# 資通安全法律案例宣導彙編

## 第 11 輯

行政院國家資通安全會報技術服務中心編印

中華民國 103 年 12 月

# 序

在社會高度資訊化的發展趨勢下，網路通訊科技成為資訊傳遞與交換的重要管道。因應雲端、社群網站的興起、智慧型手機及平板電腦等行動應用裝置的蓬勃發展，亦開始影響到個人與組織資訊運用的行為模式；而在國內開始實施個人資料保護法後，不論是個人或與組織下所面臨之資通安全法律議題挑戰，更趨複雜與多元。

「資通安全法律案例宣導彙編」，自 91 年發行第 1 輯，至今已發行 10 輯。「資通安全法律案例宣導彙編」，持續蒐集每年發生之資安時事新聞與法院實際案例，內容分別涵蓋資訊保護、資訊公開、資訊監察及資訊應用等不同面向，除了保持深入淺出的說明及專業法律觀點外，並與 ISO 27001 資訊安全管理標準之控制條文觀念結合，釋疑資通安全法律案例。

為擴散本案例彙編能量，103 年首度舉辦「資通安全法律案例彙編分享說明會」，會中從法律觀點與資訊安全管理觀點，進行資通安全法律案例的分享，藉由生活化資安實例分享與精闢簡要解說，讓大家對資訊安全有更深入之應用與探討，並邀集關注資訊安全趨勢與法制動態之產官學界人士，於會中共同激盪對於本案例彙編未來發展與推廣形式的意見，以期本彙編能為更多國人廣知，強化國人對資安法制之認知。

期藉由對近年來廣受社會矚目且生活化的實際案例，從法規面與管理面進行精要的說明解析，協助公務機關人員與一般民眾了解資通安全相關法律資訊，並建立新興資訊應用發展應有的基本法律概念。誠摯希望本案例彙編，能多為各界利用並成為政府機關與社會大眾進行資訊安全法治教育時之重要參考。

行政院國家資通安全會報 技術服務中心

劉培文主任 謹識

# 編者序

「行政院資通安全辦公室」(以下簡稱「行政院資安辦」)與「行政院國家資通安全會報技術服務中心」(以下簡稱「技服中心」),秉持資訊安全專業,積極提升國家整體資訊安全水準,甚為感佩。

個人資料保護法自 101 年 10 月施行至今,已累積不少實務案例,而營業秘密法於 102 年 1 月修正施行,增訂侵害營業秘密之刑事責任,亦促進企業導入營業秘密管理制度,以強化本身資產保護之意願。因此,本所將選輯個案相關的資訊安全法律與資訊安全管理系統之整合呈現,將可供政府單位與企業瞭解法律與管理相互檢視之重要性。此外,本冊資訊安全管理部分之「管理 Tips」,特別商請安侯企業管理股份有限公司協助提供資訊,併為致謝。

第 11 冊除延續第 10 冊之作業模式外,在擷取新聞議題時間主要以民國(以下同)102 年 1 月迄至 103 年 11 月新聞案例與判決為主。同時,因應網際網路訊息傳播的迅速,以及現今各界對智慧財產的重視,本次於「資訊保護」類中,新增「著作權法」案例,協助讀者從智慧財產權角度更為了解資訊保護所涉層面。

在「資訊公開」類,主要以「政府資訊公開法」為介紹案例,並因應政府開放資料此新興議題,就政府資訊公開層面,提供開放資料法規架構之說明。「資訊監察」類,以甫修正通過之「通訊保障及監察法」,作為政府從事資訊監察作業規範之介紹對象。有關「資訊應用」類,是以電子簽章在各類政府資訊服務與業界實務應用案例,作為介紹對象,可作為促進電子簽章制度推展之範例。

整體案例分布,仍以「資訊保護」佔大宗,有 21 則案例;「資訊公開」則為 2 則;「資訊監察」2 則與「資訊應用」5 則,共計 30 則。另,本冊新增自我評量單元,針對各篇案例提供評量題目供讀者自行

檢測理解程度，以強化對於案例內容的掌握。

在政府與企業各界正開發各項資料加值與雲端應用服務，以提升國家整體競爭力之際，應考量資訊安全法制架構與相關管理標準發展趨勢，以在相關資訊應用發展同時，平衡兼顧資訊安全與組織管理效能之需求。

國巨律師事務所

朱瑞陽律師

# 說　明

## 壹、案例彙編類別

本案例彙編分為四大類別，再由四大類別歸納所屬之資安法規範圍。

一、資訊保護 (Security)

01 個人資料保護法

02 國家機密保護法

03 營業秘密法

04 刑法

05 醫師法

二、資訊公開 (Disclosure)

01 政府資訊公開法

三、資訊監察 (Monitors)

01 通訊保障及監察法

四、資訊應用 (Application)

01 電子簽章法

## 貳、編碼原則

案例編碼共有 8 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 3 碼及上述各小類之編碼 2 碼，最後 2 碼為該小類中之第幾篇案例。例如：S1010101，即代表資訊保護類 101 年度之個人資料保護法第 1 則案例。

# 目　次

# 壹、　資訊保護（Security）

# 一、個人資料保護法

類別：資訊保護【**案號：S1030101**】

## 民眾欠繳國民年金保費，某機關網路公告全名惹議

### 【焦點話題】

某機關近日在其機關網站上，以 102 年 6 月 20 日保國二字第 10260400421 號公告「公示送達黃○○君等 49,963 人繳款單」，該名冊揭露 4 萬 9963 名保費欠繳者之姓名、身分證字號前 2 碼和後 3 碼、設籍縣市地區、欠費期間、累計月數及欠繳數額，有洩漏民眾個資疑慮，引發爭議。

該機關表示公示送達名冊所載人員均設籍於戶政事務所，應為送達之處所不明，係該局依行政程序法規定本權責所為公示送達之行政行為，於法有據，且遮蔽身分證字號部分號碼等資料，無違反個人資料保護法規定。

【資料來源：今日新聞 102/8/5】

### 【重點摘要】

1.機關網站公告不屬於法律規定的公示送達方式，機關若單僅以公告於機關網站作為唯一公示方式，恐不生送達效力。

2.公務機關為維護應受送達人權益，於職務範圍內併同於機關網站公告公示送達名冊時，應就身分資料採取適當遮蔽。

### 【法律觀點】

依國民年金法第 17 條之規定，被保險人未依規定期限繳納保險費及利息者，不予計入保險年資，且欠費逾 10 年之部分亦不得請求補繳，故某機關表示為避免民眾因未於期限繳納保險費而影響保險年資計算，且因欠費逾

10 年無法補繳保險費致影響其保險權益，對於送達處所不明之欠繳保費者，依行政程序法規定辦理公示送達[1]。

公示送達是為避免行政程序遲延，認為有必要時，藉由公示方法，使不能送達或無法送達之應受送達人，知悉應向何人領取應送達之文書。另，針對公務機關辦理公示送達之方式，法務部函釋指出公示送達事由之應為送達之處所不明，係指應受送達人之住居所、營業所、事務所或其他應為送達之處所全部不明，不能以其他方法為送達者而言，而道路交通管理處罰條例所稱之「公告」係屬公文程式條例所定公文程式類別之一，得以張貼於機關之公布欄、電子公布欄，或利用報刊等大眾傳播工具廣為宣布，與行政程序法上公示送達並不相同[2]。因此，公告與公示送達之效力應予區別，行政程序法就公示送達之方式，其文義並未涵蓋張貼於機關電子公布欄[3]。

惟，公示送達之制度目的係公開以利應受送達人知悉，且此類資料亦係依行政程序法公示送達規定得予公開。然而，公務機關辦理公示送達時，仍

---

[1] 行政程序法第 78 條：「對於當事人之送達，有下列各款情形之一者，行政機關得依申請，准為公示送達：一、應為送達之處所不明者。二、於有治外法權人之住居所或事務所為送達而無效者。三、於外國或境外為送達，不能依第 86 條之規定辦理或預知雖依規定辦理而無效者。有前項所列各款之情形而無人為公示送達之申請者，行政機關為避免行政程序遲延，認為有必要時，得依職權命為公示送達。當事人變更其送達之處所而不向行政機關陳明，致有第一項之情形者，行政機關得依職權命為公示送達。」；同法第 80 條：「公示送達應由行政機關保管送達之文書，而於行政機關公告欄黏貼公告，告知應受送達人得隨時領取；並得由行政機關將文書或其節本刊登政府公報或新聞紙。」

[2] 法務部 97 年 2 月 26 日法律字第 0960050744 號函釋指出：「行政程序法第 80 條所定『於行政機關公告欄黏貼公告』者，係屬公示送達之必備方式，除此之外，行政機關並得將文書或其節本刊登政府公報或新聞紙。至於道路交通管理處罰條例第 85 條之 3 第 3 項所稱『公告三個月』者，該『公告』並非應為送達處所不明所為公示送達之公告，應係屬公文程式條例第 2 條所定公文程式類別之一…[依]文書處理手冊規定，『其方式得張貼於機關之公布欄、電子公布欄，或利用報刊等大眾傳播工具廣為宣布。如需他機關處理者，得另行檢送。』自無本法公示送達相關規定之適用。」

[3] 另參法務部 98 年 10 月 26 日法律字第 0980035546 號函釋，就「行政程序法各條文中有關刊登於政府公報或新聞紙之規定，其所稱『政府公報或新聞紙』是否包括政府機關於網路上之電子公報或電子公布欄」乙節，指出：「本部曾於 89 年 7 月 28 提請本部行政程序法諮詢小組第 11 次會議討論獲致結論略以：『 1、行政程序法各條文中所稱之『政府公報』者，係指具有公報形式性（含以機關名義發行之）、定期性（包括按季、按月或按週發行者）、對外性及開放性之文書而言，包括行政機關於網路上之具有待與其他相關機關會商統一結論（惟為求明確，建請以修法方式解決之為妥）。』嗣本部於 89 年 8 月 8 日邀請相關機關開會研商『行政程序法各條文中有關刊登政府公報或新聞紙規定之涵義』，獲致具體結論略以：『基於目前電腦及網路使用之普及度與接受度仍屬可議、電腦資料之安全性無法確保及其他相關法制尚不完備等考量，暫不宜將行政程序法各條文中所稱之『政府公報』解釋為包括行政機關於網路上之電子公報，亦不包括電子公布欄』在案（法務部 90 年 1 月 18 日法律決字第 048924 號及同年 5 月 28 日法律字第 016818 號函參照）。」

應考量比例原則[4]，於使受送達人知悉之必要範圍內揭露其個資，以避免有過度揭露個資之疑慮。

因此，公務機關為執行法定職務並維護應受送達人之權益，於職權範圍內併於其網站上公告公示送達名冊，雖尚得主張符合特定目的內利用，惟應注意若單僅以公告於機關網站作為公示送達方式，可能不生送達效力，且機關公告應受送達人之相關個人資料，亦應就身分資料採取適當遮蔽，以符合比例原則。

## 【管理 Tips】

本案例中公務機關係執行法定職務而處理、利用保險對象個資，惟基於保護個人隱私起見，公務機關仍應有適當之控制措施，例如加密、遮蔽或隱碼等，避免因控制措施未確實落實，而逾越必要範圍、過度揭露個人資料，致使公示送達名冊成為個人資料外洩管道。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.8.1.3　資產之可被接受使用

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

A.8.2.1　資訊之分級

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予以分級。

A.8.2.2　資訊之標示

應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示

[4] 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。」

程序。

A.8.2.3　資產之處置

應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.18.1.1 適用之法規及契約的要求事項之識別

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。

A.18.1.4 個人可識別資訊之隱私及保護

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。

類別：資訊保護【案號：S1030102】

# 歐盟挺「被遺忘權」，Google 需移除個資搜尋結果

## 【焦點話題】

歐盟法院(Court of Justice of the European Union)作出具指標意義的判決，認為當個人資料顯然已過時且不相關時，一般民眾有權利要求美國網際網路搜尋巨擘 Google，刪除由該公司的搜尋引擎檢索出的鏈結，亦即行使「被遺忘權」(right to be forgotten)。

該案起因於一西班牙公民指控，只要在 Google 以他的姓名進行搜尋，就會連結到先前房地產遭拍賣的新聞，雖然債務糾紛早已透過司法程序解決，但相關紀錄仍能透過網路搜尋查得，讓他深受其擾。歐盟法院在本案判決指出，搜尋引擎以自動化、系統性方式蒐集網路資料，加以記錄、儲存並以清單方式提供使用者閱覽，符合歐盟個資指令定義之個人資料蒐集與處理活動，自應遵循歐盟個資保護指令相關要求。尤其當使用者以個人姓名進行檢索時，搜尋引擎可將個人私生活各種面向的資料相互連結，鉅細靡遺地呈現個人相關歷程，因此歐盟法院在肯認個人隱私與資料應予保護之情況下，判決認定當使用者網路檢索結果連結到的網頁資料，已為過時、無關或逾越原初處理目的範圍的資訊時，無論該資料原先是否為合法公開，搜尋引擎除有其他正當理由以外，應配合使用者提出的請求，於搜尋結果中移除該類網頁的連結[1]。【資料來源：自由時報 103/5/14】

## 【重點摘要】

1.以任何方式蒐集個人資料者，於其保有範圍內，負有依個資法規定提供個資當事人行使權利之義務。

[1] 關於歐盟本案判決簡要說明，可參照 Court of Justice of the European Union PRESS RELEASE No70/14, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos,Mario Costeja González, Judgment in Case C131/12, 13 May 2014, *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

2.若搜尋檢索結果所連結之網頁內容已過時、無關或逾越原初處理目的範圍的資訊時，搜尋引擎服務者即有依個資當事人請求而移除該連結之必要。

**【法律觀點】**

我國電腦處理個人資料保護法立法之初，即參考歐洲理事會個人資料自動化處理公約，而嗣後修正草案亦比照歐盟個資保護指令的架構，區分一般與特種個人資料，並依個人資料蒐集與處理等階段，課予資料保有者相應之責任與義務。是以歐盟個資保護指令的發展，對於我國個人資料保護法之適用與落實，即有可資借鏡參考之處。

搜尋服務提供者以搜尋程式連結含有特定檢索字串之資訊，符合我國個人資料保護法(以下簡稱個資法)第 2 條下所謂蒐集係指「以任何方式取得個人資料」之定義，且搜尋服務提供者將檢索結果，以特定方式排列並提供使用者點選查閱，亦符合我國個資法關於處理活動之定義[2]，因此搜尋服務提供者就其保有之個人資料，以及其連結本身所涉及之資料蒐集或處理，仍有我國個資法之適用。儘管目前 Google 僅提供歐盟公民請求移除其網頁連結之管道[3]，惟我國個資當事人依法亦享有請求停止蒐集、處理或利用其個資以及請求刪除之權利[4]。然而，搜尋服務提供者是否依使用者請求，即應刪除或停止處理、利用含有其個人資料之網路連結及其暫存資訊，仍應視有無符合個資法第 11 條第 3 項「因執行職務或業務所必須」之情形[5]，例如

---

[2] 個人資料保護法第 2 條：「本法用詞，定義如下：三、蒐集：指以任何方式取得個人資料。四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。」

[3] Google 自 103 年 6 月底已初步提供使用者線上申請移除連結資訊之表單文件，搜尋引擎無法自網路中直接移除該網頁內容，但使用者向 Google 提出申請後，Google 會停止在搜尋結果中顯示相關資訊。詳見 Search removal request under European Data Protection law, *available at* https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en

[4] 個人資料保護法第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：四、請求停止蒐集、處理或利用。五、請求刪除。」

[5] 個人資料保護法第 11 條第 3 項：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」同法施行細則第 21 條：「有下列各款情形之一者，屬於本法第 11 條第 3 項但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由。」

個資當事人為公眾人物，而該類資訊具有相當公共利益，而應賦予社會大眾知的權利時，即可得主張有「其他不能刪除之正當事由」而拒絕刪除。

為兼顧公眾知的權利，歐盟法院本案判決將「被遺忘權」之適用範圍，限於以個人姓名檢索所得之連結，且該連結資料與該個人已無關聯或已然過時，在此情形下，搜尋服務提供者原則上須依使用者請求而刪除。惟我國實務上，就個資當事人能否請求網路服務提供者移除連結、移除範圍或方式，以及網路服務提供者在何種情況下得主張具有「其他不能刪除之正當事由」，尚未累積相關實務見解，恐會對網路服務提供者受理當事人權利行使之作業造成衝擊，有賴我國主管機關與法院透過實務案例，以建立平衡公共利益與個人隱私保護之操作標準。

## 【管理 Tips】

本案例中搜尋引擎 Google 基於其所提供的服務內容特性，在維護社會大眾對公開資訊知的權利，與個人隱私保護問題之間，和歐盟隱私政策存有歧見。歐盟法院判決對於 Google 此類業者而言，未來如何在產業的創新發展與個人隱私保護上取得平衡，實為一大考驗。

惟在網路使用者個人隱私意識提高，以及對網路業者在個人資料的蒐集、處理或利用上普遍心存疑慮，業者應主動揭露及提供公開透明的個人資料蒐集、處理或利用相關政策，並加強與相關單位及使用者的溝通及聯繫，如權責機關（目的事業主管機關或相關政府單位）或特殊關注方（民眾、公民團體等），將有助於了解必須遵循的法律法規即將出的變化或趨勢，以預做準備。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.6.1.3　與權責機關的連繫

應維持與相關權責機關之適切聯繫。

A.6.1.4　與特殊關注方之連繫

應維持與各特殊關注方或其他各專家安全論壇及專業協會之適切聯繫。

A.18.1.1 適用之法規及契約的要求事項之識別

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。

A.18.1.4 個人可識別資訊之隱私及保護

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。

類別：資訊應用【**案號：S1030103**】

## 《機器戰警》翻版？警察拍人臉看光個資

### 【焦點話題】

台灣基層警察，2 月分開始增添新裝備。這款「M-Police」人臉辨識系統，只要將儀器拿起來對準人臉一照，10 秒鐘就能調出所有身家資料，而且以身分證上的照片及資料做為建檔基準。立委質疑，這根本是在侵犯人權，難道警政署要把台灣變成警察國家嗎？

新裝備「M-Police 查詢系統」，外表看起來像普通手機，其實裡面建置了人臉辨識系統，透過即時相片比對系統，10 秒鎖定人臉即可知該對象身分。原本用途為偵查犯罪，卻遭擴充使用連結戶政系統。民進黨立委即表示：「我們在學運期間，坐在門口就發現警察拼命拍，他們其實在作這樣的建置。」

