理必須符合法定要件，且原則不得為特定目的外之利用。而當組織未針對其保有之個資採行適當之安全措施，導致資料被竊取、竄改、毀損、滅失或洩漏時，則可能負有行政[2]及民事[3]等相關責任。

因此，為確保對於所保有個資之保護，以及避免因資料或技術外流造成相關損失，組織應於考量成本與風險後，建立適當且有效之個資管理制度，並將該制度納入員工工作規則。有關員工工作規則，按勞動基準法第 70 條[4]之規定，雇主僱用勞工人數在 30 人以上時，組織必須訂立包括員工所應遵守之紀律之工作規則並報主管機關核備。而臺灣高等法院 106 年勞上易字第 17 號民事判決表示，雇主訂定規範員工之工作條件之工作規則，既為雇主為統一工作條件及服務規律所訂定，除非當事人有反對之意思表示外，當然成為僱傭契約內容之一部。因此，對個人而言，於組織工作必須遵守工作規則，如因為未遵守工作規則導致組織損失，則為違反僱傭契約致組織受有損害，對組織負有損害賠償責任。

本案中，該員工因希望配偶能幫忙調整試算表檔案的格式，而郵寄出含有員工個資之試算表檔案至組織外部，顯非對於該個資蒐集之特定目的內利用，屬違反個資法之個資非法利用，縱使尚未造成損害，組織亦可依工作規則對該員工進行處置。

## 【管理 Tips】

組織對所持有資料，如員工資料、客戶資料或營業祕密等重要資訊，均應分

---

護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」。

[2] 個人資料保護法第 48 條第 4 款：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：…四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」。

[3] 個人資料保護法第 29 條第 1 項略以：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」。

[4] 勞動基準法第 70 條第 5 款：「雇主僱用勞工人數在三十人以上者，應依其事業性質，就左列事項訂立工作規則，報請主管機關核備後並公開揭示之：五、應遵守之紀律。」。

級管控，而為避免資料外洩，應該從內而外加以防護，相關措施諸如防毒軟體、AD 權限等內部防護，以及避免外部威脅侵入之防火牆等均屬之。惟相關防護措施均應配合有效之管理制度，方可降低因人為疏失導致系統失效之風險。

因此，組織應將各類資訊予以分級管控，定義所要保護之資訊，並且針對該等資訊可能會被洩漏之情況，設定管控流程，以及訂定工作規則，使人員作業時有所依循。其次，宜透過保密條款以及競業禁止條款，避免人員故意將資訊洩漏；並透過教育訓練以及定期內、外部稽核等方式，以降低人為過失導致資料外洩之可能。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.9.1.2　對網路及網路服務之存取

(1)標準內容：　應僅提供予使用者存取其已被特定授權使用之網路及網路服務。

(2)適用說明：　組織可透過權限設定之方式，限制使用者得使用之網路服務。本案如限制使用者僅能在特定環境及對象使用外部寄信功能，則帶有員工個資之檔案亦無法進行傳輸，則可有效防止資料外洩之風險。

●A.7.2.2　資訊安全認知、教育及訓練

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

(2)適用說明：　組織應透過諸如教育訓練等方式，確保其員工、外包廠商於平時即妥善瞭解組織之相關政策及程序等規範。若本案之組織平時均有對人員進行教育訓練，確保相關員工瞭解

資安之重要性，對於因人員過失所造成之個資等敏感資訊外洩情況之發生風險，應可有效降低。

類別：資訊保護【案號：S10612】

## 美國政府下令禁用俄跨國公司卡巴斯基實驗室之軟體

### 【焦點話題】

美國政府下令所有聯邦機構禁止使用俄羅斯跨國電腦安全公司卡巴斯基實驗室（Kaspersky Lab）生產的軟體。

根據法新社報導，由於當局認為卡巴斯基與俄羅斯情報機構有關係，而這種危險將威脅美國國家安全，因此美國國土安全部代理部長杜克( Elaine Duke ) 下令所有聯邦機構在 90 天內將卡巴斯基受人歡迎的反駭客軟體移除，並且以其他軟體取代。

【參考資料來源：中央社，106/9/14】

### 【重點摘要】

1. 政府機關辦理資訊服務採購時，如所涉及之業務屬於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」，招標單位應將經濟部投資審議委員會公告之陸資資訊服務業者，列為禁止參與之對象。
2. 行政院公共工程委員會公告之資訊服務採購契約範本，除禁止經公告之陸資資訊服務業者參與「具敏感性或國安（含資安）疑慮之業務範疇」之資訊服務採購外，此類採購案之分包廠商亦不得為上述經公告之陸資資訊服務業，且相關廠商如於履約期間被列入上述業者名單時，機關得因此終止或解除契約。

### 【法律觀點】

政府採購法之立法目的在於提升採購效率與功能，確保採購品質[1]。因此機關辦理採購時，得依實際需要，設定投標廠商之基本資格，且如為特殊或巨額

[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。」。

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。

完善的資訊設備是政府日常運作或維護國家安全所必要的，因此行政院公共工程委員會為免發生國安或資安疑慮，限制機關在辦理資訊服務[3]採購時，如所涉及之業務屬於經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」，應將經濟部投資審議委員會公告之陸資資訊服務業者列為禁止參與之對象，並於招標文件載明[4]。行政院公共工程委員會並修正資訊服務採購契約範本，於契約範本中明文規定前開陸資資訊服務業亦不得為上述敏感業務之分包商[5]，且廠商如於履約期間因股權或資本額變動而被列入上述陸資業者名單時，機關更得因而終止或解除契約[6]。

而目前經濟部投資審議委員會所公告「具敏感性或國安（含資安）疑慮之業務範疇」[7]包括能源類、水資源類、通訊傳播類、交通類、金融與銀行類、緊

---

[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] 機關委託資訊服務廠商評選及計費辦法第 3 條：「本法第二十二條第一項第九款所稱資訊服務，指提供與電腦軟體或硬體有關之服務；包括整體規劃、系統整合、系統稽核、系統管理、網路管理、軟體開發、軟體驗證、軟體維護、硬體維護、硬體操作、機房設施管理、備援服務、網路服務、顧問諮詢、資料庫建置、資料處理、資料登錄或訓練推廣等服務。」故當涉及軟體開發、軟體驗證、軟體維護時，均屬於政府採購法所稱之資訊服務。

[4] 行政院公共工程委員會工程企字第 10400024610 號函釋：「機關辦理資訊服務採購，如屬經濟部投資審議委員會公告『具敏感性或國安(含資安)疑慮之業務範疇』，於招標文件載明不允許經濟部投資審議委員會公告之陸資資訊服務業者參與，屬投標廠商資格與特殊或巨額採購認定標準第 4 條第 1 項第 6 款規定情形。」。

[5] 資訊服務採購契約範本第 8 條第 6 項第 1 款後段：「本採購如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」，廠商不得以經濟部投資審議委員會網站公告之陸資資訊服務業者為分包廠商。」。(106 年 7 月 13 日版本)

[6] 資訊服務採購契約範本第 18 條第 1 項第 15 款：「(一)廠商履約有下列情形之一者，機關得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失：…15.本採購如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」，廠商於履約期間因股份或資本額變動而成為經濟部投資審議委員會網站公告之陸資資訊服務業者。」。(106 年 7 月 13 日版本)

[7] http://web.moi.gov.tw/psu/files/news/20152393255I3-01%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

急救援與醫院類、中央政府與地方機關與科技園區與工業區中被選定之重要系統，其中包括許多重要資通系統。

綜合上述可知，目前我國政府機關進行資訊服務採購時，均需確認所採購項目是否屬上述能源類等經濟部投資審議委員會所公告「具敏感性或國安(含資安)疑慮之業務範疇」，如屬之，則須於招標文件載明，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。換言之，我國政府機關採購資訊服務，當涉及採購軟體開發及其後續維護時，亦有如同案例所示之基於國安理由而限制特定國家廠商參與採購之情形。

## 【管理 Tips】

現代社會分工細膩，組織在建置資訊系統時，常必須委託外部供應商協助辦理，但資安供應商之穩定性與可靠度甚為重要，因此組織應建立選商標準，必要時並進行相關之背景調查，汰除不合適之廠商；再者，並應評估組織對於資訊系統可接受風險，並藉由風險分析，判斷對於資訊系統之需求，以確保資安供應商之服務可達到組織所需之資訊安全要求。除於締約前之選商，於雙方合作階段，組織亦應透過契約與供應商議定雙方之責任義務，而契約裡關於資訊安全注意事項，可參考行政院公共工程委員會所提出之資訊服務採購契約範本關於資訊安全責任的內容[8]來加以約定。

分析上述範本所載內容可知，組織在與供應商約定資訊安全責任時，應要求

---

%E6%A5%AD%E5%8B%99%E7%AF%84%E7%96%87.pdf，具敏感性或國安(含資安)疑慮之業務範疇。

[8] 資訊服務採購契約範本第 16 條第 19 項：「(十九)資訊安全責任：1.廠商應遵守行政院所頒訂之各項資訊安全規範及標準，並遵守機關資訊安全管理及保密相關規定。此外機關保有對廠商執行稽核的權利。2.廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。3.契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄。4.廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。5.廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。6.廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合機關對系統品質及資訊安全的要求。7.廠商如違反第 1 目至第 6 目規定，應適用第 15 條之違約責任，並就機關所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。」( 106 年 7 月 13 日版本 )

其遵守組織之資安管理規範及保密規定;此外組織應保留對廠商之稽核權利，並要求廠商在向組織繳交資料之前，應先確認該資料之安全性。其他如：契約履約或終止後之物件返還、留存執行紀錄、服務提供者之資安事件處理、組態管理以及違反契約之損害賠償責任等，均宜在雙方契約約定內容之列；透過契約規範，使雙方對於工作內容有所依循，避免發生權責不明的狀態。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.7.1　聘用前

(1)標準內容：　確保員工及承包商瞭解其將承擔之責任，且適任其角色。

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

類別：資訊保護【案號：S10613】

## 不滿遭攔查 警方：依法行使職權

### 【焦點話題】

兩位民眾在台北轉運站一樓大廳，遭到 4 名員警攔查，要求出示身分證明文件。其中一位因不服攔查，遂於現場向警方表示，警方應該要見到民眾有犯罪行為，才可以臨檢，否則即屬違反憲法。對此，警方回應，依警察職權行使法，只要警察合理懷疑民眾有犯罪嫌疑，或於符合一定要件時，即有查證民眾身分的權利，若民眾拒絕，依該法之規定，亦可以將民眾帶回警局，進行身分確認[1]；不過此次執勤中，警方並未將二人帶回警局或強制要求出示身分證件。警方強調，該地為警方重點盤查地帶，也是核定的巡邏場所，過往就在此地查獲多起攜毒或是通緝罪犯，此次也屬一般的例行盤查，並無不法。

【參考資料來源：蘋果日報，106/3/19】

### 【重點摘要】

1. 如臨檢場所係受警察機關主管長官指定之公共場所、路段及管制站等地點，則不需有其他合理懷疑或犯罪情事即可臨檢並查證路經民眾之身分，惟此地點之指定應以防止犯罪，或處理重大公共安全或社會秩序事件而有必要之情形為前提。
2. 民眾若不同意接受臨檢時，得當場陳述理由，表示異議，並要求警方開立「實施臨檢盤查（身分查證）民眾異議紀錄表」，以作為日後透過行政爭訟釐清爭議時之證明。

### 【法律觀點】

警察職權行使法之立法目的在於保障人民權益，維持公共秩序，保護社會安

[1] 警察職權行使法第 7 條第 2 項：「依前項第二款、第三款之方法顯然無法查證身分時，警察得將該人民帶往勤務處所查證；帶往時非遇抗拒不得使用強制力，且其時間自攔停起，不得逾三小時，並應即向該管警察勤務指揮中心報告及通知其指定之親友或律師。」。

全[2]，而維護整體公共秩序時，或有影響個人權益之可能，尤其如以臨檢方式進行，因其對人或物之查驗、干預，影響人民自由、財產及隱私權等甚鉅，因此大法官透過釋字第 535 號解釋限縮臨檢此等執行勤務方式，該號解釋認為「警察人員執行場所之臨檢勤務，應限於已發生危害或依客觀、合理判斷易生危害之處所、交通工具或公共場所為之。」

釋字第 535 號解釋亦促成了警察職權行使法於 92 年修正時，將臨檢要件明文化[3]，限縮僅在符合下列要件時，方得進行臨檢：一、合理懷疑其有犯罪之嫌疑或有犯罪之虞者。二、有事實足認其對已發生之犯罪或即將發生之犯罪知情者。三、有事實足認為防止其本人或他人生命、身體之具體危害，有查證其身分之必要者。四、滯留於有事實足認有陰謀、預備、著手實施重大犯罪或有人犯藏匿之處所者。五、滯留於應有停(居)留許可之處所，而無停(居)留許可者。六、行經指定公共場所、路段及管制站者。

其中行經指定公共場所、路段及管制站者，係指受警察機關主管長官指定之公共場所、路段及管制站，此時則不需有其他合理懷疑或犯罪情事即可任意臨檢。惟仍須注意指定該場所時，亦應以防止犯罪，或處理重大公共安全或社會秩序事件而有必要之情形為前提；如非因上開情形而指定，則據以指定合理事由即不存在，此時對公共場所、路段及管制站之指定即應認為屬於無效之指定，故不可於此任意臨檢。

本案警察係於上述受指定之公共場所進行臨檢，而考量車站常為犯罪發生場所，因此該指定應屬合理，即警方可任意臨檢，然仍宜於臨檢前先行說明，避免造成民眾誤解；民眾若不同意接受臨檢時，得當場陳述理由，表示異議，

---

[2] 警察職權行使法第 1 條：「為規範警察依法行使職權，以保障人民權益，維持公共秩序，保護社會安全，特制定本法。」。

[3] 警察職權行使法第 6 條：「警察於公共場所或合法進入之場所，得對於下列各款之人查證其身分：一、合理懷疑其有犯罪之嫌疑或有犯罪之虞者。二、有事實足認其對已發生之犯罪或即將發生之犯罪知情者。三、有事實足認為防止其本人或他人生命、身體之具體危害，有查證其身分之必要者。四、滯留於有事實足認有陰謀、預備、著手實施重大犯罪或有人犯藏匿之處所者。五、滯留於應有停（居）留許可之處所，而無停（居）留許可者。六、行經指定公共場所、路段及管制站者。前項第六款之指定，以防止犯罪，或處理重大公共安全或社會秩序事件而有必要者為限。其指定應由警察機關主管長官為之。警察進入公眾得出入之場所，應於營業時間為之，並不得任意妨礙其營業」。

並要求警方開立「實施臨檢盤查（身分查證）民眾異議紀錄表」，以作為日後透過行政爭訟釐清爭議時之證明。

**【管理 Tips】**

警察於實施臨檢盤查時，會涉及到個人資料在何種情況下必須提供，應提供之內容，提供時後續又應如何處理等等議題。民眾在面臨臨檢時，為確認是否為合法臨檢，可請警察出示證件，並請其告知臨檢原因，如果無法證明其身分或拒絕告知臨檢原因時，民眾可以拒絕接受臨檢[4]。其次，民眾若不同意接受臨檢時，得當場陳述理由，表示異議，要求警方開立「實施臨檢盤查（身分查證）民眾異議紀錄表」，並得作為行政爭訟時之證明。

而組織如欲蒐集個人資料或是其他營業所需資訊時，其判斷是否可予蒐集之流程亦相同，包括蒐集是否符合法規或契約規定，所蒐集之內容為何，如被蒐集者對於資料蒐集有疑義時之處理方式，而被蒐集者應注意是否依法或依契約需提供，以及蒐集者嗣後應如何使用該資訊，以保障權益。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.18.1.1　適用之法規及契約的要求事項之識別

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

(2)適用說明：　主管機關應識別出法規所要求之政策據以遵守，並應瞭解其中蘊含意義，使成員能清楚知悉並依法規作為，以本案而言，如員警能清楚向民眾闡述法規內容及依據時，應可

[4] 警察職權行使法第 4 條「警察行使職權時，應著制服或出示證件表明身分，並應告知事由。警察未依前項規定行使職權者，人民得拒絕之。」。

提高民眾的配合意願。

類別：資訊保護【案號：S10614】

# 惡男密錄散布性愛影片 遭判刑3月

## 【焦點話題】

鄧男與林女交往期間，偷拍兩人性愛影像私藏，但兩人關係交惡後，鄧男竟將影像上傳到林女微信帳號相簿內。林女直到友人告知後才發現此事，氣憤提告。警方隨即前往鄧男住處搜索，查扣隨身碟 3 只、筆記型電腦 1 部、密錄筆 2 支、用以上傳檔案之行動電話 1 支。鄧男坦承犯行，法官認為鄧男所為，損及林女名譽，有害社會善良風氣，實有可議，雖考量雙方於偵訊時達成和解，但仍判刑 3 月。

【參考資料來源：臺灣新北地方法院 105 年簡字第 7007 號刑事判決】

## 【重點摘要】

1. 電磁紀錄特性之一，在於其透過電腦複製之指令，可以輕易進行複製，且每一個複製出的電磁紀錄，與原始電磁紀錄幾無二致，並可以被輕易地散布，資料外洩風險會高於普通紙本，使用者必須特別注意。
2. 組織於建置適當的資訊安全管理系統時，必須將機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)等資訊安全三要素納入考量，以為良好的資訊安全管理。

## 【法律觀點】

男女交往時濃情蜜意，有時會拍攝私密照片留存紀念，而在數位時代，照片通常係以手機或數位相機等設備拍攝，而成為以電磁紀錄形式存在之數位相片。電磁紀錄特性之一即在其可透過電腦複製之指令，輕易進行複製，且透過網路更可以輕易地散布這些影像。

因為數位相片較實體相片更易於傳播，導致近年來出現愈來愈多因當事人一時不慎或是遭他人陷害，而使得私密照片、影片被公開於網站上供人下載的新聞事件。如不考量雙方是否達成和解等與犯行本身無關之因素，類似本案

鄧男以工具偷錄與他人性愛影片之行為，實已嚴重侵害被害人之隱私權[1]；依刑法第 315-1 條第 2 款[2]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，可處 3 年以下有期徒刑、拘役或 30 萬元以下罰金。而若嗣後又散布這些因竊錄而得之私密影像，因惡性更為重大，依刑法第 315-2 條第 3 項[3]的散布竊錄之非公開活動內容罪規定，最高可處 5 年以下有期徒刑。

**【管理 Tips】**

網際網路發展迅速，且雲端硬碟與電子郵件容量幾乎可說是無上限。；而通訊網路早已由 3G 演化至 4G，更即將邁入 5G 時代，不論是手機、智慧手錶或數位相機等數位產品，多標榜可與業者的雲端設備結合，而可自動將所記錄、拍攝或錄像結果備份至雲端，不論是所攝得影像、個人位置、生活習慣、健康狀況以及私密紀錄，在有意無意間均可能被上傳至網路。因此個人所使用之數位裝置或雲端硬碟若未經良好管控，又或使用者設定有誤，將大幅提高發生資料外洩的風險。

故若組織決定以雲端硬碟或聯網設備來儲存、備份組織之資料時，應先瞭解所備份內容、頻率以及使用之設備品質或雲端硬碟環境等事項；建議可使用資訊安全的三要素加以判斷是否適合，亦即以機密性(Confidentiality)；完整性(Integrity)；可用性(Availability)加以判斷。就機密性而言，應針對資訊性質判斷是否所有資訊都適合以外部雲端硬碟備份；就完整性而言，應針對資料備份之頻率、回覆可能性等面向加以評估；就可用性而言，則可思考雲端服務中斷之回復時效，並與服務提供者建立及議定所有相關資訊安全要求事項，使服務提供者知悉與踐行所應遵循之規範。

---

[1] 刑法第 315-1 條立法理由：「未得他人同意而任意以工具偷窺或偷錄他人隱私部位，已侵害個人隱私權，如有製造或散布之行為，影響尤為嚴重，應有處罰必要，為避免此種行為是否構成犯罪之疑義，於各款之行為客體增訂「身體隱私部位」以杜爭議。」。

[2] 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。」。

[3] 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。」。

**【相關標準】**

ISO27001：2013(CNS27001)

●A.8.2.1 資訊之分級

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

(2)適用說明： 組織或個人於使用雲端設備時，應先行就資訊性質分級，並判斷是否適合以外部雲端硬碟備份，本案中所傳送之私密照片於分級上應屬重要性之敏感資料。

●A.15.1.2 於供應者協議中闡明安全性

(1)標準內容： 應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。

(2)適用說明： 組織使用雲端設備，則應與其建立及議定所有相關資訊安全要求事項，以確保服務提供者知悉所應遵循規範並遵守之。

類別：資訊保護【案號：S10615】

## 證券商遭網路攻擊 金融主管機關要求加強資安防範

### 【焦點話題】

106 年 2 月爆發國內首次駭客對證券商威脅進行網路攻擊事件，並要求券商須支付折合新台幣約 17 萬元至 30 萬元不等的比特幣。金融主管機關表示，網路駭客是採取「分散式阻斷服務攻擊」（DDOS），導致證券商對外網頁頻寬滿載，投資人無法正常網路下單。對此，金融主管機關指出遭到網路攻擊的證券商已立即向警方報案處理；由於駭客是用 DDOS 來癱瘓或阻礙業者網路系統，因此，也要求業者向電信廠商申請流量清洗，讓網路下單能正常使用。此外，金融主管機關亦已擬具因應 DDOS 攻擊之措施予業者參考，且將全部證券期貨業者之網站納入監看，以提早通知業者因應，隨時與業者保持密切聯繫以瞭解下單是否正常。

【參考資料來源：自由時報電子報，106/7/6，106/8/14】

### 【重點摘要】

1. 駭客常透過分散式阻斷服務攻擊進行攻擊，以耗盡被攻擊者網路資源及系統資源，達到癱瘓特定網站之目的，藉此勒索被攻擊者獲得利益，造成經濟上嚴重損害。
2. 金融機構辦理電腦系統資訊安全評估辦法要求金融機構建構評估計畫依資訊資產之重要性及影響程度進行分類，定期或分階段辦理資訊安全評估作業。

### 【法律觀點】

依據刑法第 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。」其立法理由[1]即說明係因近年來分散式阻斷服務攻擊

[1] 刑法第 360 條立法理由二：「鑒於電腦及網路已成為人類生活之重要工具，分散式阻斷攻擊(DDOS)或封包洪流(PingFlood)等行為已成為駭客最常用之癱瘓網路攻擊手法，故有必要以刑法保護電腦及網路設備之正

等手法，愈來愈常出現於癱瘓網路攻擊，破壞電腦及網路設備運作情形，而新增該條規定。透過分散式阻斷服務攻擊進行攻擊時，以耗盡被攻擊者網路資源及系統資源，達到癱瘓特定網站之目的，當被攻擊者受到干擾而無法正常操作其電腦時，即已達成干擾電腦或其相關設備之結果，而屬該條之涵攝範圍。又刑法第 4 條規定：「犯罪之行為或結果，有一在中華民國領域內者，為在中華民國領域內犯罪。」是以，只要犯罪之駭客發動攻擊時所在地或被入侵的電腦所在地或網站架設地有一發生在我國，皆屬我國刑法得處罰之對象。

本案中，駭客是用分散式阻斷服務攻擊癱瘓證券商業者網路系統，造成證券商對外網頁頻寬滿載，投資人無法正常網路下單，已造成損害證券商以及投資人之損害，且駭客要求支付比特幣，除涉及刑法第 360 條無故以電腦程式干擾他人電腦罪外，亦有觸犯刑法第 346 條恐嚇罪之問題。

## 【管理 Tips】

金融機構在建置或執行資安管理制度時，所必須注意事項者眾，因此銀行商業同業公會全國聯合會，為確保金融機構提供電腦系統均具有符合一定標準之基本系統安全防護能力，於 106 年 2 月修正發布「金融機構辦理電腦系統資訊安全評估辦法」，希冀透過各項資訊安全評估作業，發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力[2]。

該辦法要求金融機構依照評估辦法建構評估計畫，將資訊資產依其重要性及

---

常運作，爰增訂本條。又本條處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為，為避免某些對電腦系統僅產生極輕度影響之測試或運用行為亦被繩以本罪，故加上「致生損害於公眾或他人」之要件，以免刑罰範圍過於擴張。」。

[2] 金融機構辦理電腦系統資訊安全評估辦法第 1 點：「壹、前言 為確保金融機構提供電腦系統具有一致性基本系統安全防護能力並遵循中華民國銀行商業同業公會全國聯合會制訂之『金融機構資訊系統安全基準』及『金融機構辦理電子銀行業務安全控管作業基準」，擬透過各項資訊安全評估作業，發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力，訂定本辦法。」。

影響程度區分為三類[3]，定期或分階段辦理資訊安全評估作業[4]；並依 PDCA 管理循環[5]，先完成各項資訊安全評估作業，區分電腦系統重要性以進一步安排定期評估，並針對評估結果提出電腦系統資訊安全評估報告，據以進行缺失改善，以及定期追蹤複查。

組織如欲防範或處理類似於本案金融機構所面對之資安攻擊事件時，亦可如金融機構一般，透過建立資通安全檢查機制、設置資安通報系統及資訊分享等方式，加強資訊安全防護措施，以有效降低事故發生時之損害。

**【相關標準】**

ISO27001：2013(CNS27001)

●A.8.2.1 資訊之分級

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

(2)適用說明： 金融機構辦理電腦系統資訊安全評估辦法要求金融機構依個別電腦系統所涉服務的資訊重要性加以區分，並對電腦系統進行不同等級之安全性評估。

●9 績效評估

(1)標準內容： 組織應評估資訊安全績效及資訊安全管理系統之有效性。

[3] 金融機構辦理電腦系統資訊安全評估辦法 3 點。

[4] 金融機構辦理電腦系統資訊安全評估辦法第 2 點第 1 項：「貳、評估範圍一、金融機構應就整體電腦系統（含自建與委外維運）依據本辦法建構一套評估計畫，基於持續營運及保障客戶權益，依資訊資產之重要性及影響程度進行分類，定期或分階段辦理資訊安全評估作業，並提交『電腦系統資訊安全評估報告』，辦理矯正預防措施，並定期追蹤檢討。」。

[5] PDCA 管理循環（Plan-Do-Check-Act）指針對工作按規劃、執行、查核與行動來進行活動，金融機構辦理電腦系統資訊安全評估辦法中亦以此方式進行操作，包括該辦法第 2、3、4 點為進行評估規劃，第 5 點為實際操作演練，第 6 點為進行評估，第 7 點則必須針對評估事項提出改善辦告，藉此確保系統持續維運，並進而持續改善。

(2)適用說明： 金融機構辦理電腦系統資訊安全評估辦法，要求金融機構應委由外部專業機構或由金融機構內部單位進行安全評估，提交「電腦系統資訊安全評估報告」，評估辦理矯正預防措施，並藉由金融機構定期追蹤檢討，以評估其資安情況，即屬此標準之體現。

類別：資訊保護【案號：S10616】

## 中國網軍 轉攻擊我關鍵基礎設施

### 【焦點話題】

包括中國在內的網路駭客，對我政府、民間重要建設的惡意網路攻擊未曾停歇；根據國安主管機關今年度預算內容指出，依所建置的資通安全防禦系統偵測統計，在 105 年 1 至 6 月間，國安主管機關對外網路或公開網站，遭受駭客攻擊次數高達 17659 次，幸虧即時成功偵測與阻絕，未發生駭客成功入侵事件。資安業者發表的報告亦指出，一度被認為是全球資訊安全主要威脅來源之一的中國駭客，其網路攻擊活動有了顯著改變，相關攻擊事件次數已經明顯減少；但這不代表中國網路威脅消除，因為這些攻擊的精準度與有效度，都較過去更高。

【參考資料來源：自由時報報，106/1/17】

### 【重點摘要】

1. 犯罪之行為或結果，有一發生在我國時，即有我國刑法適用之餘地，因此，無論是本國人或外國人，如透過網路攻擊以侵害我國之關鍵基礎設施，由於其結果係發生於我國，仍得以刑法相繩。
2. 與外國開戰或將開戰期內，透過網際網路毀壞橋樑、鐵路等交通運輸之關鍵基礎設施，所犯者為外患罪，較承平時期之妨害公眾往來安全罪為重。

### 【法律觀點】

資訊科技於國家安全領域扮演的角色日益重要，除了各國政府積極研究以資訊科技提升整體軍事戰力外，因發動資訊攻擊的危險性遠小於傳統攻擊，因此網路遂成為另一個戰場。我國於 106 年 6 月 29 日，將資電作戰指揮部升格為「資通電軍指揮部」，亦即俗稱之第四軍種，希冀得以提昇國家整體資訊戰爭能力。

依據我國刑法第 4 條[1]，犯罪之行為或結果，有一發生在我國時，即有我國刑法適用之餘地，因此如透過網路攻擊以侵害我國之關鍵基礎設施，由於其結果係發生於我國，故有我國刑法之適用。如於承平時期，透過網際網路，對交通運輸之關鍵基礎設施加以破壞，造成鐵公路損壞或壅塞，係觸犯刑法第 185 條[2]妨害公眾往來安全罪，但如與外國開戰或將開戰期內，將要塞、軍港、軍營、軍用船艦、航空機及其他軍用處所建築物，與供中華民國軍用之軍械、彈藥、錢糧及其他軍需品，或橋樑、鐵路、車輛、電線、電機、電局及其他供轉運之器物，交付敵國或毀壞或致令不堪用者，則可能觸犯刑法第 107 條[3]外患罪，其刑度非前述妨害公眾往來安全罪可比。