也就是說，只要持有身分證的國民，資料就都被掌握在警方手裡，任何一個員警在任何時候，只要對準人臉一照就能調出資料，未來警方想找人很便利，但對於民眾的個人隱私卻成了最大威脅。立委親自實驗後卻嚇了一跳，擔心這樣的設備廣發給全國基層員警使用太過浮濫，還有侵犯人權的問題。

【資料來源：三立新聞 103/5/29】

### 【重點摘要】

1. 警察機關利用 M-Police 查詢系統，於公共活動現場攝錄參與者現場活動之影音資料，如與戶政系統之個人資料結合時，仍應有個資法之適用。
2. 警察機關利用 M-Police 查詢系統，於公共活動現場全面蒐集參與者個人資料時，仍應注意有無違反比例原則。

### 【法律觀點】

警察機關透過「M-Police 查詢系統」連結戶政系統，可即時確認通緝犯、

犯罪嫌疑人等身分資訊，而可及時防範相關犯罪行為之發生，有利於提升社會治安。依警察職權行使法第 9 條規定[1]，警察機關對於參與公共活動的行為人，如對公共安全或秩序有危害之虞時，可予以攝影、錄音或以其他科技工具，蒐集參與者現場活動資料。對此，個人資料保護法(以下簡稱個資法)第 51 條第 1 項第 2 款雖規定，「於公開場所或公開活動中所蒐集之未與其他個人資料結合之影音資料」，不適用個資法規定，但警察機關利用「M-Police 查詢系統」於現場蒐證，若與戶政系統之個人資料連結，已非單純記錄現場活動狀況時，仍無法豁免個資法規定之適用。

我國內政部戶政司掌管全國戶政資料，依個資法第 16 條規定，戶政機關對個人資料之利用，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。另一方面，警察機關基於犯罪預防、刑事偵查或執行等特定目的，利用「M-Police 查詢系統」與戶政系統連結，並進行個人資料的查詢或利用等行為，依個資法第 15 條[2]規定，警察機關於執行法定職務之必要範圍內，應得為之；而戶政機關將該等資料提供給警察機關，雖屬特定目的外之利用，但如係為協助警察機關偵查犯罪需要，應符合「為維護國家安全或增進公共利益」之情形，亦未違反個資法規定。

不過，在「交通部台灣國道高速公路局提供高速公路電子收費行車記錄資料與內政部警政署刑事警察局，作為刑事偵查使用」一案，法務部曾表示公務機關蒐集、處理或利用個人資料，應符合個資法第 5 條[3]及行政程序法第 7 條[4]比例原則之要求，因而認為「若刑事局進行『事前全面』蒐集高速公路行車紀錄資料之作為，在客觀上並非達成『刑事偵查』特定目的之『唯

[1] 警察職權行使法第 9 條第 1 項：「警察依事實足認集會遊行或其他公共活動參與者之行為，對公共安全或秩序有危害之虞時，於該活動期間，得予攝影、錄音或以其他科技工具，蒐集參與者現場活動資料。資料蒐集無法避免涉及第三人者，得及於第三人。」第 2 項：「依前項規定蒐集之資料，於集會遊行或其他公共活動結束後，應即銷毀之。但為調查犯罪或其他違法行為，而有保存之必要者，不在此限。」

[2] 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 6 條第 1 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。…」

[3] 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。」

[4] 行政程序法第 7 條：「行政行為，應依下列原則為之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。」

一或最小侵害方式』者，則仍不宜為之」[5]。因此，警察機關利用「M-Police查詢系統」，於公共活動現場全面攝錄參與者現場活動之影音資料，進而與戶政系統之個人資料連結進行查詢時，仍應注意有無逾越刑事偵查等目的之範圍，且該手段是否為達成其目的之「唯一或最小侵害方式」，以符合比例原則。

## 【管理 Tips】

本案例係因警政署近年所推動之「警政雲端運算發展計畫」，將「M-Police查詢系統」導入智慧型手機，透過即時相片比對系統，10 秒鎖定人臉以判知對象身分。其用途為偵查犯罪，卻因連結戶政系統，遭立法委員質疑嚴重侵犯民眾隱私。警政署之初衷是為協助治安防制，且認為對個人資料之利用是基於增進公共利益，符合法定權限。

惟對於民眾個人隱私之保護，政府機關間個人資料之交叉利用，仍應審慎考量法律之規定，於侵害人民基本權利和所欲達成之目的間，應有相當的平衡。而在執行業務的層面，則應考量資料遭濫用的可能性，因此可在存取控制上採取預防性措施（如資料使用之教育訓練）、管理性措施（如制定使用規範）、嚇阻性措施（如制定懲處規定）、偵測性措施（如存取活動如實記錄並分析存取記錄以發現異常），以杜絕弊端。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.7.2.2　資訊安全認知、教育及訓練

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。

A.7.2.3　懲處過程

應具備有正式及並已傳達溝通之的懲處過程，以對來採取行動處理

[5] 法務部 103 年 02 月 07 日法律字第 10303501220 號函。

違反資訊安全之的員工採取行動。

A.12.4.1 事件存錄

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。

A.18.1.4 個人可識別資訊之隱私及保護

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。

# 違個資法 農會總幹事拘役 30 日

## 【焦點話題】

A 是新北市某農會的總幹事，於民國 101 年 12 月間承辦該農會次屆理、監事、農事小組長（副組長）及會員代表的選務工作。A 為使與其同派系的農事小組小組長候選人 B 順利當選，乃將於職權範圍所掌有，且經公告供核對選舉人身分資料的各區組選舉人名冊，於 102 年 2 間的某日將公告後選舉人名冊提供給 B 使用，以利 B 向有選舉資格的會員拜票。然而，A 之行為已洩漏名冊上所列 C 等選舉人的姓名、出生年月日、入會日期與住址等個人資料，足生損害於 C 等人，遭新北地院認為已違反個人資料保護法，而處拘役 30 日。

【資料來源：新北地方法院 103 年度簡上字第 172 號判決】

## 【重點摘要】

1. 農會為辦理選舉，將選舉人名冊公告並予公開陳列以供閱覽一事，已由農會法授權訂定的農會選舉罷免辦法予以規範，屬特別法性質，應優先適用。
2. 農會總幹事將選舉人名冊提供他人作為助選之用，違反農會選舉罷免辦法規定，已逾越蒐集選舉人個人資料的特定目的必要範圍。

## 【法律觀點】

我國經濟活動目前雖以工商業為主，但因早期農業活動興盛，為保障農民權益，提高農民知識技能，促進農業現代化，增加生產收益，改善農民生活及發展農村經濟等目的，乃制定有農會法等規範。

我國的農會為社團法人組織，採會員制[1]，依法須設置理、監事，組成理事

[1] 農會法第 12 條：「凡中華民國國民，年滿二十歲，設籍農會組織區域內，實際從事農業，並合於左列各款之一者，經審查合格後，得加入該組織區域之基層農會為會員：一、自耕農。二、佃農。三、農業學校畢業或有農業專著或發明，現在從事農業推廣工作。四、服務於依法令登記之農、林、牧場員工，實際從

會與監事會，其理、監事由會員(代表)選任之[2]，故有辦理選舉之必要。依農會選舉罷免辦法規定，農會於辦理選舉時，應依會員會籍檔案及會員名冊編造選舉人名冊，載明編號、姓名、性別、出生年月日、入會年月日、會員種類及戶籍地址等個人資料，並應公告且公開陳列該選舉人名冊供選舉人核對身分資料是否正確。惟該選舉人名冊編造後，除農會及主管機關依法使用外，不得以抄寫、複印、攝影、錄音或其他任何方式對外提供[3]。可見農會與其承辦人員不但可能蒐集會員個人資料，更可能有處理或利用的行為，應受個人資料保護法(以下簡稱個資法)規定的拘束。

就公告並公開陳列選舉人名冊之部分，法務部曾揭示，個資法屬普通法性質，如其他法規另有特別規定時，仍應優先適用之[4]。是以，農會選舉的選舉人名冊公開陳列供閱覽事項，係因農會法所授權訂定的農會選舉罷免辦法已另為規範，自應優先適用，而排除適用個資法相關規定。

惟回歸本案，法院認為依前開相關規定可知，該名冊蒐集選舉人個人資料的特定目的，僅在提供選舉人核對身分資料。A 身為農會總幹事，屬非公務機關，於承辦該選舉人名冊的業務時，應依個資法第 20 條第 1 項前段規定，於蒐集的特定目的範圍內予以利用[5]。然而，A 卻違反不得對外提供選舉人名冊的規定，將該選舉人名冊提供給 B，作為助選之用，已逾越蒐集選舉人個人資料之特定目的必要範圍，而屬特定目的外之利用，且足生損害於其他選舉人，遂判處拘役 30 日。

---

事農業工作。」

[2] 農會法第 19 條第 1 項：「農會置理、監事，分別組成理事會、監事會。…」

[3] 農會選舉罷免辦法第 11 條：「農會辦理選舉應依會員會籍檔案及會員名冊編造選舉人名冊，載明編號、姓名、性別、出生年月日、入會年月日、會員種類及戶籍地址，並得按農事小組分別編訂，加蓋農會圖記。……選舉人名冊編造後，除農會及主管機關依法使用外，不得以抄寫、複印、攝影、錄音或其他任何方式對外提供。」第 12 條：「農會應於農事小組選舉投票日前六十日在農會與其辦事處、信用部分部及各農事小組公告，敘明選舉人名冊於農會及其辦事處、信用部分部公開陳列供閱覽七日，當事人發現錯誤或遺漏時，或會員種類及戶籍地址於公告日之前有異動者，應於公告之日起七日內，以書面向農會申請更正。……」

[4] 法務部 102 年 1 月 16 日法律字第 10100713340 號函、102 年 4 月 19 日法律字第 10203503430 號函。

[5] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之。…」

## 【管理 Tips】

本案例係因被起訴人基於個人利益，而將含有個人資料之選舉人名冊提供他人使用，已違反當初個人資料蒐集的使用目的。在本案例中，除被起訴人之行為已違反法令，組織於資訊安全管理中對資訊的保護亦有待改善之處，包括應明確定義資訊資產可被接受使用的規則（如存取、複製、散播、個人資料蒐集/處理/利用等），以防止資訊被誤用或濫用。另外也需強化人員對組織資訊（包括個人資料）保護責任與相關法規的認知，以及針對違反規定者應有適切的懲處，以遏止違反規定的情事發生。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.7.2.2　資訊安全認知、教育及訓練

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。

A.7.2.3　懲處過程

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。

A.8.1.3　資產之可被接受使用

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

A.18.1.4 個人可識別資訊之隱私及保護

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。

類別：資訊保護【**案號：S1030105**】

# 金管會有條件開放銀行消金系統跨境委外

## 【焦點話題】

金融機構作業委託他人處理內部作業制度及程序辦法(以下稱本辦法)自民國(下同)95 年 9 月 18 日發布施行，迄今已逾五年，並於 101 年 2 月 8 日修正，明定禁止本國銀行將消費金融業務相關資訊系統之資料登錄、處理或輸出等事項委託至境外辦理。

惟為配合我國積極與其他國家洽簽雙邊自由貿易協定，因應我國加入「跨太平洋夥伴協定」與「推動區域全面經濟夥伴協定」的需求，金融監督管理委員會(以下簡稱金管會)基於資訊安全風險管理、確保消費者權益保障及主管機關監理權限不受影響之原則下，就本國銀行得將消費金融業務相關資訊系統跨境委外辦理，增訂其資格條件與風險管理機制，以解決金融相關開放議題。本辦法修正案嗣於 103 年 5 月 9 日發布施行。

金管會官員表示，雖然開放本國銀行消金資訊系統可跨境委外，但銀行仍應確實落實客戶資料保護，金管會將執行定期金融檢查或專案金檢。

【資料來源：中央社 103/3/15】

## 【重點摘要】

1. 本國銀行經主管機關核准後，得將消費金融業務相關資訊系統之資料登錄、處理或輸出等事項委託至境外辦理。
2. 本國銀行若將作業項目委託至境外處理，應建立營運備援計畫、日常監督機制並符合主管機關相關規定。

## 【法律觀點】

本辦法於 101 年 2 月 8 日修正時，考量到本國銀行應具有在我國境內提供

客戶即時、完整及正確服務之能力，且為降低資訊系統集中境外及資料國際傳輸所衍生之風險，並強化對客戶個人資料的保護，故本國銀行不得將消費金融業務相關資訊系統之資料登錄、處理或輸出等事項，委託至境外辦理。但為配合我國積極與其他國家洽簽雙邊自由貿易協定，暨推動加入「跨太平洋夥伴協議」與「區域全面經濟夥伴協定」等國際區域整合之重大政策，金管會參考各國規範及銀行實務情形，於 103 年 5 月 9 日修正原辦法第 18 條第 5 項禁止本國銀行跨境委外之規定，開放符合一定資格條件[1]並檢具相關書件[2]的銀行，向金管會申請並獲核准後，得將消費金融業務相關資訊系統委託至境外辦理。

本項修正有助於銀行解決客戶資料跨境處理的需求，並透過專業分工降低整體成本。為強化對銀行消金系統跨境委外的資訊安全控管，銀行除應遵守個人資料保護法施行細則第 8 條關於個資業務委外監督事項[3]以外，尚應符合本辦法新增關於跨境委外風險管理機制的相關要求，包含本國銀行應就受委託機構對客戶資訊之使用、處理及控管情形，確認符合我國個人資料保護法相關規定、留存完整稽核紀錄及定期進行查核，且本國銀行對資訊系統的資安檢測標準不得低於我國規範等，以確保銀行境外消金系統具有基本系統安全防護能力，而能確實保護客戶資料安全與相關權益。本辦法亦規定若本國銀行於本辦法修正施行前，已將消金系統跨境委外辦理，

[1] 本辦法第 18 條第 6 項：「前項所稱資格條件係指符合下列規定之本國銀行：一、最近一年內無因違反金融相關法令，受主管機關處分之情事，或有違反法令情事已具體改善，並經主管機關認可。二、申請前一年底經主管機關或中央銀行糾正之缺失，均已切實改善。三、最近一年內無重大資安事故未改善之情事。」

[2] 本辦法第 18 條第 5 項：「本國銀行符合資格條件者，得檢附第一項、第二項規定書件連同下列書件，向本會申請核准後，將消費金融業務相關資訊系統之資料登錄、處理、輸出等事項委託至境外辦理：一、委託具資訊專業之獨立第三人出具海外資訊系統不低於我國資訊安全標準之查核報告。二、針對海外資訊中心發生無法提供服務情事，建立營運備援計畫，並由具資訊專業之獨立第三人出具該計畫符合以下要求之評估報告...。三、日常監督機制之計畫書。四、報經董事會通過之成本效益與集團內費用分攤合理性之評估報告。」

[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，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。」

即應於本辦法施行後 1 年內取得金管會核准，否則應於調整期屆滿二年內將消金系統移回境內辦理。因此，有此情事的本國銀行即應於上開期限內，盡速調整並取得金管會核准，以落實法規遵循。

**【管理 Tips】**

在基於資訊安全風險管理、確保消費者權益保障及主管機關監理權限不受影響之原則下，金管會修法並適度開放本國銀行得將消費金融業務相關資訊系統，跨境委外辦理，惟必須確保客戶資料的保護，不得因此作業方式而受到影響。

由於事涉與外部單位的資訊交換，故組織應從政策面、管理面、實作面及法規面，規劃與外部單位資訊交換事宜。包括建立資訊傳送的管理政策，依不同的資訊內容、資訊系統、傳送媒介與管道，訂定適當的管理措施與保護要求，並且採用必要的安全技術，如加密、安全傳輸通道、安全協定等。

與外部單位的資訊交換，也應透過正式的協議，說明組織與外部單位間，對資料保護與資訊安全措施的權責義務，協議內容也應定期審查，以反映及符合法規、資訊科技環境的變化，針對資訊安全要求適時調整。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.13.2.1 資訊傳送政策及程序

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

A.13.2.2 資訊傳送協議

協議應闡明組織與外部各方間營運資訊之安全傳送。

A.13.2.3 電子傳訊

應適切保護電子傳訊時所涉及之資訊。

A.13.2.4 機密性或保密協議

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。

類別：資訊保護【**案號：S1030106**】

## 知名廠牌手機洩個資，通傳會推手機資安認證

### 【焦點話題】

經資訊安全公司測試證實，手機製造商北京○○科技有限責任公司(以下簡稱北京○○公司)生產的手機，會自動將使用者背景資料傳送至北京伺服器。北京○○公司隨後坦承，使用者利用其「網路簡訊服務」時，在未經使用者同意下，該服務會自動將使用者電話號碼、國際行動用戶識別碼(International Mobile Subscriber Identity)及國際行動裝置識別碼(International Mobile Equipment Identity number)，回傳至北京○○公司位於中國北京的伺服器上。○○公司表示資訊均以明碼傳輸，因此有能力的網管人員確實能夠利用監控工具，竊取使用者的電話號碼。

我國國家通訊傳播委員會(以下簡稱通傳會)表示已展開調查，將發函請台灣○○通訊有限公司(以下簡稱台灣○○公司)，針對事件始末與後續因應措施一併說明，並同時調查其他手機業者有無類似情形。通傳會資源技術處長表示，行政院日前在資通安全會報上指示經濟部工業局與通傳會，針對手機軟、硬體資安進行分工。因此，通傳會目前鼓勵手機製造廠商進行自願性檢測後，公開資訊以利消費者參考，並規劃檢測機制，預計最快於 104 年底上路。

【資料來源：自由時報 103/8/13】

### 【重點摘要】

1. ○○公司若能將使用者門號與相關識別碼，與其本身保有的資料連結比對而識別特定使用者時，即涉及個人資料之蒐集、處理及利用。

2. 北京○○公司若未經使用者書面同意，亦與台灣消費者無直接契約關係下，逕行蒐集使用者資料，恐違反我國個資法相關規定，且使用者資料傳

輸過程均以明碼顯示，亦衍生資訊安全疑慮。

## 【法律觀點】

我國個人資料保護法(以下簡稱個資法)第 51 條第 2 項規定：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」而所謂中華民國領域外，依法務部函釋可推知，係指我國政府法權未及之地域[1]。北京○○公司為中國電子科技產品生產商，並由台灣○○公司負責手機在台銷售與行銷事宜，但北京○○公司所蒐集的資料，若可得識別特定中華民國國民使用者，其資料作業相關活動仍應有我國個資法之適用。例如，北京○○公司蒐集個資前，原則上應向使用者告知法定應告知事項、符合個資法規定之合法蒐集法定事由，並有提供當事人行使請求更正、停止蒐集或刪除等權利之義務，且應就資料傳輸過程採取適當安全維護措施，以避免個人資料遭到不法蒐集、處理、利用或其他侵害。