**【管理 Tips】**

面對國安等級之網路攻擊，政府單位會考量關鍵基礎設施重要性，建立對於外部網路攻擊時之處理方式，透過整合政府機關間對於攻擊時安全維護權責，使機關間建立分工機制，並整合民間技術和能力，以達成全民聯防的目的；其次亦會加強培育資通人才、強化臺灣資安產業的發展，以提升對關鍵基礎設施之資安防護能力。

就組織角度而言，面對網路攻擊，應提出有效之經營與應對策略並定期調整，避免因外部威脅導致系統潰敗；而組織內應建立適當權責分工機制，當資安事故或類似本案之外部威脅事件發生時，組織成員便能處變不驚的依據各自分工進行處理與應對；另組織亦應定期舉辦資訊安全相關教育訓練，使自身所應遵守之安全規範內化為組織文化的一部分，以提升組織成員對於資訊安

[1] 刑法第 4 條：「犯罪之行為或結果，有一在中華民國領域內者，為在中華民國領域內犯罪。」。

[2] 刑法第 185 條第 1 項：「損壞或壅塞陸路、水路、橋樑或其他公眾往來之設備或以他法致生往來之危險者，處五年以下有期徒刑，拘役或五百元以下罰金。」。

[3] 刑法第 107 條第 1 項：「犯前條第一項之罪而有左列情形之一者，處死刑或無期徒刑：一、將軍隊交付敵國，或將要塞、軍港、軍營、軍用船艦、航空機及其他軍用處所建築物，與供中華民國軍用之軍械、彈藥、錢糧及其他軍需品，或橋樑、鐵路、車輛、電線、電機、電局及其他供轉運之器物，交付敵國或毀壞或致令不堪用者。二、代敵國招募軍隊，或煽惑軍人使其降敵者。三、煽惑軍人不執行職務，或不守紀律或逃叛者。四、以關於要塞、軍港、軍營、軍用船艦、航空機及其他軍用處所建築物或軍略之秘密文書、圖畫、消息或物品，洩漏或交付於敵國者。五、為敵國之間諜，或幫助敵國之間諜者。」。

全的敏感度；此外，組織亦可與外部資安單位合作，以彌補組織資安專業上不足之處。

**【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： 組織應建立有效之經營與應對策略，並對策略定期進行調整，藉以確保具有完整且可用的網路，以保護資訊系統及應用，避免遭到攻擊時影響到涉及資訊系統之關鍵基礎設施，以降低發生危害結果的可能性。

類別：資訊保護【案號：S10617】

## 整形診所洩密　數百女性豐胸裸照曝光

### 【焦點話題】

澳洲雪梨一家知名整型整所將其來自澳洲各地數百名的顧客資料，存儲在診所網站的公共索引工具，其中除包含約 500 名女性客戶的姓名、住址、病例等資料外，還有客戶的術前體檢表，以及豐胸前後的對比圖與私密照等，造成隱私受害的女性感到崩潰，覺得遭受侵犯。

【參考資料來源：蘋果日報，106/6/4】

### 【重點摘要】

1. 醫師、律師等專業技術人員其執行業務時，多會涉及當事人之隱私，法律亦多要求此類人員對所執行業務負有保密義務。
2. 保密義務亦有其界線，如有正當理由，必要時專業技術人員並非不得揭露保密內容。

### 【法律觀點】

包括醫師、律師等專業技術人員，通常會被法律賦予高於一般人之責任，其主要原因在於「信任」，當信任關係不存在時，所破壞不僅是單一專業人員與其客戶間之關係，更會動搖民眾對醫療或法律專業整體制度的信任。因此，為建立民眾對於專業技術人員的信任，一般多會透過法律規範，要求專業技術人員對因業務知悉的祕密事項負擔一定程度的保密義務。

以醫師為例，醫師法第 22 條[1]與 23 條[2]規定，因業務知悉之病情或健康資訊，原則僅在受有關機關詢問或委託鑑定時，方得提供。亦即，原則上醫師不得洩露病人資訊，違反者處新臺幣 2 萬元以上 10 萬元以下罰鍰[3]。而醫療機成員

[1] 醫師法第 22 條：「醫師受有關機關詢問或委託鑑定時，不得為虛偽之陳述或報告。」。

[2] 醫師法第 23 條：「醫師除依前條規定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩露。」。

[3] 醫師法第 29 條前段：「違反第 11 條至第 14 條、第 16 條、第 17 條或第 19 條至第 24 條規定者，處新臺幣

[4]、護理人員[5]、藥師[6]、職能治療師[7]、醫事檢驗師[8]、呼吸治療師[9]亦均有因業務而知悉他人之秘密之禁止洩漏規定。相同的，律師法[10]授權全國律師聯合會所訂定之律師倫理規範第 33 條，亦規定律師對於受任事件內容應嚴守秘密，非經告知委任人並得其同意，不得洩漏[11]。

不過保密義務亦有其限制，專業人員因業務上獲得之秘密，並非完全不得揭露。事實上，醫事相關規定多以「不得無故洩露」為保密義務之界線，如有正當理由亦得於必要時揭露[12]。

本案如發生於我國，其雖非專業人員違反保密義務之情形，然醫療機構將病人豐胸前後的對比圖、私密照片及手術前填寫的體檢表於網路上公開揭露，亦已違反醫療法第 72 條，得處新臺幣 5 萬元以上 25 萬元以下罰鍰[13]，且可能須負擔民事侵權行為之損害賠償責任。

---

2 萬元以上 10 萬元以下罰鍰。」。

[4] 醫療法第 72 條：「醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩漏。」。

[5] 護理人員法第 28 條:「除依前條規定外，護理人員或護理機構及其人員對於因業務而知悉或持有他人秘密，非依法、或經當事人或其法定代理人之書面同意者，不得洩漏。」。

[6] 藥師法第 14 條：「藥師對於因業務而知悉他人之秘密，不得無故洩漏。」。

[7] 職能治療師法第 31 條：「職能治療師、職能治療生或職能治療所之人員，對於因業務而知悉或持有他人之秘密，不得無故洩漏。」。

[8] 醫事檢驗師法第 32 條：「醫事檢驗師、醫事檢驗生或醫事檢驗所之人員，對於因業務而知悉或持有他人之秘密，不得無故洩漏。」。

[9] 呼吸治療師法第 16 條：「呼吸治療師對於因業務而知悉或持有他人之秘密，不得無故洩漏。」。

[10] 律師法第 15 條第 2 項：「全國律師公會聯合會應訂立律師倫理規範，提經會員代表大會通過後，報請法務部備查。」。

[11] 律師倫理規範第 33 條：「律師對於受任事件內容應嚴守秘密，非經告知委任人並得其同意，不得洩漏。但有下列情形之一，且在必要範圍內者，得為揭露：一、避免任何人之生命、身體或健康之危害。二、避免或減輕因委任人之犯罪意圖及計畫或已完成之犯罪行為之延續可能造成他人財產上之重大損害。三、律師與委任人間就委任關係所生之爭議而需主張或抗辯時，或律師因處理受任事務而成為民刑事訴訟之被告，或因而被移送懲戒時。四、依法律或本規範應揭露者。」。

[12] 護理人員法之規定較其他相類似醫事人員略有不同，護理人員法第 28 條於 104 年修正時之立法理由一稱「『護理人員法』對於『病歷隱私權』之保護規範採行概括性的『不得無故洩露』，所謂『無故』，一般係指『無正當理由』;反之『有正當理由』即可揭露資訊，儼然為病歷資訊的流動開了一道不容易清楚掌握的門。」以此明定僅在法令規定或經當事人或其法定代理人之書面同意時方得揭露，亦即限縮揭露要件。

[13] 醫療法第 103 條第 1 項第 1 款：「有下列情形之一者，處新臺幣五萬元以上二十五萬元以下罰鍰：一、違反…第七十二條…。」。

## 【管理 Tips】

現代社會隱私意識高漲，許多人尋求服務時都會將自己的隱私是否能被妥善保護納入考慮。相對的，為保護當事人隱私權，專業技術人員於其入職或提供服務時，也多會被要求簽署保密協議，並負有保密義務。而組織在聘用此類需接觸當事人隱私之專業技術人員時，因其職業守則已有規範，通常會給予較高之自主性，惟為保障組織權益，仍應與專業技術人員簽訂保密協議，使人員瞭解自身所負之責任與義務。

組織如屬擁有大量當事人敏感資料的專業機構，除應將當事人隱私資料當作組織機密予以保護外，為落實保護，更需要制定一系列完善管理制度，包含個資蒐集、處理及利用的流程，或是個資外洩事件通報處理流程等，以避免當事人隱私外洩，或因此衍生其他更嚴重的損害。

## 【相關標準】

ISO27001：2013(CNS27001)

●A.8.2.1 資訊之分級

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

(2)適用說明： 資料因其屬性不同，其重要性就會有差異；就本案而言，客戶健康資料除係屬組織營運之必要資產，更事關客戶之私密資訊，應認定為最高或較高等級之資料。

●A.9.1.1 存取控制政策

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

(2)適用說明： 組織應明確定訂定存取控制政策，視需要針對不同業務內容建立不同等級的存取控制政策以加以控管，藉以規範組

織內部可以觸及到機敏資料的人員,避免不必要的人員擁有過多的權限，造成機敏資料外洩的風險。

●A.13.2.4 機密性或保密協議

(1)標準內容： 應定期審查並文件化保密協議,以反映組織對機敏資訊保護的要求。

(2)適用說明： 針對具有機密性之文件,組織應與可能接觸者建立保密協議,並定期審查保密協議內容,確保符合實際狀況以及具備應有之要求。

類別：資訊保護【案號：S10618】

## Windows 10「默默蒐集」個資 遭怒控侵犯隱私

### 【焦點話題】

荷蘭資料保護局(The Dutch Data Protection Authority, DPA)調查發現，微軟未明確告知 Windows 10 用戶，當系統為預設設定時，其將透過網路瀏覽器 Edge 持續不斷蒐集有關 app 使用、網路瀏覽行為等個資。而微軟也未明確告知使用者有關該公司處理何種資料以及其蒐集之目的，且亦未提供有效方式使用戶同意該公司處理其等之個資。

惟微軟認為荷蘭相關機關之認定，並未正確反映出 Windows 10 之資料保護措施，惟仍會繼續與荷蘭相關機關合作，以找出適當之解決方案。

【參考資料來源：中央社，106/10/15】

### 【重點摘要】

1. 按個人資料保護法 ( 下稱個資法 ) 之規定，組織於蒐集個人資料時，原則應告知諸如組織名稱、蒐集目的、利用時間、地區、對象、方式、當事人權利及行使方式以及不提供個資之權益影響等事項。
2. 按個人資料保護法施行細則之規定以及相關主管機關之函釋，為達到「明確告知」之目的，蒐集者應以個別通知之方式使當事人知悉或可得知悉告知內容之方式，始屬具確實告知。

### 【法律觀點】

個人資料之蒐集涉及當事人之隱私權益，為使當事人明知其個人資料被何人蒐集及其蒐集之目的等資訊，個資法規定除有免為告知之法定情形外[1]，組織於蒐集個人資料時，應告知當事人諸如蒐集目的、蒐集資料類別、個人資料

[1] 個人資料保護法第 8 條第 2 項：「有下列情形之一者，得免為前項之告知：一、依法律規定得免告知。二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。三、告知將妨害公務機關執行法定職務。四、告知將妨害第三人之重大利益。五、當事人明知應告知之內容。」。

利用之期間、地區、對象及方式、當事人權利及行使方式以及不提供個資之權益影響[2]等相關事項，俾使當事人能知悉其個人資料被他人蒐集之情形。

而為使當事人能確實知悉上開事項，蒐集者必須以使當事人能以知悉之方式對其進行告知程序，諸如言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之[3]。法律主管機關曾補充指出，個資法第 8 條之告知義務，並未要求當事人須簽署相關文件，亦未限制不得與其他文件（例如契約）併同為之，惟為達到「明確告知」之目的，蒐集者仍應以個別通知之方式使當事人知悉，不得僅以單純擺設（張貼）公告或上網公告之概括方式為之，而須足以使當事人知悉或可得知悉該公告內容之方式始屬之[4]。

本案若發生於我國，按我國個資法以及其施行細則與主管機關之函釋，對於個人資料之蒐集，除有依法律規定、告知將妨害公共利益、當事人明知應告知內容等法定免為告知之情形，原則應先為告知，而應告知而未違者，經限期改正，而切其未改正者，由中央目的事業主管機關或直轄市、縣（市）政府按次處新臺幣二萬元以上二十萬元以下罰鍰[5]。

## 【管理 Tips】

個人資料保護法通過後，對當事人進行告知義務之判斷流程應可簡化為下列幾點：

---

[2] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」。

[3] 個人資料保護法施行細則第 16 條：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」。

[4] 參見法務部法律字第 10603509640 號函。

[5] 個人資料保護法第 48 條略以：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：一、違反第八條或第九條規定。」。

一、是否為個人資料：當組織所蒐集的資料並非屬於個人資料時，即不負有個資法上之告知義務，當然也不需要進行告知；二、雖是個資，是否排除個資法適用：個資法規定，自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料，以及於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，均排除個資法之適用，因此如所蒐集之資料為上開二者，亦不需進行告知；三、是否有免告知事由：當組織於蒐集個資時，有免告知之法定情形時，亦不須進行告知；四、告知內容：由於不具免為告知之情形，因此組織必須對當事人進行告知，此時組織必須斟酌所告知內容不應過於概括，以符合「明確告知」之要件[6]；五、告知方式：應以個別通知之方式使當事人知悉。組織在進行個人資料蒐集時，如可確實依上開流程進行管理，應可避免發生違反個資法的情形。

**【相關標準】**

ISO 29100：2011（CNS29100）

●5.2 同意及選擇

(1)標準內容： 堅持同意原則，意指下列事項。

- 向 PII 當事人表明，以選擇是否允許處理其 PII，除非 PII 當事人無不同意之自由，或所適用法律允許無須該自然人同意即可處理 PII。PII 當事人之選擇必須是自由提供、特定且基於充分理解。
- 取得 PII 當事人選擇加入之同意以蒐集或其他方法處理敏感 PII，除非適用之法律允許無須該自然人同意下處理敏感之 PII。
- 於取得同意前，通知 PII 當事人關於其在個人參與及存

[6] 參見法務部法律字第 10203503280 號函。

取原則下之權利。

- 於取得同意前，向 PII 當事人提供以公開、透明及告知原則所表明之資訊。
- 向 PII 當事人解釋給予或不予同意之涵義。

宜制定條款，提供機會讓 PII 當事人選擇如何處置其 PII，及允許 PII 當事人方便且免費撤回同意。此要求宜依隱私權政策辦理。即便撤回同意，PII 控制者可能需持有某些 PII 一段時間，以便遵循法律或契約義務（例：資料持有、可歸責性）。無須同意，即可依法處理 PII 時，宜儘可能告知 PII 當事人。當 PII 當事人有撤回同意之能力並選擇撤回時，除非法律強制，不宜為任何目的處理該 PII。

對 PII 控制者而言，堅持選取原則，意指下列事項。

- 對 PII 當事人就有關其 PII 處理在蒐集、初次利用或爾後適用時，儘快提供清楚、明確、易懂、可取得及可負擔之機制，以便其行使選擇及給予同意。
- 實作 PII 當事人於其同意中表達之取捨。

此外，可定義於同意以外（例：合約績效，PII 當事人及其重要之利益、或法律之遵循）處理 PII 當事人及其重要之利益之額外條款。某些實例中，適用之法律規定 PII 當事人之同意並不構成得以處理 PII 之充分法律基礎（例：未成年者在無父、母或監護人許可下，所給之同意）。此外，PII 之國際傳輸需考量額外之要求事項。於處理或傳輸資料前，遵循上述額外條款係 PII 控制者之責任。

(2)適用說明：　以當事人同意之方式蒐集個人資料，原則上必須對當事人進行告知義務，而告知事項的公開以及透明，可以使當事

人更容易的接受相關資訊。本案即係組織於蒐集當事人相關資料前，應先告知之蒐集之行為等事項，方得為資料之蒐集。

類別：資訊保護【案號：S10619】

## App浮濫蒐集個資 消保主管機關將進行整頓

### 【焦點話題】

消保主管機關表示，目前許多行動裝置 App，蒐集個資時僅具「同意」與「不同意」之選項，並未區分必要或非必要資訊，而消費者若勾選「不同意」，即不能進行下載，此類模式與個資法規定精神不符，將以針對與民生相關之四大類 App 為優先，採取分階段作法進行整頓，先以輔導之方式，由各主管機關與相關業者溝通、並進行輔導，而 App 蒐集資料亦須區分「必要」及「非必要」，若涉及蒐集「非必要資料」者，App 宜就該等事項予以特別說明，並提供消費者是否同意提供該項「非必要資料」之選項。

另中央主管機關亦要求業者建立自律機制及儘速完備相關管理規範，以及督促業者於發布前，檢視 App 所需權限應與所提供之服務相當，以利綜合評估是否符合已善盡個人資料保護法之告知義務，並強化消費者之個人資料保護。

【參考資料來源：聯合新聞網，106/3/10】

### 【重點摘要】

1. 按個人資料保護法( 下稱個資法 )之規定，關於個資之蒐集、處理、利用，必須符合「誠信原則」、「必要性原則」、「不當連結禁止原則」三大原則，以保護民眾之人格法益。
2. 消費者下載 App 時，與 App 開發者間建立了買賣契約，原則上僅能基於履行買賣契約事務之特定目的及要件之必要範圍內，蒐集、處理或利用個人資料；若 App 開發者蒐集超越必要範圍之個人資料時，將可能違反消費者之「隱私合理期待」。

### 【法律觀點】

根據我國個人資料保護法之規定，個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯[1]，亦即關於個資蒐集、處理、利用，必須符合「誠信原則」、「必要性原則」、「不當連結禁止原則」三大原則，以保護民眾之人格法益。

然而近年行動應用軟體（Mobile Application, 下稱 App）蓬勃發展下，大量蒐集使用者興趣、習慣等資訊以供行銷等大數據利用之技術，幾乎遍佈於各式 App。更有甚者，許多 App 軟體之主要獲益來源，並非其服務本身，而是背後之個人資料蒐集及利用。正因如此，為了大量獲取使用者個資，許多 App 安裝前之定型化服務約款，會刻意模糊蒐集個資類別之範圍以及未來如何利用等[2]，甚至技術性地透過條款複雜化等方式，使用戶直接略過條款內容而逕為同意。以媒體撥放器為例，若 App 服務本身僅係單純提供影音播放服務，但蒐集個資時卻刻意蒐集用戶手機內與影音播放無關之通訊錄內容，作為業者推播參考，則可能違反前述「必要性原則」、「不當連結禁止原則」；而刻意透過條款複雜化等技術性方式，意圖使用戶不予充分審閱服務約款，則可能有違「誠信原則」。

個資法規主管機關曾就職業計程車之計費表內建 APP 程式衍生功能，強制蒐集、處理或利用計程車駕駛人之可直接或間接識別特定個人資料一事，表示意見，因職業駕駛人係直接向製造商購買計費表，與計費表製造商間具有買賣契約關係，若計費表製造商於計費表中內建 APP 之衍生功能，有強制蒐集、處理或利用計程車駕駛人之行車軌跡、營業收入、錄影錄音等可直接或間接識別特定個人之資料之可能，此一個人資料之蒐集行為，尚難認與計費表買賣契約間具有正當合理之關聯，已逾越買賣契約特定目的之必要範圍，則該

[1] 個人資料保護法第 5 條。

[2] 請參照個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」。

計費表製造商對於該等資料之蒐集、處理或利用，顯違反計程車駕駛人之「隱私合理期待」，而與個資法第 5 條、第 19 條之規定有違[3]，值得參考。

綜上所述，本案所提之相關 App 業者對於個資之蒐集與利用，除蒐集前應先行告知消費者外，於利用時，亦不得超出蒐集目的範圍，若有違法之情事，而屆期未改正者，由中央目的事業主管機關或直轄市、縣（市）政府處以罰鍰。

**【管理 Tips】**

為提升 App 資安品質與產品競爭力，主管機關為建構 App 基本資安自主檢測體系，提供業界開發 App 自主遵循之參考，於 106 年 3 月正式公告「行動應用 App 基本資安規範 V1.1」、「行動應用 App 基本資安檢測基準 V2.1」與「行動應用 App 基本資安自主檢測推動制度 V3.0」等編修文件，並另新增「行動應用 App 安全開發指引 V1.0」[4]，共 4 份文件，鼓勵業者自主管理。上開要求雖非強制規定，不過其內容係由資安、法制與認證領域專家共同編撰，並收納產官學研之各界建議而訂定，可作為 App 開發者所遵循之依據。

App 開發者依上開文件之要求，在開發過程中，應留意避免 App 過度蒐集不必要之個人資料；技術上也不可在未告知用戶並取得其同意下，設計 App 於背景運作中任意蒐集用戶之個資[5]。此外，App 之授權條款有關蒐集用戶之個資應先取得用戶之同意，且告知用戶有拒絕之權利，並承諾使用於所聲明之用途內；不同行動應用程式間亦應取得用戶同意後始得分享個人資料[6]。設計

[3] 參見法務部法律字第 10503505850 號函。

[4] https://www.mas.org.tw/news_detail.php?id=38，行動應用資安聯盟新聞稿，（最後瀏覽日：106 年 10 月 29 日）。

[5] 行動應用 App 安全開發指引 V1.0　3.1.4.敏感性資料蒐集(D) CPD-06:應依 CPD-03 實作行動應用 App 存取敏感性資料權限，不要授與過度蒐集不必要敏感性資料權限或於未告知使用者取得同意前於行動應用 App 背景運作蒐集敏感性資料活動。

[6] 行動應用 App 基本資安規範 V1.1　4.1.2.1.敏感性資料：蒐集行動應用程式應於蒐集敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。4.1.2.3.敏感性資料儲存：…行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途。4.1.2.5.敏感性資料分享：行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

之 App 倘有蒐集「非必要資料」之情形，應特別說明蒐集該資料之目的，及不提供將對用戶造成之影響，再由用戶選擇是否同意提供。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●14.2.1 保全開發政策

(1)標準內容： 應建立軟體及系統開發之規則，並應用至組織內之開發。

(2)適用說明： 行動裝置上網佔有率已超越桌機，諸多廠商亦將軟體開發主力轉至 APP 開發，而開發者可依據主管機關所提供之開發 APP 相關資安規範，建立自己的 APP 開發規則，使所開發之 APP 符合法規要求。

ISO 29100：2011（CNS29100）

●5.2 同意及選擇

(1)標準內容： 堅持同意原則，意指下列事項。

- 向 PII 當事人表明，以選擇是否允許處理其 PII，除非 PII 當事人無不同意之自由，或所適用法律允許無須該自然人同意即可處理 PII。PII 當事人之選擇必須是自由提供、特定且基於充分理解。
- 取得 PII 當事人選擇加入之同意以蒐集或其他方法處理敏感 PII，除非適用之法律允許無須該自然人同意下處理敏感之 PII。
- 於取得同意前，通知 PII 當事人關於其在個人參與及存取原則下之權利。
- 於取得同意前，向 PII 當事人提供以公開、透明及告知

原則所表明之資訊。

- 向 PII 當事人解釋給予或不予同意之涵義。

宜制定條款，提供機會讓 PII 當事人選擇如何處置其 PII，及允許 PII 當事人方便且免費撤回同意。此要求宜依隱私權政策辦理。即便撤回同意，PII 控制者可能需持有某些 PII 一段時間，以便遵循法律或契約義務（例：資料持有、可歸責性）。無須同意，即可依法處理 PII 時，宜儘可能告知 PII 當事人。當 PII 當事人有撤回同意之能力並選擇撤回時，除非法律強制，不宜為任何目的處理該 PII。

對 PII 控制者而言，堅持選取原則，意指下列事項。

- 對 PII 當事人就有關其 PII 處理在蒐集、初次利用或爾後適用時，儘快提供清楚、明確、易懂、可取得及可負擔之機制，以便其行使選擇及給予同意。
- 實作 PII 當事人於其同意中表達之取捨。

此外，可定義於同意以外（例：合約績效，PII 當事人及其重要之利益、或法律之遵循）處理 PII 當事人及其重要之利益之額外條款。某些實例中，適用之法律規定 PII 當事人之同意並不構成得以處理 PII 之充分法律基礎（例：未成年者在無父、母或監護人許可下，所給之同意）。此外，PII 之國際傳輸需考量額外之要求事項。於處理或傳輸資料前，遵循上述額外條款係 PII 控制者之責任。

(2)適用說明：　以當事人同意之方式蒐集個人資料，原則上必須對當事人進行告知義務，而告知事項的公開以及透明，可以使當事人更容易的接受相關資訊。本案即係 App 於蒐集當事人相關資料前，應先告知之蒐集之行為等事項，方得為資料

之蒐集。

類別：資訊保護【案號：S10620】

## 旅行社個資外洩 民眾遭詐騙近 20 萬元

### 【焦點話題】

某旅行社傳遭駭客入侵，竊取旅客購買機票、訂房或自由行訂單資料，業者內部統計，共約 36 萬筆銷售資料恐遭外洩，其可能涵蓋旅客姓名、聯絡電話和購買商品內容。業者表示，已向警方報案，並請外部專業資安防護顧問公司協助提升資訊防護，提升加密等級。刑大科偵組調查發現詐騙集團先以佯稱該旅行社客服人員，說明因作業疏失，誤將帳戶設定重複扣款，需被害人協助取消並通知銀行協助處理，隨後，被害人會接到銀行來電，要求前往 ATM 操作查詢餘額並按指示轉帳，以此手段進行詐騙。

【參考資料來源：聯合新聞網，106/5/24】

### 【重點摘要】

1. 按個人資料保護法 ( 下稱個資法 ) 組織於發生個資外洩事件時，應通知當事人之內容，包括侵害之事實及已採取之因應措施，如組織為特許行業時，更應通知當事人其所採取之因應措施及所提供之諮詢服務專線。
2. 按個資法施行細則，個資外洩事件之通知方式，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式，且如果費用所需過鉅時，亦得考量技術之可行性及當事人隱私之保護後，以適當公開方式通知。

### 【法律觀點】

近年來個資外洩事故頻傳，當組織違反個資法規定，導致相關事故發生時，為免損害擴大，個資法即要求該組織應查明後，以適當方式通知當事人[1]。故組織於違反個資法致個資外洩時之通知，所應作為之事項有二，首先，應查

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

明事件相關事項，而在事件查明後，組織則可採諸如言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式，以及若通知費用所需過鉅時，亦得考量技術之可行性及當事人隱私之保護後，以網際網路或新聞媒體等適當方式[2]，通知當事人個人資料被侵害之事實及已採取之因應措施[3]，此外若組織屬特許行業者，除前二項應通知之項目，須另外通知「所提供之諮詢服務專線」[4]。

就本案而言，依據「旅行業管理規則」規定[5]，旅行業領有執照方得經營，並應專業經營，以公司組織為限，屬特許行業之類，並按旅行業個人資料檔案安全維護計畫及處理辦法，以及參照前述特許行業所需另外通知之事項，該旅行社應將個資外洩之事實、所採取之因應措施及所提供之諮詢服務專線，通知受影響之當事人。

**【管理 Tips】**

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

---

[2] 個人資料保護法施行細則第 22 條第 1 項：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。」

[3] 個人資料保護法施行細則第 22 條第 2 項：「依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。」

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

[5] 旅行業管理規則第 3 條第 4 項：「前三項業務，非經依法領取旅行業執照者，不得經營。」第 4 條：「旅行業應專業經營，以公司組織為限；並應於公司名稱上標明旅行社字樣。」

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.16.1.2 通報資訊安全事件

(1)標準內容： 應循適切之管理管道，儘速通報資訊安全事件。

(2)適用說明： 資安事件、事故發生時，儘速透過適當窗口通報予相關單位、主管機關，以降低事件、事故發生之衝擊。本案如於發現個資外洩後儘速通報予主管機關，並將相關內容一併通知當事人，應可有效降低個資外洩所造成之損害風險。

類別：資訊保護【案號：S10621】

## 人為疏失 Verizon六百萬客戶資訊被披露

### 【焦點話題】

軟體安全公司 UpGuard 今年 6 月告知 Verizon 公司，其供應商尼斯系統(Nice Systems)洩漏該公司數百萬客戶包含安全密碼等資訊。主因在於尼斯系統員工將客戶個人資訊儲存在雲端存儲區(Cloud storage area)時之錯誤指令，導致未經授權者可逕自進入雲端存儲區，而取得計約 600 萬名客戶之相關資訊。消費者權益組織─公共知識(Public Knowledge)亦提出「電信公司有義務保護使用者的個人資訊，應確保他們的員工、承包商和業務夥伴在處理敏感客戶資料時，採取適當的安全措施。」