北京○○公司以軟體自動回傳方式，蒐集台灣○○手機使用者的電話號碼、國際行動用戶識別碼及國際行動裝置識別碼，依法務部函釋見解指出「蒐集者如能將行動電話號碼與其他資料對照、組合、連結而得識別特定個人，即屬本法所稱之個人資料而有本法適用」[2]。是以，北京○○公司若能將門號與相關識別碼，與其本身保有之資料，例如台灣○○公司所提供的預購單或服務註冊資料等，進行比對而識別特定使用者時，即涉及蒐集、處理及利

[1] 參照法務部 94 年 8 月 26 日法律字第 0940029553 號法規諮詢意見：「本法有關國際傳遞之規定，其立法目的係為落實個人資料保障之落實，避免跨境個人資料流通失控，故就我政府法權未及地域之跨境傳遞予以規範管理。準此，機關（公務或非公務）將個人資料傳輸至我國法權未及之地域，即屬本法所稱之國際傳遞，從而向大陸地區傳輸個人資料，自為本法所定之國際傳遞。」

[2] 法務部 102 年 5 月 12 日法律字第 10203502260 號函釋：「按本法第 2 條第 1　款規定：『本法用詞，定義如下：一、個人資料：指自然人之姓名、.....、聯絡方式、.....、社會活動及其他得以直接或間接方式識別該個人之資料。』是以，蒐集者如能將行動電話號碼與其他資料對照、組合、連結而得識別特定個人，即屬本法所稱之個人資料而有本法適用。至行動電話用戶蒐集、處理及利用個人資料行為，若係基於自然人單純為個人活動目的而為者，則無本法適用。」另參照法務部 103 年 6 月 18 日法律決字第 10303506790 號函釋：「電話號碼未顯示用戶個人姓名等資料，僅顯示相關攜碼轉移電信公司資訊，是否屬個人資料乙案，查行動電話（代碼 C001 ：識別個人者）是否得以直接或間接方式識別者，需從蒐集者本身綜觀各種情況與事證加以判斷，原無一致性之標準，此宜於個案中加以審認，尚未可僅依單一資料類型，即遽論是否為個資法所稱之個人資料。」

用我國使用者的個人資料[3]。

此外，我國個資法修正新增告知義務規定，修正理由即指出：「個人資料之蒐集，事涉當事人之隱私權益。為使當事人明知其個人資料被何人蒐集及其資料類別、蒐集目的等，爰規定蒐集時應告知當事人之事項，俾使當事人能知悉其個人資料被他人蒐集之情形。」在本案中，北京○○公司除違反前述告知義務外，若未經使用者書面同意，亦與台灣消費者無直接契約關係下，逕行蒐集使用者資料，已侵害個資當事人隱私權益，並恐欠缺蒐集個資之合法事由。而本案使用者資料在傳輸過程中，均以明碼顯示，亦衍生資訊安全疑慮。是以，我國○○手機使用者可能得以北京○○公司違法蒐集個資，向其請求民事損害賠償。

另，依我國電信法規之規定，手機等電信終端設備均應符合通傳會訂定之技術規範，並經審驗合格，始得輸入或販賣[4]，但手機內建軟體的資安認證尚不在審驗範圍。通傳會針對此一事件，目前已積極規劃相關驗證標準暨檢測機制，以期全面改善手機產品的資訊安全，並維護消費者權益。

## 【管理 Tips】

本案例係因北京○○公司所製造及銷售的手機，會自動將使用者背景資料傳送至北京伺服器，因而引發消費者對於個人資料、隱私遭到監控的質疑，甚至引起社會大眾對中國製通訊產品可能危害國家安全的疑慮。

此一案例與組織資訊安全的關聯及所衍生的課題，可分為兩個方面。首先是個人所使用的行動裝置如手機、平版電腦及筆記型電腦等，隨著員工自行攜帶行動裝置上班(Bring your own device)議題的發酵，組織不得不正視並採取因應措施，無論開放與否，都應建立必要的行動裝置管理與限制的政

[3] 附帶說明，通訊傳播委員會於 101 年 9 月 25 日衡酌大陸地區之個人資料保護法令尚未完備，通訊傳播事業於國際傳遞及利用個人資料時，應考量接受國家或地區對個人資料有完善之保護法令，遂頒布命令限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。該命令雖於舊法時代作成，惟至今仍為有效。故通訊傳播事業依法不可將其用戶之個人資料，傳輸至大陸地區處理或利用。惟，北京○○公司與台灣○○公司均非經通傳會特許或許可的通訊傳播事業，尚無須受通傳會前開國際傳輸命令之限制。

[4] 電信終端設備審驗辦法第 4 條第 1 項規定：「連接第一類電信事業所設電信機線設備之電信終端設備，應符合技術規範，並經審驗合格，始得輸入或販賣。」

策，以避免組織資料藉由個人的行動裝置，遭人有心或無意的洩漏。

另一方面，組織所採購的資通訊設備，亦應評估納入必要的安全規格或安全等級要求，對於提供資通訊服務的供應商，也應約定資訊安全品質或明確要求產品的安全規格。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.6.2.1　行動裝置政策

應採用政策及支援之安全措施，以管理使用行動裝置所導致之風險。

A.15.1.3 資訊及通訊技術供應鏈

與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。

# YouBike 211 萬會員個資恐外洩

## 【焦點話題】

「小小黃」YouBike 廣受歡迎，台北市現已建置 163 個租借站，註冊會員卡數達 211 萬。台北市議員甲質詢指出，民眾租借 YouBike 必須提供姓名、手機號碼、電子信箱及悠遊卡卡號等資料，註冊成為會員，但會員服務條款允許承攬公共自行車業務的 A 公司，將個資用於「其他經營公共事業業務」與「其他經營合於營業登記項目或組織章程所訂之業務」。議員甲質疑 A 公司營業項目五花八門，個資恐遭不當使用。

議員甲另指出，台北市政府交通局（以下簡稱北市交通局）與 A 公司簽訂契約明定「不得將台北公共自行車資料洩漏予第三人」，但 A 公司卻將會員資訊，包含登錄、傳輸與保存全都分包給 B 公司，該公司網站還稱「看不到的後台會員、金流系統，B 都默默地 24 小時監看」，更有個資外洩之虞。

北市交通局科長乙稱 A 公司承攬公共自行車業務時，有籌組團隊，包含 B 公司、C 公司等。乙強調會員資料僅在租借系統與發送會員通知信使用，針對議員甲之質疑，該局將會檢討修正服務條款，限縮個資使用範圍。

【資料來源：中時電子報 103/7/30】

## 【重點摘要】

1. 公務機關委託業者辦理業務若涉及個人資料，應依個資法相關規定進行監督，以確保業者蒐集、處理或利用個人資料符合規定。
2. 業者受公務機關委託蒐集個人資料時，應於委託機關指示之範圍內為之，不得逾越特定目的之必要範圍。

## 【法律觀點】

本件 YouBike 公共自行車系統，係由北市交通局委託 A 公司所組團隊營運，包含 A 公司經營該 YouBike 租借所蒐集、處理或利用個人資料之業務。此時，A 公司係受公務機關委託蒐集、處理或利用個人資料，並將會員資料之登錄、傳輸及保存等事宜分包予 B 公司，依個人資料保護法(以下簡稱個資法)第 4 條與個人資料保護法施行細則(以下簡稱個資法施行細則)第 7 條規定[1]，A 公司與 B 公司（下稱承包商）將視同委託機關(即北市交通局)，並應遵守委託機關適用之相關法規。

北市交通局將 YouBike 租借等相關蒐集、處理及利用個人資料之業務，委託承包商辦理，依法須對受託者負適當之監督義務[2]，包括個資蒐集、處理或利用之範圍、類別、特定目的及其期間，所採取的適當安全維護措施等事項，以確保委託處理個人資料之安全管理，且受託者亦僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料[3]，是以北市交通局對承包商於辦理 YouBike 租借業務過程所蒐集之個人資料，自應注意並監督其涉及之個資範圍是否符合個資法第 5 條規定[4]及是否符合委託目的。另由於個資法施行細則前開規定，「有複委託者，其約定之受託者」亦屬北市交通局監督事項，故北市交通局應於契約要求 A 公司對於複委託予 B 公司的行為進行監督、管理，並約定 A 公司負有使 B 公司遵守委託契約及相關個資法規定等責任。此外，北市交通局亦應定期確認受託者執行之狀況，並記錄確

[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。」個資法施行細則第 7 條：「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」

[2] 個人資料保護法施行細則第 8 條第 1 項：「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。」

[3] 個人資料保護法施行細則第 8 條第 3 項：「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。…」

[4] 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。」

認結果[5]。

承包商既視同公務機關，依個資法第 8 條[6]及第 15 條[7]規定，對於租借者個人資料之蒐集或處理，除應符合特定目的外，亦須符合執行法定職務必要範圍，或須經當事人書面同意等法定要件，並應明確告知公務機關名稱、蒐集目的、個人資料類別、個人資料利用期間、地區、對象及方式等事項。是以，承包商受北市交通局委託辦理 YouBike 租借業務，如已逾越委託機關指示之範圍，將蒐集特定目的擴大至該公司「其他經營公共事業業務」、「其他經營合於營業登記項目或組織章程所訂之業務」等事項，即可能違反個資法規定。為避免前開爭議，北市交通局基於監督義務應要求承包商進行調整，故承包商亦已配合修正該使用條款所告知之個資使用目的，排除用於「其他經營公共事業業務」與「其他經營合於營業登記項目或組織章程所訂之業務」，以限縮個資使用範圍。

## 【管理 Tips】

本案例為北市府委託廠商營運公共自行車租賃系統，而廠商將其中有關資訊處理的部份如會員登錄與借還資訊系統，另委由其他系統廠商處理，引發民眾對於個資遭到外洩的疑慮。

本案例除北市府應先釐清與廠商所簽訂的契約，針對廠商將資訊轉包委外是否已有規範外，鑑於資訊委外作業已成為許多組織資訊作業的常態，對於委外廠商的管理應有適當的規範。包括組織應透過明確的協議，來界定雙方的權利義務以及資訊安全的要求，對於廠商將受委託的資訊服務再轉包，除應於契約中予以規範外，若允許再轉包，則必須將資訊安全的要求

[5] 個人資料保護法施行細則第 8 條第 2 項：「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。…」

[6] 個人資料保護法第 8 條：「公務機關或非公務機關依第 15 條或第 19 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。…」

[7] 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、經當事人書面同意。三、對當事人權益無侵害。」

擴及到其下包商或供應鏈中的相關廠商。同時組織也應依據契約規定，透過對廠商的監視與審查，確保下包商遵守協議中所要求的資訊安全要求，以保護重要的資產（如個人資料）。對於執行業務所需的個資蒐集，也應事先定義及要求，以符合使用目的，避免過度蒐集及誤（濫）用。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.15.1.1 供應者關係之資訊安全政策

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。

A.15.1.2 於供應者協議中闡明安全性

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。

A.15.1.3 資訊及通訊技術供應鏈

與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。

A15.2.1 供應者服務之監視及審查

組織應定期監視、審查及稽核供應者服務交付。

A.18.1.4 個人可識別資訊之隱私及保護

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。

## 好萊塢大咖陷 iCloud 艷照門，「尋找我的 iPhone」惹的禍

### 【焦點話題】

好萊塢女星私密照越爆越多，目前多數矛頭指向是「尋找我的 iPhone」（Find My iPhone）和「iCloud」漏洞釀禍，駭客可以無限次嘗試明星的密碼組合，直到成功為止。因此，破解許多明星 iCloud 的駭客，不僅將照片流出，也將暴力破解密碼的軟體「ibrute」傳上網。

使用者有了這套「ibrute」，就能對 Find My iPhone 帳號發動暴力破解攻擊，更因為系統漏洞，讓駭客可不斷嘗試不同電子郵件和密碼，也不會被攔截。一旦密碼強度太差，該破解軟體嘗試上萬次後，就能取得他人 iCloud 上的所有資料。

雖有女星表示「那些都是很久前已刪除的相片」，但因 iCloud 具有備份功能，即使已經把 iPhone 上照片刪除，駭客駭入雲端依然能取得過去的照片。由於這次的洩密風波牽連眾多知名的明星，Apple Inc.公司（以下簡稱蘋果公司）目前已經迅速更新「尋找我的 iPhone」系統，現在只要在頁面上輸入 5 次錯誤的密碼，就會遭到鎖定，同時也已經針對整起事件進行徹底調查。

【資料來源：東森新聞 103/9/3】

### 【重點摘要】

1. 廠商提供具儲存功能系統時，為避免他人利用暴力攻擊軟體破解該系統，應於採取適當防護機制，以維護使用者隱私與資料安全。
2. 使用者於使用雲端或軟體服務時，應了解其隱私設定及可能的風險，並避免將高度機密或私密文件儲存於相關系統，以減少資料外洩之可能。

### 【法律觀點】

本件 Find My iPhone 及 iCloud 是內建於 iPhone 手機的軟體，iCloud 提供使用者將手機相關資料，包括連絡人資訊與照片等，上傳至雲端備份，倘若手機遺失等時，則可利用 Find My iPhone 尋找手機。iCloud 儲存主機雖位於中華民國境外，但因提供備份功能，其所蒐集的資料如包含我國民眾的個人資料時，亦應適用我國的個人資料保護法（下稱個資法）[1]，故應遵循包括須符合蒐集法定事由，依法向使用者進行告知，並提供當事人行使請求更正、停止蒐集或刪除等權利，且應就保有的個人資料檔案採取適當安全維護措施[2]等規範。

蘋果公司雖於使用者註冊 Apple ID 時，已要求密碼長度、至少應包含之字元，以及不得與帳號相同等措施。然而，於 iCloud 與 Find My iPhone 軟體登入系統時，卻缺少帳密登入錯誤次數限制或暫停登入等防護機制，造成駭客利用「ibrute」軟體自動無限次組合 Apple ID 與密碼，以破解並取得他人資料。蘋果公司於事件發生後已緊急更新，加上只要輸入 5 次錯誤的密碼就會鎖定的防護機制，以保護使用者隱私及資料之安全。又此事件如確實是因為 iCloud 與 Find My iPhone 軟體登入系統缺少防護機制，造成資料外洩，依我國個資法第 12 條[3]規定，蘋果公司尚負有就本事件查明後，以適當方式通知使用者之責任，如致使用者受有損害時，除非蘋果公司能證明其無故意或過失，否則須負損害賠償責任[4]。

此外，駭客的行為在我國亦涉及多項刑事犯罪：其無故以「ibrute」軟體自動組合帳密，登入他人帳號之行為，在我國將可能構成刑法第 358 條「入

[1] 個人資料保護法第 51 條第 2 項：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」

[2] 個人資料保護法施行細則第 12 條：「本法第 6 條第 1 項第 2 款所稱適當安全維護措施、第 18 條所稱安全維護事項、第 27 條第 1 項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」

[3] 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。」

[4] 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。」

侵電腦或相關設備罪」[5]。而其取得 iCloud 伺服器中他人之私密照片或其他個人資料，則可能構成刑法第 359 條「無故取得、刪除或變更電磁紀錄罪」[6]，且因屬違法蒐集個人資料之行為，而有違反個資法第 41 條第 1 項[7]規定之虞。其後，駭客將利用電腦等設備取得的他人私密照片流出之行為，除可能違反刑法第 318 條之 1 的「無故洩漏他人秘密罪」[8]外，亦可能屬違法利用個人資料之行為，而有違反個資法第 41 條第 1 項規定之可能。

是以，使用者於利用相關軟體、系統或雲端服務時，須了解相關系統或服務的隱私設定及可能的風險，同時應避免將高度機密或私密文件儲存於相關系統或服務內，以保障自身的隱私與資料安全。

## 【管理 Tips】

隨著行動裝置日益普及且功能越來越強大，人們使用行動裝置在公、私領域的分野，開始不再有那麼清楚的界線，對組織的管理者而言，這是一個不得不予以正視的問題。從此次爆發的蘋果 iCloud 案例，無論是因使用者的習慣所造成的個人私密資料外洩，或是系統本身的漏洞而使惡意人士有可趁之機，對組織在行動裝置的管理上，都有可供參考之處。

首先是個人所使用的行動裝置如手機、平版電腦、筆記型電腦等，無論現階段組織是否開放個人行動裝置於公務上使用，都應未雨綢繆，預先建立必要的行動裝置管理政策。對於資訊類的資產或與組織相關的重要資訊，如果透過行動裝置存取或處理，亦應規範其複製、儲存的相關使用規定，如避免使用遠端存取或將其儲存於雲端系統。

而在本案例中，通行碼無疑是一個最平常卻也是最常被疏忽的問題，組織

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

[6] 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。」

[7] 個人資料保護法第 41 條：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，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。」

[8] 刑法第 318 條之 1：「無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處二年以下有期徒刑、拘役或五千元以下罰金。」

除應教育使用者擁有良好的通行碼保管及使用習慣外，亦應從系統面著手，建立嚴謹的通行碼使用規則（包括系統設定與系統開發），以避免系統之通行碼因使用者疏失或遭惡意人士破解，而導致重要資訊外洩。

另此次事件，也有可能是因為設備本身存有漏洞所引起，因此組織對於使用的裝置，應蒐集及留意其相關的安全威脅及發布的系統更新或修正程式，在評估後予以適時更新或修補，以避免重要資訊因系統漏洞而有外洩之虞。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.6.2.1　行動裝置政策

應採用政策及支援之安全措施，以管理使用行動裝置所導致之風險。

A.9.4.3　通行碼管理系統

通行碼管理系統應為互動式，並應確保嚴謹通行碼。

A.12.6.1 技術脆弱性管理

應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

類別：資料保護【**案號：S1030109**】

## 報導牙醫打病患，判 A 報須隱個資

### 【焦點話題】

B 牙醫 11 年前為 6 歲某男童看診時，因男童哭鬧不休，打了男童一巴掌，A 報乃以「看診哭鬧牙醫打耳光」為標題刊登新聞，並公布了 B 牙醫姓名、診所名稱和部分地址。B 牙醫認為 A 報之報導已揭露過多個人資料，使他屢遭網友揚言列入黑名單，訴請排除侵害。最高法院維持二審判決，認定 A 報揭露 B 牙醫的相關資料與公益無關，判決 A 報敗訴確定，其相關網頁須隱匿牙醫個資。