【參考資料來源：大紀元時報，106/7/14】

### 【重點摘要】

1. 按個人資料保護法施行細則 ( 下稱個資法施行細則 ) 之規定，組織進行委外蒐集、處理或利用個人資料時之監督管理責任包括：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間；二、受託者之安全維護措施；三、複委託之受託者；四、違法時之通知義務及補救措施；五、保留指示事項；六、委託關係終止或解除時資料刪除銷毀。
2. 按個人資料保護法 ( 下稱個資法 ) 之規定，組織若違反個資法之規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，應自負舉證其無故意或過失，否則負有損害賠償責任( 舉證責任倒置 )，委外辦理時，組織則必須要求受委託者提出無故意或過失之證明以免除其責任。

### 【法律觀點】

業務委外時，如因受委託者導致資訊外流時，委託方將直接受到損害，個資法第 4 條[1]明文，受委託者視同委託者負同一責任，有關賠償責任部分，按個

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

資法第 29 條第 1 項[2]規定，除組織能證明無故意或過失外，必須對遭受資料外洩之當事人為損害賠償（舉證責任倒置）。準此，在進行業務委外時，組織應對委外廠商進行確實之監督。而個資法施行細則第 8 條[3]規定，組織進行委外蒐集、處理或利用個人資料時所必須進行之監督管理責任，監督內容包括：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間；二、受託者之安全維護措施；三、複委託之受託者；四、違法時之通知義務及補救措施；五、保留指示事項；六、委託關係終止或解除時資料刪除銷毀，且委託者應定期確認受託者執行之狀況，並將確認結果記錄。

再者，因個資法對於民事損害賠償責任如前所述，採取舉證責任倒置，亦即如組織委託他人蒐集、處理或利用個人資料時，發生個人資料遭不法蒐集、處理、利用或其他侵害當事人權利之情形，組織必須要求受委託者提出無故意或過失之證明以免除相關責任。本案情形如發生於我國，在受委託者之受雇人有過失時，因視同受委託者負同一責任，故當事人可向委託者或受委託者請求其損害賠償[4]。而委託者若遭求償時可再依內部關係對受委託者進行求

[2] 個人資料保護法第 29 條第 1 項：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

[3] 個人資料保護法施行細則第 8 條：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

前項監督至少應包含下列事項：

一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

二、受託者就第十二條第二項採取之措施。

三、有複委託者，其約定之受託者。

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

五、委託機關如對受託者有保留指示者，其保留指示之事項。

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

第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

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

[4] 個人資料保護法第 28 條略以：「被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。　　依前二項情形，如被害人不易或不能證明其實際損害額時，得請求

償。

**【管理 Tips】**

組織於考量是否要進行委外時，主要考量者乃係節省成本、核心業務與否、資源之運用、或為獲得獨立及專業人士之專業服務等。因此，進行管控時仍應以上開項目為參考指標。

首先，對於是否委外，應考量組織之何種業務為核心業務，以及各該業務適合委外與否，如為核心業務則委外時就應詳細評估委外風險，又或法令有無限制、簽署之契約是否禁止委外。在決定委外業務後，必須建立流程並管理之，而管理流程則宜包含委外業務之合作對象、工作內容、契約期程、服務地點、以及其他等必要事項。

其次，進行委外管理時，應指派專案經理，通常為委外廠商合作負責人，透過組織內部人員對委外廠商進行監督與審查,以確保委外作業符合管理規範，並定期審視、調整嗣後委外業務之作法。

最末，組織應定期確認執行狀況之紀錄，其功能在於與受委託者間權利義務關係，如因可歸責於受委託者之事由，導致個人資料外洩、被竊或竄改等情事，前開紀錄對於責任釐清將有一定程度幫助，且組織更可另行約定懲罰性違約金，盡量減低企業擔負委託機關之法律責任。

**【相關標準】**

ISO 27001：2013(CNS 27001)

---

法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。　　對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。　　同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。　　第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」

●A.12.4.1 事件存錄

(1)標準內容： 應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。

(2)適用說明： 組織對於日常之各項活動均應產生紀錄並妥適保存之，以及確認相關紀錄具備定期審視，此有助於異常情形之適時發現，並作為相關事證之參照。若本案之相關公司均有遵照其所訂定之記錄保存規範，予以保存資訊之流通紀錄，並定期審查，應可提早發現資訊存取指令錯誤之情事，並降低所產生之風險。

●A.15.1.1 供應者關係之資訊安全政策

(1)標準內容： 應與供應者議定並文件化，降低與供應者存取組織資產關聯之風險的資訊安全要求事項。

(2)適用說明： 組織於委外業務時，應明確化雙方之權利義務，並將要求受委託者遵守一定規範，透過落實組織所要求之作業規範，可降低本案所發生風險。

類別：資訊保護【案號：S10622】

## 盜拷布袋戲上網分享 檢察官透過谷歌抓到大學生

### 【焦點話題】

檢察官接獲檢舉，有不法份子，違法重製盜版「大霹靂國際整合行銷股份有限公司」享有著作權之布袋戲影片，重製檔案後上傳至網路 Google 雲端，再經由論壇分享，供不特定人瀏覽觀看，經檢調機關調取犯罪嫌疑人使用之電腦 IP 位置，並向美國科高公司（Google Inc.）函查相關資料後，逮捕家住雲林的 19 歲郭姓男子，而其表示只是想與人分享，全案目前由檢察官深入追查中。

【資料來源：聯合報，106/9/7】

### 【重點摘要】

1. 按著作權法及民法相關規定，著作物之所有權係物權的一種，屬民法規定的範疇;著作權則屬無體財產權的一種，屬著作權法規定，二者並不相同，取得著作物之所有權不必然取得著作權。如著作人讓與著作物之所有權時，未同時讓與著作財產權者，則受讓人僅取得著作物之所有權，並未取得著作財產權，其著作財產權仍屬著作人享有。

### 【法律觀點】

著作權法所稱之著作指屬於文學、科學、藝術或其他學術範圍之創作[1]，亦即具有原創性，能具體以文字、語言、形像或其他媒介物加以表現而屬於文學、科學、藝術或其他學術範圍之創作，均係受著作權法所保護之著作[2]。而著作

[1] 著作權法第 3 條第 1 款：「本法用詞，定義如下：一、著作：指屬於文學、科學、藝術或其他學術範圍之創作。」

[2] 智慧財產法院 104 年度民著上字第 17 號民事判決：「按著作權法所保障之著作，係指屬於文學、科學、藝術或其他學術範圍之創作，著作權法第 3 條第 1 項第 1 款定有明文。是故，除屬於著作權法第 9 條所列之著作外，凡具有原創性，能具體以文字、語言、形像或其他媒介物加以表現而屬於文學、科學、藝術或其他學術範圍之創作，均係受著作權法所保護之著作。而所謂「原創性」，廣義解釋包括「原始性」及「創作性」，「原始性」係指著作人原始獨立完成之創作，而非抄襲或剽竊而來，而「創作性」，並不必達

物指著作所附著之物，可分為著作原件與著作重製物，著作原件[3]指著作首次附著之物，例如小說原稿、美術原畫、攝影原檔或錄音及電影母帶等，而著作重製物[4]，則指以印刷、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之物，如小說原稿印刷成冊、複製畫、將影像檔沖洗為實體照片，錄音及電影母帶之重製品。

著作權與著作物之所有權為二不同權利，著作權法係保護「著作權」，而非保護「著作物之所有權」。著作物之所有權係物權之一類，屬民法規定範疇，物的所有人於法令限制範圍內，有完全支配所有物之權利；著作權則屬無體財產權之一種，包括著作人格權（如公開發表權、姓名表示權）及著作財產權（如重製權、公開演出權、散布權）[5]。其中著作人格權[6]係專屬於著作人本身，不得讓與或繼承，而著作財產權則可以全部或部分轉讓[7]或授權他人行使[8]。因此，著作人讓與著作物（著作原件或其重製物）之所有權時，如未同時讓與著作財產權，則受讓人僅取得著作物之所有權，並未取得著作財產權，其著作財產權仍屬著作人享有[9]，受讓人不得任意行使包括重製權、公開演出權以及散布權等著作財產權。

本案中郭男將所購得之布袋戲影片予以重製後上網分享，但因其僅有著作物之所有權，並無著作財產權，依法不得任意重製分享，其行為已侵害造成重

---

於前無古人之地步，僅依社會通念，該著作與前已存在之作品有可資區別的變化，足以表現著作人之個性為已足。其次，創作須具備最低程度之創作或個性表現，始可受到保護，亦即該著作仍須具有最低限度之創意性，且足以表現著作個性或獨特性之程度，方屬著作權法所保護之著作，如其精神作用之程度甚低，不足讓人認識作者之個性，則不得為著作權之客體，即無保護之必要。」

[3] 著作權法第 3 條第 16 款：「原件：指著作首次附著之物。」

[4] 著作權法第 3 條第 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；或依建築設計圖或建築模型建造建築物者，亦屬之。」

[5] 經濟部智慧財產局電子郵件字第 1041013 號。

[6] 著作權法第 21 條：「著作人格權專屬於著作人本身，不得讓與或繼承。」

[7] 著作權法第 36 條第 1 項：「著作財產權得全部或部分讓與他人或與他人共有。」

[8] 著作權法第 37 條第 1 項：「著作財產權人得授權他人利用著作，其授權利用之地域、時間、內容、利用方法或其他事項，依當事人之約定；其約定不明之部分，推定為未授權。」

[9] 經濟部智慧財產局台(85)內著字第 8506850 號函釋。

製權之侵害，最重可處 3 年有期徒刑[10]，且依著作權法第 88 負損害賠償責任[11]。

**【管理 Tips】**

市售影片是受到著作權法所稱之著作重製物，當消費者購買相關影片時，僅購得著作物之所有權，著作財產權並未因為物權移轉而有所變更，因此組織於採購物件時，應確認其是否為著作物及其授權範圍，確保使用情形均為授權範圍內。

而如為組織出資聘請他人完成著作之情形，於契約中宜訂有授權條款，亦即將權利歸屬述明，確保著作權歸屬，避免發生組織雖得利用該著作，但因並未取得著作財產權，或使組織有權限對著作為適當合理之運用，導致組織無法享有重製、改作等權利[12]。組織並應定期盤點權利與授權範圍，可確保相關權利之使用情形均為授權範圍內。

**【相關標準】**

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之相關之法律、法令、法規及契約的要求事項。

(2)適用說明：　組織對於其所持有之諸如智慧財產權、產品使用權等相關權利，應知悉並於其作業規定中符合相關法令、契約等要求，確保權利之使用符合授權範圍，以避免違反相關法

[10] 著作權法第 91 條第 1 項：「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。」

[11] 著作權法第 88 條第 1 項前段：「因故意或過失不法侵害他人之著作財產權獲致版權者，負損害賠償責任。」

[12] 著作權法第 12 條：「出資聘請他人完成之著作，除前條情形外，以該受聘人為著作人。但契約約定以出資人為著作人者，從其約定。依前項規定，以受聘人為著作人者，其著作財產權依契約約定歸受聘人或出資人享有。未約定著作財產權之歸屬者，其著作財產權歸受聘人享有。依前項規定著作財產權歸受聘人享有者，出資人得利用該著作。」

規，以及契約要求之落實。

類別：資訊保護【案號：S10623】

## 駭客入侵出國登錄系統 外交機關公開致歉

### 【焦點話題】

外交機關日前進行安全查核時，發現有不明來源 IP 成功駭入數十個外館領務信箱，估算系統異常活動時間為近 3 個月，範圍涵蓋日本、英國、東南亞等，最多恐使 1.5 萬人之個資遭竊取，確切數量仍需進一步清查。外交機關表示經委請資安專家進行數位鑑識，已確認機關之護照簽證等主機未遭駭客入侵，受影響之資料僅限於出國登錄系統，其餘個人資料仍屬安全無虞，其次，本事件亦已進行事件通報，並辦理伺服器防護等級之提升，以及要求外館立刻更改信箱密碼等措施。

【參考資料來源：自由電子報，106/2/8】

### 【重點摘要】

1. 按個人資料保護法（下稱個資法）之規定，公務機關有指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏之義務。
2. 參考 CNS 29100 資訊安全個資管理國家標準，組織進行資料蒐集時，宜以資料最小化辦理之，此可降低資料遭不當使用時之風險。

### 【法律觀點】

政府機關對於所保有之資料，不論型態均有責任維護資料之機密性(Confidentiality)、完整性(Integrity)以及可用性(Availability)，而行政院亦定有行政院及所屬各機關資訊安全管理要點以及行政院及所屬各機關資訊安全管理規範，以推動各機關強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全、保障民眾權益協助政府各級機關建立安

全的網路應用環境[1]。

其次，按個資法第 18 條之規定，保有個人資料之公務機關，應指定專人辦理安全維護事項，以防止個人資料事故發生[2]，且該法施行細則亦要求前述專人應具有管理及維護個人資料檔案之能力，並足以擔任機關之個人資料檔案安全維護經常性工作[3]。而如公務員因故意或過失導致應祕密之資料外洩時，尚有可能觸犯刑法第 109 條[4]、第 110 條[5]或第 132 條[6]之規定。

本案機關已委請資安專家進行鑑識，確認相關主機未遭駭客入侵[7]，然若該機關未指派專人辦理安全維護事項，將直接違反個資法規定，如又因此導致事故發生而使他人產生損失，公務機關負有損害賠償責任[8]。

## 【管理 Tips】

持有大量個資之公務機關於維護公共利益與資料保護間之平衡須仔細衡量。

---

[1] 行政院及所屬各機關資訊安全管理要點第 1 條。

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

[3] 個人資料保護法施行細則第 25 條第 1 項：「本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。」

[4] 刑法第 109 條：「洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處一年以上七年以下有期徒刑。洩漏或交付前項之文書、圖畫、消息或物品於外國或其派遣之人者，處三年以上十年以下有期徒刑。前二項之未遂犯罰之。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。」

[5] 刑法第 110 條：「公務員對於職務上知悉或持有前條第一項之文書、圖畫、消息或物品，因過失而洩漏或交付者，處二年以下有期徒刑、拘役或一千元以下罰金。」

[6] 刑法第 132 條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。非公務員因職務或業務知悉或持有第一項之文書、圖畫、消息或物品，而洩漏或交付之者，處一年以下有期徒刑、拘役或三百元以下罰金。」

[7] 「領事事務局『出國登錄』系統出現異常活動事」新聞說明會紀要。網址：http://www.mofa.gov.tw/News_Content_M_2.aspx?n=70BCE89F4594745D&sms=700DE7A3F880BAE6&s=44159AB5579442EB（最後瀏覽日：106 年 10 月 22 日）。

[8] 個人資料保護法第 28 條第 1 項略以：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」

而資料保護，首在於蒐集時，是否僅蒐集所需之最小資料量。以本案為例，事發時「出國登錄」網站需登錄中英文姓名、出生年月日、登錄者身分、身分證字號、護照號碼、性別、出國目的、電話、電子信箱、在台住址、在台緊急聯絡人及與在台緊急連絡人之關係等資訊；而事發後，登錄項目已減少至中英文姓名、護照號碼、電話、電子信箱與緊急連絡人等內容，有關資料之蒐集範圍明顯縮小。

其次，公務機關指派專人進行資訊、資通安全管理有其必要，包括依政府機關（構）資通安全責任等級分級作業規定，各機關除資安管理規範外，更分層推動資訊安全管理，包括資訊系統分類分級，定期進行資安稽核、實施資安教育訓練等，以防範潛在資安威脅，降低風險產生之可能。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.13.1.2　網路服務之安全

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

(2)適用說明：　組織應確保無論是內部或外部服務，其所使用之網路已具備相關安全機制，以進行網路服務之管理與安全維護。本案之機關對於系統、資訊傳輸空間即應具備相關安全機制，以降低駭客攻擊成功造成資料外洩等資安事故風險。

●A.13.2.3　電子傳輸

(1)標準內容：　應適切保護電子傳輸時所涉及之資訊。

(2)適用說明：　組織應確保相關資訊透過電子方式傳輸時已具備相關安全機制。本案之機關利用電子方式傳輸相關資訊時應具備相關安全機制，以降低駭客攻擊成功造成資料外洩等資安事

故風險。

ISO 29100：2011（CNS29100）

●5.5　資料極小化

(1)標準內容：　資料極小化密切連結“蒐集限制”原則，但不僅如此。“蒐集限制”意旨被蒐集之有限資料與特定目的相關聯，而“資料極小化”則嚴格將 PII 之處理極小化。

堅持資料極小化原則，意指以下列方式設定及實作資料處理程序與 ICT 系統。

-將所處理之 PII、隱私權利害相關者及 PII 接露對象或可存取 PII 之人員的數目最小化。

-確保採用“僅知(need-to-know)”原則，亦即於 PII 處理之合法目的框架下，宜僅對執行正式職務所必要之人員賦予 PII 存取權限。

-使用或提供視為預設選項，只要不涉及 PII 當事人之識別的互動及交易，儘能降低其行為之可觀察性並限制所蒐集 PII 的可連結性。

-一旦 PII 處理之目的終止，無法定要求保有 PII，或是實務上需如此做時，即刪除或廢棄 PII。

(2)適用說明：　組織進行資料蒐集時，應採以資料最小化並予以分級，並在合法目的下揭露個別所需資料，可降低資料遭不當使用時之風險。本案於事件發生後，該機關已據此原則減量蒐集資料。

類別：資訊保護【案號：S10624】

## 被炒抓狂 研發副處長刪光公司5千筆檔案

### 【焦點話題】

新竹科學園區某公司簡姓研發副處長，因不滿遭公司資遣，雖知電腦內電磁紀錄乃公司所有，且屬公司之營業資料，仍安裝「SafeErase」資料清除軟體至筆電內，於安裝該軟體後接續操作，刪除電腦硬碟內與公司營業相關之研發專案檔案，並利用該軟體移除公司配發筆電內之 5 千餘筆營業檔案，才交還電腦。負責人懷疑簡男所歸還電腦檔案過少，委託業者檢查交還之硬碟有無異狀，方確認有變更硬碟檔案資料情事，始具狀向檢調依刑法「刪除他人電腦電磁紀錄」罪嫌，提出告訴。

【資料來源：自由電子報，105/10/25】

### 【重點摘要】

1. 按刑法之規定，破壞電磁紀錄罪之要件包括「無故」、「取得、刪除或變更」、「他人電腦或其相關設備之電磁紀錄」以及「致生損害於公眾或他人」。
2. 員工對於組織之資訊安全責任及義務，於僱傭關係結束後仍應有效。

### 【法律觀點】

電腦系統已成為當前各組織營運之重要工具，組織的電腦系統中都存有各式重要檔案，但若重要檔案被離職員工惡意刪除，將導致組織重大損失，因此刑法為了有效制止此類損壞他人電腦的惡劣行為，特在刑法中增訂第 36 章「妨害電腦使用罪」，其中第 359 條規定「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

分析破壞電磁紀錄罪，可分解為下列要件：第一個要件是「無故」，司法實

務上則認為「無正當理由」便是所謂「無故」；第二個要件是「取得、刪除或變更」，即本罪之行為部份，無論是自電腦中取得資料，或是使電腦中資料消失，又或是將電腦中原始資料予以更改，均屬破壞；第三個要件是「他人電腦或其相關設備之電磁紀錄」，所謂他人，即指非自己所有，而電腦或其相關設備之電磁紀錄[1]（包含以電子、磁性、光學或其他相類方式，存儲在電腦主機或相關設備之資料）；第四個要件是「致生損害於公眾或他人」，亦即造成公眾或他人之損害。

以本案而言，簡男擔任公司研發副處長，掌握研發資料，因為遭資遣即於未經授權之情況下，刪除電腦內之相關資料手腳，便是「無故」；而安裝資料清除軟體至筆電內，接續操作 4 次刪除電腦硬碟內與公司營業相關的研發專案檔案，並確認電腦內遭刪除檔案已無還原可能，已屬「刪除電磁紀錄」；既然電腦為公司提供予其做為業務上使用，則滿足「他人電腦或其相關設備」之要件；最末，其所刪除之資料包括研發專案檔案以及其他營業相關檔案，如果有因此造成公司之損害時，即可能構成前開罪名，不可不慎。

## 【管理 Tips】

資訊安全的保護除了從技術面著手外，對於人員的管理亦有一定程度的重要性。以 CNS 27001 資訊安全管理系統國家標準為例，其針對人力資源安全予以明確規範，包括聘僱前，應確保員工了解自身責任，且適任於其所被指派的角色；聘僱中應確保員工認知並履行其資訊安全的責任；聘僱終止與變更時，則是要確保組織利益未被侵害。雖然組織無法預期人員故意或過失行為發生時機，但其可以透過訂定相關補償措施以降低人員所帶來的風險，如：聘僱前應進行有效篩選、聘僱期間要求員工接受與其工作職務相關之認知宣導及教育訓練、簽訂契約時要求其於離職後仍受一定程度規範。

## 【相關標準】

[1] 刑法第 10 條第 6 款：「電磁紀錄係指稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」

ISO 27001：2013(CNS 27001)

●A.7.3.1　聘用責任之終止或變更

(1)標準內容：　應對員工及承包者定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。

(2)適用說明：　員工對於組織之資訊安全責任及義務，得於僱傭關係結束後仍應有效，本案簡男於離職後，仍對所掌握之研發資料負有保密義務。

類別：資訊保護【案號：S10625】

## 立委提案 患者有愛滋病須主動告知救護人員

### 【焦點話題】

日前一名救護技術員（EMT），於出勤時於救護車上，其傷口疑和傷患有血液接觸，然直到醫院通報才知該名病患染有愛滋，該消防機關遂行文中央衛生主管機關請示相關處置，中央衛生主管機關回應，現行法條規定中，愛滋病患者並不需主動告知救護人員其染有愛滋。準此，有立委提案，針對人類免疫缺乏病毒傳染防治及感染者權益保障條例第 12 條進行修正，規範愛滋感染者於醫療機構治療時，所應告知病情義務之對象，須包括救護車上之救護人員，同時也規定救護技術員不能因救護對象為愛滋病患，就不予以協助，藉此保障愛滋病患與救護人員雙方權益。

【參考資料來源：聯合報，106/6/25】

### 【重點摘要】

1. 為防止病毒感染、傳染之風險發生，人類免疫缺乏病毒感染者於就醫時應告知醫事人員，以及與他人進行危險性行為前應告知性行為對象，其已感染人類免疫缺乏病毒。

2. 按個人資料保護法之規定除依法律明文規定、具有適當安全維護措施履行法定義務必要範圍、當事人自行或其他合法公開之個人資料等法定要件，，各機關、人員不得蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，而有關人類免疫缺乏病毒感染者之姓名及病歷等有關資料亦屬前述之個人資料之一，對於該資料之蒐集、處理或利用亦應符合個資法之規定。

### 【法律觀點】

人類免疫缺乏病毒傳染防治及感染者權益保障條例之立法目的在於防止人類

免疫缺乏病毒之感染、傳染及維護國民健康，並保障感染者權益[1]。感染者本無義務告知他人，其已感染人類免疫缺乏病毒，惟為防止病毒感染、傳染之風險發生，有二種情況，感染者必須盡告知義務，第一、就醫時告知醫事人員[2]；第二、與他人進行危險性行為前，告知性行為對象[3]。就後者而言，係為確保國民健康，避免疾病擴散，就前者而言，其目的在於保障醫事人員權益，使醫事人員能對感染者之醫療特別注意，特別加強感染者之告知義務。

因此，感染者在就醫時，應向醫事人員告知其已感染人類免疫缺乏病毒，然救護人員並非醫療法所稱之醫事人員[4]，感染者不需主動告知救護人員。立法委員據此認為，救護人員在執勤時，有接觸到病患血液、體液，或不慎遭使用過的針頭扎傷等風險，故提出修正草案，要求感染者於接受緊急救護時，應向救護人員告知其已感染人類免疫缺乏病毒，以保障救護人員權益，且同時課予救護人員提供服務之義務，以符合法之衡平原則[5]。

另為避免標籤化及污名化感染者，人類免疫缺乏病毒傳染防治及感染者權益保障條例第 14 條規定，主管機關、醫事機構、醫事人員及其他因業務知悉感染者之姓名及病歷等有關資料者，除依法律規定或基於防治需要者外，對於該項資料，不得洩漏。無論立委提案是否通過，感染者於救護現場無有告知

---

[1] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 1 條。

[2] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 12 條：「感染者有提供其感染源或接觸者之義務；就醫時，應向醫事人員告知其已感染人類免疫缺乏病毒。」

[3] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 21 條第 1 項：「明知自己為感染者，隱瞞而與他人進行危險性行為或有共用針具、稀釋液或容器等之施打行為，致傳染於人者，處五年以上十二年以下有期徒刑。」

[4] 醫療法第 10 條：「本法所稱醫事人員，係指領有中央主管機關核發之醫師、藥師、護理師、物理治療師、職能治療師、醫事檢驗師、醫事放射師、營養師、藥劑生、護士、助產士、物理治療生、職能治療生、醫事檢驗生、醫事放射士及其他醫事專門職業證書之人員。」

[5] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 12 條修正草案：「感染者有提供其感染源或接觸者之義務；於接受緊急救護或就醫時，應向救護人員或醫事人員告知其已感染人類免疫缺乏病毒。主管機關得對感染者及其感染源或接觸者實施調查。但實施調查時不得侵害感染者之人格及隱私。感染者提供其感染事實後，救護隊及救護人員與醫事機構及醫事人員不得拒絕提供服務。」立法院議案關係文書院總第 1433 號委員提案第 21036 號。

救護人員，其已感染人類免疫缺乏病毒之義務，救護人員如因進行緊急救護時知悉受救護者為感染者時，亦屬其他因業務知悉感染者之姓名及病歷等有關資料者，同樣負有保密義務。

如救護人員違法洩漏相關資訊，依該條例第 23 條第 1 項[6]規定，可處新臺幣 3 萬元以上 15 萬元以下罰鍰，且如為醫師違反規定時，更負有刑事上責任[7]。故無論是主管機關、醫事機構、醫事人員，甚至是救護人員等，均應注意其保密義務，以保障感染者權益。

又依照個人資料保護法規定，有關人類免疫缺乏病毒感染者之姓名及病歷等有關資料亦屬個資法第 2 條[8]所稱之個人資料，故對於該資料之蒐集、處理或利用亦應符合個資法規定。而此類關於受感染者主動告知其已感染人類免疫缺乏病毒之情形，係屬於法律要求當事人主動提供，無論是否屬於個資法第 6 條[9]之病歷、醫療、基因、性生活、健康檢查及犯罪前科等個人資料，或是普通個人資料，均是法律明文規定作為蒐集之法定要件[10]，故得以據之蒐集、處理或利用，惟其他個資法上之必要作為，例如個資法第 8 條[11]所規定之告知義務仍須遵守，以免違反相關法令。

---

[6] 人類免疫缺乏病毒傳染防治及感染者權益保障條例第 23 條第 1 項：「違反第十一條第三項、第十二條、第十四條、第十五條第一項及第四項、第十五條之一或第十七條者，處新臺幣三萬元以上十五萬元以下罰鍰。」

[7] 刑法第 316 條：「醫師、藥師、藥商、助產士、心理師、宗教師、律師、辯護人、公證人、會計師或其業務上佐理人，或曾任此等職務之人，無故洩漏因業務知悉或持有之他人秘密者，處 1 年以下有期徒刑、拘役或 5 萬元以下罰金。」

[8] 個人資料保護法第 2 條第 1 款：「一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」

[9] 個人資料保護法第 6 條第 1 項第 1 款：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。…」

[10] 個人資料保護法第 19 條第 1 項第 1 款：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。…」

[11] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

## 【管理 Tips】

醫事機構基於醫療之目的，本即有蒐集、處理或利用愛滋感染者個人資料之必要，但整體醫療救護過程中發生資訊流動情形者眾，從事故發生、救護人員到場、送達醫事機構開始治療，直到療程結束，甚至可能會有必要對患者進行後續追蹤等情況，均有資訊流動的節點，當節點存在，個人資料外洩的風險亦隨存在。

因此，組織應採取有效管理制度，避免人員因違反法令，如醫事機構未有適當管理措施，避免會有因防護程度不足或執行人員操作不當，導致個人醫療資料遭到外洩。而醫事人員及其他因業務知悉感染者資料等相關人員，亦應謹慎保護因業務知悉或持有之他人秘密者，以避免將資料外洩。

## 【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：　人類免疫缺乏病毒傳染防治及感染者權益保障條例中，對於人類免疫缺乏病毒感染者之姓名及病歷等有關資料，有特別保護之要求，業務執行人員應更加謹慎保護相關資料，避免將其散佈或洩漏予他人。

類別：資訊保護【案號：S10626】

## 採購案洩密 警政機關承辦人員判處 2 月有期徒刑

### 【焦點話題】

警政單位負責承辦其單位標案採購業務之謝姓組員，於採購案公告前於辦公室將招標文件洩漏予宋姓廠商等人。檢方指控謝員洩漏標案資訊，先予緩起訴處分，經臺灣高等法院檢察署發回重新偵查，謝員遭起訴，並經臺灣臺北地方法院依洩密罪判處有期徒刑 2 個月，得易科罰金 6 萬元，全案可上訴。

【參考資料來源：聯合報，106/4/12】

### 【重點摘要】

1. 按政府採購法（下稱採購法）之規定，辦理政府採購時，招標文件於公告前應予保密；公告後，於開標前不得洩漏底價，領標、投標廠商之名稱與家數等資訊；開標後，除底價外之資訊則應公開。
2. 採購流程分階段所應祕密事項，其作業資料如屬公務上應祕密之文書，機關承辦、監辦採購等相關人員將其職務上知悉、持有應秘密之資料外洩，自屬違背職務上之行為。

### 【法律觀點】

採購法[1]之目的在於建立政府採購制度，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。

在採購準備階段，為避免發生廠商於招標前即取得招標文件，造成先行準備等不公平之情事，採購法第 34 條[2]明文招標文件原則於公告前應予保密；正式

[1] 政府採購法第 1 條。

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

招標後，則為防止廠商藉先行了解底價及其他競爭者之資料，而造成不公平競爭之現象，故同法亦明文不得於開標前洩漏底價，領標、投標廠商之名稱與家數等資訊，但機關依實際需要，仍得於招標文件中公告底價；至於開標後到決標前之階段，則因尚有審標或減價之需要，故底價仍有保密之必要；決標後，基於程序透明，底價於決標後除有特殊情形外，應予公開。

因此在招標、開標、決標一直到驗收過程中，分階段有不同之應保密事項，當行為人將非屬國防領域之應保密事項洩漏時，將有洩漏國防以外之祕密罪[3]之可能，最高法院 104 年台上字第 2669 號刑事判決[4]即表示，因採購準備階段作業資料屬公務上應祕密之文書，如公務員將其職務上知悉持有應秘密之資料外洩，自屬違背職務上之行為。本案中，謝員身為承辦採購業務之公務人員，明知招標文件依政府採購法第 34 條之規定，公告前應予保密，竟基於洩漏國防以外應祕密之文書之犯意，於採購案公告前將招標文件之規格表洩漏予他人，犯有刑法洩漏國防以外之秘密罪，故遭處有期徒刑 2 月，實值得警惕[5]。

## 【管理 Tips】

在管理面而言，組織成員對於自身因業務上所取得之資料，本即應有認知，無論該資料本身是否具備財產價值，重要的是在人員是否意識到自己所肩負之責任，以及該資料於組織之目的與功能或法令是否有相關限制。

承辦政府採購案件，組織應建立標準作業流程，明確告知同仁相關規則，更

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

[4] 最高法院 104 年台上字第 2669 號刑事判決：「為維護將來採購作業之公平性，一般軍事採購案於計畫申購階段之作業資料，仍應採取保密措施，而屬公務上應行秘密之事項。上訴人利用會辦審查「新中案」之機會，將其職務上知悉持有應秘密之「新中案規劃資料」影印交付予林治崇，自屬違背職務上之行為等情綦詳。而所謂「先期規劃階段」，自屬於計畫申購階段。原判決因認「新中案規劃資料」確屬公務上應秘密之文書，上訴人將之影印後洩漏交付予林治崇，自屬違背職務之行為。…上訴人並無正當理由，竟於林治崇交付上開賄賂及不正利益後，違背職務交付「新中案規劃資料」影本予林治崇，其間縱有假借其他名義情形，惟上訴人違背職務之行為，與林治崇交付之上開賄賂及不正利益間，自有對價關係等情綦詳。」

[5] 臺灣台北地方法院 106 年審簡字第 588 號刑事判決。

可納入工作規則內，並訂定內部罰則，

公務機關或承辦政府採購之組織應將相關政府採購的案例，藉由教育訓練以及宣導的方式，讓同仁能夠提高警覺，瞭解所應遵循之政府採購規範，並清楚說明可能涉犯違法情事以及相關罰則，以降低違法情事發生之風險。

此外，承辦政府採購案件，組織應建立標準作業流程，明確告知同仁相關規則，更可納入工作規則內，並訂定內部罰則，使相關人員得以依循其作業流程，並避免發生違法情事。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.7.2.2　資訊安全認知、教育及訓練

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

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

●A.13.2.4　機密性或保密協議

(1)標準內容：　宜識別、定期審查及文件化，以反映組織對資訊保護之需要的機密性或保密協議之要求事項。

(2)適用說明：　組織應判別其組織內資訊之分類及密等，針對具有機密性之文件，應更予以重視，並定期審查內容。以本案而言，組織即因有進行保密文件之控管，因而發現洩密情事。

類別：資訊保護【案號：S10627】

## 英國新法令 上色情網站必須驗證年齡

### 【焦點話題】

英國政府宣布，明年 4 月起將透過「新數位經濟法案」加強管制色情網站，新法令適用付費色情網站以及不要求付費、註冊的免費網站，而各色情網站必須設有年齡認證裝置，以確認使用者年齡。英國政府傾向由網站自行決定採用方式，以判斷使用者是否已達得接觸網站。目前大多數評論家認為各色情網站可能會採用類似簽賭網站的方式，要求民眾上色情網站或許必須提供信用卡資料，以作為證明使用者年齡已經是超過 18 歲之成年人。

【參考資料來源：經濟日報，106/7/18、dailymail，106/7/16】

### 【重點摘要】

1. 組織如有需蒐集使用者資料以確認其身分時，應以風險較低方式進行，並避免不必要資訊之蒐集，以減少事故發生時之損害。
2. 組織對於管理其網際網路時，得依人員職務及需求之不同，限制傳送網際網路郵件或瀏覽特定網頁，或透過使用權限管理予以管控得使用之網際網路功能，可有效降低資安風險。

### 【法律觀點】

網路發達的現代，透過網際網路使得任何人皆得輕易地接觸到各式色情網站，要如何杜絕不適當的人接觸則是一道難題。英國於今年通過數位經濟法案（Digital Economy Act 2017），第 3 部分即係規範情色網路（ONLINE PORNOGRAPHY），該部分之第 14 條[1]即明文要求應防止 18 歲以下人士存取情色網路。

[1] Digital Economy Act 2017 §14「Internet pornography: requirement to prevent access by persons under 18.」http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted，（最後瀏覽日：106 年 10 月 27 日）。

而我國對於未成年人接觸網路色情亦有所規範，兒童及少年福利與權益保障法第 46 條[2]規定，通訊傳播主管機關應委託民間團體成立內容防護機構，辦理網際網路防護機制，以防止兒童及少年接觸有害身心發展之網際網路內容。網際網路內容防護機構依法負責包括兒童及少年使用網際網路行為觀察、申訴機制之建立及執行、內容分級制度之推動及檢討、過濾軟體之建立及推動、兒童及少年上網安全教育宣導、推動網際網路平臺提供者建立自律機制，以及其他防護機制之建立及推動。

色情網站業者屬網際網路平臺提供者之一[3]，按規定網際網路平臺提供者應訂定自律規範採取明確可行防護措施；未訂定自律規範者，應依相關公協會所定自律規範採取必要措施[4]。目前台灣網際網路協會訂有「網際網路平臺提供者網站內容自律公約」[5]，針對兒少上網安全，要求網際網路平臺提供者得以一定方式管理限制級內容之瀏覽，而可採用之方式包括設置專區、過橋頁面、採行會員制、設置管理人員及設置檢舉通報管道[6]。

本案中，英國政府制定之數位經濟法案，要求情色網路服務提供者必須採取年齡認證機制，以確認使用者年齡，相較於我國係以設置過橋頁面、採行會員制，或設置管理人員等方式，由操作者自由證明是否已達合法年齡之作法，

---

[2] 兒童及少年福利與權益保障法第 46 條第 1 項：「為防止兒童及少年接觸有害其身心發展之網際網路內容，由通訊傳播主管機關召集各目的事業主管機關委託民間團體成立內容防護機構，並辦理下列事項：一、兒童及少年使用網際網路行為觀察。二、申訴機制之建立及執行。三、內容分級制度之推動及檢討。四、過濾軟體之建立及推動。五、兒童及少年上網安全教育宣導。六、推動網際網路平臺提供者建立自律機制。七、其他防護機制之建立及推動。 」。

[3] 兒童及少年福利與權益保障法第 46 條第 3 項：「前三項所稱網際網路平臺提供者，指提供連線上網後各項網際網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能者。」。

[4] 兒童及少年福利與權益保障法第 46 條第 2 項：「網際網路平臺提供者應依前項防護機制，訂定自律規範採取明確可行防護措施；未訂定自律規範者，應依相關公（協）會所定自律規範採取必要措施。」。

[5] 網際網路平臺提供者網站內容自律公約，http://www.twia.org.tw/about_2_04.htm，（最後瀏覽日：106 年 10 月 16 日）。

[6] 網際網路平臺提供者網站內容自律公約第 4 條：「網際網路平臺提供者為維護兒少上網安全，得以下列任一方式管理限制級內容之瀏覽：（一）設置專區。（二）設置過橋頁面。（三）採行會員制。（四）設管理人員。（五）設置檢舉通報管道。」。

更可確保未成年人無法接觸情色網路，我國將來或可借鏡其作法以達到保護兒少之立法目的，而若師法英國之作法，隨之而來姓名、出生年月日、信用卡資訊等個人資料之蒐集、處理，相關業者亦須符合個人資料保護法之規範，應符合法定要件，且原則不得為目的外利用。

**【管理 Tips】**

有關使用年齡認證機制存在許多方式，有論者認為網站可採取信用卡註冊後方得使用之方式。然從資訊安全角度觀之，此法所提供之資料除身分證明資訊外，亦可能包含如信用卡卡號等財務資料，如發生資訊外洩，將可能導致信用卡盜刷、持卡人遭勒索等侵害。故組織如有需要蒐集使用者資料以確認其身分時，亦宜採資訊最小化之方式，並以風險較低方式進行，透過避免不必要資訊的蒐集，減少事故發生時之損害。

**【相關標準】**

ISO 29100：2011（CNS29100）

●5.5　資料極小化

(1)標準內容：　資料極小化密切連結“蒐集限制”原則，但不僅如此。“蒐集限制”意旨被蒐集之有限資料與特定目的相關聯，而“資料極小化”則嚴格將 PII 之處理極小化。

堅持資料極小化原則，意指以下列方式設定及實作資料處理程序與 ICT 系統。

- 將所處理之 PII、隱私權利害相關者及 PII 接露對象或可存取 PII 之人員的數目最小化。
- 確保採用“僅知(need-to-know)”原則，亦即於 PII 處理之合法目的框架下，宜僅對執行正式職務所必要之人員賦予 PII 存取權限。
- 使用或提供視為預設選項，只要不涉及 PII 當事人之識

別的互動及交易，儘能降低其行為之可觀察性並限制所蒐集 PII 的可連結性。

- 一旦 PII 處理之目的終止，無法定要求保有 PII，或是實務上需如此做時，即刪除或廢棄 PII。

(2)適用說明： 組織進行資料蒐集時，應採以資料最小化並予以分級，並在合法目的下進行所需資料之使用，可降低資料遭不當揭露時之風險。本案對於網路使用者之年齡核對，宜僅蒐集與使用者年齡相關之資料即可。

類別：資訊保護【案號：S10628】

# 指紋捺印建檔 可協助走失者快速辨識身分與提供家屬聯絡資訊

## 【焦點話題】

為協助失智老人找到回家的路，警政主管機關透過「警政相片比對系統」，比對臉部特徵，9 年來協助失蹤人口返家 12 萬餘件。警政主管機關提醒民眾，若家中有失智老人，除可申請愛心手鍊、QR code 布標、配戴衛星定位裝置外，也可由家屬陪同，攜帶當事人印鑑、照片，到當地警政機關申請「志願者指紋捺印建檔」，事故發生時可透過指紋辨識，協助走失者找到回家的路。

【參考資料來源：中國時報，106/2/7】

## 【重點摘要】

1. 警政機關為疑似發展遲緩、發展遲緩或身心障礙兒童及少年之失蹤協尋，得由兒童及少年之父母或監護人，申請建立指紋資料，所蒐集之指紋資料，按個人資料保護法（下稱個資法）之規定，應與蒐集之特定目的相符之利用，故除作為失蹤協尋外，原則不得作為其他用途之使用。
2. 警政機關之資料建檔，必須遵守資訊安全相關規範，並由專責人員管理及維護，於建檔、比對過程或其他原因發現指紋資料與受捺人資料不符時，應查明後更正受捺人資料，以維護指紋資料之正確。

## 【法律觀點】

隨著高齡化的時代來臨，有鑑於社福機構或收容中心經常有不明失蹤人口，目前各地警政機關均有「志願者指紋捺印建檔」之服務[1]，希冀透過指紋建檔加強協尋機制，以協助失智老人、精神病患及身心障礙者不幸走失時，能迅速確認身分、通知家屬。

[1] https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=82931&ctNode=12274&mp=28 ，內政部警政署 106 年 2 月 6 日新聞稿。

因指紋屬於個資法所稱之個人資料[2]，各地警政主管機關如要蒐集指紋時，必須符合個資法第 15 條規定，公務機關對個人資料之蒐集或處理應有特定目的，並符合執行法定職務必要範圍內、經當事人同意或對當事人權益無侵害等法定情形[3]。

，按警察法之規定，警察依法負有協助地方治安等保安義務[4]，以及失蹤人口查尋之責任[5]。而為使失智老人、精神病患及身心障礙者不幸走失時能迅速確認身分，警政主管機關預先蒐集當事人提供之指紋，並建置資料庫，其特定目的屬加強失蹤人口之協尋，合於個資法之規範，具有特定目的，並執行法定職務而得蒐集者。

為了加強失蹤人口協尋機制，警政主管機關對於民眾指紋之蒐集，除依個資法之規定外，尚得依兒童及少年福利與權益保障法（下稱兒少權益法）規定辦理。按兒少權益法規定，警政主管機關為疑似發展遲緩、發展遲緩或身心障礙兒童及少年之失蹤協尋，得由兒童及少年之父母或監護人，申請建立指紋資料，而依據兒少權益法蒐集之兒童及少年指紋資料，除作為失蹤協尋外，不得作為其他用途之使用[6]。當警政主管機關取得指紋資料後，在指紋資料之傳輸、儲存及運用過程中，必須遵守資訊安全相關規範，並由專責人員管理及維護指紋資料，於建檔、比對過程或其他原因發現指紋資料與受捺人資料

[2] 個人資料保護法第 2 條第 1 款：「本法用詞，定義如下：一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」。

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

[4] 警察法第 9 條第 7 款：「警察依法行使左列職權：…七、有關警察業務之保安、正俗、交通、衛生、消防、救災、營業建築、市容整理、戶口查察、外事處理等事項。」。

[5] 失蹤人口查尋作業要點第 1 點：「內政部警政署（以下簡稱本署）為加強失蹤人口查尋，提升工作成效，特訂定本要點。」。

[6] 兒童及少年福利與權益保障法第 30 條：「疑似發展遲緩、發展遲緩或身心障礙兒童及少年之父母或監護人，得申請警政主管機關建立指紋資料。前項資料，除作為失蹤協尋外，不得作為其他用途之使用。第一項指紋資料按捺、塗銷及管理辦法，由中央警政主管機關定之。」。

不符時，應查明後更正受捺人資料，以維護指紋資料之正確[7]。

本案中，警政主管機關蒐集失智老人、疑似發展遲緩、發展遲緩或身心障礙兒童及少年之指紋資料時，因查尋失蹤人口為警政主管機關之法定職務，故應符合個資法或兒少權益法之規定。

## 【管理 Tips】

指紋除供政府機關作為身分辨識以查尋失蹤人口外，因其屬於具有獨特性與不變性之生物特徵，如同虹膜、靜脈一般，愈來愈多設備將其作為身分辨識之用，例如手機解鎖、組織門禁。然而也因為生物特徵所具有之獨特性與不變性，使其無法如同文字密碼一般可任意更改，如果資訊外洩將所造成之影響亦較文字密碼外洩為大。

基於生物特徵之特殊性，無論是政府機關或民間組織於使用生物辨識技術作為身分辨識方式時，應建立管理規定，確保生物辨識資訊安全，防範不法入侵及資料外洩。而管理規定中，首應考量將生物識別資訊限制於使用者設備，而非組織之資料庫中，以避免當組織資安事故發生時，造成大量具獨特性與不變性之生物識別資訊外流。其次，當生物識別資訊存在於使用者設備時，設備本身應具有安全防護機制，確保設備於未經授權時無法啟用或窺視其中資訊，更進一步，可使設備於未經授權之嘗試啟用或窺視時，主動通知具授權者，以降低設備遺失時之資料外洩風險。

## 【相關標準】

ISO 29100：2011（CNS29100）

●5.6　利用、持有及揭露原則

(1)標準內容：　堅持利用、持有及揭露限制原則，意旨下列事項。

[7] 發展遲緩疑似發展遲緩或身心障礙兒童及少年指紋管理辦法第 7 條：「指紋資料之傳輸、儲存及運用過程，應遵守資訊安全相關規範，確保指紋資料安全，防範不法入侵及資料外洩。指紋資料應由專責人員管理及維護。指紋資料與受捺人資料不符時，應立即查明處理。如有錯誤，應於查明後更正受捺人資料。」。

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

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

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

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

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

(2)適用說明： 個人可識別資訊之利用、持有及揭露 ( 包含移轉 ) 限制於為履行特定、明確及合法目的所必要者。除非適用之法律明確要求不同的目的，否則將個人可識別資訊之利用限於蒐集之前個人可識別資訊控制者所規定之目的。

類別：資訊保護【案號：S10629】

## 搜尋結果頻現「假球」 職棒老闆告Google求移除敗訴

### 【焦點話題】

中華職棒 2008 年爆發職棒簽賭案，某隊多名球員涉與地下賭盤組頭配合打假球，球團老闆等 33 名管理職人員及球員被依詐欺罪起訴。球團老闆雖在 2013 年獲判無罪確定，但不滿於 Google 網站搜尋其姓名時仍會出現與「假球」字眼相關之連結，遂對其提告主張「被遺忘權」，請求 Google 移除上述搜尋結果，卻被法院駁回其主張而敗訴。

【參考資料來源：蘋果日報，106/7/10】

### 【重點摘要】

1. 資訊隱私權包含個人自主控制個人資料的權利，保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。
2. 資訊隱私權與言論自由、新聞自由等公共利益間，各有其欲實現之基本權價值，當個人拒絕揭露或要求刪除其個人資料時，如果有其他公共利益存在，二者間將發生基本權衝突，此時須為利益衡量決定是否停止揭露或刪除其個人資料。

### 【法律觀點】

臺灣台北地方法院民事法庭於 106 年 7 月，針對人民得否請求搜尋引擎網站於搜尋結果中移除與自己相關的新聞報導，作成了 104 年度訴更一字第 31 號民事判決。判決中將討論重點置於：網路搜尋引擎業者，有無義務依當事人主張歸屬於人格權中的被遺忘權，或依個人資料保護法中資訊刪除權，除去搜尋中關於當事人之資料連結？

首先，我國民法並無明文規定被遺忘權，因此判決書說明在原告主張之脈絡

下，縱使已於網路上揭露之個人資料，凡屬於個人有意隱匿、不欲使外界知悉之個人私密，均應受隱私權保護，並引用司法院大法官釋字第 603 號解釋理由書[1]，表示資訊隱私權包含個人自主控制個人資料的權利，保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權，進而認定原告所稱之被遺忘權為隱私權，並屬於人格權的一種。惟，大法官亦同時表示隱私權並非絕對，因此在符合憲法第 23 條[2]規定意旨時，可以法律加以限制之。據此，法院以個人資料保護法第 19 條立法理由[3]說明，當新聞自由或知的權利與隱私權之衝突時，因其各有其欲實現之基本權價值，故得以公共利益作為衡平基準，依比例原則處理，決定是否對資訊隱私權加以限制。

而針對個人資料保護法中資訊刪除權部分，因搜尋引擎在網路使用者鍵入關鍵字後，即將搜尋結果摘要及連結網頁以列表呈現，其行為性質已符合個人

---

[1] 大法官解釋釋字第 603 號解釋文「其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」。

[2] 憲法第 23 條：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」。

[3] 個人資料保護法第 19 條立法理由：「八、由於新聞自由屬於憲法第十一條所保障言論自由之範圍（司法院大法官釋字第三六四、四o七、四一四、五o九號解釋參照），其目的為使資訊流通順暢，並使人民參與公共事務能獲得最充分資訊之知的權利，以維持社會開放及民主程序之運作，使人民得有效地監督公共事務，新聞自由之制度性保障固有其存在之必要。然而，今日新聞媒體已非昔比，其所擁有之巨大影響力亦非任何政治實力可以掌握，稍有偏差，即有可能對於報導之個人造成難以彌補之傷害。從而，為維護人性尊嚴與個人主體性及尊重人格自由發展，隱私權亦為不可或缺之基本權利，尤其是資訊科技及傳播工具之發達，個人生活私密領域免於他人侵擾及個人資料之自主控制，均有其必要，並受憲法第二十二條所保障（司法院大法官釋字第六o三號解釋參照）。因此，公共事務之知的權利如涉及個人資料或個人隱私時，應特別慎重，以免過度侵入個人私的生活，故隱私權與新聞自由之界限有更具體明確之必要。新聞自由或知的權利與隱私權之衝突，如何確立二者間之界限，各國均陸續建立其判斷標準。在美國聯邦最高法院有關侵權行為或誹謗訴訟之判例中，以「新聞價值」（Newsworthiness）和「公眾人物」（PublicFigure）為判斷標準，上開二概念最終仍以「公共的領域」，即「公共事務」或「與公共相關之事務」為必要條件，故新聞自由或知的權利與隱私權之界限，其劃定標準應在於「事」而非在於「人」，故「公共利益」已足供作為判斷標準並簡單明確，此亦與中華民國報業道德規範宗旨相符，爰增訂第六款之規定。」。

資料保護法關於蒐集、處理及利用之規範適用範圍，故在無個人資料保護法規定例外情形時，如當事人有請求刪除、停止處理或利用該個人資料，則受請求者依法應依其請求為刪除、停止處理或利用該個人資料。但同樣地，法院亦認為個人資料保護法的資料刪除權雖亦受法律保障，但因其取自一般可得來源，必須判斷當事人對該資料之禁止處理或利用，是否顯有更值得保護之重大利益，亦即考量公共利益以決定是否得以將拒絕刪除予以正當化。據此，法院考量有關報導、評論等網頁文章內容涉及到公共利益，權衡要求刪除事項之公開之目的及其社會意義、個人資料主體之社會地位或影響力、因公開對個人資料主體所造成損害之重大性及回復困難性等因素，於衡平後認定公共利益大於隱私權，因此認為原告請求無理由。

**【管理 Tips】**

無論組織之性質為何，若當事人依個人資料保護法規定，請求查詢或請求閱覽、製給複製本、更正、補充或刪除、停止蒐集、處理或利用個人資料等當事人權利時，組織可依下列程序判斷是否應其主張作為。

首先，組織必須判斷當事人所主張者是否為個人資料之請求，如果並非個人資料保護法上請求，則應視是否有其他法律規範得以據以請求。其次，其請求是否具有理由，如當事人主張理由成立時，組織原則上應依其請求使當事人得以行使權利，然如果組織有其他正當理由，如涉及妨害國家安全、外交及軍事機密、整體經濟或其他國家重大利益、妨害公務機關執行法定職務、妨害該蒐集機關或第三人的重大利益的情況下，當事人雖有正當理由，組織仍應拒絕其查詢、提供或製給複製本。

因此，組織應建立完整流程，判斷當事人之請求是否為個人資料保護法或其他法律上之請求標的，其次判斷當事人之請求有無理由，當其請求有理由時，再判斷有無法律上得拒絕其行使權利之依據，最末，應對此加以紀錄並保存，避免將來發生爭訟時舉證發生困難。

**【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： 組織應識別所適用關於個人資料之法令，並確認應作為及不作為之事項，本案中，組織應瞭解民法以及個人資料保護法對於人格權之保護等法規要求，並建立適當程序建立完整流程，判斷當事人請求合法性，並據以決定對其請求之准駁以及後續作為。

# 貳、資訊公開（Disclosure）

類別：資訊公開【案號：D10630】

## 公布戴奧辛蛋來自特定蛋雞場，立委疑衛福部未審先判

### 【焦點話題】

國內某毒物研究中心執行風險評估計畫時，發現雞蛋戴奧辛含量超標，隨即通報衛生福利部食品藥物管理署，依照食品安全衛生管理法之相關流程規定，該署於接獲通報後，應主動查驗，並依照檢驗結果對外說明，而該署即會同有關機關經聯合調查後，對外說明相關蛋雞場之雞蛋現場封存及禁止出貨，下游業者亦不得再使用[1]。陳姓立委出席立法院社會福利及衛生環境委員會時表示，經委外檢測，結果顯示前述蛋雞場均檢測通過，惟農委會毒藥所之檢測結果超標，二者檢驗結果不同，相關機關怎能據此直接判定毒蛋來源？有關機關則回應，依據食品安全衛生管理法第 5 條等相關規定，政府有必要將資訊公開透明化，因此無論是發佈新聞稿或是公布複驗結果等，均係遵從「食安第一、透明公開」原則，使資訊公開透明以供民眾知曉。

【參考資料來源：自由時報，106/4/27】

### 【重點摘要】

1. 食品衛生安全事件之發生對於國民之健康即可能產生衝擊，為預防此情況之發生，相關主管機關平時應採行食安管理措施，並以風險評估為基礎，兼顧事先預防原則、資訊透明原則等要件，建構風險評估、諮議體系。
2. 依據各級機關之食品衛生安全監測體系，若有食品衛生安全之虞等事件發生時，應主動查驗，並發布預警或採行必要管制措施。
3. 針對重大或同發性之食品衛生安全事件，主管機關依食品安全衛生管理法經風險評估或相關調查結果，得公告辦理對特定產品或特定地區之產品採取諸如停止製造及加工、下架、封存、沒入銷毀等相關管理措施。

### 【法律觀點】

[1] 衛福部、農委會、環保署辦理雞蛋戴奧辛初步調查結果說明，網址：https://www.fda.gov.tw/TC/newsContent.aspx?cid=4&id=22074

食品安全是政府職責，為於事先預防、監測，食品安全衛生管理法第 5 條[2]規定各級主管機關本身即應建立食品衛生安全監測體系，以作為風險管理之一環。而於監測發現有危害食品衛生安全之虞之事件發生時，應主動查驗，並發布預警或採行必要管制措施，而必要管制措施，包含主管機關應抽樣檢驗、追查原料來源、產品流向、公布檢驗結果及揭露資訊，並令食品業者自主檢驗。其目的在於強化各級主管機關主動查驗之措施，包含應抽樣檢驗、追查原料來源、產品流向、公布檢驗結果及揭露資訊。

食品安全衛生管理法第 4 條[3]之規定，因重大或突發性食品衛生安全事件，主管機關對特定產品或特定地區之產品採取管理措施。且如業者不願配合而違反主管機關公告之管理措施時，主管機關更對其可處新臺幣 3 萬元以上 300 萬元以下罰鍰，情節重大者更有受歇業、停業一定期間、廢止其公司、商業、工廠之全部或部分登記事項，或食品業者之登錄等處罰[4]。

因此，如係因安全監測時發現事件發生，為確保民眾之食安，避免造成公共危害，主管機關得依法發布相關資訊以供民眾預警與權益保障。

## 【管理 Tips】

[2] 食品安全衛生管理法第 5 條第 1 項：「各級主管機關依科學實證，建立食品衛生安全監測體系，於監測發現有危害食品衛生安全之虞之事件發生時，應主動查驗，並發布預警或採行必要管制措施。前項主動查驗、發布預警或採行必要管制措施，包含主管機關應抽樣檢驗、追查原料來源、產品流向、公布檢驗結果及揭露資訊，並令食品業者自主檢驗。」。

[3] 食品安全衛生管理法第 4 條：「主管機關採行之食品安全管理措施應以風險評估為基礎，符合滿足國民享有之健康、安全食品以及知的權利、科學證據原則、事先預防原則、資訊透明原則，建構風險評估以及諮議體系。　　前項風險評估，中央主管機關應召集食品安全、毒理與風險評估等專家學者及民間團體組成食品風險評估諮議會為之。　　第一項諮議體系應就食品衛生安全與營養、基因改造食品、食品廣告標示、食品檢驗方法等成立諮議會，召集食品安全、營養學、醫學、毒理、風險管理、農業、法律、人文社會領域相關具有專精學者組成之。　　諮議會之組成、議事、程序與範圍及其他應遵行事項之辦法，由中央主管機關定之。　　中央主管機關對重大或突發性食品衛生安全事件，必要時得依風險評估或流行病學調查結果，公告對特定產品或特定地區之產品採取下列管理措施：一、限制或停止輸入查驗、製造及加工之方式或條件二、下架、封存、限期回收、限期改製、沒入銷毀。」。

[4] 食品安全衛生管理法第 47 條：「有下列行為之一者，處新臺幣三萬元以上三百萬元以下罰鍰；情節重大者，並得命其歇業、停業一定期間、廢止其公司、商業、工廠之全部或部分登記事項，或食品業者之登錄；經廢止登錄者，一年內不得再申請重新登錄：一、違反中央主管機關依第四條所為公告。…」。

風險管理（Risk Management）係針對組織或個人在可能面對之各種潛在風險時，找出潛在風險，並對其加以判斷、評估，進而選擇適當之處理對策，並期以最低成本，以達成適當之處理方式。而風險管理之策略可分為：風險規避、風險降低、風險轉嫁以及風險接受。