A 報法務經理不服該判決，並強調：「報導內容都是事實，此判決如同限制媒體監督功能，非常不合理。」但 B 牙醫認為報導已影響病患看診信心，並侵害他的名譽權。法院判決則認為，報導前 B 牙醫雖同意受訪，但要求以打馬賽克及匿名方式報導，A 報卻執意揭載 B 牙醫的相關個資，造成社會制裁作用，已過度減損其名譽，且當事人雙方已和解，B 牙醫已獲不起訴處分，而該事件當事人又均非公眾人物，新聞自由應顧及個人隱私，本案亦與公益無關，故判令 A 報須隱匿 B 牙醫的個人資料。

【資料來源：蘋果日報 103/8/15】

### 【重點摘要】

1. 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件涉及公共利益的程度。
2. 倘當事人已依個資法請求停止蒐集、處理或利用其個人資料時，新聞報導即不應揭露其姓名、地址、肖像等資料，以免產生爭議。

### 【法律觀點】

我國實務認為避免箝制新聞自由，新聞媒體工作者倘就涉及公共利益事務的報導，經合理查證，且依所得資料有相當理由確信其為真實者，即認已盡善良管理人之注意義務而無過失[1]。另實務上亦認為，公眾人物的言行事關公益，應盡最大之容忍，接受新聞媒體監督，但仍不因此剝奪公眾人物的隱私權[2]。是以，我國就新聞採訪自由與隱私權界限的判斷標準，係以事件的公共性為區分界限；亦即，衡酌新聞採訪或報導手段是否已侵害個人不受侵擾的私人活動領域；採訪或報導手段，是否已逾越社會通念所得容忍的界限；以及新聞事件是否具一定之公益性，而屬大眾所關切並具有新聞價值者等，以為判斷[3]。

本件 B 牙醫因某 6 歲男童看診時，哭鬧不休，打了男童一巴掌，並遭男童家長提告等情，遭 A 報報導。法院認為[4]，B 牙醫於報導前同意 A 報進行採訪，A 報報導內容已詳載雙方說法，進行平衡報導，且該內容亦為真實，可認 A 報已盡新聞媒體工作者應盡的合理查證義務。又法院認為[5]B 牙醫與該患者均非公眾人物，該事件亦僅涉特定患者的權利，不致對公眾產生廣泛影響，既 B 牙醫於報導前，已要求須以打馬賽克或匿名方式進行報導，A 報自不應將足以識別 B 牙醫個人的姓名、診所名稱及部分地址等揭露於報導中。因 A 報揭露 B 牙醫相關資料，導致消費者將其列入黑名單，對 B 牙醫已生社會制裁效果，而有減損 B 牙醫名譽的情形，B 牙醫可依民法第 18 條[6]規定，要求 A 報隱匿或移除有相關其個人資料之內容。

此外，B 牙醫於受訪前，已要求 A 報須以打馬賽克或匿名遮蔽其個人相關

[1] 最高法院 103 年度台上字第 558 號判決、最高法院 100 年台上字第 861 號判決。
[2] 最高法院 93 年度台上字第 851 號判決、高等法院 102 年度上字第 758 號判決。
[3] 大法官會議釋字第 689 號解釋理由書：「…惟就新聞採訪者之跟追行為而論，是否符合上述處罰條件，除前述跟追方式已有侵擾被跟追人之身體安全、行動自由之虞之情形外，就其跟追僅涉侵擾私密領域或個人資料自主之情形，應須就是否侵害被跟追人於公共場域中得合理期待不受侵擾之私人活動領域、跟追行為是否逾越依社會通念所認不能容忍之界限、所採訪之事件是否具一定之公益性等法律問題判斷，並應權衡新聞採訪自由與個人不受侵擾自由之具體內涵，始能決定。…」
[4] 台灣高等法院高雄分院 102 年度上字第 10 號判決。
[5] 同前註 4。
[6] 民法第 18 條：「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。前項情形，以法律有特別規定者為限，得請求損害賠償或慰撫金。」

資料之方式進行報導，乃屬行使個人資料保護法（下稱個資法）第 3 條[7]所定請求停止蒐集、處理或利用個資之當事人權利，A 報竟仍揭露 B 牙醫的姓名、診所名稱和部分地址，不但未尊重當事人權益，亦與個資法第 5 條[8]所定不得過度蒐集、處理或利用的原則相違，而有違反個資法之虞。

綜上所述，我國實務乃以公共利益作為新聞自由與隱私權保障的折衷點，是以，倘被報導者並非公眾人物，且事件內容不涉及公共利益時，報導者應避免揭露足以識別被報導者的相關個人資料，包括姓名、地址、肖像等，以避免發生爭議。

## 【管理 Tips】

本案例由於被告為新聞媒體，因此涉及新聞自由與個人隱私衝突的爭議，對於一般組織就個人資料處理及利用的角度來看，仍有參考價值。

組織在執行與個人資料相關的業務時，基於保護個人隱私，應從內部要求與外部要求兩個層面來看。內部要求是指組織自發性的個人資料保護措施，而為使組織業務之執行與隱私保護不相衝突。

而外部要求則是應識別外部單位如主管機關、合作夥伴等對組織在個人資料（或敏感資訊）的保密及保護要求並遵守之，以避免有違反法規及契約的情事發生，造成組織損失。透過內部與外部要求之落實，以降低組織業務運作之資料安全風險。

## 【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

[7] 個人資料保護法第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」

[8] 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。」

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。

## 門市聯網個資全都露，A 電信急鎖討論區

### 【焦點話題】

A 電信台中、東山等 4 個加盟服務中心區域聯網「超可愛討論區」獎金區，把客戶姓名、電話號碼及費率等資料全都露，輸入電話號碼可查一年來洽辦門號的客戶資料，違反個人資料保護法。

市議員陪同受害人 B 男召開記者會，B 男說日前看到售屋廣告，以手機撥打該仲介電話問價錢，隨後接到回撥報價，卻直呼他母親的名字，驚訝之餘詢問仲介如何得知母親名字（手機門號以母親名義申請），仲介告知上網輸入手機號碼，便可在討論區看到。B 男即按照該房仲講的程序操作，在 Google 搜尋，果然發現母親姓名、使用費率及申辦時間等個資出現在「超可愛討論區」一月份 A 電信獎金區中。討論區內還有 A 電信台中市其他服務中心近一年來的獎金區，每月每筆申辦門號資料一覽無遺。

市議員表示門市業者的作法，很容易淪為詐騙集團竊取使用，應徹底解決。A 電信則回應，設定內部討論區時，因疏忽未予鎖碼而公開，獲知後已馬上鎖掉討論區，至於留在 google 的暫存檔，正設法聯繫。

【資料來源：自由時報 102/09/25】

### 【重點摘要】

1. 公司內部討論區應採取權限管控，並為必要遮蔽之適當安全防護措施，以避免任何人得透過網路檢索取得相關資料。
2. 公司發生個資外洩事故後，應採取補救措施，並將事故原因及已採取之因應措施等通知受害當事人。

### 【法律觀點】

民眾辦理申請或續約門號事宜時，電信公司依法須核對、登錄其姓名、身分證字號及住址等資料[1]，已屬非公務機關蒐集個人資料之行為，應依個人資料保護法（下稱個資法）相關規範辦理。而為了擴大服務區域，電信公司多會約定由各獨立經營的通訊行，協助辦理手機門號申辦或續約等電信服務，使通訊行成為加盟商，本件的加盟服務中心即屬此類。是以，加盟服務中心如係以 A 電信之名義，蒐集、處理或利用其用戶姓名、手機號碼或費率等資訊，即應視同委託機關，依 A 電信應適用之規定為之[2]，並僅得於 A 電信指示的範圍內蒐集、處理或利用個人資料[3]。至於 A 電信則須負適當的監督責任，包括受託者即加盟服務中心預定蒐集、處理或利用個人資料的範圍、類別、特定目的及其期間、應採取的適當安全維護措施、事故發生的通知及補救措施等，並須定期確認受託者的執行狀況[4]。

在本案例中，各加盟服務中心建置內部討論區，並於討論區公開用戶資料之行為，倘若已逾越 A 電信的指示範圍時，A 電信基於委託監督義務，自得要求加盟服務中心停止此行為。又加盟服務中心因受 A 電信委託蒐集、處理或利用個人資料，亦應對個人資料檔案採取適當安全維護措施[5]，於建置內部討論區時，對其網路或軟、硬體設備有無系統漏洞應定期檢視，避

[1] 例如，行動通信業務管理規則第 73 條第 1 項：「經營者應核對及登錄其使用者之資料，經載入經營者之系統資料檔存查後始得開通，並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之。以預付卡或其他預付資費方式經營本業務之服務者，亦同。 」同條第 2 項：「前項使用者之資料包括使用者姓名、身分證或護照之證號、身分證或護照外之其他足資辨識身分之證明文件證號、住址及所指配號碼等資料。」另第三代行動通信業務管理規則第 77 條及行動寬頻業務管理規則第 77 條等亦有類似規定。

[2] 個人資料保護法第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」個人資料保護法施行細則第 7 條：「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」

[3] 個人資料保護法施行細則第 8 條第 4 項：「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] 個人資料保護法施行細則第 8 條第 1、2、3 項：「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 12 條第 2 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 1 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。」

[5] 個人資料保護法第 27 條：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」

免遭駭客入侵或攻擊，對於該內部討論區亦應採行權限控管等[6]安全維護措施，以避免發生任何人可透過網路搜尋功能，取得個人資料之情形。

此外，本件加盟服務中心因疏忽未將內部討論區鎖碼，使他人可藉由網路輕易搜尋獲取用戶個人資料，致生個資外洩情形，事發後加盟服務中心雖已緊急鎖掉討論區，並為處理暫存檔而聯繫 Google，亦須依個資法第 12 條[7]與個資法施行細則第 22 條[8]規定，應將個人資料被侵害之事實與已採取之因應措施，通知 A 電信與被害當事人。而 A 電信除能證明其無故意或過失外，遭資料外洩的用戶亦可要求 A 電信負損害賠償責任[9]。

## 【管理 Tips】

本案例為電信業者之加盟服務中心，於公開網路所建立之網路社群進行內部資訊交換與分享，由於未留意該討論區屬公開性質而未進行鎖碼，以致客戶之個人資料被意外揭露。

本案例雖為加盟服務中心之行為，然業者仍需負起必要之責任。因此組織對於委託或授權外部單位（如廠商）處理、維運組織之重要資訊或系統，應透過適當的方式或途徑，確保其了解組織對於資料保護及資訊安全的要求，必要提供其所需的教育訓練，尤其是對於透過公共網路進行的（個人）資料分享、傳輸活動，更應要求注意資訊保密的保護事項，以避免資料遭不當揭露而淪為詐欺活動或非法利用的工具。

---

[6] 個人資料保護法施行細則第 12 條：「本法第 6 條第 1 項第 2 款所稱適當安全維護措施、第 18 條所稱安全維護事項、第 27 條第 1 項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。」

[7] 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。」

[8] 個人資料保護法施行細則第 22 條：「本法第 12 條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。依本法第 12 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。」

[9] 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。」

另一方面，組織一旦發生資安或個資事故，應有適切的管道通報相關事件，以避免組織因無法快速掌握事由而致事態及影響擴大。同時為保護組織以及受影響之當事人，組織應建立必要之事故回應及處理程序，針對事故進行處理，必要時亦應通知受影響之當事人。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.14.1.2 保全公共網路之應用服務

應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。

A.14.1.2 保全公共網路之應用服務

應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。

A.16.1.2 通報資訊安全事件

應循適切之管理管道，儘速通報資訊安全事件。

A.16.1.5 對資訊安全事故之回應

應依文件化程序，回應資訊安全事故。

# 二、國家機密保護法

類別：資訊保護【**案號：S1030201**】

## 銷毀機密檔，監察院秘書長遭彈劾

### 【焦點話題】

監察委員日前發現監察院秘書長於民國(下同)100 年 6 月指示辦理「監察院調查案件檔卷清理計畫」，就監察院已歸檔且未逾保存年限，以及需要永久保存的調查案與行政案卷，逕自抽取部分內容銷毀，總計有 1654 件檔案「無從查考」。秘書長擅自銷毀高達 161.5 公尺，相當於新光大樓高度的檔案，遭到監察院彈劾，並將其移送公務員懲戒委員會懲戒。

秘書長解釋「檔案的數量太大，為節省空間，才清理檔案」，監察委員表示表示，「整個院內的檔案被銷毀將近三分之一，且沒有留下備份與電子存檔，這是何其嚴重的事情！」。惟監察院彈劾審查會 102 年 6 月 10 日以 4 票對 7 票，未通過彈劾案，監察委員表示將提出第二次彈劾。

【資料來源：東森新聞雲 102/6/10】

### 【重點摘要】

1. 定期保存之檔案，未逾法定保存年限或未依法定程序，不得銷毀。將屆保存年限之檔案，應依法製作檔案銷毀目錄並訂定銷毀計畫，始得辦理銷毀事宜。

2. 經核定為機密的檔案，未經解密，不得逕予銷毀，經解密後始得依檔案法相關規定辦理銷毀。

### 【法律觀點】

依我國檔案法規定，檔案依其保存年限，可分為永久保存或定期保存，定

期保存的檔案未逾法定保存年限或未依法定程序，不得銷毀[1]。又依監察院檔案管理要點規定，各單位處理公務或因公務產生之結案文件及附件、各種會議紀錄及人事任免銓審獎懲之紀錄等文件，均應送檔案管理單位歸檔，並於文卷歸檔時，依案情填明保存年限[2]。監察院就業已歸檔之文件應依檔案法規定加以管理，且定期保存之檔案，於法定保存年限內應妥善保存。除非因情況急迫，檔案有變質、散發有毒物質而嚴重危害人體，或是遭遇戰爭、暴動或事變，為保護國家安全或利益而須即時銷毀之情形外，尚不得任意銷毀[3]。

再者，縱使檔案已屆保存年限，公務機關亦應依機關檔案保存年限及銷毀辦法的相關規定，辦理銷毀事宜，包含製作檔案銷毀目錄後送會相關業務單位表示意見，並訂定銷毀計畫，且執行銷毀時應由檔案管理單位會同相關單位派員全程監控[4]。若經核定銷毀的檔案，在仍有保存價值等必要情形時，仍應先經電子儲存，始得銷毀。此外，檔案若涉及核定為機密之文件，尚須由公務機關的檔案管理單位會商業務承辦單位辦理解密後，始得銷毀[5]，以確實落實政府機關檔案管理。

---

[1] 檔案法第 10 條：「檔案之保存年限，應依其性質及價值，區分為永久保存或定期保存。」同法第 12 條：「定期保存之檔案未逾法定保存年限或未依法定程序，不得銷毀。各機關銷毀檔案，應先制定銷毀計畫及銷毀之檔案目錄，送交檔案中央主管機關審核。經檔案中央主管機關核准銷毀之檔案，必要時，應先經電子儲存，始得銷毀。機關檔案保存年限及銷毀辦法，由檔案中央主管機關擬訂，報請行政院核定之。」

[2] 監察院檔案管理要點第 2 點：「本院各單位處理公務或因公務產生之下列文件，均應送檔案管理單位歸檔：（一）辦理結案之文件及附件。（二）各種會議紀錄。（三）簽及有關公務之文件。（四）印信之模式。（五）契約或其副本。（六）人事任免銓審獎懲之紀錄。（七）其他應行歸檔之文件。前項以外之其他各類型公務紀錄資料，具下列性質，足供機關內外部使用者，應審酌辦理歸檔：（一）機關法定職能運作，可供業務參考或權責稽憑者。（二）具保障個人、團體或政府機關法定權益者。（三）具滿足民眾「知」的權利之資訊價值者。（四）具學術研究參考者。（五）具影響國家、地方發展及社會公益者。（六）具保存歷史文化、典章制度或科技價值者。存置於首長、副首長辦公室檔案，具前揭性質者，亦同。免予歸檔或不得歸檔之文件類型，除相關檔案法令另有規定外，依本院各單位公文歸檔作業注意事項規定。」

[3] 機關檔案保存年限及銷毀辦法第 14 條第 1 項：「檔案有下列情形之一，且情況急迫時，得逕行銷毀之：一、因變質而散發有毒物質，嚴重影響人體健康者。二、遭遇戰爭、暴動或事變，為保護國家安全或利益而須即時銷毀者。」

[4] 機關檔案保存年限及銷毀辦法第 8 條：「各機關辦理定期保存檔案之銷毀，以每年一次為原則。已屆保存年限之檔案，各機關檔案管理單位或人員應依檔案中央主管機關規定之格式製作檔案銷毀目錄，送會相關業務單位表示意見，各單位認有延長保存年限之必要者，應簽註延長年限及理由。」同辦法第 10 條：「本法第 12 條第 2 項所定銷毀計畫，應包括下列事項：一、擬銷毀檔案年度及數量。二、擬銷毀檔案現在存放地點。三、擬銷毀時間、地點及方式。四、其他經檔案中央主管機關指定事項。前項銷毀計畫及第 8 條檔案銷毀目錄，應依本法施行細則第 10 條第 1 項各款規定程序，函送檔案中央主管機關審核。」

[5] 機密檔案管理辦法第 18 條：「機密檔案未經解密，不得銷毀。但有機關檔案保存年限及銷毀辦法第 14 條第 1 項所定情形者，不在此限。」同辦法第 22 條：「業務承辦單位應依有關法規之規定，主動辦理機密檔

本案中，監察院秘書長指示並核定辦理「監察院調查案件檔卷清理計畫」時，就監察院已歸檔的未逾保存年限，以及應永久保存的調查案與行政案卷，逕予抽除部分內容並銷毀，致有大量監察院調查檔卷內容遭抽除而無從查考。因此，監察院秘書未依檔案法相關規定辦理檔案銷毀事宜，恐將因違反檔案法規定而負有刑責[6]。

## 【管理 Tips】

本案例中，由於人員未依規定逕行銷毀組織之資料，導致組織重要資料永久無法回復，嚴重影響資訊（料）之完整性。

無論是政府機關（構）或一般民間企業組織，對於各種型態的資料保管與處置，大多有一定的規範，不論是外部法令法規的規定，或者是內部作業的要求，都會要求對資料本身及保存資料的媒介提供適當且必要的保護，並在保管至規定的期限後，始得以依程序予以處置或銷毀。