本案相關機關依法進行風險評估後，係依風險評估結果進行風險規避，亦即將可能具有食品安全危險之戴奧辛蛋予以下架，降低後續發生損害之可能性。然，公告可能具有戴奧辛蛋之廠商名稱，必將對其造成直接影響，因此主管機關於公告前，應妥善衡量公共利益與受直接影響者之權益，僅在需要的範圍內揭露必要資訊，以免過於侵害人民之權益。

自一般企業組織角度觀之，進行風險管理之效益在於使組織充分瞭解己所面臨之風險及其性質與嚴重程度，以及時採取措施避免或減少風險損失，或者當風險損失發生時能夠得到及時反應，從而保證組織之存續並迅速恢復正常。

**【相關標準】**

ISO 27001：2013（CNS 27001）

●A.6.1　因應風險及機會之行動

(1)標準內容：　建立管理框架，以於組織內啟動及控管資訊安全之實作及運作。

(2)適用說明：　本案中，戴奧辛蛋事件可能對於國民健康產生不利益之風險，主管機關對此有食安風險之事件發生時，即應依法主動查驗，並採行預警機制與有關之必要管制措施。

類別：資訊公開【案號：D10631】

## 健康風險評估不給看 環團怒向市府提訴願

### 【焦點話題】

某市府環保主管機關曾於 103 年進行臨海工業區鄰近區域居民之健康風險評估，惟評估報告迄今仍未公布，環保團體去函要求市府環保主管機關報告公開上網，但日前收到回函表示該評估內容依政府資訊公開法屬「應限制公開或不予提供」之資訊，而回絕公開要求。對此，環保團體表示政府一方面宣示啟動緊急應變、管制揮發性有機化合物，但應公開給社會知曉之重要資訊卻未予公開，認為基於保障人民知的權利、增進人民對公共事務的瞭解、信賴及監督，政府沒有理由反對，已向市府提出訴願，爭取報告公開。

對環團之質疑與訴願，市府解釋，該份調查報告是以排放係數方式推估排放量，不是以實際檢測到的數據來計算，推估方式易造成誤導，所以已請中央環保主管機關在今年以實際檢測污染源排放量來進行風險評估，目前已進行中，也尊重環團提訴願，市府會依照程序答辯。

【資料來源：蘋果日報，106/9/23】

### 【重點摘要】

1. 政府資訊中，除為應限制公開或不予提供之國安資訊或依法應保密事項、執法資訊、特定公務資訊以及祕密資訊等資訊外，主管機關應主動公開或應人民申請提供之。
2. 政府機關應建立完善之資料盤點流程，盤點出機關所持有之政府資訊，並建立清冊，藉以降低處理行政救濟案件時之成本，進而提高行政效率。

### 【法律觀點】

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均屬政府資訊[1]。

依政府資訊公開法第 7 條規定，包括施政計畫、業務統計及研究報告等政府資訊，除有同法第 18 條限制公開或不予提供之事由外，均屬政府應主動公開之資訊[2]，其中研究報告係指由政府機關編列預算委託專家、學者進行之報告或派赴國外從事考察、進修、研究或實習人員所提出之報告[3]。

本案之臨海工業區鄰近區域居民健康風險評估計畫[4]，屬於政府機關編列預算委託專家、學者所進行之報告，亦即政府資訊公開法所稱之研究報告，因此除有第 18 條第 1 項[5]限制公開事由外，均應主動公開。該相關限制事由，依其性質可分為，國安資訊或依法應保密事項(第 1 款)、執法資訊(第 2、4 款)、特定公務資訊(第 3、5、8、9 款)以及祕密資訊(第 6、7 款)。市府相關機

[1] 政府資訊公開法第 3 條。

[2] 政府資訊公開法第 7 條第 1 項第 5 款：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：...五、施政計畫、業務統計及研究報告。」

[3] 政府資訊公開法第 7 條第 2 項：「前項第五款所稱研究報告，指由政府機關編列預算委託專家、學者進行之報告或派赴國外從事考察、進修、研究或實習人員所提出之報告。」

[4] 103 年高雄市臨海工業區鄰近區域居民健康風險評估計畫決標資訊，網址：https://web.pcc.gov.tw/tps/main/pms/tps/atm/atmAwardAction.do?newEdit=false&searchMode=common&method=inquiryForPublic&pkAtmMain=51370928&tenderCaseNo=H03066（最後瀏覽日：106 年 10 月 29 日）

[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。」

關以調查報告是以排放係數方式推估排放量，推估方式易造成誤導為理由，而拒絕提供研究報告，檢視前述限制公開事由，相關機關所據以之理由似非屬政府資訊公開法第 18 條第 1 項所載應限制公開或不予提供之政府資訊事項，市府機關並無法據此拒絕提供研究報告。

因此，市府相關機關應主動公開所委託學者作成的臨海工業區鄰近區域居民健康風險評估研究報告。如於民眾提出申請後 15 日期間[6]，不為准駁之決定或拒絕其申請，申請人得依法提起訴願、行政訴訟等行政救濟[7]。

**【管理 Tips】**

政府資訊公開之目的，在於增進一般民眾對公共事務之瞭解、信賴及監督，故機關應確實知悉在政府資訊公開法中，何類政府資訊屬於應主動公開或應人民申請而公開，以及何類政府資訊屬於應限制公開或不予提供，確保其公開或不公開均符合法律規定，以使一般民眾能確實瞭解公共事務，進而促進民主參與。

當人民對政府資訊屬限制公開或不予提供之決定有疑義，而對政府機關提出訴願及行政訴訟等行政救濟時，政府機關需對其限制公開或不予提供之緣由提出說明，因此政府機關應建立完善之資料盤點流程，分類盤點出機關所持有之政府資訊，藉以降低處理行政救濟案件時成本，進而提高行政效率。

**【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

[6] 政府資訊公開法第 12 條第 1 項：「政府機關應於受理申請提供政府資訊之日起十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日。」

[7] 政府資訊公開法第 20 條：「申請人對於政府機關就其申請提供、更正或補充政府資訊所為之決定不服者，得依法提起行政救濟。」

持此等資產之清冊。

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

類別：資訊公開【案號：D10632】

## 全國9萬補教師學經歷公開 歡迎各界來找砸

### 【焦點話題】

教育部自 90 年起開始建置「短期補習班資訊管理系統」，要求補習班登錄老師姓名、任教科目及最高學經歷等資料，由於過去沒有嚴格實施實名制，導致許多補習班老師皆以化名登錄。配合 106 年 6 月《補習及進修教育法》修正公布，補習班實名制上路，教育部召開配套措施研擬會議時，因與會者認為，短期補習班資訊管理系統將公布補習班老師的學經歷等資料，恐違反個人資料保護法，因此教育部曾暫時將資料下架，隨即逐步釐清法令方面疑義，後確定將補教老師的學經歷資料公開係符合增進公共利益，並未違法。

【參考資料來源：中時電子報，106/6/6】

### 【重點摘要】

1. 政府機關對於短期補習班相關專業教教學人員之資訊蒐集、處理、利用本係為短期補習班之管理，惟按個人資料保護法規定，短期補習班資訊管理系統之建置以及開放補習班教學人員學經歷欄位供民眾查詢，係屬維護國家安全或增進公共利益所必要，即可為其他「特定目的外之利用」。
2. 而依補習及進修教育法規定，短期補習班執行業務或對外招生時，涉及負責人、教職員工姓名時必須揭露真實姓名。
3. 另按消費者保護法規定，企業經營者對於其提供之商品或服務，應提供消費者充分與正確之資訊，而揭露專業教學人員之真實資料，則屬於企業經營者所應提供之充分且正確之資訊。

### 【法律觀點】

短期補習班之專業教學人員之姓名等資料，屬個人資料之一種，受個人資料保護法之保護，政府機關對於其蒐集、處理、利用時，須符合法定要件，且原

則不得為特定目的外之利用(本案例將著重於資訊處理、利用之說明)。

對於政府機關而言，建置短期補習班資訊管理系統以及開放補習班教學人員學經歷欄位供民眾查詢，雖為對於蒐集之個資為目的外利用，但因屬個人資料保護法第 16 條所定「為維護國家安全或增進公共利益所必要」[1]。且參照政府資訊公開法第 18 條[2]有關限制政府資訊公開之例外規定，若涉及侵害個人隱私原則係限制公開或不予提供，惟「對公益有必要…」則不再此限，故對於政府機關所為短期補習班相關教學人員資訊之公開，依據個資法第 16 條、政府資訊公開法第 18 條等規定為合法利用並公開個人資料。

其次，按消費者保護法第 4 條之相關規定，企業對於商品、服務，本提供消費者充分與正確之資訊，以短期補習班業者而言，相關專業教學人員資訊與其所提供之教學服務息息相關，另參短期補習班設立及管理準則第 21 條第 1 項規定，補習班應聘請具備開設科目專業資格之教學人員。且按今年度六月修正公布之補習及進修教育法第 9 條規定[3]，相關業者進行廣告或宣傳時若涉及負責人、教職員工姓名時，除立案名稱外，均應揭露其真實姓名。故而揭露專業教學人員之真實資料，無論係消費者保護法上，企業經營者提供之充分且正確之資訊義務，抑或於廣告宣傳時所涉及之法定揭露義務，短期補習班業者均必須為之。

綜上，無論從補習及進修教育法或消費者保護法來看，機關建立資料庫以開放補習班教學人員學經歷欄位供民眾查詢，係屬法律明文規定或為增進公共利益所必要之情形，應符合個人資料保護法第 16 條、政府資訊公開法第 18

[1] 個人資料保護法第 16 條：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安全或增進公共利益所必要。…」。

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

[3] 補習及進修教育法第 9 條第 3 項：「短期補習班之招生、書面契約及利用其場址、傳播媒體或其他方法所為之廣告或宣傳，涉及負責人、教職員工姓名時，除立案名稱外，均應揭露其真實姓名，且不得有虛偽不實之情形；其負責人、教職員工執行業務及對外招生或廣告時，亦同。」。

條規定，惟除此公開查詢外，個人資料之處理與利用仍需符合法律規定。

**【管理 Tips】**

政府機關公開涉及個人資料之政府資訊時，已構成「利用」個人資料之行為，惟為強化維護學生於課後學習的安全，此類公開對於補強短期補習班不適任人員之管理機制，以建構全面防護網係屬必要。因此，權衡相關法令規定，判斷公開相關資料所增進之公共利益是否大於對當事人個人隱私之影響，則為風險判斷之必要條件。

政府機關執行此類業務之過程中，本於資訊公開之原則，應保障民眾知的權利，但由於政府機關所掌握之資訊遠大於所應公開之資訊，因而需有完善的資訊管理程序與個人資料保護評估作業，僅公開必要資料且降低涉及個人隱私部分，以期達到資訊保護與公開之平衡。

**【相關標準】**

ISO 27001：2013（CNS 27001）

●A.18.1.4　個人可識別資訊之隱私及保護

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

(2)適用說明：　本案中，主管機關暫時將資料下架以確認所適用之相關法令，即為確保所適用之相關法令係屬正確。

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。

(2)適用說明：　本案中，主管機關於揭露負責人、教職員工之個人資料

時，僅得依法揭露如姓名等必要之資訊。

●5.6　利用、持有及揭露原則

(1)標準內容：　個人資料之利用及揭露，僅限於為履行特定、明確且合法目的所必要。

(2)適用說明：　本案中，縱使依法政府有資訊公開之要求，個人資料之揭露仍應係履行補習及進修教育法所要求者方得為之。

# 參、資訊監察（Monitors）

類別：資訊監察【案號：M10633】

# 監看電郵惹議 美國安局宣布停止

## 【焦點話題】

美國國安局(National Security Agency)日前宣布將停止監看部分監看對象之電子郵件和簡訊等通訊紀錄；按該國之外國情報監控法(Foreign Intelligence Surveillance Act)第 702 節，係允該局於完備一定程序之前提下，蒐集其人民與外國人間可能涉及恐怖主義威脅等電子郵件或簡訊之通訊內容；然該等規定引發公民自由團體強烈抨擊，並要求應修正、限制法規之適用，否則將阻撓年底該法第 702 節之適用期限之展延。

【參考資料來源：中央社，106/4/29】

## 【重點摘要】

1. 通訊保障及監察法 ( 下稱通保法 ) 所定辦理及准許通訊監察所需具備之要件，包括重罪原則、必要性、關聯性、令狀原則、事中監督以及事後通知等。

2. 通保法規定電信、郵政業者有協助執行通訊監察機關進行通訊監察之義務。且電信業者必須建置且維持足夠的通訊設備以為通訊監察之用。

## 【法律觀點】

自從 911 後，世界各國以維安為由開始加強各種管制措施。按美國外國情報監控法規定，於當局進行情報監察時，需透過該法所設立之外國情報監視法院，依據美國外國情報監控法，核發監察令[1]。

我國之通訊監察相關規範，係以通保法作為政府機關進行通訊監察之依據；

[1] FISA also established the United States Foreign Intelligence Surveillance Court ( FISC ), a special US Federal court that holds nonpublic sessions to consider issuing search warrants under FISA. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286，最後瀏覽日：106 年 8 月 31 日。

依通保法規定，當調查發現相關情事可能危害國家安全之情節重大、通訊內容與案件相關，且無法以其他方式進行調查時，得發通訊監察書進行監察。有關通保法准許通訊監察之要件如下：一、重罪原則，涉犯三年以上有期徒刑之罪及其他所列舉之重罪者[2]；二、必要性，須無法以其他方式為調查者；三、關聯性，通訊內容與案件相關者；四、令狀原則，須視情況由法院或綜理國家情報工作機關首長核發通訊監察書，由情報機關首長核發者，並須經法院事後補行同意；五、事中監督[3]，每十五日至少作成一次以上之報告書；六、事後通知，通訊監察結束後應通知受監察人[4]。

而為有效進行通訊監察，電信業者有義務提供設備，以利相關權責機關依法進行監聽等監察作業。且電信業者必須在合理範圍內建置、維持足夠的通訊設備以為監察之用[5]。當有關機關於進行通訊監察時，須符合相關法令規定，如違法監察他人通訊時，違法人員可處 5 年以下有期徒刑，若不法行為係意圖營利者，則最重可處 7 年以下有期徒刑[6]；違法監聽取得之資料均應沒收[7]，

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

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

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

[5] 通訊保障及監察法第 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。」。

[6] 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

亦無證據能力；此外，違法監聽時亦須負損害賠償責任[8]。

## 【管理 Tips】

公務機關對於資訊保護與資訊（通訊）監察間應取得平衡，這也是為什麼通訊監察結束後，原則上必須針對受監察人為事後通知，使其知悉有通訊監察之情事發生。若以通訊監察之透明化角度思考，如通訊監察得以透明化，可有助於降低政府濫權監聽之可能，亦有助於政府運作之穩定性、透明性，此外，透過事後監督之檢視，得以釐清受監察人是否遭受侵害，以保障相關人員之權益。

## 【相關標準】

ISO 29100：2011（CNS29100）

●5.8　公開、透明及告知

(1)標準內容：　堅持公開、透明及告知原則，意指下列事項。

— 提供予個人可識別資訊(personally identifiable information, PII)當事人，關於 PII 控制者對於處理 PII 之政策、程序及實務的清楚且易取得之資訊。

—告知中包括，處理中之 PII、處理目的、PII 可能接露對象之隱私權利害相關者型式，以及 PII 控制者身分含 PII 控制者之聯絡資訊。

---

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。」。

[7] 通訊保障及監察法第 26 條第 1 項：「前二條違法監察通訊所得之資料，不問屬於犯人與否，均沒收之。」

[8] 通訊保障及監察法第 19 條：「違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，負損害賠償責任。　　被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。　　前項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」。

—揭露 PII 控制者提供予 PII 當事人之選擇及方式，以限制處理、存取、修正及移除其資訊。

—當 PII 處理程序發生重大變更時，告知 PII 當事人。

可要求包含 PII 處理邏輯之一般資訊的透性，尤其是 PII 處理涉及影響當事人之決策時更應如此。處理 PII 之隱私權利害相關者宜使大眾容易取得關於管理 PII 有關之政策及實務的特定資訊。適當時，宜在內部紀錄及溝通，所有影響 PII 處理之契約義務。亦宜對外溝通該等契約義務之非機密範圍。

此外，PII 處理之目的宜足夠詳盡，以便使 PII 當事人瞭解下列事項。

—所規定目的所要求之規定 PII。

—PII 蒐集之所規定目的。

—所規定之處理(包括蒐集、溝通及儲存機制)。

—將存取 PII 及 PII 可轉移對象之授權自然人的型式。

—所規定之 PII 資料持有及廢棄要求。

(2)適用說明： 組織於處理個人可識別資訊時，其程序、機制應可被檢驗且透明，並使該資訊之權利人知悉蒐集、使用之目的、處理及保存方式等。如此可使相關權利人對組織產生信任，亦可幫助避免濫為蒐集、處理或利用權利人資料行為之發生。我國機關辦理之通訊監察，為使當事人瞭解受監察之範圍，以及是否有權益受侵害等情形，按通保法相關規定，除係為避免國家安全遭受危害而對外國勢力或境外敵對勢力情報之蒐集必要者外，執行機關應於通訊監察結束

後，將通訊監察內容告知受監察者。

類別：資訊監察【案號：M10634】

# 澳洲防恐 逼臉書等交加密訊息

## 【焦點話題】

由於恐怖分子及犯罪集團等，利用諸如社群媒體等方式進行犯案訊息傳遞之作法日盛，澳洲警方對於目前僅能得透過電信商取得資料之方式感到不足，冀望可透過立法程序來增加相關規定，以利檢警執法。因此，澳洲政府將提出新法案，強制臉書、WhatsApp 等社群媒體，向警方提供恐怖分子等嫌犯之加密訊息，若新法通過後，當局將可自相關網路公司取得經加密之資料，且電子裝置生產商、科技公司等亦需協助執法人員攔截及解讀犯嫌所發出之訊息。

【參考資料來源：世界日報，106/7/15】

## 【重點摘要】

1. 通訊保障及監察法(以下簡稱通保法)規定電信、郵政業者有協助執行通訊監察機關進行通訊監察之義務。且電信業者必須建置且維持足夠的通訊設備以為通訊監察之用。
2. 電子通訊軟體業者並非電信業者，因而權責機關尚無法依通保法要求此類業者協助辦理通訊監察，且許多電子通訊軟體業者屬外國公司，伺服器亦設於國外，實質上亦不易向其要求提供協助。

## 【法律觀點】

我國之通訊監察相關規範，係以通保法作為政府機關進行通訊監察之依據，其立法目的在於保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序[1]。

[1] 通訊保障及監察法第 1 條。

依通保法規定，當調查發現相關情事可能危害國家安全之情節重大、通訊內容與案件相關，且無法以其他方式進行調查時，得發通訊監察書進行監察。有關通保法准許通訊監察之要件如下：一、重罪原則，涉犯三年以上有期徒刑之罪及其他所列舉之重罪者[2]；二、必要性，須無法以其他方式為調查者；三、關聯性，通訊內容與案件相關者；四、令狀原則，須視情況由法院或綜理國家情報工作機關首長核發通訊監察書，由情報機關首長核發者，並須經法院事後補行同意；五、事中監督[3]，每十五日至少作成一次以上之報告書；六、事後通知，通訊監察結束後應通知受監察人[4]。

故如事涉國家安全，而相關權責機關依通保法規定得為合法之通訊監察時，電信業者有義務提供設備，以利相關權責機關依法進行監聽等監察作業。且電信業者必須在合理範圍內建置、維持足夠的通訊設備以為監察之用[5]。

然電子通訊軟體業之業務，看似與電信業務相似，但目前並未被認定為電信

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

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

[5] 通訊保障及監察法第 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。」。

事業[6]，且電信法規亦未將其納入第一、二類電信業者管理[7]，故權責機關尚未能將電子通訊軟體業認定為電信事業，並依通保法之相關規定，要求此類業者配合辦理通訊監察事務。

又，許多電子通訊軟體業者為外國業者，其伺服器亦常設於國外，執法機關因管轄權問題，時有無法請求業者提供必要協助之狀況。有論者認為，應修正電信法，將電子通訊軟體業者納入電信法之管理範圍，以要求電子通訊軟體業者配合執法機關依法進行通訊監察。惟於修法時仍應謹慎避免因反恐或其他執法事由，而任由政府輕易監控民眾；在反恐與人權間如何取得平衡，是規劃修法時，務必加以正視之課題。

## 【管理 Tips】

未來對於電子通訊軟體應如何管理，宜以基本人權與國家安全間之平衡為原則，依通保法第 1 條，公務機關於進行通訊監察任務時，對於通訊監察之申請，應符合比例原則，尤應以相當性、必要性等原則為依歸。

其次，雖我國目前對電子通訊軟體進行通訊監察之相關法規，仍待訂定，然於相關法規完備後，所進行之通訊監察，亦應具備有效之管理措施，以避免相關疏漏、誤失之發生，諸如機關於辦理監察之申請、執行前準備、執行時、執行後，均須注意控制風險避免疏失、符合相關法令，以及紀錄留存等事務之辦理。

## 【相關標準】

[6] 按行政院主計總處於 105 年 1 月發布之行業分類標準，電信業指「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。不包括：線上提供可安裝於個人行動裝置之通信軟體供應者，應依其主要經濟活動歸入適當類別。」。

[7] 電信法第 11 條:「電信事業分為第一類電信事業及第二類電信事業。第一類電信事業指設置電信機線設備，提供電信服務之事業。前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備。第二類電信事業指第一類電信事業以外之電信事業。」。

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。本案如為我國國安單位基於防恐而欲進行通訊監察，目前所適用之法規應屬通保法，依該法之規定，針對通訊監察應符合重罪原則、必要性原則、關聯性原則、令狀原則等辦理原則，且該法亦規定須配合之業者為電信、郵政業者，故若欲要求電子通訊軟體業者配合通訊監察，宜進行通保法之修法或另立新法，以供日後執行時之依歸，並符合依法行政原則。

類別：資訊監察【案號：M10635】

## 查私菸偷裝GPS不起訴 法官打臉：加重判刑

### 【焦點話題】

具有司法警察身份之王男，為查緝私菸，擅自將 GPS 衛星定位追蹤器裝置在陳男使用的貨車底盤下，監看貨車行蹤 7 天，在取回時遭陳男發現並被告妨害秘密，地院審理認為，刑法妨害秘密罪保護的是人民免於身心傷害之身體權，以及行動自由、生活私密領域不受侵擾的自由與個人資料自主權，其中生活私密領域不受侵擾之自由及個人資料之自主權，更屬憲法所保障的權利。而車輛在公共道路上的行跡與駕駛或乘員的活動，除了在車身上標示駕駛姓名等明示放棄隱私期待等情形外，通常來說可以認為駕駛人並不欲公開其個人行蹤，此時個人的行蹤就屬於妨害秘密罪規範「非公開活動」。且王男具公務員身份，據此，法院對其加重其刑，判刑拘役 50 天，得易科罰金，緩刑 2 年確定。

【參考資料來源：蘋果日報，106/2/7】

### 【重點摘要】

1. 以 GPS 接收器追蹤他人位置，除了受追蹤者有明白表示要放棄隱私期待外，應認以駕駛人並不欲公開其個人行蹤，此時個人的行蹤屬於刑法妨害祕密罪規範「非公開活動」。
2. 組織宜規劃並建立切適的觀察及動態掌握等資料蒐集活動程序並予以文件化，讓成員得以依循規範，進行適當決定，避免其自行決定蒐集活動之發動與作法，藉由程序規定控制作業方式，達到有效的防範與管理。

### 【法律觀點】

警察主管機關利用 GPS 接收器與傳統跟監之目的，均是要得知受追蹤人所在位置，但是相較於傳統跟監，透過 GPS 接收器可連續多日、全天候不間斷追蹤他人車輛行駛路徑及停止地點，可鉅細靡遺長期掌握他人行蹤，也就是利

用「拖網式監控」大量地蒐集、比對定位資料，私人行蹤將因此被迫揭露[1]，而實務見解認為，駕駛車輛行駛於供公眾往來道路，除了有明白表示要放棄隱私期待外，通常來說可以認為駕駛人並不欲公開其個人行蹤，也就是個人主觀上對於其行蹤具有不欲公開的隱私合理期待，如果當事人就其行蹤具有隱私合理期待，此時個人的行蹤就屬於「非公開活動」[2]，因此無故在他人車上裝設 GPS 接收器追蹤他人行蹤，即有觸犯刑法第 315-1 條[3]妨害祕密罪的可能[4]。

本案被告得合法進行觀察及動態掌握等蒐集活動之依據，係規定在警察職權行使法第 11 條[5]，被告必須出於「防止犯罪」所必要，才可以藉由目視或科技工具，進行觀察及動態掌握等蒐集活動，如果是為已經違法之犯罪行為而蒐證時，並無法藉由警察局長書面同意將蒐集活動合法化，且受追蹤人駕駛車輛行駛於供公眾往來道路，仍為隱私權保護範疇，警察主管機關所蒐集的資料屬於「非公開活動」，因未有合法蒐集要件，故仍觸犯刑法第 315-1 條妨害祕密罪。

## 【管理 Tips】

[1] 臺灣高等法院 106 年度上易字第 1322 號刑事判決。

[2] 臺灣高等法院 104 年度上易字第 352 號刑事判決、臺灣高等法院 100 年度上易字第 2407 號刑事判決均同此見解。

[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] 依通訊保障及監察法第 3 條第 1 項規定，通訊係包括利用電信設備發送、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；郵件及書信；言論及談話，因此針對 GPS 接收器所蒐集的資訊，是否適用通訊保障及監察法一事，法務部作出法檢字第 10100511840 號函表示，所謂信息均應含有意思表示，也就是進行通訊雙方之間，能夠通過各種方式進行溝通，而達到意思表示之目的，如無法藉信息之傳達，使通訊雙方得以互相溝通及理解彼此意，那麼就不是通保法所應予保障對象，因此，為偵辦案件而於犯罪嫌疑人之車輛裝設 GPS 接收器，因為 GPS 接收器所蒐集者僅為「位置」之資訊，並不包括意思表示之信息傳達，因此並無通保法之適用。

[5] 警察職權行使法第 11 條第 1 項：「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動：一、有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。二、有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。」

在管理程序上，警調機關如為偵辦刑案，欲對有犯罪之虞者進行觀察及動態掌握等資料蒐集活動時，可從下列面向加以思考，以避免發生違法情事。首先，進行資料蒐集活動前，必須經由警察局長書面同意，以作為程序管控，避免不必要的資料蒐集；其次，受蒐集者應為有事實足認其有觸犯最輕本刑 5 年以上有期徒刑之罪之虞，或有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞；再者，進行觀察目的必須為了防止犯罪，而非對已經違法之犯罪行為進行蒐證；另外，必須在長官同意的一定期間內進行，該一定期間不得超過一年，且至多延長一次；最末，得觀察之內容，必須是受蒐集者無隱私或秘密合理期待之行為或生活情形，因此如果是透過 GPS 等拖網式監控手段進行追蹤，將破壞受蒐集者的隱私合理期待。

因此，警調機關宜依據上開說明，規劃並建立切適之觀察及動態掌握等資料蒐集活動流程並予以文件化，透過程序讓成員可以依循規範，做出適當的決定，避免相關人員自行決定觀察內容及資料蒐集活動之發動與作法，藉由程序規定以控制作業方式，並傳達至全體成員並落實於日常作業，以達到有效之風險管理。

**【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：　組織應確認本身業務以及業務所涉及之法律，並透過文件化建立相關程序，俾使相關人員能有所依循，透過流程化之操作，落實於日常作業，確保避免因人員未依照程序進行，本案中有關機關宜了解相關法規對於蒐證、偵查等要

求後，建立適當程序與完整流程，以供機關人員依循。

類別：資訊監察【案號：M10636】

## 兒孫燒炭亡 嬤控警延誤害命

### 【焦點話題】

去年 11 月，郭姓女子帶著一歲兒子於車內燒炭雙亡。郭女母親指控，她發現女兒失蹤後，約於晚上 9:50 至派出所報案。因其心急，乃不斷請求警員，甚至對警員下跪，希望警員能儘速派人協助找尋女兒，但警員卻仍堅持先做完筆錄，直到深夜 11 時許，該警員才通知電信公司定位，最後仍未能救回郭女及稚兒。郭母認為警方製作筆錄耗時過久，才未能救回兩人，遂於今年 1 月提起國賠訴訟，並盼警方改善查詢失蹤者之流程，別再因此貽誤救人時機。警方對此表示，因郭女案例，已修正相關作法，日後失蹤查尋將依「電信事業處理有關機關查詢電信通信紀錄實施辦法」辦理，並已發文通報全國警局。依修正後作法，警方於受理報案取得 E 化編號，即可先查詢失蹤人行動電話發話基地位置，方便查尋、救人，事後再補製作筆錄。

【參考資料來源：蘋果日報，106/7/6】

### 【重點摘要】

1. 失蹤人口緊急查尋具特殊性，受理人員接受報案後，應詳細調查失蹤人之身分背景、交往對象及可能去向，積極展開查尋作為。必要時得依相關規定報請調閱失蹤人之通信紀錄等資料，以利查尋。遇緊急狀況，如發現依既有機關程序，可能緩不濟急時，為免除當事人生命、身體等危險，仍得逕依個資法之規定，蒐集並據以利用個人資料。
2. 依「電信事業處理有關機關查詢電信通信紀錄實施辦法」之規定，警方如係為免除當事人之生命危險，在人員失蹤時，其可先依該辦法向電信業者申請查詢通信定位資料，事後再補具正式文件。

### 【法律觀點】

通信紀錄屬於個人資料之一種，受到個人資料保護法之保護，必須符合法定

要件方可蒐集、處理，且原則不得為特定目的外之利用。

警方為救護當事人生命，如有必要請求電信公司提供通信紀錄，屬個人資料保護法第 15 條之「執行法定職務必要範圍」，依據個資法第 15 條，為合法蒐集個人資料，之後並可將該蒐集取得之資料用於蒐集時之特定目的。

對電信公司而言，其提供通聯定位資料給警方，雖係對通信紀錄為特定目的外之利用，但因屬個資法第 20 條所定「為免除當事人生命、身體...之危險」之情形，所提供資料亦為協尋失蹤人之必要，故亦合法。

雖然依個資法之規定，警方如係為緊急查尋失蹤人位置，以救護其生命，而要求電信公司提供失蹤人通信紀錄，係屬合法；但警方辦理失蹤人查尋案件時，可能仍會先依「失蹤人口查詢作業要點」第 7 點[1]，製作詳盡報案筆錄，再將筆錄併電信查詢資料申請表，申請調閱相關通聯定位資料。為恐緩不濟急，程序上改依電信法所授權訂定之「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 3 條第 1 項但書[2]規定，由查詢機關首長等，依程序提出申請，並於查詢後三個工作日內補具正式文件，確實更為適當。

## 【管理 Tips】

檢警等公務機關為免除當事人之生命、身體等之危險，如確有必要，依法本即可向電信事業調閱通信紀錄，而為使機關人員能在合法的前提下儘速反應，

[1] 失蹤人口查尋作業要點第 7 點「受理緊急查尋案件應注意下列事項：(一) 製作報案筆錄應載明緊急查尋情狀，並詳細調查失蹤人之身分背景、交往對象及可能去向，積極展開查尋作為；必要時，得將筆錄連同查詢電信資料申請表，併傳勤務指揮中心依相關規定報請調閱失蹤人及特定對象通聯紀錄，或報請分局防治（戶口業務）單位調閱失蹤人健保就醫等資料，以利查尋。所調取通聯資料應於事後移由分局防治（戶口業務）單位併案持續追蹤、管考及複查。(二) 視個案情形，立即報請勤務指揮中心通報轄內或他轄有關單位、線上警力緊急查尋，或洽請大眾媒體報導協尋。(三)未滿七歲者於緊急查尋二十四小時後仍未尋獲，且經查疑涉刑事案件時，比照重大刑案列管偵辦。(四) 其他必要之適當查尋處置作為。」。

[2] 電信事業處理有關機關查詢電信通信紀錄實施辦法第 3 條第 1 項但書：「但案情特殊、情況緊急之查詢，得由法官、軍事審判官、檢察官、軍事檢察官、查詢機關首長或其書面指定人於電信通信紀錄查詢單署名並加蓋職章及連絡人之資料，視同機關正式公文書先傳真之，並經回叫確認為之，查詢後應於三個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本。未於三個工作日內補具公文或查詢單者，電信事業得拒絕受理其再次傳真查詢。」。

機關先釐清法律規定，並據以明定具體程序供機關人員遵循辦理，確屬良策。在訂定程序時，應先確認法律規定之內容，儘量將可能之作法納入程序規定中。在程序具體之餘，針對緊急狀況，亦需在合法的前提下權留調整與應變之空間。

電信事業於各機關要求調閱資料時，應注意機關所提出之調閱需求是否有法源依據，並符合相關要件，例如是否符合個人資料保護法、電信法、電信事業處理有關機關查詢電信通信紀錄實施辦法等，並留存依法提供資料之紀錄。

**【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：　本案中，機關可在確實瞭解相關法令後，依法令之要求與其所賦予之空間，訂定或適用程序，以符合法律規定並提升機關之效能。

ISO 29100：2011（CNS29100）

●5.6　利用、持有及揭露原則

(1)標準內容：　堅持利用、持有及揭露限制原則，意旨下列事項。

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

- 除非適用之法律明確要求不同的目的，否則將 PII 之利

用限制於蒐集之前 PII 控制者所規定之目的。

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

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

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

(2)適用說明：個人可識別資訊之利用、持有及揭露 ( 包含移轉 ) 限制於為履行特定、明確及合法目的所必要者。除非適用之法律明確要求不同的目的，否則將個人可識別資訊之利用限於蒐集之前個人可識別資訊控制者所規定之目的。

本案中，電信事業應認知到將當事人之通聯定位資料提供給警方係屬特定目的外利用，故在提供前，應先確認其已具備特定目的外利用之合法化要件。

# 肆、資訊應用（Application）

類別：資訊應用【案號：A10637】

## 未來無人機使用者 可能須先註冊方得操作

### 【焦點話題】

民航主管機關今年 3 月預告擬修正《民用航空法》(下稱民航法)部分條文，未來民眾持有最大起飛重量高於 250 公克以上之遙控無人機，或此類無人機係屬公務機關或法人所有者，應辦理註冊。且操作遙控無人機者，亦須經測驗合格，並取得操作證。違反相關規定者，將被處以罰鍰。此外，民航主管機關表示，由於無人機使用者於辦理註冊時，須以真實姓名及聯絡方式為之，民航主管機關規劃與健保卡結合，惟此部分尚須經衛福主管機關同意，故有待透過共同上級機關與衛福主管機關進行溝通。

【參考資料來源：蘋果日報，106/7/19】

### 【重點摘要】

1. 民航法修正草案之遙控無人機係指自遙控設備以信號鏈路進行飛航控制之無人航空器。
2. 為求有效管理，民用航空法修正草案要求最大起飛重量高於 250 公克以上等之遙控無人機，使用者必須以真實姓名及聯絡方式，向主管機關註冊。

### 【法律觀點】

遙控無人機之風行，時聞有致生飛安、公安、國安等問題之虞，而目前又欠缺適當法令可予事前規範，而必須於危安事件發生後，再視狀況加以處理。例如：於機場四周管制範圍內，有礙飛航安全物體係依民航法處理；撞毀他人建築物時，建築物所有權人依照民法請求損害賠償；於要塞堡壘地帶之禁航區內為非法偵查時，則依要塞堡壘法加以規範[1]，適用上未必均能及時妥適處置遙控無人機所引發的問題。為求對相關問題能有更切合實際之處理，民

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

航主管機關於 106 年 3 月預告「民用航空法」部分條文修正草案[2]，為遙控無人機訂定專章。

民航法修正草案，定義遙控無人機為：自遙控設備以信號鏈路進行飛航控制之無人航空器[3]。而最大起飛重量高於 250 公克以上等之遙控無人機，使用者必須以真實姓名及聯絡方式，向民航主管機關註冊；而操作最大起飛重量 25 公斤以上、公務機關或法人所有之遙控無人機，或最大起飛重量 1 公斤以上而不逾 25 公斤且裝置導航設備之遙控無人機時，使用者亦須通過測驗取得操作證[4]。

因遙控無人機係以信號連結進行飛航控制，他人不易預測其實際運作狀態，為避免因人為控制或資通設備發生故障，進而影響飛航及國家安全，故該法亦擬限制遙控無人機之活動範圍，日後將由民航主管機關公告禁止使用遙控無人機之區域[5]；此外亦明定從事遙控無人機活動應遵守之規定[6]，包括遙控無人機距地表高度不得逾四百呎、不得以遙控無人機投擲或噴灑任何物件等。且如草案獲通過，則日後因遙控無人機造成損害時，遙控無人機之所有人依

[2] 民用航空法部分條文修正草案已由交通部陳報行政院審查，本案例所引用草案為 106 年 3 月 15 日交航(一)字第 1068100072 號公告之版本，網址：http://motclaw.motc.gov.tw/wfrmDownload.aspx?Type=Draft&ID=2586。

[3] 民用航空法修正草案第 2 條第 26 款。

[4] 民用航空法修正草案第 99-10 條：「自然人所有之最大起飛重量二百五十公克以上及公務機關或法人所有之遙控無人機應辦理註冊並將註冊號碼標明於遙控無人機上顯著之處。 下列遙控無人機操作人應經測驗合格，發給操作證後，始得操作遙控無人機： 一、操作最大起飛重量二萬五千公克以上之遙控無人機者。二、操作公務機關或法人所有之遙控無人機者。三、操作最大起飛重量一千公克以上而不逾二萬五千公克且裝置導航設備之遙控無人機者。」。

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

[6] 民用航空法修正草案第 99-14 條第 1 項：「從事遙控無人機飛航活動應遵守下列規定:一、遙控無人機距地表高度不得逾四百呎。二、不得以遙控無人機投擲或噴灑任何物件。三、不得裝載依第四十三條第三項公告之危險物品。四、依第九十九條之十六所定規則之操作限制。五、不得於人群聚集或露天集會遊行上空活動。六、不得於日落後至日出前之時間飛航。七、在目視範圍內操作，不得以除矯正鏡片外之任何工具延伸飛航作業距離。八、操作人不得在同一時間控制二架以上遙控無人機。九、操作人應隨時監視遙控無人機之飛航及其周遭狀況。十、應防止遙控無人機與其他航空器、建築物或障礙物接近或碰撞。」。

規定必須負絕對責任[7]，亦即縱使所有人無故意或過失，例如，因為天災而導致損害發生，所有人仍應要負損害賠償責任。

**【管理 Tips】**

若遙控無人機出現狀況時，諸如於空中因程式設計不當而墜毀、因駭客入侵系統使遙控無人機無法正常運行等，均可能因而致生人民生命、財產之損失，特別是目前有關駭客主要攻擊之對象，其一即為控制無人機之物聯網裝置設備，該等設備之資訊安全問題已成為網路安全新興風險議題，準此，相關產品之開發單位於產品設計時，即須將資通安全相關事項加入產品功能中，而使用者於產品使用時，亦須注意相關資訊安全相關措施，以避免或抵禦駭客攻擊等侵害行為而導致無法操控之損失。

**【相關標準】**

ISO 27001：2013（CNS 27001）

●A.11.2.8　無人看管的資訊設備

(1)標準內容：　使用者應確保無人看管之設備具適切保護。

(2)適用說明：　因無人機可能之運行方式可能為人為操控，抑或為自動運行，而為確保無人機設備之安全性，無人機擁有者應確保無人機在運行過程中有適當保護措施，不致遭人惡意攻擊致無法正常運行，或是成為恐怖攻擊之器具。

●A.13.1.2　網路服務之安全

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

[7] 民用航空法修正草案第 99-15 條第 1 項：「操作遙控無人機而致他人死傷，或毀損他人財物時，不論故意或過失，遙控無人機所有人應負賠償責任；其因不可抗力所生之損害，亦應負責。自遙控無人機上落下或投下物品，致生損害時，亦同。」。

或委外提供。

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

類別：資訊應用【案號：A10638】

# 無人小巴 凌晨試行台北街頭

## 【焦點話題】

台北市政府辦理「自動駕駛小巴實驗」專案，自 8 月 1 日迄 8 月 5 日，讓無人駕駛之小巴士，於凌晨時段行駛於信義路雙向公車專用道。該府官員表示，礙於現行法令並無相關檢驗標準，因此，自動駕駛車輛仍無法像一般車輛領牌上路。在試行結束後，民眾尚無法於道路上搭乘自動駕駛小巴，自動駕駛小巴暫時仍僅能運行於封閉路段，例如，於動物園中，充當遊園車，如果肇事，則可能由動物園負起責任。客運業者則表示，自動駕駛巴士是未來發展趨勢，很期待自動駕駛能解決現行公車駕駛人力不足的問題。

【參考資料來源：自由電子報，106/7/28】

## 【重點摘要】

1. 自動駕駛設備為未來趨勢，惟我國並未針對自動駕駛設備規定安全檢驗標準，因此亦無從對其進行安全檢驗，而此類設備尚無法領牌於道路上行駛。

2. 從技術面安全而言，自動化駕駛設備對道路之規劃、定位、目標識別、判斷等能力是否足夠仍是主要問題；從資訊面安全問題而言，自動化駕駛設備則仰賴大量資料蒐集並進行資料傳輸，須面臨作業系統遭受駭客連網入侵等相關風險，故須確保相關安全機制之有效性。

## 【法律觀點】

車輛欲於道路上行駛，依公路法第 63 條第 1 項[1]規定，汽車及電車均應符合交

[1] 公路法第 63 條第 1 項：「汽車及電車均應符合交通部規定之安全檢驗標準，並應經車輛型式安全檢測及審驗合格，取得安全審驗合格證明書，始得辦理登記、檢驗、領照。國產汽車及電車製造業，應具備完善之汽車安全檢驗設備，嚴格實施出廠檢驗。製造業及進口商之檢驗設備經公路主管機關查驗合格發給證照者，得受委託為其製造或進口汽車之申請牌照檢驗。」。

通部規定之安全檢驗標準，並應經車輛型式安全檢測及審驗合格，取得安全審驗合格證明書，始得辦理登記、檢驗、領照，進而合法上路。而無合法牌照行駛者，按道路交通管理處罰條例第 12 條第 1 項第 1 款[2]規定應處罰鍰。目前我國並未針對自動駕駛設備定有安全檢驗標準，因此亦無從對其進行安全檢驗，遑論允許其於道路上行駛。

再者，如為非完全自動駕駛系統，肇事時駕駛人可能須擔負相關責任，但如為完全自動化駕駛系統時，因為實際上已無駕駛人，而乘客並無操控車輛之權限，因此如果發生事故，導致人身安全或財產之損失，被害人是否可主張產品瑕疵，向車輛製造商請求賠償，仍有爭議。此外，自動駕駛設備如須連網以協助駕駛或進行程式更新，即提高了被駭客入侵之風險，如此，除了肇事責任之歸屬將更難判斷外，也會涉及隱私保護等事項。因此，未來政府於評估、推動自動駕駛車輛上路政策時，亦應同步檢視諸如道路交通管理處罰條例、道路交通安全規則等交通法規，並應由相關主管機關針對諸如民法、消費者保護法、個人資料保護法等法規之規定，應如何適用於涉及自動駕駛設備之情形，進行研析與函釋說明。

**【管理 Tips】**

自動化駕駛設備所面臨到的問題在於如何取得有效辨識道路狀況，以達到確保用路順暢，以及駕駛人與其他用路人安全之平衡。

從技術面安全而言，包含自動化駕駛設備對道路的規劃、定位、目標的識別、判斷等能力是否足夠等，均屬該技術必須克服之問題。而有關資訊面安全部分，自動化駕駛設備之判讀仰賴數據分析，亦即需大量資料蒐集並進行資料傳輸，自動化駕駛設備勢必面臨作業系統遭入侵之風險，而因道路行駛為高風險行為，如果因為資訊安全導致事故發生，所造成損害將遠大於一般連網設備事故。

[2] 道路交通管理處罰條例第 12 條第 1 項第 1 款：「汽車有下列情形之一者，處汽車所有人新臺幣三千六百元以上一萬零八百元以下罰鍰，並禁止其行駛：一、未領用牌照行駛。」。

因此，對於有意於生產自動化駕駛設備廠商，所應注意者並不僅止於法規開放等問題，更重要的是意識到且面對技術安全及資訊安全所可能產生之風險，方可在後續法規開放後，予以即時、有效之因應。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.13.1.2　網路服務之安全

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

(2)適用說明：　組織應確保無論是內部或外部服務，其所使用之網路已具備相關安全機制，以進行網路服務之管理與安全維護。本案自動駕駛設備係需要透過網際網路進行資料傳輸，因此應具備相當之通訊安全措施，以避免遭到駭客攻擊等入侵導致相關損害。

●A.18.1.1　適用之法規及契約的要求事項之識別

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

(2)適用說明：　組織應瞭解並依循其應適用之法令，進行相關業務之執行，以避免觸法。本案所提目前法規尚無針對自動駕駛設備訂定相關標準等規範，現有規定究應如何適用於涉及自動駕駛之情形，亦待釐清；惟未來如有上述規範出現，或主管機關已就相關法規適用進行闡釋時，組織即應適時瞭解相關內容，並切實遵循，以免觸法。

類別：資訊應用【案號：A10639】

## 開放網路申辦月租型門號 可用數位簽章方式申辦

### 【焦點話題】

通傳主管機關審查通過 5 家電信業者「行動寬頻業務營業規章」，於網路申請電信門號新增數位簽章方式。通傳主管機關表示，民眾只要傳真雙證件影本，再以符合電子簽章法之數位簽章方式進行身分識別後，就可透過網路辦理月租型門號。

過去民眾要申辦月租型門號，都必須拿雙證件到門市辦理，對於居住在偏鄉或行動不便的民眾來說相當不方便。這次 5 家行動寬頻業者修訂營業規章，主要是針對自然人申辦月租型門號時，得以網際網路方式辦理，民眾只要傳真雙證件影本後，再以數位簽章方式進行身分識別，就可以辦理月租型門號，減少過去要攜帶雙證件到門市親辦的往返和等候時間。

隨著新科技的發展，各項創新服務與應用不斷推陳出新，通傳主管機關除了兼顧民眾便利性外，也將關注對於資安和治安可能疑慮的影響，未來將持續視實施情況與各界反應，並在兼顧消費者便利性、業者競爭力和治安需求下檢討精進。

【參考資料來源：經濟日報，106/10/12】

### 【重點摘要】

1. 內政部憑證管理中心所簽發及管理的自然人憑證，適用於網路中的身分識別及資料保護，無論是公部門或是私部門，均可以用自然人憑證作為在網路中的身分辨識。
2. 組織於使用電子文件時，可透過應用數位簽章，確認簽署者的身分，確保內容不受到變更或竄改，更可使簽署人難以否認知悉文件內容，達到如同紙本文件之效力。

**【法律觀點】**

電子簽章法第 2 條第 3 款：「指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。」同法第 9 條第 1 項規定：「依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。」第 10 條規定：「以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第一項之效力：一、使用經第十一條核定或第十五條許可之憑證機構依法簽發之憑證。二、憑證尚屬有效並未逾使用範圍。」因此，當事人間如要以數位簽章方式簽署文件時，必須是經主管機關核定或許可之憑證機構依法簽發之憑證，才具有法律上之效力。

目前經主管機關所核定之憑證機構，包括政府機關與民間企業位共有 7 個單位[1]，其所發行的憑證各有對應之適用範圍。以內政部憑證管理中心為例，內政部憑證管理中心所簽發及管理的憑證為自然人憑證，而其適用於網路中的身分識別及資料保護[2]。因此，無論是公部門或是私部門，均可以用自然人憑證作為在網路中的身分辨識。

惟基於電信業者為特許事業，相關服務內容均必須載明於營業規章中，並報請通傳主管機關核准後，才得以公告實施[3]，因此電信業者如欲以數位簽章作為身分辨識之手段，也必須得到主管機關核准後方可使用。在通傳主管機關於 106 年 10 月核准行動寬頻業務經營者所修訂之營業規章之後，自然人辦理

[1] 經核定之憑證機構名單一覽表，http://gcis.nat.gov.tw/mainNew/subclassNAction.do?method=getFile&pk=690 ，（最後瀏覽日：106 年 11 月 2 日）

[2] 內政部憑證管理中心憑證實務作業基準第 1.9 版 1.3.7.1 憑證之適用範圍：「憑證管理中心所簽發及管理的憑證類別為自然人憑證，且包含簽章用及加密用憑證。憑證管理中心所簽發的憑證符合憑證政策保證等級第三級之規定，本憑證適用於網路中的身分識別及資料保護。」。

[3] 電信法第 27 條第 1 項：「第一類電信事業，應就其服務有關之條件，訂定營業規章，報請電信總局轉請交通部核准後公告實施；變更時亦同。」而國家通訊傳播委員會組織法第 2 條規定：「自本會成立之日起，通訊傳播相關法規，包括電信法、廣播電視法、有線廣播電視法及衛星廣播電視法，涉及本會職掌，其職權原屬交通部、行政院新聞局、交通部電信總局者，主管機關均變更為本會。其他法規涉及本會職掌者，亦同。」因此，於電信法所規定應報請核准之主管機關亦隨之變更。

申請月租型門號時，得以符合電子簽章法之數位簽章方式簽署申辦文件，透過上傳包括國民身分證、護照或外僑永久居留證，及其他足資辨識身分之證明文件的影像檔，留存於行動寬頻業者系統，供其進行身分核對即可[4]。

隨著通傳主管機關開放月租型行動寬頻承租之自然人身分核對，得以電子簽章法之數位簽章方式進行後，可想見將來會有愈來愈多業務可透過此方式進行身分確認或是資料加密，將有助於提昇民眾使用各項服務的便利性，更有利業者之服務推動及競爭力提升。

**【管理 Tips】**

數位簽章是透過簽署人之私鑰所形成的電子簽章，再以公鑰加以驗證後，可確認簽章者的身分，防止文件的偽造；亦可確保內容不受到變更或竄改，防止文件遭到攔截後變更內容；更可使簽署人因無法在不否認其數位金鑰的情況下否認該文件上的簽章，進而無法否認文件內容為其簽署。

因此，無論是電信業者或是其他得以利用網際網路作為業務媒介的工作型態者，均可藉由數位簽章作為身分認證機制之一環，確保電子文件的真實性，並透過適當的安全防護，讓使用者得以安心接受無紙化服務，進而拓展其業務發展。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.13.2.2　資訊傳送協議

(1)標準內容：　協議應詳細闡述組織與外部各方間營運資訊之安全傳送。

(2)適用說明：　組織進行資訊傳送時，必須驗證身分並確保文件內容的完

[4] 此處係以中華電信股份有限公司之行動寬頻業務營業規章為例，http://www.cht.com.tw/portal/rule_detail?rule_id=112，其他包括台灣大哥大股份有限公司、台灣之星電信股份有限公司、亞太電信股份有限公司及遠傳電信股份有限公司，均於其行動寬頻業務營業規章有相類條文。（最後瀏覽日： 106 年 11 月 2 日）

整，在本案例中，即是以數位簽章的方式來確保上開目的之達成。

類別：資訊應用【案號：A10640】

## 跨國資訊交換 台灣準備好了

### 【焦點話題】

台灣雖無法參加多邊的共同申報準則 (Common Reporting Standard for Automatic Exchange of Financial Account Information in Tax Matters, CRS)，但稅捐稽徵法第 5-1 條、第 46-1 條已修正通過，相關規定之修正被視為是 CRS 的前置工作。財政主管機關也多次表示，台灣將按國際新資訊透明標準(稅務用途金融帳戶資訊自動交換準則)，完善與有租稅協議的締約國，完善雙邊資訊交換機制。惟現有稅捐稽徵法只牽涉到與其他「國家」間之租稅協定，所涉範圍並不包含港、澳和中國大陸，未來是否需於台灣地區與大陸地區人民關係條例、香港澳門關係條例等特別法中，增訂金融資訊交換等相關規定，有待各界討論。

【資料來源：經濟日報，106/7/29】

### 【重點摘要】

1. 按稅捐稽徵法之規定，財政主管機關或其授權之機關執行租稅條約或協定所需資訊，不受特定金融及稅務法律之保密規定限制，且應配合提供資訊者不得規避、妨礙或拒絕。
2. 因香港、澳門及中國大陸之特殊性，稅捐稽徵法所規範租稅資訊交換的條約或協定之對象是與外國政府或國際組織，參照台灣地區與大陸地區人民關係條例、香港澳門關係條例之規定，暫不包括該等區域，然民眾仍應持續注意有無新增相關規定。

### 【法律觀點】

稅捐稽徵法第 5-1 條第 1 項[1]規定，基於互惠原則，我國得與外國政府或國際

[1] 稅捐稽徵法第 5-1 條第 1 項：「財政部得本互惠原則，與外國政府或國際組織商訂稅務用途資訊交換及相互提供其他稅務協助之條約或協定，於報經行政院核准後，以外交換文方式行之。」

組織訂定稅務用途之資訊交換及相互提供其他稅務協助之條約或協定，以作為稅務用途資訊交換依據。但亦因為依法納稅為憲法所保障之義務，具有彰顯國家主權的功能，因此同條第 2 項規定，在特定情形下，縱使雙方已經簽訂條約或協定，為保障公共利益以及基於互惠原則，仍不得與他國進行稅務資訊交換：一、外國政府或國際組織無法對等提供我國同類資訊；二、取得之資訊予以保密，顯有困難；三、請求提供之資訊非為稅務用途；四、請求資訊之提供將有損我國公共利益；以及五、未先盡其調查程序之所能提出個案資訊交換請求等情形[2]。另，稅捐稽徵法中所稱之租稅條約或協定，係排除港澳和大陸地區[3]，未來立法機關是否要另行針對港澳和大陸地區訂定金融資訊交換的相關規定，亦待觀察。

此外，本次修法更排除特定法律之保密規定，當財政主管機關或其授權之機關依前開規定執行時，應配合提供資訊者不得規避、妨礙或拒絕，並不受稅捐稽徵法或其他已明定或經公告之金融及稅務法律有關保密規定的限制[4]。有關機關、機構、團體、事業或個人如受要求提供資訊時，不得規避、妨礙或拒絕，否則最重可罰鍰 30 萬元，並得按次處罰，如果未依規定進行金融帳戶

[2] 稅捐稽徵法第 5-1 條第 2 項。

[3] 稅捐稽徵法第 5-1 條第 1 項所規範係與「外國政府或國際組織」訂稅務用途資訊交換及相互提供其他稅務協助之條約或協定，因此現階段並不包含中國大陸、香港、澳門等地區。

[4] 稅捐稽徵法第 5-1 條第 3、4、5 項：「財政部或其授權之機關執行第一項條約或協定所需資訊，依下列規定辦理；應配合提供資訊者不得規避、妨礙或拒絕，並不受本法及其他法律有關保密規定之限制：一、應另行蒐集之資訊：得向有關機關、機構、團體、事業或個人進行必要之調查或通知到財政部或其授權之機關辦公處所備詢，要求其提供相關資訊。二、應自動或自發提供締約他方之資訊：有關機關、機構、團體、事業或個人應配合提供相關之財產、所得、營業、納稅、金融帳戶或其他稅務用途資訊；應進行金融帳戶盡職審查或其他審查之資訊，並應於審查後提供。　　財政部或其授權之機關依第一項條約或協定提供資訊予締約他方主管機關，不受本法及其他法律有關保密規定之限制。　　前二項所稱其他法律有關保密規定，指下列金融及稅務法律有關保守秘密規定：一、銀行法、金融控股公司法、國際金融業務條例、票券金融管理法、信託業法、信用合作社法、電子票證發行管理條例、電子支付機構管理條例、金融資產證券化條例、期貨交易法、證券投資信託及顧問法、保險法、郵政儲金匯兌法、農業金融法、中央銀行法、所得稅法及關 稅法有關保守秘密規定。二、經財政部會商各法律中央主管機關公告者。」

盡職審查或其他審查，最重可罰鍰 1000 萬元[5]。

**【管理 Tips】**

稅務與金融資訊透明已是不可逆的國際趨勢，世界各國為財源、為租稅公平均是不遺餘力在進行租稅資訊交換或協助，故財政主管機關如果要求組織提供用以與外國政府或國際組織交換稅務用途之資料時，組織在確認與該他國間存在報經行政院核准關於稅務協助或資訊交換之條約或協定後，就應該配合進行，以免受罰。

惟目前關於該條文所應適用之範圍、執行方法、提出請求、蒐集、資訊之內容、配合提供之時限、方式、盡職審查或其他審查之基準、提供資訊予締約他方之程序及其他相關事項之辦法，尚由財政主管機關會商金融監管機關訂定中，組織應定期追蹤主管機關公告事項，以瞭解未來執行範圍、執行方法等事項。

**【相關標準】**

ISO 27001：2013(CNS 27001)

●A.13.2.2　資訊傳送協議

(1)標準內容：　協議應詳細闡述組織與外部各方間營運資訊之安全傳送。。

(2)適用說明：　基於租稅資訊的高度敏感特性，政府機關於依條約或協定，進行與他國或國際組織間的租稅資訊交換時，應在條約或協定內訂有對於資料傳送的保護規範，降低資安事件

[5] 稅捐稽徵法第 46-1 條：「有關機關、機構、團體、事業或個人違反第五條之一第三項規定，規避、妨礙或拒絕財政部或其授權之機關調查或備詢，或未應要求或未配合提供有關資訊者，由財政部或其授權之機關處新臺幣三千元以上三十萬元以下罰鍰，並通知限期配合辦理；屆期未配合辦理者，得按次處罰。未依第五條之一第三項第二款後段規定進行金融帳戶盡職審查或其他審查者，由財政部或其授權之機關處新臺幣二十萬元以上一千萬元以下罰鍰。」

發生之風險。

# 自我評量

# 是非題

1. (X) 為避免網路犯罪事件發生，除與執法機關合作外，只須定期更新系統與重要資料備份，不必刻意避免盜版軟體與注意社交工程郵件夾帶病毒，均可有效降低侵害發生。**【資訊保護 S10601】**