對組織而言，所持有的資料在其資料生命週期，無論資料是以何種型態存在，或存在何種介質媒體上，除應確保其安全之外，對於資料的相關活動，如存取、複製、傳輸、刪除、汰除、銷毀，都應依程序加以限制。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.8.3.2　媒體之汰除

當不再需要媒體時，應使用正式程序加以安全汰除。

A.18.1.3 紀錄之保護

應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽

案之機密等級變更或解密事宜。檔案管理單位應定期清查機密檔案。清查時，得請業務承辦單位依法辦理機密檔案機密等級之變更或解密事宜。但保密期限屆滿者，其解密事宜，由檔案管理單位會商業務承辦單位辦理之。」

[6] 檔案法第 12 條：「明知不應銷毀之檔案而銷毀者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 5 萬元以下罰金。違反第 12 條之銷毀程序而銷毀檔案者，亦同。」

造、未經授權存取及未經授權發布。

# 三、營業秘密法

類別：資訊保護【**案號：S1030301**】

## 科技公司告前總經理案，竹檢不起訴

### 【焦點話題】

某知名科技股份有限公司(以下簡稱科技公司)向新竹地檢署提出告訴，指控前手機事業群總經理甲在 101 年 2 月 17 日上午 10 時左右，辦理離職稽核手續後，竟在同一天下午 2 時左右，未經該公司同意，擅自使用員工系統帳號登入公司的電腦系統，無故從公司配發給他工作使用的筆記型電腦中，重製 2,053 筆資料至行動硬碟內並攜離公司，嗣後於 102 年 4 月間即跳槽至大陸公司任職。該科技公司以洩漏工商秘密罪、違反營業秘密法等罪嫌，向新竹地檢署提出告訴。

本案承辦檢察官認為甲所備份之工作資料，是基於主管指示工作交接所授權進行之重製，且檢方亦查無證據顯示甲有洩漏其任職期間所持有或接觸營業秘密資料的行為，故全案不起訴處分。

【資料來源：工商時報 103/6/11】

### 【重點摘要】

1. 公司就具有經濟價值之機密資料應建立管理措施，應控管員工存取權限並於其離職時註銷帳號權限，以降低營業秘密外洩的風險。
2. 營業秘密法修正施行後，員工逾越主管指示範圍而重製公司資料，或經主管要求刪除、銷毀重製之檔案卻故意不為刪除或銷毀時，恐負有刑事責任。

### 【法律觀點】

營業秘密法對於營業秘密的定義，明定應具備「非一般涉及該類資訊之人所知」、「因其秘密性而具有實際或潛在之經濟價值者」以及「所有人已

採取合理之保密措施者」等三項要件。鑑於營業秘密的價值乃在其秘密性，因此企業若欲就其具有經濟價值的內部機密資訊，例如市場銷售資料或新產品設計圖等，依營業秘密法保護而排除他人侵害時，即有必要就這類資訊採取適當的保密或其他管理措施。

在電子化工作環境下，企業機密資料可能儲存於內部網路電腦共用資料夾或資料庫，導致企業難以採取限制攜出或影印等對傳統紙本的管控機制。因此，針對員工帳號採取存取權限控管，或要求有接觸企業營業秘密機會之人員簽署保密條款等措施，以確保人員認知，並遵循企業的營業秘密保護政策與相關作業規定，成為企業愈益重視的管理面向。然而，企業經常面臨人才流動問題，為避免持有或得接觸營業秘密的人才跳槽或自行創業後，使用或洩漏原公司的營業秘密，進而打擊原公司的競爭優勢，企業除基於工作交接考量，有必要請離職人員交付所有業務檔案文件或提供資料清單以外，基於保護企業營業秘密，亦應考量於離職手續辦理完成後，立即關閉該人員存取權限，並要求人員應刪除任職期間儲存於其個人設備的機密資料，以降低企業營業秘密外洩的風險。

102 年 1 月 30 日營業秘密法修正施行前，我國刑法對於無故竊視、竊聽或竊錄他人非公開活動或言論之行為[1]，與無故洩漏他人業務秘密、工商秘密或因利用電腦或其他相關設備知悉或持有他人之秘密等行為[2]，在「妨害秘密罪」章雖設有刑責，惟其行為態樣仍屬有限，罰則亦輕。在營業秘密法修正施行後，已新增侵害營業秘密的刑罰規範，該法第 13-1 條除加重罰責外，亦擴大了構成侵害他人營業秘密之行為類型，以強化對營業秘密的保護[3]。例如，原本具正當理由持有營業秘密之員工，如離職後經原公司告知

[1] 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。」

[2] 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，處一年以下有期徒刑、拘役或五萬元以下罰金。」；第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」；第 318-1 條：「無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處二年以下有期徒刑、拘役或五千元以下罰金。」

[3] 營業秘密法第 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

刪除、銷毀該營業秘密，而故意不為刪除、銷毀或有隱匿情事時，即可依營業秘密法課予刑責。因此，本案如發生於營業秘密法修正施行後[4]，雖因總經理甲以公司配發帳號登入系統並重製多筆公司資料，乃係基於主管指示與授權，尚不構成擅自重製或以其他不正方法取得營業秘密之行為，但總經理甲如已逾越主管指示範圍而重製其他公司資料，或經主管要求刪除、銷毀重製之檔案卻故意不為刪除或銷毀時，仍可能依營業秘密法上開規定負有刑責。

## 【管理 Tips】

本案例可從人員安全管理面與存取控制實作面來強化重要資料的保護。在人員安全管理上，組織應有適當的人員規範，使員工能意識到相關的保密義務及違反時的法律責任，如於人員聘用或離職時，透過簽署保密協議書或離職訪談，使人員了解其對公司重要機敏資訊，仍負有持續保密之責任與義務。

而在存取控制的實作面，本案例顯然在使用可攜式媒體的管理上有所疏漏，以及在人員存取權限之移除或調整的作業上仍有待改善之處。組織宜重新評估現行資訊保護控制措施是否有效，包括評估是否採用及部署資料外洩防護 (Data Loss Prevention)之技術工具，以管制並偵測對資料的存取行為和提供必要的資料保護。另外針對資訊存取限制與權限管理異動的時效性，應在人員異動時，於規定的時間內予以調整，例如刪除、停用或僅保留最小權限等，以降低潛在人為不良意圖的資料外洩風險。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

---

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。」

[4] 刑法第 1 條：「行為之處罰，以行為時之法律有明文規定者，為限。」

A.7.1.2　聘用條款及條件

組織與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。

A.7.3.1　聘用責任之終止或變更

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。

A.8.3.1　可移除式媒體之管理

應依組織所採用之資訊分級方案，實作管理可移除式媒體之程序。

A.9.2.6　存取權限之移除或調整

所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。

# 不動產委託銷售資料屬工商秘密

## 【焦點話題】

A 男於民國（下同）99 年至 101 年間，任職於 H 不動產經紀股份有限公司（下稱 H 公司），負責不動產之仲介銷售業務，且曾簽署 H 公司員工規範及人事保證書，同意對任職期間，透過職務所獲取及建立的秘密、因職務取得的客戶資料，或於職務上所完成之著作及相關無形權利，皆以 H 公司為所有人及著作人，其所知的秘密及智慧財產權皆歸 H 公司所有，非經 H 公司的同意，不得擅加使用洩漏與他人。

然而，A 男卻於 100 年間將客戶委託 H 公司仲介買賣的不動產銷售總價額，包括底價、物件編號與地址等訊息，透過電腦發送簡訊方式，傳送「a213989，底 390，OO 路二段 183 號 10F 之 2，a217361，底 570，OO 路 225 巷 36 號」、「a219111，底 1180，OO 街 32 巷 17 之 1 號，a216793，底 1137，OO 街 68 號 10F」等訊息予已自 H 公司離職，改任職於 Y 公司的 B 男，使 B 男獲知相關物件之底價。後因 H 公司資訊人員檢索公司內部系統時始知悉上情，並提起告訴，法院認 A 男雖犯行明確，但因犯後態度良好，判處拘役 40 日，並得易科罰金。

【資料來源：台灣高等法院台中分院 102 年度上易字第 1077 號判決】

## 【重點摘要】

1. 不動產買賣之實際委託銷售總價額，攸關賣方獲利、仲介利潤、與買方磋商空間，及仲介業者往後之商譽評價，因非一般人可輕易得知，且多採取合理保密措施，已屬工商秘密範疇。

2. 賣方縱委託數家仲介業者處理不動產銷售事宜，其實際委託銷售總價額仍因涉及利潤、報酬等因素，非屬一般人得輕易知悉的資料，不因授權多家

業者而喪失其秘密性。

## 【法律觀點】

A 男任職於 H 公司期間，已簽署員工規範及人事保證書，同意就任職期間因職務所獲取或建立的秘密、客戶資料、智慧財產權等，負有保密義務，卻擅自將客戶委託不動產買賣之銷售總價額（即底價）洩漏給他人，似涉洩漏工商秘密行為。而我國營業秘密法於 102 年 1 月 30 日公布增訂刑事責任，因 A 男行為發生於修法前，尚不適用營業秘密法刑罰之規範。是以，本案關鍵在於不動產買賣的實際委託銷售總價額，是否屬於刑法上的工商秘密。

刑法第 317 條[1]雖規定，行為人依法令或契約有保守工商秘密之義務，卻無故洩漏時，構成洩漏工商秘密罪而負有刑責，但並未對工商秘密加以定義。本案法院認營業秘密法已對營業秘密加以定義[2]，即「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、所有人已採取合理之保密措施者之方法、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」，可資參酌作為本案判斷的基礎。

是以，法院認 A 男所洩漏者，乃是客戶委託仲介買賣不動產的實際委託銷售總價額，除影響買方開價成交的價格外，亦涉及委託人所得利潤高低與仲介業者之服務報酬。仲介業者基於受託關係，自會竭力達到委託人期待，同時提高服務報酬，自不可能任意向買方公開底價，故此價額屬一般人不得輕易知悉，且因其秘密性具有實際或潛在的經濟價值。此外，H 公司採取須以公司人員身分並使用公司電腦登錄查詢之機制，已具合理保密措施，足認該價額屬工商秘密的範疇。A 男未經 H 公司同意，將該價額無故洩漏予他人，已構成刑法第 317 條的洩漏工商秘密罪。

---

[1] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處 1 年以下有期徒刑、拘役或 1 千元以下罰金。」

[2] 營業秘密法第 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。」

一般不動產仲介網站或傳單上對物件所標示的底價，多作為廣告性質，以公開方式促發買方意願，與賣方委託仲介買賣不動產的實際委託銷售總價額，因涉及賣方與仲介業者的利益，且為保留與買方磋商空間，自不會輕易公開的特性不同。縱使賣方基於成本等考量，委託數家業者處理銷售事宜，並提供予各家不同的實際委託銷售總價額，仍涉及利潤或磋商空間等因素，一般人無法輕易得知，與前開廣告性質的底價自有不同，仍可認為屬工商秘密的範疇。受僱人倘已承諾負職務上保密義務者，自不可無故洩漏，以免涉犯刑責。

## 【管理 Tips】

本案例係員工違反與公司簽立之員工規範及人事保證書，擅自將關係公司利益之營業機密傳送給競爭對手。在此案例中，該公司之機敏資料外洩，除了該員工違反與公司約定之誠信原則是主要原因之外，該公司對於資料之保護亦有可再改善加強之處。

由於該員工是以電腦傳送相關資訊，若組織對於機敏資料之保護有其必要，應將資訊之存取控制政策以及資訊及資訊處理設備的相關使用規則予以明確規範，確保人員知悉其職責範圍內的責任與義務，並應謹慎管理資訊之存取權限，評估是否有採用及部署資料外洩防護 (Data Loss Prevention) 技術工具的必要，以管制及偵測對資料的存取行為和提供必要的資料保護。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.8.1.3　資產之可被接受使用

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

A.9.1.1　存取控制政策

存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審

查之。

# 四、刑法

類別：資訊保護【**案號：S1030401**】

## 裝監視器侵害鄰居隱私 判賠 1 萬

### 【焦點話題】

A 男不滿住家同樓的鄰居 B 男在住處門口及走廊樑柱，裝設 2 支監視器，其拍攝範圍包括 A 家門口與電梯出入口。A 男發現 B 男裝設監視器後，曾寄出存證信函給 B 男，但雙方未獲得共識，A 男認為 B 男的行為已侵害隱私，提訴要求拆除並賠償 10 萬元。

B 男於法院主張，因與 A 男曾有糾紛，對方不斷騷擾，加上該棟大樓出租房屋較多，且常有出租給吸毒者等原因，他才於 102 年間於住家門口裝設監視器。然而，法官認定 B 男未經同意私自裝設監視器，已侵害鄰居隱私，判決 B 男應拆除監視器並賠償 A 男 1 萬元。

【資料來源：自由時報 103/6/27】

### 【重點摘要】

1. 電梯出入空間因與住戶私領域活動空間連結，可揭露住戶私領域活動相關訊息，住戶對此有隱私之合理期待，屬應受隱私權保護的範圍。
2. 未經區分所有權人同意，擅自架設監視器拍攝、監視他人私領域活動者，已屬侵害隱私權的行為，行為人應除去該侵害外，亦可能負賠償責任。

### 【法律觀點】

近來住家治安事件屢屢發生，民眾越發注意居家安全，因此許多民眾以裝設監視器的方式，嚇阻宵小入侵。但因監視器拍攝範圍除公共區域如樓梯間以外，亦可能會涉及他人生活空間，是否侵害他人隱私權即有爭議。

我國法院過去曾認為公寓大廈各層的電梯走廊，雖非住戶即區分所有權人的專有部分，但因與專有部分有直接或間接之連結，透過電梯走廊的通行及使用情形，得以明瞭或知悉住戶的作息動態及交友狀況等私人資訊，故公寓大廈住戶對於該層電梯走廊所能透露的前述私人資訊，仍有隱私之合理期待，性質上仍屬該層住戶的私領域空間，應受保護。至於住家安全，包括防範社區內、外人員所生維安狀況等，屬於公寓大廈管委會（下稱管委會）的權責，應由其加強大樓的保全管理、施予門禁措施等，因此欲加強住家安全，可由管委會採取加強門禁等措施。在未經管委會、住戶大會決議或同層住戶一致同意裝設監視器前，就擅自架設監視器時，其手段與目的已有失衡，也非屬最小侵害手段，未能符合比例原則，故認為屬不法侵害他人隱私權之行為，行為人除應除去該侵害外，並應負包括精神慰撫金在內的損害賠償責任[1]。

而本件 B 男所裝設之監視器拍攝範圍，包括 A 男家門口與電梯出入口，從 A 男家門口與電梯出入口拍攝到的影像，可能會透露 A 男的生活習性或出入狀況等情形，屬於隱私權範圍。B 男於未經住戶大會或 A 男同意下，即擅自裝設監視器監視他人私領域活動，依前述見解，已屬不法侵害他人隱私權，法院亦判命 B 男應拆除監視器，並賠償 A 男因此所受精神上損害之慰撫金 1 萬元。

住家安全雖為個人可得安居樂業的重要因素，但公寓大廈涉及多人居住與使用空間之權益，為避免涉及侵權爭議，如住戶對於住家安全有所疑慮，欲架設監視器時，應獲得區分所有權人或相關住戶的同意，且僅於必要範圍進行拍攝，避免擴及他人私領域活動，以減少爭議發生。

## 【管理 Tips】

本案例係因被告人未經同意私自裝設監視器，侵害鄰居隱私，因而被判必須拆除且賠償。鑑於監視器（或其他如行車記錄器、手機錄影）之使用，

[1] 參台灣板橋地方法院 101 年度訴字第 681 號、台灣高等法院 100 年度上字第 1001 號判決及 101 年度上易字第 704 號等判決。

已成為現今執法機關、私人機構或民眾做為治安防制、財產與人身保護的一項利器，惟在使用上仍不時有侵害隱私的爭議或疑慮。如台北市正爭取修法，希望能利用全市 1.3 萬台的監視器畫面取締交通違規，就引發適法性與侵犯民眾隱私的疑慮。

本案例雖屬個人行為，但從此一案例，組織應了解民眾對於個人自身之隱私保護的意識已大幅提升，組織為提升安全而施行之安控措施，應事前審慎評估，尤其是有違法或侵害隱私疑慮者。可透過和權責機關（如請法務部解釋）與特殊關注方（如隱私團體、民眾）之互動，釐清相關問題後再採取行動，以降低觸法之風險。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.6.1.3　與權責機關之聯繫

應維持與相關權責機關之適切聯繫。

A.6.1.4　與特殊關注方之聯繫

應維持與各特殊關注方或其他各專家安全論壇及專業協會之適切聯繫。

A.18.1.4 個人可識別資訊之隱私及保護

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。

# 公務帶回家，主管個資被盜玩遊戲

## 【焦點話題】

擔任基層公務員的陳姓女子，將含有主管證件資料的公務檔案，帶回自家住處核對處理。不料，陳女的林姓前夫利用陳女疏於保管公務檔案之際，趁機偷走檔案夾內主管的身分證影本，並自行影印留存，嗣後再以該主管身分資料向網路遊戲公司申請遊戲帳號。

主管直到某日突然接獲遊戲公司寄來要繳娛樂稅的扣繳憑單，主管納悶「自己沒在玩網路遊戲，為何要繳娛樂稅？」經向遊戲公司查詢後，始查出自己身分遭他人盜用。林姓男子坦承盜用主管身分資料申請網路遊戲帳號，儲值遊戲點數並因玩遊戲中獎而得到 5 千餘元的獎品。警方訊後依刑法瀆職、偽造文書等罪嫌送辦陳女及林男。

【資料來源：自由時報 103/8/14】

## 【重點摘要】

1. 盜用他人身分資料申請遊戲帳號，侵害實質名義人權益，並影響遊戲公司對遊戲點數儲值資料管理之正確性，恐構成刑法上偽造文書罪。
2. 公務員應注意服務機關對於其經手公務文件之核定機密範圍、等級與相關安全管制事項，避免因洩漏公務機密而負有刑責。

## 【法律觀點】

本案中林男透過網路連線到遊戲公司網頁，在註冊頁面登打輸入前妻長官的基本資料[1]，致遊戲公司核准林男使用該會員帳號。林男線上填具之遊戲

[1] 依經濟部 99 年 12 月 7 日經授工字第 09920421120 號函發布實施之線上遊戲定型化契約範本，一般線上遊戲註冊申請流程通常需消費者填載姓名、電話、電子郵件及住居所等資料。

帳號註冊資料，屬於刑法所規範的電磁紀錄，為「準文書」[2]，故林男冒用他人名義註冊會員帳號，顯已涉嫌偽造不實申請紀錄，侵害實質名義人即其前妻主管之權益，亦影響遊戲公司對遊戲點數儲值資料管理的正確性，即可能構成刑法上的偽造文書罪。

再者，本案陳姓公務員將公務文件攜回住處處理。依行政院秘書處 99 年 3 月修正函頒之文書處理手冊，機密文書分為國家機密文書與一般公務機密文書，前者是指依國家機密保護法核定之絕對機密、極機密及機密文件，後者則為國家機密以外，由機關持有或保管並依法令或契約負有保密義務之資訊，例如稅捐稽徵法有關對納稅義務人所得資料負保密義務之規定[3]，或是考績法有關公務人員辦理考績過程負保密義務之規定等[4]，上開納稅義務人所得資料或考績審定資料，即屬公務機密。若公務員洩漏之公務資料，屬於依法核定的國家機密，該公務員依國家機密法將負有刑責[5]；若所洩漏者為一般公務機密，則依該機密有無涉及國防秘密事項，另依刑法洩漏國防秘密或國防以外秘密罪論處[6]。

因此，本案陳姓公務員是否構成洩漏國家機密罪或刑法上的洩漏秘密罪，應視其公務文書有無經核定為機密，或是否為依法負有保密之資訊而定。但陳姓公務員攜回住處處理的公務文件，縱使並非公務機密，其故意提供主管的個人資料予他人，仍可能依個人資料保護法(以下簡稱個資法)負有違

---

[2] 依刑法第 210 條規定：「偽造、變造私文書，足以生損害於公眾或他人者，處五年以下有期徒刑。」第 220 條第 2 項規定：「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，亦以文書論。」

[3] 稅捐稽徵法第 33 條第 1 項前段：「稅捐稽徵人員對於納稅義務人之財產、所得、營業、納稅等資料，除對下列人員及機關外，應絕對保守秘密…」。

[4] 公務人員考績法第 20 條：「辦理考績人員，對考績過程應嚴守秘密，並不得遺漏舛錯，違者按情節輕重予以懲處。」

[5] 國家機密保護法第 32 條：「洩漏或交付經依本法核定之國家機密者，處一年以上七年以下有期徒刑。因過失犯前項之罪者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。第一項之未遂犯罰之。」

[6] 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。」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。」另同法第 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。」

法特定目的外利用之刑事責任[7]。又，陳姓公務員攜回住處處理的公務文件含有主管個資，該公務員因任意攜回公務文件且未妥善保管，致其主管個資遭不當利用致權利受侵害時，其所屬公務機關未盡監督亦恐負國家賠償責任[8]。

**【管理 Tips】**

本案例中由於人員將公事帶回家中處理，卻未妥善保護好相關敏感資料，以致資料遭盜用。員工因為公務家辦而導致資料外洩的事件屢見不鮮，主要是員工家中網路及電腦的安全防護等級通常較為薄弱，可能多為共用或安裝了具有安全風險的應用程式如 P2P 軟體，因此很容易遭到病毒、木馬、惡意程式的攻擊，進而導致資料外洩。

組織除應向員工宣達及教育公務家辦的安全風險外，對於員工可能將公務資料攜出的管道也應予以管制。包括對可移除式媒體如隨身碟、行動硬碟於組織內的使用限制與管理，以及因應行動辦公室及員工自行攜帶行動裝置上班(Bring your own device)的風潮，對於使用行動裝置如手機、平版電腦、筆記型電腦處理公務或存取資料，也應考量相關對組織資訊安全造成的威脅，採取適切的對策。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.6.2.1 行動裝置政策

應採用政策及支援之安全措施，以管理使用行動裝置所導致之風險。

A.7.2.2 資訊安全認知、教育及訓練

[7] 個資法第 41 條：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，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。意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

[8] 個資法第 28 條第 1 項：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。」第 31 條：「損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。」

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。

A.8.3.1 可移除式媒體之管理

應依組織所採用之資訊分級方案，實作管理可移除式媒體之程序。

## 戴針孔眼鏡竊錄開庭過程，婦判刑 10 月

### 【焦點話題】

A 女多次到台中地檢署按鈴申告後，於開庭時戴著有錄影與錄音功能的眼鏡，竊錄開庭過程再上傳至網站，供人點閱，於 102 年 3 月開庭時，被檢察官當場抓包，命法警取鏡制止，A 女竟抓咬並踹踢法警。惟 A 女稱其目的是維護自身利益，且她是當事人，有權公布開庭過程，並未侵犯檢察事務官等人的隱私，也未公布他們的姓名。而開庭當天與檢察官有言語爭執，她才會激烈抵抗，無妨害公務意圖。

然法院指出，因偵查不公開，偵查庭過程屬「非公開之活動」，A 女未經檢察官及檢察事務官同意，無故竊錄他人非公開活動，即侵犯他們的隱私權，縱使未揭露姓名，但媒體無遠弗屆，只要稍加比對，就會暴露個資，侵害人格權。且法警奉命取下 A 女眼鏡，卻遭抓咬、踹踢，已構成妨害公務等情事。此外，A 女因於 101 年 2 月至 102 年 3 月，共 8 次竊錄偵查庭開庭過程，其中 7 次將影片上傳至網站散布於眾，另犯 1 次妨害公務罪，合併判處 10 個月徒刑，得易科罰金，本案仍可上訴。

【資料來源：蘋果日報 103/9/1】

### 【重點摘要】

1. 基於偵查不公開原則，偵查庭活動屬非公開活動，不論是否屬執行業務或公務，參與庭訊者對該活動均有合理隱私期待，而不得私下錄音或錄影。
2. 以竊錄方式取得偵查庭參與者的容貌、聲音等足以識別特定人之資料，已屬於蒐集個人資料的行為，如未符合個資法規定，即屬違法蒐集的行為。

### 【法律觀點】

本件 A 女以具有攝錄功能的眼鏡，竊錄偵查庭開庭狀況後，將影片上傳至網站供人點閱。然而，依刑事訴訟法第 245 條第 1 項偵查不公開之規定，參與偵查庭期活動之人，不論被告、檢察官或書記官等人，於主觀上均可合理期待該活動具有隱密性而不被公開；客觀上，偵查庭亦禁止與案件無關之人進入，以確保活動的隱密性。因此，A 女行為對於偵查活動進行竊錄，即有違反刑法第 315 條之 1[1]規定之可能性。

刑法第 315 條之 1 規定之「非公開活動」，係指活動者主觀上具有隱密進行其活動而不欲公開之期待，且在客觀上已利用環境或採取適當設備，確保其活動之隱密性者而言[2]。是以，偵查庭期活動如前所述，因須遵循不公開原則，乃符合「非公開活動」的概念，不論是否屬於執行公務，參與者對此均有合理隱私期待。因此，A 女在未經參與者同意的情況下，竟無故竊錄屬非公開活動的偵查庭活動、言論與談話等，已違反我國刑法第 315 條之 1 第 2 款的規定，將面臨 3 年以下有期徒刑、拘役或 30 萬元以下罰金之刑責。此外，A 女將影片上傳至網站供人點閱，已屬散布所竊錄的內容，更進而違反刑法第 315 條之 2 第 3 項規定[3]，得處五年以下有期徒刑、拘役或科或併科五萬元以下罰金。

另我國個人資料保護法（下稱個資法）已於 101 年 10 月 1 日施行，倘 A 女行為發生於個資法修正施行後，因 A 女攝錄影片包含檢察官、檢察事務官、書記官或法警等人的臉部容貌、聲音等資料，為個資法第 2 條第 1 款[4]所指足以識別特定個人之資料，而有蒐集個人資料的行為，至於將存有個人資料的影片，上傳於網站上供人點閱，屬於利用個人資料之行為，不符合個

[1] 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。」

[2] 台中地方法院第 102 年度易字第 1625 號判決。

[3] 刑法第 315 條之 2：「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。意圖散布、播送、販賣而有前條第二款之行為者，亦同。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。前三項之未遂犯罰之。」

[4] 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。…」

資法第 51 條第 1 項第 2 款所定「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」，因此 A 女行為亦涉及違反個資法第 41 條第 1 項的規定[5]，得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，併予說明。

## 【管理 Tips】

本案例係當事人以隱藏式之錄音、錄影設備錄下偵查庭訊過程，違反偵查不公開之法律規範。從此一案例，可以了解到基於保護組織資訊，每一組織都可能有其特別的資訊保護規定。

以本案例來說，和組織較有直接關聯的應為組織對實體安全的要求，基於保護組織資訊的必要，組織可能針對特定的敏感區域如機房、電腦中心等執行較嚴格的人員進出與物品攜出入管制，並落實相關的核對與檢查。為防止人員藉由接觸重要資訊系統或設備的機會，伺機將重要資訊帶出，或未依規定將自行攜入的設備與資訊系統連接而導致系統異常或遭受破壞，組織應制定相關的物品攜出入管制程序並執行之，落實物品攜出入敏感區域的申請、審核、檢查、及記錄。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A11.1.2 實體進入控制措施

保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。

A.11.2.5 資產之攜出

[5] 個人資料保護法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」第 41 條第 1 條：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，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。」

未經事前授權，不得將設備、資訊或軟體帶出場域外。

類別：資訊保護【**案號：S1030404**】

## 竄改打卡紀錄，技士遭判刑

### 【焦點話題】

S 科學研究院技士兼軟體發展小組小組長 A 男，4 年前因上班「摸魚」，竟登入電腦門禁系統，更改工作出勤時間及刪除休假紀錄逾百次。A 男依規定每天工作需滿 8 小時，但他為了縮短上班時間，竟使出偷吃步，利用因職務所知悉的系統資料庫及考勤系統的帳號與密碼，在民國（下同）99 年 1 月到 8 月間以電腦登入門禁及考勤系統，篡改上班打卡時間，把打卡時間提前 10 多分鐘，以便早點下班，甚至還把別人的上班打卡時間改成自己的。此外，他也刪除休假紀錄，前後刪改電磁紀錄共 104 次，後來遭人抓包。

法院以證人證詞及電腦相關紀錄等證據，認 A 男犯行明確，並審酌 A 男擅用電腦篡改其到、退勤時間及休假紀錄，嚴重影響 S 科學研究院對門禁考勤的正確性，且 A 男犯後未思悔悟，矢口否認犯行，遂依偽造、變造私文書罪判處有期徒刑 10 月。A 男雖提起上訴，但最高法院維持二審判決，駁回 A 男上訴。

【資料來源：中時電子報 103/10/01】

### 【重點摘要】

1. 行為人為縮短上班時間，以帳密登入門禁與考勤系統，篡改出缺勤及休假紀錄，其偽、變造電磁紀錄的行為，構成刑法偽（變）造私文書罪。

2. 使用電腦門禁或考勤系統，應採取帳密權限分級、定期檢視與變更帳密，及留存軌跡資料等措施，以提升資安程度，避免發生資料外洩或竄改事件。

### 【法律觀點】

過去企業或政府機關為了人力資源管理，多會透過紙本簽到等方式，由人

員記錄出缺勤時間或休假，作為管理依據。隨著科技普及，出缺勤或請假作業多改以電腦系統方式進行，雖可節省撰擬、整理紙本等投入的成本，但系統所儲存的電磁紀錄[1]，仍可能因遭人破解或盜用帳號而侵入系統，存有遭到竄改的風險。

依我國刑法第 210 條規定，「偽造、變造私文書，足以生損害於公眾或他人者，處五年以下有期徒刑。」所謂文書，是指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[2]。又因現代社會對電腦的使用，日趨普遍，且逐漸取代紙本文書的製作，故我國刑法明文規定，電磁紀錄係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，亦屬文書[3]。從而，對電磁紀錄為偽造或變造者，亦構成偽造、變造私文書之犯罪行為。

法院認為本件 A 男擔任 S 科學研究院軟體發展小組的小組長，由於該組組員負責出缺勤及休假系統的管理，A 男進而得知門禁系統管理人的帳密，於是利用該帳密登入門禁與考勤系統，除了更改自己的到勤時間、刪除休假之退勤時間外，亦更改他人識別號的到、退勤時間為己用時間，使該些遭更改的資料顯示於電腦螢幕上，用以表彰其為系統管理人之意。是以，前開資料性質上屬電磁紀錄與刑法上的準文書，A 男的行為已構成偽造、變造私文書罪。此外，A 男因職務知悉門禁與考勤系統之帳密，卻擅自以該帳密登入上開系統，若其所刪除或變更的電磁紀錄，包括不具文義性的電子檔案如某些系統檔時，亦可能另涉犯屬告訴乃論之刑法第 359 條破壞電磁紀錄罪[4]。

如前所述，企業或政府機關透過電腦系統管理人員出缺勤等紀錄，雖可節

[1] 刑法第 10 條第 6 項：「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。」
[2] 刑法第 220 條第 1 項：「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。」
[3] 刑法第 220 條第 2 項：「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] 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。」同法第 363 條：「第 358 條至第 360 條之罪，須告訴乃論。」

省成本，但為避免發生資料外洩或遭人竄改資料等情形，對於相關系統應採取適當安全措施，例如帳密保管權限分級、定期檢視權限與帳密變更之必要性、留存登錄的軌跡資料等，以降低資安風險，並建立事後追蹤的資料紀錄。

## 【管理 Tips】

本案例為當事人因個人私利，進而篡改個人之上下班打卡時間與休假之電磁紀錄，並偽造不實資訊，後因東窗事發而遭開除。

從本案例中可以發現幾點組織能夠引以為鑑或討論的管理缺失。首先就是對於職務的區隔仍有改善的空間，該員雖然負責單位資訊工程業務，但並不代表其可以存取所有的資訊系統，因此組織應針對人員於職責內所能接觸、存取的系統或資訊做適當的區隔，以免因權責不清而被有心人士利用從事不法行為，如偷窺、篡改、資料竊盜等。另一方面，該單位人員對於存取系統之秘密鑑別資訊（如帳號密碼）之保管亦不夠周延，而使該員得以取得門禁及考勤系統資料庫的帳號密碼，組織宜再教育人員確實保管使持有之帳號密碼等秘密鑑別資訊，如不告知他人、不分享及共用等，以及提供秘密鑑別資訊必要的安全保護，如加密、安全儲存等。

其次，對系統有存取權限、以及具有特殊存取權限（如管理者）之人員，應定期審查授予其對資訊或系統存取權限的必要性，以避免人員職務異動後仍具有相關權限，增加資訊遭不當使用或洩漏的風險。而在此一案例中，也可以體會到記錄稽核軌跡的重要性，人員或許可利用個人權限存取系統或資訊，但若有適當的相關存取活動之事件記錄機制，將所有的存取活動予以記錄，或可遏阻人員的不法意圖，以及在必要時提供資安事故的追蹤線索或佐證。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.6.1.2　職務區隔

衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或未蓄意修改或誤用之機會。

A.9.2.3　具特殊存取權限之管理

應限制及控制具特殊存取權限之配置及使用。

A.9.2.5　使用者存取權限之審查

資產擁有者應定期審查使用者之存取權限。

A.9.3.1　秘密鑑別資訊之使用

於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。

A.12.4.1 事件存錄

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。

A.18.1.3 紀錄之保護

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。

# 六、著作權法

類別：資訊保護【**案號：S1030601**】

## 設美食網提供部落客文章　工程師挨告

### 【焦點話題】

某工程師 A 因熱愛美食，喜歡看網友對餐廳的食記或評價，進而彙整相關文章，建立「瘋美食」網站，希望方便消費者搜尋網友食記，不料遭一名美食部落客提告指控侵犯著作權。該提告的部落客平日喜歡上餐廳吃美食，拍照記錄後放上自己的部落格，累計近 700 篇食記，101 年 5 月他發現其中 5 篇食記，被超連結貼上「瘋美食」網站，令他十分不滿進而提告。

但 A 喊冤指「瘋美食」網站和 Google 網站性質雷同，僅利用程式架設檢索資料庫。士林地檢署認為，該網站雖重製食記一小部分文章並提供網頁超連結，但內容和原著作相差甚遠，屬於合法使用範圍，予以不起訴處分。

【資料來源：蘋果日報 103/3/10】

### 【重點摘要】

1. 以超連結單純提供他人文章、圖像之網址或連結者，因未將文章或圖像重製於自己網站作為內容的一部分，應不涉及侵害重製權或公開傳輸權。
2. 如有涉及他人文章部分內容時，屬於重製與公開傳輸他人著作之行為，須符合著作權法合理使用的要件，否則會有侵害他人著作財產權之虞。

### 【法律觀點】

由於網際網路發達，網路使用者經常利用超連結方式，將文章、圖片或影像之網路連結張貼於網站或部落格，讓其他使用者點選超連結以後，即可連線至文章、圖片或影像所在的網站或部落格讀取相關內容。是以，透過網路超連結可輕易串聯相關網路資訊，加速資訊的流通。由於網路文字、

圖片及影像易於重製，且超連結尚包括超文字連結、圖像連結、視框連結或深層連結等不同類型，是否均涉及著作權侵害，即有討論的空間。

本件瘋美食網站蒐集網路使用者分享的美食記錄，透過超文字連結與圖像連結，讓使用者點選超連結，即可連結至他人網站，閱讀相關文章或圖片，而遭指控侵害他人重製權與公開傳輸權。就超文字連結與圖像連結部分，係以他人部落格名稱、文章標題或他人網站圖像作為連結型態，使用者只要點擊該文字或圖像，即連結至他人網站，依主管機關見解[1]，此種行為性質上並未將他人的文章或圖像，重製於自己網站作為內容一部分，僅係單純提供他人網站之連結，不涉及侵害重製權或公開傳輸權。惟瘋美食網站就某些文章除提供超連結外，尚會顯示部分原美食紀錄之文字，由於原文章已屬作者評論或分析的文字創作，應受著作權法保護，依主管機關見解[2]，此行為已非屬單純提供他人網站之連結，而涉及重製他人著作，須依著作權法第 65 條第 2 項規定[3]，衡量該利用是否具有商業目的，其利用方式是否具有轉換性，並考量著作的性質、所使用質量的比例，以及是否影響原著作潛在市場與現在價值等要件，進而判斷是否符合合理使用，始能認無侵害著作財產權。如未符合合理使用要件，則屬侵害重製權與公開傳輸權，須負刑事責任，均可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[4]，並應負擔民事賠償責任[5]。