   解析：

   隨著科技進步，網路攻擊層出不窮，恣意下載來路不明的盜版軟體與不注意社交工程郵件是否夾帶病毒，皆大幅增加遭受網路攻擊之風險。

2. (O) 機關單位為建立正確的資訊安全規範，除技術面外，亦須加強於人員管理，並定期進行教育訓練與宣導。**【資訊保護 S10602】**

   解析：

   參考行政院及所屬各機關資訊安全管理規範，其明示資訊安全教育訓練，應定期對員工進行資訊安全教育及訓練，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

3. (X) 為達到有效的針對電子支付機構予以管控的目的，金融監督管理委員會要求電子支付機構在進行電子支付交易時，必須對於所有的交易類型，採用一致的交易安全設計。**【資訊保護 S10603】**

   解析：

   按電子支付機構資訊系統標準及安全控管作業基準辦法第 6 條第 1 項規定：「電子支付機構對於不同交易類型，應依其不同交易限額，採用下列交易安全設計：一、辦理代理收付實質交易款項（含實體通路支付服務交易），於使用者以電子支付帳戶款項支付、以約定連結存款帳戶付款支付、提出提前付款請求或提出取消暫停支付請求時，及使用者以約定連結存款帳戶付款支付儲值款項時，應依其不同交易限額，採用下列交易安全設計：...二、於使用者進行電子支付帳戶間款項移轉之支付時，應依其不同交易限額，採用下列交易安全設計：...」，故本題答案為否。

4. (O) 小瓜因前科累累的哥哥欠錢不還與哥哥發生激烈爭吵，因心生不滿遂從司法院判決書查詢系統找到哥哥過去的判決並張貼在自己的臉書上，公告示人。哥哥知悉後報警處理，認為小瓜侵犯自身個人資料，警察稱判決書為公開資料，不受個人資料保護法保障，故不願受理案件。**【資訊保護 S10604】**

解析：

個人資料法第 6 條規定有關特種個人資料不得蒐集、處理或利用，與其例外。本題司法院判決書查詢系統之判決書為已合法公開之個人資料，故符合個人資料保護法第 6 條第 1 項第 3 款。

5. (O) 民眾如不想其名下不動產之第二類謄本遭房仲濫用，可向選擇向地政機關申請將部分地址隱匿。**【資訊保護 S10605】**

解析：

按土地登記規則第 24-1 條規定略以：「申請提供土地登記及地價資料，其資料分類及內容如下：二、第二類：隱匿登記名義人之出生日期、部分姓名、部分統一編號、債務人及債務額比例、設定義務人及其他依法令規定需隱匿之資料。但限制登記、非自然人之姓名及統一編號，不在此限。前項第二款資料，得依登記名義人之請求，隱匿部分住址資料。但為權利人之管理人及非自然人，不適用之。」，故民眾可向地政機關申請隱匿部分住址資料。

6. (O) 政府資訊公開制度，目的是在於便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務的瞭解、信賴及監督，並促進民主參與，而相關資訊除諸如涉及國家機密等得依規定限制公開或不予提供者外，應主動公開。**【資訊保護 S10606】**

解析：

按政府資訊公開法第 1 條：「為建立政府資訊公開制度，便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與，特制定本法。」，以及同法第 6 條、第 7 條等規定，故所述正確。

7. (X) 花花的電子郵件信箱每日平均收到約百封垃圾郵件，花花可依濫發商業電子郵件管理條例向違法發信人請求違法使用電子郵件之民事損害賠償金。**【資訊保護 S10607】**

解析：

目前我國現行法規並未制訂濫發商業電子郵件管理條例，故無法依此請求民事損害賠償；如花花確受有損害，目前須視具體情形，依個資法或其他法律求償。未來如數位通訊傳播法草案通過施行後，類似花花之情形，則可參照數位通訊傳播法草案規定並配合相關法規，請求損害賠償。

8. (O) 某股份有限公司於各家商店提供免費 WIFI 供人使用，並於使用者條款中提及會

蒐集使用者資料等內容，此類條款應有消費者保護法關於定型化契約條款規定之適用。**【資訊保護 S10608】**

解析：

消費者保護法第 2 條第 7 款：「七、定型化契約條款：指企業經營者為與多數消費者訂立同類契約之用，所提出預先擬定之契約條款。定型化契約條款不限於書面，其以放映字幕、張貼、牌示、網際網路、或其他方法表示者，亦屬之。」，某股份有限公司之條款，乃其為與多數消費者訂立同類契約，所預先擬定者，故屬消費者保護法所稱之定型化契約條款，應有該法相關規定之適用。

9. (O) 電信事業資訊通訊安全管理作業要點要求電信事業建立資通安全之管理標準、等級評估、管理機制、教育訓練、應變通報及實施評鑑，可作為一般組織在進行資通安全管理時之參考。**【資訊保護 S10609】**

解析：

按電信事業資訊通訊安全管理作業要點第 2 點第 1 項：「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。」，相關要點內容係可作為一般事業之資通安全參考。

10. (O) 跨境電信詐騙案件層出不窮，造成民眾財產鉅大損害並損害國家形象，對於該類利用網際網路之跨境加重詐欺案件，我國刑法相關罰則仍有適用。**【資訊保護 S10610】**

解析：

按刑法第 5 條第 11 款規定：「本法於凡在中華民國領域外犯下列各罪者，適用之：十一、第三百三十九條之四之加重詐欺罪。」，依本題所示，加重詐欺案件適用於國外犯罪，故選項為正確。

11. (O) 巧巧工作室已僱用工作人員 50 人，為利於對其人員之管理以避免資料或技術外流造成損失，巧巧工作室具有工作規則規範並已報請主管機關核備。**【資訊保護 S10611】**

解析：

按勞動基準法第 70 條規定：「雇主僱用勞工人數在三十人以上者，應依其事業性質，就左列事項訂立工作規則，報請主管機關核備後並公開揭示之：一、工作時間、休息、

休假、國定紀念日、特別休假及繼續性工作之輪班方法。二、工資之標準、計算方法及發放日期。三、延長工作時間。四、津貼及獎金。五、應遵守之紀律。六、考勤、請假、獎懲及升遷。七、受僱、解僱、資遣、離職及退休。八、災害傷病補償及撫卹。九、福利措施。十、勞雇雙方應遵守勞工安全衛生規定。十一、勞雇雙方溝通意見加強合作之方法。十二、其他。」，依該法要求組織僱用人數應達 30 人以上得訂立工作規則，故本題為正確。

12. (X) 我國政府機關辦理資訊服務採購，屬於經濟部投資審議委員會所公告「具敏感性或國安（含資安）疑慮之業務範疇」，雖不須於投標文件載明不允許經濟部投資審議委員會公告之陸資資訊服務業者參與，但仍應以口頭告知投標業者。**【資訊保護 S10612】**

解析：

按行政院公共工程委員會工程企字第 10400024610 號函釋：「機關辦理資訊服務採購，如屬經濟部投資審議委員會所公告『具敏感性或國安（含資安）疑慮之業務範疇』於招標文件載明不允許經濟部投資審議委員會公告之陸資資訊服務業者參與，屬投標廠商資格與特殊或巨額採購認定標準第 4 條第 1 項第 6 款規定情形」，故本題答案為錯誤。

13. (X) 民眾遇警察臨檢，為配合公務進行，任何情況下民眾皆不得拒絕之。**【資訊保護 S10613】**

解析：

按警察職權行使法第 4 條規定：「警察行使職權時，應著制服或出示證件表明身分，並應告知事由。　　警察未依前項規定行使職權者，人民得拒絕之。」故並非在任何情況下，警察臨檢均不得拒絕，本題答案為錯誤。

14. (X) 小鄧平時喜歡偷拍其女友身體隱私部位並私藏觀賞，因未意圖散佈、播送、販賣，故小鄧之行為並未違反法律規定。**【資訊保護 S10614】**

解析：

按刑法第 315-1 條第 2 款規定：「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。」小鄧之行為即便未散佈、播送、販賣，仍屬違法，故本題答案為錯誤。

15. (O) 駭客利用電腦程式干擾他人電腦及系統資源，使特定網站功能癱瘓、電腦系統無

法正常運作，駭客恐涉犯干擾電腦或其相關設備罪。**【資訊保護 S10615】**

解析：

按刑法第 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。」本題駭客利用電腦程式癱瘓他人電腦與系統等行為，故符合干擾電腦或其相關設備罪，故本題答案為正確。

16. (O) 小瓜利用病毒程式攻擊台北市捷運系統，造成捷運行駛運作大停擺，小瓜恐遭處五年以下有期徒刑。**【資訊保護 S10616】**

解析：

按刑法第 185 條第 1 項：「損壞或壅塞陸路、水路、橋樑或其他公眾往來之設備或以他法致生往來之危險者，處五年以下有期徒刑，拘役或五百元以下罰金。」因該法並不區分造成往來危險之手法，縱使以病毒攻擊系統而造成捷運停擺亦屬於該法之規範，因此小瓜之行為符合損壞或壅塞其他公共往來之設備，故本題答案為正確。

17. (O) 吳醫師日前受邀參加電視節目，分享從醫多年之經驗，並於節目中暢談其病患案例，指名道姓說明某位當紅藝人亦是其病患，並講述該藝人之就診歷程與病情，節目播出時，媒體紛紛報導，導致該藝人情緒崩潰。吳醫師之行為已違反醫師法，得處新臺幣 2 萬元以上 10 萬元以下罰鍰。**【資訊保護 S10617】**

解析：

按醫師法第 23 條：「醫師除依前條規定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩露。」與醫師法第 29 條前段：「違反第十一條至第十四條、第十六條、第十七條或第十九條至第二十四條規定者，處新臺幣二萬元以上十萬元以下罰鍰。」吳醫師於節目上暢談病患病歷之行為，屬無故外洩病患之病歷，並得處新臺幣二萬元以上十萬元以下罰鍰，故本題答案為正確。

18. (X) 好旺旺購物商場開幕歡慶活動只要消費，即可掃描置於服務台的 QR code 加入會員，因加入會員時會蒐集到消費者個人資料，因此好旺旺購物商場將個資法中所要求之告知事項，以 A4 紙張列印並張貼於結帳台，但不須特別告訴消費者告知事項之張貼處，仍然符合個資法要求。**【資訊保護 S10618】**

解析：

按個人資料保護法第 8 條規定：「公務機關或非公務機關依第十五條或第十九條規定

向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」另按法務部法律字第 10603509640 號函：「…蒐集者仍應以個別通知方式使當事人知悉，不得以單純擺設公告或上網公告概括方式為之，須足以使當事人知悉或可得知悉該公告內容方式始屬之…」故好旺旺購物商場蒐集會員資料時，需對消費者進行告知，不得僅以公告為之，故答案為錯誤。

19. (O) 計程車司機阿財向製造商購買里程計費表僅作為計算車資之營業用途，若該製造商於里程計費表私自內建衍生計算車資以外之功能，例如強制蒐集阿財之行車軌跡、營業收入、錄影錄音等可直接或間接識別特定個人之資料，該製造商顯然有違反個人資料保護法之虞。**【資訊保護 S10619】**

解析：

按個人資料保護法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」法務部法律字第 10503505850 號函，因此，製造商僅能基於雙方買賣約定之特定目的內蒐集必要資料，不得逾越特定目的，故答案為正確。

20. (O) 個人資料保護法賦予組織義務，當組織違反個人資料保護法規定，導致事故發生時，組織應查明後以適當方式通知當事人。**【資訊保護 S10620】**

解析：

按個人資料保護法第 12 條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人」故本題答案為正確。

21. (O) 就民事責任而言，個人資料保護法採取舉證責任倒置的規定。**【資訊保護 S10621】**

解析：

按個人資料保護法第 29 條第 1 項規定：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」意即，組織係非因己故意或過失，則必須提出證明。

22. (X) 阿弘向國考補習班購買 DVD 影音教學課程後，將教學 DVD 重製檔案後上傳至臉書考友社團與考友分享，因阿弘購買該影音光碟而取得著作物的所有權，阿弘並未違反著作權法。**【資訊保護 S10622】**

解析：

著作物的所有權係屬物權的一種，屬於民法規範的範疇；著作權法則屬無體財產權的一種，屬著作權法規定，兩者並不相同。按著作權法第 3 條第 1 款規定：「本法用詞，定義如下：一、著作：指屬於文學、科學、藝術或其他學術範圍之創作。二、著作人：指創作著作之人。三、著作權：指因著作完成所生之著作人格權及著作財產權。…」國考補習班製作之影音教學課程屬於該補習班之著作物，阿弘未按著作權法第 37 條第 1 項：「著作財產權人得授權他人利用著作，其授權利用之地域、時間、內容、利用方法或其他事項，依當事人之約定；其約定不明之部分，推定為未授權。」規定取得國考補習班之授權而擅自重製，阿弘顯然已違反著作權法，故本題答案為錯誤。

23. (O) 保有個人資料之公務機關，應指定專人辦理安全維護事項，以防止個人資料事故發生。**【資訊保護 S10623】**

解析：按個人資料保護法第 18 條規定：「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」故選項為正確。

24. (O) 人員離職前將公司資料予以刪除，恐涉犯破壞電磁紀錄罪。**【資訊保護 S10624】**

解析：按刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」人員既未得到授權便無故刪除公司資料，已屬刪除電磁紀錄，故選項為正確。

25. (O) 阿達是患有人類免疫缺乏病毒之病患，若阿達身體不適就醫看診時，必須主動向醫事人員告知其已感染人類免疫缺乏病毒。**【資訊保護 S10625】**

解析：

按人類免疫缺乏病毒傳染防治及感染者權益保障條例第 12 條第 1 項規定：「感染者有提供其感染源或接觸者之義務；就醫時，應向醫事人員告知其已感染人類免疫缺乏病毒。」故答案為正確。

26. (O) 機關辦理採購時，公務員對招標文件原則於公告前負有保密義務。**【資訊保護 S10626】**

解析：

按政府採購法第 34 條第 1 項規定：「機關辦理採購，其招標文件於公告前應予保密。但須公開說明或藉以公開徵求廠商提供參考資料者，不在此限。」故此題選項為正確。

27. (O) 為維護兒童及少年於使用網際網路時之內容適當性，網際網路平臺提供者得採取諸如設置預覽專區、過橋頁面、部分內容限制會員瀏覽等方式管理其網際網路平臺。**【資訊保護 S10627】**

解析：

按網際網路平臺提供者網站內容自律公約第 4 條：「網際網路平臺提供者為維護兒少上網安全，得以下列任一方式管理限制級內容之瀏覽：(一)設置專區。(二)設置過橋頁面。(三)採行會員制。(四)設管理人員。(五)設置檢舉通報管道。」故本題選項為正確。

28. (X) 依兒童及少年福利與權益保障法規定，所有未滿 12 歲兒童之父母或監護人均須向警政機關申請建立兒童之指紋資料。**【資訊保護 S10628】**

解析：

按兒童及少年福利與權益保障法第 30 條規定第 1 項：「疑似發展遲緩、發展遲緩或身心障礙兒童及少年之父母或監護人，得申請警政主管機關建立指紋資料。」故非所有兒童之父母或監護人均被要求向警政機關申請建立兒童之指紋資料，而係僅兒童及少年有疑似發展遲緩、發展遲緩或身心障礙之情形時，其父母或監護人若有需要，才向警政機關申請建立其指紋資料，故本題答案為非。

29. (O) 民眾對於其個人資料之使用有知悉與控制權及資料記載錯誤之更正權，如若民眾之隱私權與新聞自由或知的權利相互衝突時，為衡平二者，其判斷最終仍以「公共利益」為標準。**【資訊保護 S10629】**

解析：

按個人資料保護法第 19 條第 1 項第 6 款之立法理由亦謂：「新聞自由或知的權利與隱私權之衝突，如何確立二者間之界限，各國均陸續建立其判斷標準。在美國聯邦最高法院有關侵權行為或誹謗訴訟之判例中，以『新聞價值』(Newsworhiness)和『公眾人物』(Public Figure)為判斷標準，上開二概念最終仍以『公共的領域』，即『公共事務』或『與公共相關之事務』為必要條件，故新聞自由或知的權利與隱私權之界限，其劃定標準應在於『事』而非在於『人』，故『公共利益』已足供作為判斷標準並簡單明確，此亦與中華民國報業道德規範宗旨相符…。」故本題答案為正確。

30. (X) 風險管理(Risk Management)是就管理個體可能面對的各種潛在風險加以認知、衡量，進而選擇適當之處理方式加以控制。而風險管理的策略可分為風險規避、風險降低及風險承擔之三部分，以期降低後續損害發生的可能性。**【資訊公開 D10630】**

解析：

風險管理之策略分為風險規避、風險降低、風險轉嫁及風險承擔。本題之風險管理缺少風險轉嫁，故答案為非。

31. (O) 除法律另有規定外，政府機關委託專家研究之環境影響評估報告書係屬政府應主動公開之資訊。**【資訊公開 D10631】**

解析：

按政府資訊公開法第 7 條規定：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：…五、施政計畫、業務統計及研究報告。…。前項第五款所稱研究報告，指由政府機關編列預算委託專家、學者進行之報告或派赴國外從事考察、進修、研究或實習人員所提出之報告。…」因此，本題之政府機關委託專家研究之環境評估報告書，亦即政府資訊公開法所稱之研究報告，應主動公開，故本題選項為正確。

32. (X) 為保障個人知的權利，增進個人對公共事務之瞭解、信賴及監督，只要民眾申請，政府均須公開應民眾申請之資料。**【資訊公開 D10632】**

解析：

政府資訊公開法第 18 條規定略以：「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。」故政府資訊按政府資訊公開法並非全然可公開，仍有部分為限制公開者，本題答案為否。

33. (O) 通訊保障及監察法之立法目的在於保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序。**【資訊監察 M10633】**

解析：

按通訊保障及監察法第 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。」故所述正確。

34. (X) 如涉及國家安全而必須監聽特定通訊時，電子通訊軟體業者因所經營業務亦屬電信業務範疇，故有義務依通訊保障及監察法建置、提供監聽設備以利權責單位進行監聽。**【資訊監察 M10634】**

解析：

電子通訊軟體業之業務，依一般民眾之使用方式，雖看似與電信業務提供民眾通訊服

務相仿，但按行政院主計總處於 105 年 1 月發布之行業分類標準，電信業係指「從事有線電信、無線電信及其他電信相關服務之行業。不包括：線上提供可安裝於個人行動裝置之通信軟體供應者，應依其主要經濟活動歸入適當類別。」可知電子通訊軟體業，尚非上述電信事業，亦不受電信法規範。而依現行通訊保障及監察法規定，僅電信業者有建置、提供通訊監察設備以利權責機關監聽之義務，故電子通訊軟體業者不在規範範圍內。若因應科技趨勢，有使該類業者提供設備，並配合權責機關進行通訊監察之必要，應先對電信法或通訊保障及監察法進行修訂。

35. (O) 小美懷疑丈夫外遇，為想求證便私自瞞著丈夫安裝全球定位系統（Global Positioning System, GPS）接收器於丈夫汽車內，監視丈夫每日行蹤，即便雙方為夫妻關係，小美之行為仍恐涉犯刑法妨害秘密罪。**【資訊監察M10635】**

解析：

按刑法第 315 條之 1：「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。」再按法院多數見解認為，駕駛車輛行駛於供公眾往來道路，除有明白表示放棄隱私期待外，通常可認為駕駛人並不欲公開其個人行蹤，如果當事人就其行蹤具有隱私合理期待，此時個人的行蹤就屬於「非公開活動」,因此無故在他人車上裝設 GPS 接收器追蹤他人行蹤，即有觸犯刑法第 315-1 條妨害祕密罪的可能，故本題答案為正確。

36. (O) 警方為緊急查尋失蹤人，得合法先請電信公司提供通聯定位資料，事後再補具正式公文書。**【資訊監察 M10636】**

解析：

電信事業處理有關機關查詢電信通信紀錄實施辦法第 3 條第 1 項但書：「案情特殊、情況緊急之查詢，得由…查詢機關首長或其書面指定人於電信通信紀錄查詢單署名並加蓋職章及連絡人之資料，視同機關正式公文書先傳真之，並經回叫確認為之，查詢後應於三個工作日內補具正式公文或加蓋印信之電信通信紀錄查詢單正本。

37. (O) 國防上所必須控制與確保之戰術要點、軍港及軍用飛機場，稱為要塞堡壘地帶，除非有國防部之特別命令，否則不得擅自操作無人機進行攝影。**【資訊應用 A10637】**

解析：

按要塞堡壘地帶法第 4 條第 1 款略以：「第一區內之禁止及限制事項：一、非受有國

防部之特別命令，不得為測量、攝影、描繪、記述及其他關於軍事上之偵察事項。…」，故選項為正確。

38. (O)　駕駛設備須依法向公路監理機關申請合法牌照，使得合法上路。**【資訊應用 A10638】**

解析：

按公路法第 63 條規定：「汽車及電車均應符合交通部規定之安全檢驗標準，並應經車輛型式安全檢測及審驗合格，取得安全審驗合格證明書，始得辦理登記、檢驗、領照。」故答案為正確，然目前我國並未針對全自動化駕駛設備有符合規定之安全檢驗標準，因此並無法對其進行安全檢驗，故無法上路。

39. (O)　我國自然人憑證可使用於電子化政府等相關網路服務之身分認證機制。**【資訊應用 A10639】**

解析：

目前經主管機關所核定之憑證機構，包括政府機關與民間企業位共有 7 個單位，其所發行之憑證各有對應之適用範圍。以內政部憑證管理中心為例，內政部憑證管理中心憑證實務作業基準第 1.9 版 1.3.7.1 憑證之適用範圍：「憑證管理中心所簽發及管理的憑證類別為自然人憑證，且包含簽章用及加密用憑證。憑證管理中心所簽發的憑證符合憑證政策保證等級第三級之規定，本憑證適用於網路中的身分識別及資料保護。」據此，內政部憑證管理中心所簽發及管理的自然人憑證，其適用於網路中的身分識別及資料保護，可利用自然人憑證作為在網路中的身分辨識，故本題答案為正確。

40. (X)　財政部依稅捐稽徵法第 5-1 條進行稅務交換協定，要求配合提供資訊者提供必要資訊時，受要求者在提出理由後得規避或拒絕。**【資訊應用 A10640】**

解析：按稅捐稽徵法第 5-1 條第 3 項規定：「財政部或其授權之機關執行第一項條約或協定所需資訊，依下列規定辦理；應配合提供資訊者不得規避、妨礙或拒絕，並不受本法及其他法律有關保密規定之限制：一、應另行蒐集之資訊：得向有關機關、機構、團體、事業或個人進行必要之調查或通知到財政部或其授權之機關辦公處所備詢，要求其提供相關資訊。二、應自動或自發提供締約他方之資訊：有關機關、機構、團體、事業或個人應配合提供相關之財產、所得、營業、納稅、金融帳戶或其他稅務用途資訊；應進行金融帳戶盡職審查或其他審查之資訊，並應於審查後提供。」故選項為錯誤。

# 選擇題

1. (1)　彬彬的電腦因遭駭客攻擊以致系統癱瘓無法使用，請問以下敘述何者正確？(1)駭客可能構成刑法第 359 條未經允許取得、刪除、變更他人電磁紀錄罪。(2)駭客恐將面臨無期徒刑或七年以上有期徒刑。(3)駭客恐遭拘役或科或併科 50 萬以上罰金。(4)以上均是。**【資訊保護 S10601】**

   解析：

   刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

2. (4)　下列敘述何種行為恐涉犯營業秘密罪？(1)小宏時常因工作做不完將工作資料帶回家加班。(2)張大媽在退休後閒暇之餘喜愛參加社區大學長青舞蹈課並在上課時錄下老師教課內容於課後練習。(3)如如平時在披薩店工讀，因口味配料太繁複，無法記住，遂從店內取回因廣受顧客歡迎，由店方印在ＤＭ上宣傳的食譜配方表回家複習。(4)阿珠跳槽離職前擅自複製公司重要且嚴加保密之檔案並移作新公司使用，以提升新公司之營業績效與收入。**【資訊保護 S10602】**

   解析：

   按營業秘密須具備經濟性、秘密性、與已採取合理保護措施等要件，本題阿珠所取得之檔案資料顯然已具備上開要件，故其擅自複製並取走使用之行為，已違反營業秘密法第 13-1 條第 1 項第 1 款：「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……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。」

3. (3)　下列何者並非電子支付機構依電子支付機構資訊系統標準及安全控管作業基準辦法，於進行電子支付交易時所應遵循之規範？(1)使用者登入電子支付平臺時應進行身分確認，並得以帳號及固定密碼登入，針對帳號及固定密碼應有安全設計。(2)進行電子交易時對於不同交易類型，應依其不同交易限額，採用不同的交易安全設計。(3)依執行業務之必要，應設定相關人員接觸個人資料之權限及控管其接觸情形，但非必要與所屬人員約定保密義務。(4)應建置留存個人資料使用稽核軌跡或辨識機制。**【資訊保護 S10603】**

   解析：

   按電子支付機構資訊系統標準及安全控管作業基準辦法第 5 條第 1 項：「電子支付機

構於使用者登入電子支付平臺時應進行身分確認，得以帳號及固定密碼登入。」; 同辦法第 6 條第 1 項略以 :「電子支付機構對於不同交易類型，應依其不同交易限額，採用下列交易安全設計：…。」; 同辦法第 13 條第 1 項第 3 款 :「電子支付作業環境之個人資料保護應符合下列要求：…三、為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。」; 同條第 1 項第 5 款 :「電子支付作業環境之個人資料保護應符合下列要求…五、應建置留存個人資料使用稽核軌跡 ( 如登入帳號、系統功能、時間、系統名稱、查詢指令或結果 )或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，包括檔案、螢幕畫面、列表。故選項(1)(2)(4)為正確。

4. (2)　按個人資料保護法規定，下列何者敘述有誤？(1)格格的 iPhone 手機通訊錄上傳至雲端備份，此適用個人資料保護法。(2)個人資料僅限於自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、指紋等，得以直接識別該個人之資料。(3)個人資料應於蒐集時之特定目的範圍內利用。(4)阿瑪於聚會時與老同學合影並上傳至臉書，此不適用個人資料保護法。**【資訊保護 S10604】**

   解析：

   個人資料保護法第 2 條略以 :「本法用詞，定義如下：一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」故選項(2)應為得以直接與間接識別該個人資料。

5. (2)　乖乖向友人抱怨經常因房仲業者利用謄本資料登門叨擾，請問房仲業者是申請以下何種謄本。(1)第一類謄本。(2)第二類謄本。(3)第三類謄本。(4)第四類謄本。**【資訊保護 S10605】**

   解析：

   按土地登記規則第 24-1 條第 3 項規定 :「登記名義人或其他依法令得申請者，得申請第一項第一款資料；任何人得申請第一項第二款資料；登記名義人、具有法律上通知義務或權利義務得喪變更關係之利害關係人得申請第一項第三款資料。」故任何人皆得申請第二類謄本。

6. (3)　按國家機密保護法規定，下列何者敘述正確？(1)國家機密法之立法目的在於為建立國家機密保護制度，確保國家安全及利益。(2)辦理國家機密事項業務人員出境須經核准。(3)以上皆是。(4)以上皆非。**【資訊保護 S10606】**

解析：

國家機密保護法第 1 條：「為建立國家機密保護制度，確保國家安全及利益，特制定本法。」; 同法第 26 條：「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。前項第三款之期間，國家機密核定機關得視情形縮短或延長之。」故選項(3)正確。

7. (2) 關於「數位通訊傳播法」草案之說明，下列何者敘述錯誤？(1)草案規定商業電子訊息之發送方，應提供接收方得拒絕接收之方式。(2)如使用者與數位通訊傳播服務提供者發生紛爭，僅得向提供者要求民事損害賠償，而不得聲請定暫時狀態處分。(3)該草案希望能透過其制定，強化服務提供者與使用者的平等關係，確保資訊得充分揭露，使消費者有所救濟管道。(4)該草案希望能使政府透過公眾諮詢和參與機制，落實開放政府之理念，建構網際網路的基本規範。**【資訊保護 S10607】**

解析：

係按數位通訊傳播法草案第 19 條:「數位通訊傳播服務提供者與其使用者或第三人間，因數位通訊傳播服務之使用行為發生爭執，為防止發生重大之損害或避免急迫之危險或有其他相類之情形而有必要時，數位通訊傳播服務提供者、其使用者或第三人得依民事訴訟法之規定，聲請法院為定暫時狀態之處分。」故選項(2)所述有誤。

8. (4) 下列何者屬於消費者保護法所稱之「定型化契約條款」？(1)某電子商務公司法務部門所擬定並公告於該公司購物平台上，以利消費者瞭解之網站購物服務條款。(2)由某健身運動公司請律師代其預擬，以供會員入會使用之健身會員條款。(3)某出版公司業務經理為該公司所擬定，並由該公司之電子書銷售代表提供消費者審閱、簽約之電子書閱讀與其他服務契約。(4)以上皆是。**【資訊保護 S10608】**

解析：按消費者保護法第 2 條第 7 款：「定型化契約條款：指企業經營者為與多數消費者訂立同類契約之用，所提出預先擬定之契約條款。定型化契約條款不限於書面，其以放映字幕、張貼、牌示、網際網路、或其他方法表示者，亦屬之。」規定，因此，本題各選項所舉例子均符合上述規定，故應擇選項(4)。