至於 A 工程師稱瘋美食網站係利用程式架設檢索資料庫，和 Google 網站性

[1] 經濟部智慧財產局 94 年 9 月 2 日電子郵件字第 940902 號函、95 年 4 月 24 日電子郵件字第 950402 號函及 98 年 10 月 22 日智著字第 09800091520 號函。

[2] 經濟部智慧財產局 100 年 8 月 9 日電子郵件字第 1000809a 號函。

[3] 著作權法第 65 條第 2 項：「著作之利用是否合於第 44 條至第 63 條所定之合理範圍或其他合理使用之情形，應審酌一切情狀，尤應注意下列事項，以為判斷之基準：一、利用之目的及性質，包括係為商業目的或非營利教育目的。二、著作之性質。三、所利用之質量及其在整個著作所占之比例。四、利用結果對著作潛在市場與現在價值之影響。」

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

[5]著作權法第 84 條：「著作權人或製版權人對於侵害其權利者，得請求排除之，有侵害之虞者，得請求防止之。」第 88 條第 1 項：「因故意或過失不法侵害他人之著作財產權或製版權者，負損害賠償責任。數人共同不法侵害者，連帶負賠償責任。」

質雷同部分，如參考美國法院見解，本案 A 所架設之瘋美食網站，為一檢索資料庫，所提供他人美食記錄之超連結可被認為是指引資訊的來源，具高度轉換性質，且使用質量比例較小，更並未因此取代原本他人的文章或圖片，應不會造成原著作潛在市場與現在價值的影響，可認屬合理使用之範疇[6]。惟實際個案是否構成合理使用，仍應視具體個案能否符合前開所述合理使用的原則而定。

## 【管理 Tips】

本案例係網友整理相關美食介紹之文章，並建立網站提供連結以方便其他網友搜尋，因而引發原文章之作者提告，指其侵犯著作權，地檢署認為該網站僅提供連結，屬合法使用範圍而不起訴。

透過此一案例，組織宜體認到法規遵循為資訊安全之一環，若稍一不慎即可能誤蹈法網，造成組織商譽或實質財務損失。因此，組織應建立遵循性政策（包括符合智慧財產權的要求），並透過對員工施以資訊安全認知、教育及訓練的方式，來識別、宣導與組織相關之法律、法令、法規及契約要求事項，以確保組織營運作業之合規。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.7.2.2　資訊安全認知、教育及訓練

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。

A.18.1.1 適用之法規及契約的要求事項之識別

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

[6] Google 搜尋引擎之縮圖功能，曾遭 Perfect 10 公司控訴已侵害其著作權，但美國第九巡迴上訴法院認 Google 搜尋引擎之縮圖具高度轉化性質，亦不侵害原著作權人之利益，故屬合理使用之範圍。

法。

A.18.1.2 智慧財產權

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

# 威盛控侵權　祥碩 4 工程師起訴

## 【焦點話題】

原任 IC 設計大廠 A 公司的甲、乙、丙及丁四位工程師，民國 96 年跳槽 B 公司前，為使 B 公司順利開發符合 USB3.0 規範的高速晶片產品，縮短設計時程，涉盜拷 A 公司電路圖電子檔及紙本，帶到 B 公司製造相關產品出售，A 公司乃控告四名工程師及 B 公司董座戊背信及侵害著作權。

檢警去年搜索 B 公司，在甲及乙的辦公室查扣 A 公司簡稱「VIA」及「VT」的電路圖與技術文件共 96 張，以及記載 B 公司「ASM1042」及「ASM1051」晶片電路圖的電磁紀錄光碟。今年 4 月再度搜索，又扣到與 A 公司電路結構高度相似的電路圖 38 張。

北檢考量四名工程師在 A 公司任職時曾簽保密條約，故依妨害秘密、背信及違反著作權法將 4 人起訴，B 公司也因著作權法連坐條款遭起訴，最重可罰 75 萬元。至於 B 公司董座戊，則因無法證明涉案而獲不起訴。

【資料來源：蘋果日報 102/11/8】

## 【重點摘要】

1. 於營業秘密法修正後，倘將因職務知悉具秘密性、價值性與合理保護措施之營業秘密洩漏予他人時，將違反營業秘密法規定，須負較重的刑責。
2. 電路圖如非顯示半導體晶片或積體電路電路布局，而是屬文學、科學、藝術或其他學術範圍之創作時，即屬於受著作權法保護的圖形著作。

## 【法律觀點】

近年因工商活動頻繁，且知識經濟成國際趨勢，不論智慧財產權或營業秘密已成為企業競爭的指標。因此，各企業為避免員工離職後抄襲或洩漏智

慧財產或營業秘密相關訊息，多透過簽訂保密條約的方式，課予員工保密義務。

本案之甲、乙、丙及丁四人，原擔任 IC 設計大廠 A 公司的工程師，於任職時已簽署保密條約，倘該約無違反公序良俗等情時，自負有保密義務。又該四人因擔任工程師，於職務知悉或持有 A 公司相關產品電路結構的電路圖，該電路圖如屬工業或商業上之發明或經營計畫，具有不公開性質之工商秘密時，其無故將資料洩漏予 B 公司時，則有涉犯刑法第 317 條洩漏工商秘密罪[1]。但須注意的是，我國營業秘密法於 102 年 1 月 20 日修正後，增訂刑事責任，並已公布施行，本案雖因該四人行為發生於 96 年間，未適用營業秘密法刑責之規定，但未來如係無故洩漏具秘密性、價值性與合理保護措施之營業秘密時，即可能違反營業秘密法，而須負較重的刑責[2]。

我國著作權法乃以例示方式規定受著作權法所保護的各類著作，其中圖形著作包括地圖、圖表、科技或工程設計圖及其他圖形著作等[3]。至於該四人所拷貝的電路圖，主管機關過去曾表示電路圖如屬於文學、科學、藝術或其他學術範圍之創作時，即屬著作權法保護之科技設計圖，但科技設計圖並不包括顯示半導體晶片（或積體電路）電路布局之圖形[4]。因此，倘該四人所拷貝的電路圖，並非顯示半導體晶片（或積體電路）電路布局，而係具有科學等創作之圖形時，因該圖形係屬著作權法所保護的圖形著作，其拷貝行為已侵害著作權人的重製權，而有涉及觸犯著作權法刑事責任的疑

[1] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」我國法院實務曾表示，工商秘密之範圍大於營業秘密之範圍，如臺灣臺北地方法院 97 年易字第 500 號、臺灣高等法院 90 年上易字第 2786 號等判決。

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

[3] 著作權法第 5 條第 1 項各款著作內容例示第 2 點第 6 款：「圖形著作：包括地圖、圖表、科技或工程設計圖及其他之圖形著作。」

[4] 經濟部智慧財產局 95 年 12 月 21 日智著字第 09500121490 號函、99 年 10 月 6 日智著字第 09900095070 號函。惟須注意的是我國尚有「積體電路電路布局保護法」，故半導體晶片或積體電路電路布局之電路圖，因係其電路布局之唯一表達方法，不受著作權法保護，但可能受到前開法律之保護。

慮[5]。如此一來，基於著作權法第 101 條第 1 項之規定[6]，B 公司亦可能面臨侵害重製權罪的罰金處罰。

最後尚須注意，甲、乙、丙及丁四人因與 A 公司間簽訂有保密條約，通常為加強該條約的拘束力，多設有損害賠償或違約金條款，該四人除前開刑事責任，亦恐生民事違約賠償責任。

## 【管理 Tips】

本案例係因離職員工未能遵守保密協議，盜拷原任職公司重要資訊至跳槽公司，致使原公司權益遭受損失。因此對於組織的機密或重要資訊，除了應採行適當的資訊保護控制措施（如資訊存取限制與權限管理、資訊內容保護機制與工具等），以防止資訊竊取。於本案例中，組織也應有適當的人員規範，使員工能意識到相關的保密義務及違反時的法律責任。同時組織於此等事件中應妥善處理員工行為之相關紀錄及證據，並於事後能具體證明屬員工之行為，以維護組織權益。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.7.1.2　聘用條款及條件

組織與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。

A.7.3.1　聘用責任之終止或變更

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

[5] 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。」第 2 項：「意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處六月以上五年以下有期徒刑，得併科新臺幣二十萬元以上二百萬元以下罰金。」第 3 項：「以重製於光碟之方法犯前項之罪者，處六月以上五年以下有期徒刑，得併科新臺幣五十萬元以上五百萬元以下罰金。」

[6] 著作權法第 101 條第 1 項：「法人之代表人、法人或自然人之代理人、受雇人或其他從業人員，因執行業務，犯第 91 條至第 93 條、第 95 條至第 96 條之 1 之罪者，除依各該條規定處罰其行為人外，對該法人或自然人亦科各該條之罰金。」

及義務仍保持有效，並執行之。

A.12.4.1 事件存錄

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。

A.16.1.7 證據之收集

組織應定義及應用程序，以識別、收集、獲取及保存可用作證據之資訊。

類別：資料保護【**案號：S1030603**】

## 盜播紀錄片，捷運局處長被訴

### 【焦點話題】

99 年捷運蘆洲線通車時，台北市政府捷運局(以下簡稱北市捷運局)於沿線多媒體導覽機裡，開放民眾點選來自紀錄片「靜默沙洲」的五段影片，介紹三重、蘆洲古厝之美，卻遭紀錄片導演 A 提出告訴。

檢方指出，承辦人 C 於 98 年底接任北市捷運局中區工程處土木第一工務所主任，因交接取得光碟。處長 B 未經明察，就開會決定播放紀錄片，由 C 指示承包商分段截取五段影片後，將影片放在捷運沿線的多媒體觸控導覽機內，供民眾點閱。B 和 C 開庭時已認錯，但強調事先不知影片未取得授權，且曾希望在符合「政府採購法」的規定下購買版權，因金額差距過大，和解破裂。

然檢方認為，該片光碟外觀貼有「靜默沙洲九十分鐘 by S」等字樣，影片尾聲也註明導演、拍攝、採訪、剪輯人員與「S 影像個人工作室獨立製作」等，可輕易察覺有版權問題，B、C 等人不求證就播放，明確觸法，乃以擅自重製他人著作財產權及侵害著作人格權等罪名起訴，可處 3 年以下有期徒刑，對於台北市政府(以下簡稱北市府)則依著作權法第 101 條起訴，可處 50 萬元或 75 萬元以下罰金。

【資料來源：自由時報 102/10/12】

### 【重點摘要】

1. 政府機關於捷運等公開場所提供影片予民眾點選觀看，如非屬於合理使用的情形時，仍應於事先取得著作權人授權，以避免產生侵權爭議。
2. 政府機關應建立資產盤點制度，確認相關著作之權利義務狀態，以免擅自

加以利用，進而侵害著作權人之權益。

## 【法律觀點】

本案影片是由訪問人員拍攝古厝畫面後，加以剪輯與製作的視聽著作，足認該影片已投入相當智慧心血結晶，而屬著作權法保護的客體。又該影片光碟外觀貼有「靜默沙洲九十分鐘 by S」字樣，並於影片尾聲註明「S 影像個人工作室獨立製作」等文字，屬「以通常之方法表示著作人之本名或眾所周知之別名者」，依著作權法第 13 條規定[1]，可推定 S 影像個人工作室（以下簡稱 S 工作室）為該影片之著作人，除有將著作財產權讓與他人等情形外，原則上應依法享有著作人格權與著作財產權。

就著作財產權部分，本案 B、C 及北市府未經授權將所截取的影片存至多媒體機器，供民眾點播的行為，可能涉及侵害 S 工作室所享有的重製權[2]與公開上映權[3]。惟為調和私權與社會公益，著作的合理使用，並不構成對著作財產權之侵害，例如非以營利為目的，未對觀眾直接或肩接收取任何費用，且未對表演人支付報酬時，得於活動中以公開上映等方式使用他人已公開發表的著作[4]；此外，著作利用是否合於著作權法第 44 條至第 63 條所定之合理範圍，或其他合理使用之情形，應審酌一切情狀後判斷，著作權法第 65 條亦定有明文[5]。是以，本案 B、C 及北市府配合捷運蘆洲線通車，於捷

---

[1] 著作權法第 13 條：「在著作之原件或其已發行之重製物上，或將著作公開發表時，以通常之方法表示著作人之本名或眾所周知之別名者，推定為該著作之著作人。前項規定，於著作發行日期、地點及著作財產權人之推定，準用之。」

[2] 著作權法第 22 條：「著作人除本法另有規定外，專有重製其著作之權利。表演人專有以錄音、錄影或攝影重製其表演之權利。前二項規定，於專為網路合法中繼性傳輸，或合法使用著作，屬技術操作過程中必要之過渡性、附帶性而不具獨立經濟意義之暫時性重製，不適用之。但電腦程式著作，不在此限。前項網路合法中繼性傳輸之暫時性重製情形，包括網路瀏覽、快速存取或其他為達成傳輸功能之電腦或機械本身技術上所不可避免之現象。」

[3] 著作權法第 25 條：「著作人專有公開上映其視聽著作之權利。」至於公開上映的定義，依第 2 條第 1 項第 8 款規定，係指「公開上映：指以單一或多數視聽機或其他傳送影像之方法於同一時間向現場或現場以外一定場所之公眾傳達著作內容。」同條第 2 項：「前項第 8 款所定現場或現場以外一定場所，包含電影院、俱樂部、錄影帶或碟影片播映場所、旅館房間、供公眾使用之交通工具或其他供不特定人進出之場所。」

[4] 著作權法第 55 條：「非以營利為目的，未對觀眾或聽眾直接或間接收取任何費用，且未對表演人支付報酬者，得於活動中公開口述、公開播送、公開上映或公開演出他人已公開發表之著作。」依經濟部智慧財產局之解釋，只要經濟上利益可能轉換為無形或延後發生者，包括商業與公益結合之活動等，均仍屬以營利為目的，參 http://www.tipo.gov.tw/ct.asp?xItem=206748&ctNode=6983&mp=1。

[5] 著作權法第 65 條：「著作之合理使用，不構成著作財產權之侵害。著作之利用是否合於第 44 條至第 63 條所定之合理範圍或其他合理使用之情形，應審酌一切情狀，尤應注意下列事項，以為判斷之基準：一、

運沿線各站提供影片供民眾點選，是否屬於合理使用，仍有待司法機關依具體個案事實，審慎認定。

至於著作人格權部分，本案 B、C 及北市府未經授權，即自「靜默沙洲」影片截取出 5 段影片，若有使用 S 工作室尚未公開發表的著作，或未於著作的重製物上表示 S 工作室的名稱，甚或是以割裂、竄改等方法改變原著作的內容或形式，致損害 S 工作室名譽時，均可能涉及侵害其享有的著作人格權[6]。即使本案有前述非營利目的等可合理使用他人著作的情形，仍應明示著作出處，並以合理方式表示著作人的姓名或名稱[7]。

此外，本案除 B、C 等行為人可能涉及相關刑責外，依著作權法規定，法人之代表人、受雇人或其他從業人員涉犯著作權法上之刑事犯罪時，法人亦須科所犯法條之罰金[8]。故倘認 B、C 行為不屬於合理使用，而屬侵害著作人格權、重製權與公開上映權等著作財產權時，北市府亦須負罰金之責。

再者，B 雖係因前手交接而取得「靜默沙洲」影片光碟，但 B、C 可由光碟外觀、影片尾聲推知該影片之著作人為 S 工作室，實有於進行利用行為前，先釐清是否已取得該影片授權之必要。但因機關人員時有更迭，易產生資訊落差，故應建立資產盤點制度，釐清其是否享有著作權、有無獲得授權

---

利用之目的及性質，包括係為商業目的或非營利教育目的。二、著作之性質。三、所利用之質量及其在整個著作所占之比例。四、利用結果對著作潛在市場與現在價值之影響。…」

[6] 著作權法第 15 條第 1 項：「著作人就其著作享有公開發表之權利。但公務員，依第 11 條及第 12 條規定為著作人，而著作財產權歸該公務員隸屬之法人享有者，不適用之。」第 16 條第 1 項：「著作人於著作之原件或其重製物上或於著作公開發表時，有表示其本名、別名或不具名之權利。著作人就其著作所生之衍生著作，亦有相同之權利。」同條第 4 項：「依著作利用之目的及方法，於著作人之利益無損害之虞，且不違反社會使用慣例者，得省略著作人之姓名或名稱。」第 17 條：「著作人享有禁止他人以歪曲、割裂、竄改或其他方法改變其著作之內容、形式或名目致損害其名譽之權利。」

[7] 著作權法第 64 條：「依第 44 條至第 47 條、第 48 條之 1 至第 50 條、第 52 條、第 53 條、第 55 條、第 57 條、第 58 條、第 60 條至第 63 條規定利用他人著作者，應明示其出處。前項明示出處，就著作人之姓名或名稱，除不具名著作或著作人不明者外，應以合理之方式為之。」

[8] 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。」第 92 條：「擅自以公開口述、公開播送、公開上映、公開演出、公開傳輸、公開展示、改作、編輯、出租之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。」第 92 條：「有下列情形之一者，處二年以下有期徒刑、拘役，或科或併科新臺幣五十萬元以下罰金：一、侵害第 15 條至第 17 條規定之著作人格權者。…」第 96 條：「違反第 59 條第 2 項或第 64 條規定者，科新臺幣五萬元以下罰金。」第 101 條：「法人之代表人、法人或自然人之代理人、受雇人或其他從業人員，因執行業務，犯第 91 條至第 93 條、第 95 條至第 96 條之 1 之罪者，除依各該條規定處罰其行為人外，對該法人或自然人亦科各該條之罰金。」

及授權範圍等事宜，俾使相關人員於利用前可明確知悉，避免侵權情事。

**【管理 Tips】**

北市府捷運局配合捷運蘆洲線通車，於沿線的多媒體導覽機提供景點影音介紹導覽，其中部份紀錄片因未取得授權即逕行剪接、公開播放，因此遭著作權人提出告訴。

本案例中，除負責業務之人員對相關的法規遵循意識不足外，對於資訊資產的管理，組織應有更積極的管理作為，包括識別與組織有關的資訊資產，如實體、硬體、軟體、人員、資通訊服務、資料（訊）內容等提供組織資訊活動的資產項目，並建立資產清冊，同時在資產有異動時予以更新。對於個別的資產群組或項目，也應定義適切的使用規則，包括使用資產的方式（如公開、傳輸、複製、保存、銷毀等），以及定義資產本身的合理使用範圍，以防止資產遭誤用或濫用，或逾越法律、法令、法規及契約的要求。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.8.1.1 資產清冊