9. (4) 關於「關鍵基礎設施」之說明，下列何者敘述正確？(1)關鍵基礎設施之主部門分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八類。(2)關鍵基礎設施提供者對國家安全、社會公共利益、國民生活及經濟活動有重大影響。(3)關鍵基礎設施遭受重大人為危安事件或恐怖攻擊時，應進行通報。(4)以上皆是。**【資訊保護 S10609】**

解析：

按行政院訂定之「國家關鍵基礎設施安全防護指導綱要」規定，我國關鍵基礎設施之範圍分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八大類別。此對於國家安全、民生需求、經濟活動有重大影響。另，關鍵基礎設施提供者，應負有事件之通報義務，以有效降進行災害發生之控管。

10. (4) 消費者之個人資料若因商家違反個人資料保護法規定，導致消費者遭受不法侵害，試問下列何者並非消費者之救濟內容？(1)如致財產上之損害，得請求損害賠償。(2)如不易或不能證明其實際損害額，得請求法院依侵害情節酌定賠償額。(3)如致消費者名譽受損害，得請求回復名譽。(4)每人每一事件最高求償額為新台幣四百元。**【資訊保護 S10610】**

解析：

按個人資料保護法第 28 條第 2 項：「被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。」、同法第 28 條第 3 項：「依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。」

11. (4) 下列關於勞動基準法之規範，請問何者敘述正確？(1)工作規則應包含應遵守之紀律。(2)工作規則應包含勞雇雙方溝通意見加強合作之方法。(3)雇主僱用勞工人數達 30 人以上，應訂立工作規則。(4)以上均是。**【資訊保護 S10611】**

解析：

按勞動基準法第 70 條規定：「雇主僱用勞工人數在三十人以上者，應依其事業性質，就左列事項訂立工作規則，報請主管機關核備後並公開揭示之：一、工作時間、休息、休假、國定紀念日、特別休假及繼續性工作之輪班方法。二、工資之標準、計算方法及發放日期。三、延長工作時間。四、津貼及獎金。五、應遵守之紀律。六、考勤、請假、獎懲及升遷。七、受僱、解僱、資遣、離職及退休。八、災害傷病補償及撫卹。九、福利措施。十、勞雇雙方應遵守勞工安全衛生規定。十一、勞雇雙方溝通意見加強合作之方法。十二、其他。」故選項(1)(2)(3)為正確，答案為選項(4)。

12. (2) 關於經濟部投資審議委員會所公告「具敏感性或國安(含資安)疑慮之業務範疇」，下列何者為非？(1)水資源類。(2)娛樂類。(3)交通類。(4)通訊傳播類。**【資訊保護 S10612】**

解析：

按經濟部投資審議委員會所公告「具敏感性或國安（含資安）疑慮之業務範疇」其包括能源類、水資源類、通訊傳播類、交通類、金融與銀行類、緊急救援與醫院類、中央政府與地方機關類與科技園區與工業區類，故選項(2)為錯誤。

13. (4)　請問警察得於下列何種情形在公共場合查證民眾身分？(1)合理懷疑其有犯罪之嫌疑或有犯罪之虞者。(2)有事實足認為防止其本人或他人生命、身體之具體危害，有查證其身分之必要者。(3)行經指定公共場所、路段及管制站者。(4)以上皆是。**【資訊保護 S10613】**

解析：

按警察職權行使法第 6 條第 1 項規定：「警察於公共場所或合法進入之場所，得對於下列各款之人查證身分：一、合理懷疑其有犯罪之嫌疑或有犯罪之虞者。二、有事實足認其對已發生之犯罪或即將發生之犯罪知情者。三、有事實足認為防止其本人或他人生命、身體之具體危害，有查證其身分之必要者。四、滯留於有事實足認有陰謀、預備、著手實施重大犯罪或有人犯藏匿之處所者。五、滯留於應有停（居）留許可之處所，而無停（居）留許可者。六、行經指定公共場所、路段及管制站者。」故選項(1)(2)(3)皆符合，答案為選項(4)。

14. (4)　某公共廁所發現遭安裝針孔攝影機偷拍民眾如廁，警方循線調查後發現是一名五十餘歲男子所為，請問下列關於該男之罪責何者錯誤？(1)該男偷拍之行為，恐遭處以 3 年以下有期徒刑。(2)該男將其偷拍影片散播至網路，最重可處以 5 年以下有期徒刑。(3)該男將偷拍影片販賣與他人，除可能遭處 5 年以下有期徒刑外，更可同時科以新台幣 5 萬元以下罰金。(4)該男架設之針孔攝影機僅偷拍到民眾的隱私部位，並未明確與民眾之身分連結，故不涉犯刑法妨害秘密罪。**【資訊保護 S10614】**

解析：

按刑法第 315-1 條第 2 款規定：「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。」而刑法第 315-2 條第 3 項略以：「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。」因此，即便該名中年男子僅拍攝身體隱私部位，仍涉犯刑法妨害秘密罪，如有散布或販售行為，更可加重罪責。

15. (3)　請問下列敘述案例，何者不受我國刑法規範？(1)小忠於日本旅遊期間透過電腦程式攻擊臺灣大學選課系統，使得臺大學生無法登入選課。(2)阿翰離職後心生不滿，在

台北市的網咖發送感謝信並夾帶病毒予公司同仁，使該公司同仁電腦運作緩慢至當機癱瘓。(3)小明為美國籍，現居加拿大，經常貪玩利用電腦程式癱瘓位於墨西哥之商家系統。(4)阿洲與妹妹為台南在地人，為幫妹妹報復在美國讀書的劈腿男友，故利用自己撰寫的電腦程式攻擊對方電腦導致不得使用。**【資訊保護 S10615】**

解析：

按刑法第 4 條：「犯罪之行為或結果，有一在中華民國領域內者，為在中華民國領域內犯罪。」而刑法第 7 條：「本法於中華民國人民在中華民國領域外犯前二條以外之罪，而其最輕本刑為三年以上有期徒刑者，適用之。但依犯罪地之法律不罰者，不在此限。」本題選項(3)之犯罪行為與結果都不屬中華民國領域內，故不受本國刑法規範。且行為人屬美國籍，故亦無屬人原則適用，而縱使行為人屬中華民國國籍，但因妨害電腦使用罪之刑責僅為3年以下有期徒刑，不屬於最輕本刑為3年以上有期徒刑之罪，因此亦無法以屬人原則加以處罰。

16. (1)　請問下列何種情形恐涉犯刑法外患罪？(1)在與外國開戰或將開戰期內，透過網際網路毀壞鐵路使之無法通行。(2)在承平時期，透過侵入電腦設備方式，造成機場運作停擺。(3)在與外國開戰或將開戰期內，以公民連署罷免總統。(4)在承平時期，透過侵入電腦作業系統，將航空器控制權交付與敵國。**【資訊保護 S10616】**

解析：

按刑法第 106 條第 1 項「在與外國開戰或將開戰期內，以軍事上之利益供敵國，或以軍事上之不利益害中華民國或其同盟國者，處無期徒刑或七年以上有期徒刑。」與刑法第 107 條第 1 項：「犯前條第一項之罪而有左列情形之一者，處死刑或無期徒刑：一、將軍隊交付敵國，或將要塞、軍港、軍營、軍用船艦、航空機及其他軍用處所建築物，與供中華民國軍用之軍械、彈藥、錢糧及其他軍需品，或橋樑、鐵路、車輛、電線、電機、電局及其他供轉運之器物，交付敵國或毀壞或致令不堪用者。二、代敵國招募軍隊，或煽惑軍人使其降敵者。三、煽惑軍人不執行職務，或不守紀律或逃叛者。四、以關於要塞、軍港、軍營、軍用船艦、航空機及其他軍用處所建築物或軍略之秘密文書、圖畫、消息或物品，洩漏或交付於敵國者。五、為敵國之間諜，或幫助敵國之間諜者。前項之未遂犯罰之。」選項(2)與(4)均係承平時期作為，非戰時，而選項(3)並非外患罪之行為，故選項(1)為正確。

17. (4)　請問下列職業，何者具有其職業之禁止洩漏因業務知悉祕密之相關法律或法規命令等規範？(1)律師。(2)醫師。(3)呼吸治療師。(4)以上均有。**【資訊保護 S10617】**

解析：

按律師法第 15 條第 2 項：「全國律師公會聯合會應訂立律師倫理規範，提經會員代表大會通過後，報請法務部備查。」與律師倫理規範第 33 條：「律師對於受任事件內容應嚴守秘密，非經告知委任人並得其同意，不得洩漏。但有下列情形之一，且在必要範圍內者，得為揭露：一、避免任何人之生命、身體或健康之危害。二、避免或減輕因委任人之犯罪意圖及計畫或已完成之犯罪行為之延續可能造成他人財產上之重大損害。三、律師與委任人間就委任關係所生之爭議而需主張或抗辯時，或律師因處理受任事務而成為民刑事訴訟之被告，或因而被移送懲戒時。四、依法律或本規範應揭露者。」; 醫師法第 23 條：「醫師除依前條規定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩露。」; 呼吸治療師法第 16 條：「呼吸治療師對於因業務而知悉或持有他人之秘密，不得無故洩漏。」因此可知，醫師、呼吸治療師以及律師均有保守業務祕密義務之相關規範，故選項(4)為正確。

18. (1) 個人資料保護法規定蒐集個人資料時，蒐集者必須對資料當事人進行告知程序，請問下列選項何者不符合個人資料保護法之告知方式？(1)網路公告。(2)書面。(3)電子郵件。(4)簡訊。**【資訊保護 S10618】**

解析：

按個人資料保護法施行細則第 16 條：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」次按法務部法律字第 10603509640 號函略以：「蒐集者仍應以個別通知方式使當事人知悉，不得以單純擺設公告或上網公告概括方式為之，須足以使當事人知悉或可得知悉該公告內容方式始屬之」故選項(2)(3)(4)皆符合。

19. (4) 關於個人資料之蒐集、處理或利用，應符合下列何種原則為之？(1)誠信原則。(2)必要性原則。(3)不當連結禁止原則。(4)以上皆是。**【資訊保護 S10619】**

解析：

按個人資料保護法第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」亦即關於個資蒐集、處理、利用，必須符合「誠信原則」、「必要性原則」、「不當連結禁止原則」三大原則，以保護民眾之人格法益，故選項(1)(2)(3)皆符合，答案為選項(4)。

20. (4) 如組織因違反個人資料保護法之規定，導致事故發生，組織應查明事實並以適當方式通知當事人。請問關於「適當方式通知」，下列何者敘述何者正確？(1)電話簡訊通知。(2)發布新聞稿。(3)公告於組織網站。(4)以上皆是。**【資訊保護 S10620】**

解析：按個人資料保護法施行細則第 22 條規定：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。」故本題選項(1)(2)(3)即為正確。

21. (3)　洋洋公司接受重發公司委託，進行產品客戶意見調查，蒐集客戶使用重發公司產品後之使用心得，作為數據分析。試問下列何者非屬重發公司所應注意之監督管理責任？(1)洋洋公司的員工如果有違反個資法時，重發要求洋洋公司採行補救措施。(2)雙方應於合約內載明洋洋公司得蒐集的個人資料之範圍、類別、特定目的及其期間。(3)重發公司不得於合約內載明任何保留事項。(4)重發公司應定期確認洋洋公司執行之狀況。**【資訊保護 S10621】**

解析：按個人資料保護法施行細則第 8 條第 1 項規定：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。」故選項(3)為錯誤。

22. (1)　請問下列選項何者為正確？(1)阿凱購買周杰倫新專輯 CD，則阿凱擁有該著作物之所有權。(2)阿明購買哈利波特系列影集 DVD，故得重製贈予朋友。(3)小花編撰的推理小說新上市，故小花有權轉讓部分著作人格權予他人。(4)阿滿將自繪的油畫作品贈與予小江且未明示著作財產權歸屬問題，故小江可將該油畫重製印刷並販賣。**【資訊保護 S10622】**

解析：

周杰倫新專輯係屬著作重製物，阿凱購買後取得該著作物之所有權，屬於民法物權上之權利，故選項(1)為正確。另，阿明購買哈利波特系列影集僅取得該著作物之所有權，係屬民法物權的權利，並非取得著作財產權，故不得重製並與友人分享，故選項(2)為錯誤；次按著作權法第 21 條規定：「著作人格權專屬於著作人本身，不得讓與或繼承。」故小花即便為著作權人也不得讓與著作人格權，故選項(3)為錯誤；再按經濟部智慧財產局台內著字第 8506850 號函釋：「…著作人讓與著作物(著作原件或其重製物)之所有權時，如未同時讓與著作財產權，則受讓人僅取得著作物之所有權，並未取得

著作財產權，其著作財產權仍屬著作人享有…」故阿滿並未明確將著作財產權讓與予小江，小江不得擅自將開著作物重製印刷並販賣，故選項(4)為錯誤。

23. (1)　面對潛在的資安威脅，除依法指派專人進行安全管理以外，請問下列敘述何者得以防範威脅並降低風險？(1)以下皆是。(2)實施資安教育訓練。(3)定期進行資安稽核。(4)資訊系統分類分級。**【資訊保護 S10623】**

解析：按政府機關（構）資通安全責任等級分級作業規定，為防潛在資安威脅，降低風險發生可能，以為資料保護，故推動資訊安全管理，其中包括資訊系統分類分級、定期進行資安稽核、實施資安教育訓練，故選項為(1)。

24. (4)　下列何者係以 CNS 27001 資訊安全管理系統國家標準對於人力資源安全之要求？

(1)聘僱前，應確保員工了解自身責任，且適任於其所被指派的角色。(2)聘僱中應確保員工認知並履行其資訊安全的責任。(3)聘僱終止與變更時，則是要確保組織利益未被侵害(4)以上皆是。**【資訊保護 S10624】**

解析：按 ISO 27001:2013(CNS 27001)之目標，A.7.1 確保員工及承包者瞭解其將承擔之責任，且適任其角色，A.7.2 確保員工及承包者認知並旅行其資訊安全責任，A.7.3 將保護資之利益納入聘用變更或終止聘用過程之一部份，故選項(4)為正確。

25. (3)　阿寶為人類免疫缺乏病毒感染者，請問在下列何種情形阿寶不需依法主動告知其感染人類免疫缺乏病毒？(1)就醫時，向醫事人員告知。(2)與他人進行危險性行為前，向性行為對象告知。(3)接受緊急救護時，向救護人員告知。(4)與他人共用針具、稀釋液或容器等施打行為前，向共用對象告知。**【資訊保護 S10625】**

解析：

按人類免疫缺乏病毒傳染防治及感染者權益保障條例第 12 條：「感染者有提供其感染源或接觸者之義務；就醫時，應向醫事人員告知其已感染人類免疫缺乏病毒。主管機關得對感染者及其感染源或接觸者實施調查。但實施調查時不得侵害感染者之人格及隱私。感染者提供其感染事實後，醫事機構及醫事人員不得拒絕提供服務。」次按同法第 21 條第 1 項：「明知自己為感染者，隱瞞而與他人進行危險性行為或有共用針具、稀釋液或容器等之施打行為，致傳染於人者，處五年以上十二年以下有期徒刑。明知自己為感染者，而供血或以器官、組織、體液或細胞提供移植或他人使用，致傳染於人者，亦同。」故選項(1)(2)(4)符合上述現行法規。另外，再按人類免疫缺乏病毒傳染防治及感染者權益保障條例第 12 條修正草案：「感染者有提供其感染源或接觸者之義務；於接受緊急救護或就醫時，應向救護人員或醫事人員告知其已感染人類免疫缺

乏病毒。主管機關得對感染者及其感染源或接觸者實施調查。…」該草案目前仍未修正通過，故選項(3)為錯誤。

26. (4)　請問關於政府採購法規範機關辦理採購，下列敘述何者正確？(1)機關辦理採購，其招標文件於公告前應予保密。(2)機關對於廠商投標文件，除供公務上使用或法令另有規定外，應保守秘密。(3)底價於開標後至決標前，仍應保密。(4)以上皆是。**【資訊保護 S10626】**

解析：按政府採購法第 34 條規定：「機關辦理採購，其招標文件於公告前應予保密。但須公開說明或藉以公開徵求廠商提供參考資料者，不在此限。機關辦理招標，不得於開標前洩漏底價，領標、投標廠商之名稱與家數及其他足以造成限制競爭或不公平競爭之相關資料。底價於開標後至決標前，仍應保密，決標後除有特殊情形外，應予公開。但機關依實際需要，得於招標文件中公告底價。機關對於廠商投標文件，除供公務上使用或法令另有規定外，應保守秘密。」故選項(1)(2)(3)為正確，答案為(4)以上皆是。

27. (4)　台灣網際網路協會針對包含兒童及少年上網安全等網際網路空間之安全維護，要求網際網路平臺提供者須對限制級內容進行管理，請問下列管理限制級方式不符合網際網路平臺提供者網站內容自律公約之規範？(1)設置專區。(2)採行會員制。(3)設置檢舉通報管道。(4)採取信用卡註冊。**【資訊保護 S10627】**

解析：

按網際網路平臺提供者網站內容自律公約第 4 條：「網際網路平臺提供者為維護兒少上網安全，得以下列任一方式管理限制級內容之瀏覽：(一)設置專區。(二)設置過橋頁面。(三)採行會員制。(四)設管理人員。(五)設置檢舉通報管道。」選項(1)(2)(3)為上述公約所規範內容。反之，選項(4)並未被納入台灣網際網路協會針對網際網路平臺提供者之管理要求內。

28. (3)　身心障礙兒童之父母或監護人得依兒童及少年福利與權益保障法規定向警政主管機關申請建立指紋資料，若將來不幸走失時能透過指紋辨識迅速確認身分。警政主管機關取得指紋資料後，應確保指紋資料安全，請問下列何者錯誤？(1)指紋資料應由專責人員管理及維護。(2)指紋資料之運輸、儲存及運用過程，應遵守資通安全相關規範。(3)若指紋資料與受捺人資料不符時，應待受奈人通知後處理。(4)若指紋資料有錯誤時，應於查明後更正受捺人資料。**【資訊保護 S10628】**

解析：

按發展遲緩疑似發展遲緩或身心障礙兒童及少年指紋管理辦法第 7 條規定：「指紋資

料之傳輸、儲存及運用過程，應遵守資訊安全相關規範，確保指紋資料安全，防範不法入侵及資料外洩。指紋資料應由專責人員管理及維護。指紋資料與受捺人資料不符時，應立即查明處理。如有錯誤，應於查明後更正受捺人資料。」選項(1)(2)(4)皆符合規定，則選項(3)之待受奈人通知後處理，應為立即查明處理。

29. (3)　請問下列何種情形，組織得拒絕個人資料當事人之請求查詢、提供閱覽或製給複製本？(1)小芳向 Woowoo 商城查詢歷年消費紀錄。(2)阿滿向國稅局申請歷年所得清單。(3)阿寶房屋遭民眾檢舉違建，遂向檢調機關要求查詢檢舉之相關資料。(4)丁丁離職三個月後，因新工作需求遂向前雇主要求提供其員工資料。**【資訊保護 S10629】**

解析：

按個人資料保護法第 10 條規定：「公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」選項(3)阿寶向檢調機關要求查詢檢舉之相關資料，該資料為該檢舉事件之紀錄，內容係包含檢舉民眾之個人資料，為避免妨害第三人之重大利益，檢調機關得依法拒絕之。

30. (3)　中央主管機關針對重大或突發性食品衛生安全事件，得對特定產品或特定地區之產品採取下列哪些管理措施？(1)下架、封存、限期回收、限期改製、沒入銷毀。(2)限制或停止輸入查驗、製造及加工之方式或條件。(3)以上皆是。(4)以上皆非。**【資訊公開 D10630】**

解析：

按食品衛生安全管理法第 4 條第 5 項：「中央主管機關對重大或突發性食品衛生安全事件，必要時得依風險評估或流行病學調查結果，公告對特定產品或特定地區之產品採取下列管理措施：一、限制或停止輸入查驗、製造及加工之方式或條件。二、下架、封存、限期回收、限期改製、沒入銷毀。」

31. (3)　政府機關如有應主動公開之政府資訊卻未公開之情事發生，民眾得申請提供政府資訊。請問在未予延長期間時，政府機關應於民眾提出申請後幾日內為准駁之決定？(1)20 日。(2)5 日。(3)15 日。(4)10 日。**【資訊公開 D10631】**

解析：

按政府資訊公開法第 12 條規定：「政府機關應於受理申請提供政府資訊之日起十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日。」故答案為選項(3)。

32. (3) 按政府資訊公開法規定，下列何者敘述應限制公開或不予提供之？(1)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。(2)預算及決算書。(3)訴願審議委員會之訴願審議紀錄。(4)書面之公共工程及採購契約。**【資訊公開 D10632】**

解析：

政府資訊公開法第 18 條第 1 項第 3 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：……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。」故選項(3)符合政府資訊公開法第 18 條第 1 項第 3 款之內部單位之其他準備作業。

33. (1) 以下為通訊保障及監察法對於國安事件准許通訊監察之要件，請問下列何者錯誤？(1)事前通知。(2)令狀原則。(3)重罪原則。(4)事中監督。**【資訊監察 M10633】**

解析：

通訊保障及監察法准許通訊監察之要件如下：一、重罪原則，涉犯三年以上有期徒刑之罪及其他所列舉之重罪者；二、必要性，須無法以其他方式為調查者；三、關聯性，通訊內容與案件相關者；四、令狀原則，須視情況由法院或綜理國家情報工作機關首長核發通訊監察書，由情報機關首長核發者，並須經法院事後補行同意；五、事中監督，每十五日至少作成一次以上之報告書；六、事後通知，通訊監察結束後應通知受監察人。以上諸原則中，並不包含事前通知，因此選項(1)錯誤。

34. (4) 如權責機關擔憂可能有國安問題，希望行動通訊軟體業者，協助進行通訊監察時，請問下列敘述何者正確？(1)權責機關得依通訊保障及監察法，於擔憂國安問題發生時，逕行要求行動通訊軟體業者配合通訊監察。(2)行動通訊軟體業者有義務建置設備讓權責機關進行特定電話的監聽。(3)以上皆是。(4)以上皆非。**【資訊監察 M10634】**

解析：

縱然暫不考慮通訊保障及監察法之規範對象等問題，依據通訊保障及監察法之規定，欲進行通訊之監察必須符合重罪原則、必要性等諸多要件，不可僅依權責機關之擔憂即啟動通訊監察；而依通訊保障及監察法第 14 條第 2 項前段：「電信事業及郵政事業有協助執行通訊監察之義務。」由於目前電信事業並不包括線上提供可安裝於個人行動裝置之通信軟體供應者，故相關機關不得依通訊保障及監察法要求行動通訊軟體業者協助進行通訊監察。

35. (4) 警察機關如為偵辦案件，欲對有犯罪之虞者進行觀察及動態掌握等資料蒐集活動，請問下列何者為正確？(1)必須經由警察局長書面同意始得為之。(2)必須有足夠事實認

定犯罪之虞者有觸犯本刑 5 年以上有期徒刑者。(3)必須有足夠事實認定犯罪之虞者有參與組織性犯罪者。(4)以上皆是。**【資訊監察 M10635】**

解析：

按警察職權行使法第 11 條第 1 項：「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動：一、有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。二、有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。」故選項(1)(2)(3)皆為正確。

36. (4) 失蹤人口緊急查尋具特殊性，請問以下受理人員接獲報案標準流程何者正確？(1)應即核對報案人及失蹤人身分證明文件，並將失蹤人之基本資料、發生經過及其他有關線索，確實載明訪談筆錄。(2)詳細調查失蹤人之身分背景、交往對象及可能去向。(3)必要時報請調閱失蹤人口及特定對象之通聯紀錄或健保就醫紀錄。(4)以上皆是。**【資訊監察 M10636】**

解析：

按失蹤人口查尋作業要點第 7 點：「受理緊急查尋案件應注意下列事項：(一)製作報案筆錄應載明緊急查尋情狀，並詳細調查失蹤人之身分背景、交往對象及可能去向，積極展開查尋作為；必要時，得將筆錄連同查詢電信資料申請表，併傳勤務指揮中心依相關規定報請調閱失蹤人及特定對象通聯紀錄，或報請分局防治（戶口業務）單位調閱失蹤人健保就醫等資料，以利查尋。所調取通聯資料應於事後移由分局防治（戶口業務）單位併案持續追蹤、管考及複查。(二)視個案情形，立即報請勤務指揮中心通報轄內或他轄有關單位、線上警力緊急查尋，或洽請大眾媒體報導協尋。(三)未滿七歲者於緊急查尋二十四小時後仍未尋獲，且經查疑涉刑事案件時，比照重大刑案列管偵辦。(四)其他必要之適當查尋處置作為。」

37. (2) 關於「民用航空法」修正草案，以下敘述何者錯誤？(1)自然人所有最大起飛重量 250 公克以上的遙控無人機，使用者必向民航局註冊其無人機。(2)遙控無人機於禁航區、限航區及航空站或飛行場四周之一定距離範圍從事飛航活動，經地方公所許可即可為之。(3)操作公務機關所有之遙控無人機者，應經測驗合格。(4)從事遙控無人機飛航活動者不得以遙控無人機投擲或噴灑任何物件。**【資訊應用 A10637】**

解析：

按民用航空法修正草案第 99-10 條第 1 項：「自然人所有之最大起飛重量二百五十公克以上…之遙控無人機應辦理註冊並將註冊號碼標明於遙控無人機上顯著之處」；同法

修正草案第 99-13 條第 1 項:「禁航區、限航區及航空站或飛行場四周之一定距離範圍內，禁止從事遙控無人機飛航活動；航空站或飛行場四周之一定距離範圍由民航局公告之。」; 同法修正草案第 99-13 條第 3 項:「公務機關或法人執行業務需在第一項範圍之區域從事遙控無人機飛航活動，應申請民航局會商目的事業主管機關同意後，始得為之。」;同法修正草案第 99-14 條第 1 項:「從事遙控無人機飛航活動應遵守下列規定:...。二、不得以遙控無人機投擲或噴灑任何物件。...十、應防止遙控無人機與其他航空器、建築物或障礙物接近或碰撞。」顯見於禁航區、限航區及航空站或飛行場週圍，禁止從事遙控無人機飛航活動，如因執行業務則需民航局會商目的事業主管機關同意後，方可為之。

38. (4) 下列何者是自動化駕駛設備無法於道路上行駛之主要原因。(1)無法取得安全審驗合格證明。(2)相關主管機關尚未針對自動化設備訂定法規。(3)以上皆非。(4)以上皆是。**【資訊應用 A10638】**

解析：

按公路法第 63 條第 1 項:「汽車及電車均應符合交通部規定之安全檢驗標準，並應經車輛型式安全檢測及審驗合格，取得安全審驗合格證明書，始得辦理登記、檢驗、領照。國產汽車及電車製造業，應具備完善之汽車安全檢驗設備，嚴格實施出廠檢驗。製造業及進口商之檢驗設備經公路主管機關查驗合格發給證照者，得受委託為其製造或進口汽車之申請牌照檢驗。」與道路交通管理處罰條例第 12 條第 1 項第 1 款:「汽車有下列情形之一者，處汽車所有人新臺幣三千六百元以上一萬零八百元以下罰鍰，並禁止其行駛：一、未領用牌照行駛。」故選項(1)(2)皆為正確。

39. (4) 請問下列何者為使用數位簽章建立驗證措施所欲達到的效果？(1)確認簽章者身分，防止文件偽造。(2)確保內容不受到變更或竄改。(3)可使簽署人因無法在不否認其數位金鑰的情況下否認該文件上的簽章，進而無法否認其文件為其簽署。(4)以上皆是。**【資訊應用 A10639】**

解析：

數位簽章是透過簽署人之私鑰所形成的電子簽章，再以公鑰加以驗證後，可確認簽章者的身分，防止文件的偽造；亦可確保內容不受到變更或竄改，防止文件遭到攔截後變更內容；更可使簽署人因無法在不否認其數位金鑰的情況下否認該文件上的簽章，進而無法否認文件內容為其簽署。故選項(1)(2)(3)皆符合。

40. (4) 我國與外國政府或國際組織進行稅務用途資訊交換及提供其他稅務協助，應基於互惠原則，締約他方若符合下列何者敘述即不得進行資訊交換。(1)請求資訊之提供將

有損我國公共利益。(2)無法對等提供我國同類資訊。(3)請求提供之資訊非為稅務用途。(4)以上皆是。**【資訊應用 A10640】**

解析：按稅捐稽徵法第 5-1 條第 2 項規定：「與外國政府或國際組織進行稅務用途資訊交換及提供其他稅務協助，應基於互惠原則，依已生效之條約或協定辦理；條約或協定未規定者，依本法及其他法律規定辦理。但締約他方有下列情形之一者，不得與其進行資訊交換：一、無法對等提供我國同類資訊。二、對取得之資訊予以保密，顯有困難。三、請求提供之資訊非為稅務用途。四、請求資訊之提供將有損我國公共利益。五、未先盡其調查程序之所能提出個案資訊交換請求。」故本題選項(1)(2)(3)為正確，答案為(4)以上皆是。