應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。

A.8.1.3 資產之可被接受使用

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

A.18.1.2 智慧財產權

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

# 員工盜 P 公司圖片，T 公司判賠 40 萬

## 【焦點話題】

A 男於民國（下同）100 及 101 年間在 T 公司網路銷售部門擔任時薪員工，每天負責上傳 3C 產品的廣告文宣到 T 公司的網路商城。A 男卻盜取 P 公司購物網站關於 L 牌筆電圖片，與 P 公司人員發想的圖說「人體工學巧克力鍵盤」等廣告詞，放在 T 公司網路商城上使用，被 P 公司發現憤而提告。T 公司委任律師表示 P 公司拍的照片「沒有任何光影變化」，「沒有構圖等主觀創意」，認為並不符合著作權法中保障的原創性要件，但法官卻未採納。

一審法官審酌 A 男犯行，認為他薪資不高，每天卻要上傳 100 件商品和廣告文宣到 T 公司網站，工作量太大，一時思慮欠周才會犯案，因此給予緩刑；反觀 T 公司是每年實際營收高達 16 億元的大公司，卻讓時薪員工負責這麼龐大的業務，監督不周，判罰金 25 萬元還要賠 P 公司 40 萬元。惟 A 男與 T 公司不服該判決結果，提起上訴，二審法院卻認 P 公司廣告文宣的文字敘述，與某部落格所用的文字相同，且圖文說明僅單純的產品圖文介紹，認為不具原創性，不受著作權法保護，改判 A 男與 T 公司無罪。

【資料來源：蘋果日報 103/01/23】

## 【重點摘要】

1. 作品如係作者獨立創作而非抄襲所得，且具有少量足以表達出作者個性或獨特性之創意時，即可認已具原創性，應受著作權法之保護。
2. 編輯著作須就資料的選擇及編排具有創作性，始能以獨立的著作受到保護，故廣告文宣倘僅就產品進行圖文說明，未具創作性時，將不受著作權法保護。

## 【法律觀點】

我國著作權法所保護的著作，是指屬於文學、科學、藝術或其他範圍之創作，而創作係指具原創性之精神上創作，包含原始性與創作性的概念。前者是指著作人獨立創作，未抄襲他人著作；後者所稱創作性，雖無須達到完全獨創的地步，但至少須少量創意，以表現出作者的個性或獨特性。倘創作內容與他人作品雖屬酷似或雷同，但其間並無模仿或盜用的關係時，仍可認具原創性而受保護[1]。

本件爭議在於 P 公司的廣告文宣，包括若干圖片與文字敘述，並以圖片選擇、文字與圖片的編排或配置等作為表達方式，是否已屬著作權法所保護的語文著作與編輯著作，以及 A 男與 T 公司是否構成抄襲等。

本案法院認為[2]，P 公司廣告文宣的文字敘述部分，與某部落格於 99 年介紹 L 牌筆電之文字相同，甚至連錯字都一樣，明顯是抄襲而來，且其內容僅單純介紹產品輕薄、書本外型等特性與規格，並使用與該部落格類似的形容字詞，未有依實際使用經驗，對功能、設計或外觀為主觀描述等，以表現作者的個性與創意之處，難認具有原創性，自非屬著作權法所保護的語文著作。至於該文宣畫面編排部分，P 公司廣告文宣雖已就產品圖片進行選擇，並對文字與圖片進行編排或配置，但因其使用的圖片與 L 牌官網及其他購物中心所使用者相同，且圖文編排上，不論是產品全貌或局部的圖片，均對應著產品外型或規格等文字敘述，足認其資料選擇及編排僅是進行單純的產品介紹，未能表達出作者對於圖片選擇及圖文編排之個性或獨特性，應非屬著作權法所保護的編輯著作。

傳統廣告文宣多採取圖文說明方式，即利用文字敘述產品規格、品質或產地等特性，並將產品全貌或局部圖片放置於對應的文字旁，加強說明效果。而我國著作權法亦規定[3]，編輯著作須就資料之選擇及編排具有創作性者，

---

[1] 最高法院 97 年度台上 1214 號判決、97 年度台上字第 1587 號判決。

[2] 智財法院 103 年度刑智上易字第 18 號判決。

[3] 著作權法第 7 條：「就資料之選擇及編排具有創作性者為編輯著作，以獨立之著作保護之。編輯著作之保護，對其所收編著作之著作權不生影響。」

始受著作權保護。是以於設計廣告文宣時，如採取傳統圖文說明的編排方式，恐難認為具有原創性，故廣告創作者應依使用產品經驗加入主觀感受的文字描述，或於圖文選擇及編排上加入創意，以表達出作者之個性或獨特性，始能認為具原創性，而屬受著作權法保護的語文著作與編輯著作。

## 【管理 Tips】

本案例除當事人因為盜用競爭對手之產品文宣，導致個人及公司需承擔當法律及賠償責任，凸顯該公司及員工對於尊重智慧財產權之意識不足外，另一方面，該公司於作業流程的管理上也有不夠嚴謹之處。

組織對於變更作業之管理，包括變更作業之規劃、申請、影響評估、審核、變更計畫（執行內容、測試結果、復原程序等）擬訂、執行、變更後的檢核等流程，若缺乏適當的作業程序規定，或未依作業程序確實執行，除可能增加執行變更時的風險，也可能使人員有便宜行事之心態，增加出錯的機率。因此，組織對於足以影響資訊安全之變更作業，無論是資訊系統或資訊內容的變更，都應建立必要的管理程序並遵守及落實。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.12.1.2 變更管理

應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。

A.18.1.2 智慧財產權

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

# 貳、資訊公開（Disclosure）

# 一、政府資訊公開法

**類別：資訊公開【案號：D1030101】**

## 促進即時路況資訊服務，交通部推動交通雲

### 【焦點話題】

為滿足民眾對完整路況資訊與行動應用服務之需求，強化即時路況資訊服務品質，交通部擬建置交通資訊服務雲（以下簡稱交通雲），建置完成後將可擴大目前即時路況服務範圍，並包含日月潭、阿里山及武陵農場等熱門觀光景點連絡道路。

惟立委質詢指出，交通雲涵蓋資料過於廣泛，恐有侵害人民隱私疑慮。交通部則表示提供民眾塞車路段、時段等資訊，均已去識別化處理，且所有資訊儲存進交通雲之雲端資料庫，均以規範之格式儲存，無法識別或儲存任何個別用路人或車輛之隱私資料，因此無侵犯個人隱私及監控民眾之疑慮。

【資料來源：中時電子報 103/1/11】

### 【重點摘要】

1.交通雲所提供的資訊若均已去識別化，而無法以任何方式識別特定個人時，應無侵害隱私權之疑慮。

2.政府機關辦理行動化服務，應遵循行政院訂定之政府資通安全管理規定，以確保資訊服務品質與安全。

### 【法律觀點】

交通部係透過新興交通資訊蒐集技術與雲端運算架構，提供民眾整體交通路況即時資訊。交通部開發建置交通雲，主要在提供用路人路況相關資訊，因此交通雲資訊蒐集範圍係路段壅塞情形，蒐集對象為道路路況，並非個

別或可得識別特定人之駕駛或車輛。而依法務部函釋見解，如資料本身業經處理而無法識別特定當事人資料，則無個人資料保護法(以下簡稱個資法)之適用問題[1]。故交通資訊雲所提供的資訊若均已去識別化，而無法與其他資料對照、組合或連結而識別特定個人時，應無侵害隱私權之疑慮。但若去識別化後的資料跟其他資料對照、組合或連結而得識別特定個人時，即屬於個人資料，而應符合個資法之相關規定。

依行政院 101 年 1 月 3 日訂定發布之「行政院及所屬各機關行動化服務發展作業原則」，政府機關開發行動化應用軟體前，宜優先評估將政府資訊開放民間加值創新應用之可行性[2]。因此，交通雲未來亦擬開放承作廠商對加值業者進行合理收費，以發展各項創新服務，例如導航語音秘書、個人化即時路況行動導航服務等，希望透過政府資料加值利用，促進國內車載資通訊與智慧型運輸系統產業之發展。惟，政府機關辦理行動化服務同時，須注意在安全管理作業上應符合個資法相關規定，並遵循行政院訂定之政府資通安全管理規定，例如行政院及所屬各機關資訊安全管理規範或要點，以確保資訊服務品質與安全。

## 【管理 Tips】

本案例中交通部擬建置交通雲，引發民眾對是否侵犯個人隱私的疑慮。交通部說明，所蒐集及發布之資訊僅做為路況資訊之用，並無用路人之人、車資料。

---

[1] 法務部 102 年 3 月 12 日法律字第 10203501470 號函釋要旨：「個人資料保護法第 2、16 條等規定參照，如大學因研究需要，申請警察機關提供經處理後無從識別特定當事人之住宅竊盜報案人住宅聯絡電話，如經處理後無法識別特定當事人資料，則提供者既非個人資料，自無該法適用。」；法務部 102 年 2 月 7 日法律字第 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。」

[2] 行政院 101 年 1 月 3 日院授研訊字第 1012460006 號函訂定發布「行政院及所屬各機關行動化服務發展作業原則」第 5 條規定：「各機關開發行動化應用軟體前，宜優先評估將政府資訊開放民間加值創新應用之可行性；其經評估屬應由機關開發者，再由機關自行或委外開發。」第 11 條規定：「各機關應依據個人資料保護相關法規及行政院訂定之政府資通安全管理規定，辦理行動化服務安全管理作業，維持應用系統之安全與穩定運作。」

惟本案例中之交通雲計畫若開始推動，未來可能蒐集全面性的交通資訊，來源除包括各級交控中心的路況資訊或各政府機關的影像外，還可能包含連上 GPS 的通訊系統或 eTag 資料等，如此龐大資料量以及與個人隱私相關的專案，將由委外廠商執行，因此對委外廠商在資料的蒐集、處理與利用的規範更應謹慎。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.13.2.1　資訊傳送政策及程序

應備正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施的資訊傳送。

A.13.2.2　資訊傳送協議

協議應闡明組與外部各方間營運資訊之安全傳送。

A.13.2.4　機密性或保密協議

宜識別、定期審查與文件化，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。

A.15.1.1　供應者關係之資訊安全政策

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。

A.15.1.2　於供應者協議中闡明安全性

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。

A.15.2.1　供應者服務之監視及審查

組織應定期監視、審查及稽核供應者服務交付。

A.18.1.4　個人可識別資訊之隱私及保護

應依適用之相關法令、法規中的要求，以確保個人可識別資訊之隱私及保護。

# 政府資料平臺，錯置清單載點

## 【焦點話題】

新北市某民眾反映，為參加網路數位創作比賽，在國家發展委員會(以下簡稱國發會)政府資料開放平臺檢索資料，下載一筆電信設備審驗合格清單，但開啟檔案後卻發現內容為民國 99 年至 102 年間不知名學校學生人數統計資料。對此，國發會回應指出該平臺上所提供之資料集內容，均由各部會自行登載及審核，資料下載位址均連結至各機關網站，平臺僅提供資料集詮釋資料供外界查閱，並未存放資料內容。

有關民眾發現錯置載點一事，國發會已於接獲反應第一時間通知資料所屬主管機關進行更正，並於 1 小時內完成資料下載連結更正。為便利民眾與機關雙向互動，民眾如發現資料集內容有錯誤或其他建議，可直接於該項資料集下方表達意見。

【資料來源：蘋果日報 103/6/29】

## 【重點摘要】

1. 政府資料開放平臺(data.gov.tw)，提供民眾檢索、查閱及下載個別主管機關釋出的資料集。
2. 民眾對於政府開放資料之品質或內容有任何意見，應可循現有意見回饋機制，作為機關更正載點、調整格式、修正資料錯誤或改善品質的參考。

## 【法律觀點】

政府資料開放加值應用是將政府部門運作所持續產生的大量資料，在保障個資的前提下，開放提供作目的外的加值運用，以期達到全民參與與透明化政府的效益。為推動行政院及所屬各級機關政府資料開放，以結合民間

資源及創意，達成施政便民及公開透明之目的，行政院於民國 102 年 2 月 23 日訂定「行政院及所屬各級機關政府資料開放作業原則」(以下簡稱政府資料開放作業原則)，以中央二級機關統籌規劃其所屬機關資料集之管理，並集中列示於政府資料開放平臺(data.gov.tw)，供使用者連結下載及利用，以利民眾得透過該平台檢索、查閱由個別主管機關釋出的資料集。除公營事業機構、公立學校及行政法人，得準用本原則規定辦理外，地方政府亦得參照本原則另訂規範，以辦理其政府資料開放作業[1]。

為提高政府資料開放的效益並強化與使用需求的符合度，政府資料開放作業原則第 9 點即要求各機關應建立意見回饋機制、資料正確性回報及問題諮詢管道，以利資料內容持續精進或改善[2]。因此，在政府資料開放的風潮下，政府主動公開的目的，不僅是行政資訊透明化或滿足民眾知的權利，而更進一步滿足民間加值應用需求，並帶動相關產業發展。鑒於政府資料開放平臺展示之資料集，已多載明資料集提供機關聯絡人及其聯絡方式，民眾對於資料品質或其內容若有任何意見，應可循現有意見回饋機制，逕洽機關聯絡人或在該筆資料集頁面下方發表意見，作為機關更正載點、調整格式、修正資料錯誤或改善品質的參考，以共同促進我國政府資料開放與加值應用環境的活絡。

## 【管理 Tips】

本案例係因人為操作疏失，導致資料錯置。根據澳洲政府發表的網路犯罪暨安全 2013 年調查報告，網路安全事件發生原因有將近六成，肇因於員工人為操作錯誤或疏失[3]，故組織應要求人員確實依資訊處理設施相關之操作與作業內容程序規定執行，並且提供人員必要的訓練。針對作業的變更，

[1]行政院 102 年 2 月 23 日院授研訊字第 1022460185 號函訂定「行政院及所屬各級機關政府資料開放作業原則」，第 16 點：「公營事業機構、公立學校及行政法人，得準用本原則之規定辦理資料開放。」第 17 點：「地方政府得參照本原則，另訂規範辦理各該政府及所屬各級機關政府資料開放作業。」

[2]「行政院及所屬各級機關政府資料開放作業原則」第 9 點：「各機關設立網站提供政府資料開放服務者，應建立意見回饋機制、資料正確性回報及問題諮詢管道，並應綜整使用者意見，持續精進服務內容，必要時得請資料集提供機關對於使用者意見進行改善或說明。」

[3] CERT Australia, Cyber Crime & Security Survey Report 2013, *available* at https://www.cert.gov.au/system/files/614/679/2013%20CERT%20Australia%20Cyber%20Crime%20%2526%20Security%20Survey%20Report.pdf, at 24.

也應予制度化，建立變更之完整作業流程，包括變更之核准、執行及變更後之檢查等，確保作業內容正確。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.7.2.2　資訊安全認知、教育及訓練

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。

A.12.1.2 變更管理

應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。

# 參、資訊監察（Monitors）

# 一、通訊保障及監察法

類別：資訊監察【**案號：M1030101**】

## 不能調通聯，遺失手機滿警局

### 【焦點話題】

現代人經常發生手機遺失，遭到陌生人拾獲後持之使用的情況，層出不窮。承辦拾得物的員警表示，他們通常會先嘗試回撥手機內通話紀錄留下的號碼，詢問對方手機所有人是誰；拾獲者若占為己有，多半會更換 SIM 卡再使用手機，或賣給特定通訊行，但只要有通聯紀錄，就能以手機序號查詢手機號碼，警方仍可查到使用者，幫失主找回手機，並究辦使用者的侵占罪責。但依 103 年 6 月 29 日施行的新修正通訊保障及監察法(以下簡稱通保法)，警方對於遺失案件，無法再逕行向電信公司調閱使用者通聯紀錄或 SIM 卡序號等資料，以主動追查失主，只能公告招領後被動等手機所有人領回。警方表示「三個月來已累積十支，其中不乏蘋果、三星及 HTC 等知名大品牌，很多還是新的」。對於無法讓這些手機物歸原主，警方也相當無奈。

【資料來源：聯合報 103/9/1】

### 【重點摘要】

1. 通保法修正後，限於檢察官偵查最重本刑三年以上有期徒刑之罪，或檢察官、司法警察官為偵辦最輕本刑十年以上有期徒刑之罪或特定種類之犯罪行為時，始能調取通信紀錄。

2. 警方受理拾得物，基於維護民眾私人財產並以適當方式辦理招領，聯絡該手機持有人先前通話對象以聯繫手機持有人尚無疑義，但應注意持有人隱私保護。

### 【法律觀點】

我國大法官釋字第 631 號解釋文，就人民受憲法保障之秘密通訊自由，揭示其意義「在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。國家採取限制手段時，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當。」因此，通保法修正時，即將通訊使用者資料與通信紀錄之調取，納入該法適用範圍[1]。鑒於該法修正新增第 11-1 條規定，限於檢察官偵查最重本刑三年以上有期徒刑之罪，或檢察官、司法警察官為偵辦最輕本刑十年以上有期徒刑之罪或特定種類之犯罪行為時，始能調取通信紀錄[2]，以致引起實務界反彈，認為將會影響治安維護或緊急救援服務。

電信產業公會日前即函詢法務部，通保法施行後，有關機關得否基於救災救難、失蹤或自殺等情形，向電信公司要求調取通信紀錄，法務部函復雖曾指出：「於刑事犯罪案件以外情形，例如為救災救難、尋找失蹤人口等與生命安全有關而有需要者，因非通保法規範之範圍，得否調取該等資料，自應回歸適用電信法等相關規定，此部分尊重各該法規主管機關之權責」[3]。因此，警察機關執行犯罪偵查以外的法定職務，而有取得當事人通信紀錄或通訊使用者資料之必要時，仍應視其主管法規有無相關依據。

警察機關受理民眾拾得手機時，依民法關於治安機關招領遺失物的規定[4]，

---

[1] 通訊保障及監察法第 3-1 條：「本法所稱通信紀錄者，謂電信使用人使用電信服務後，電信系統所產生之發送方、接收方之電信號碼、通信時間、使用長度、位址、服務型態、信箱或位置資訊等紀錄。本法所稱之通訊使用者資料，謂電信使用者姓名或名稱、身分證明文件字號、地址、電信號碼及申請各項電信服務所填列之資料。」

[2] 通訊保障及監察法第 11-1 條：「檢察官偵查最重本刑三年以上有期徒刑之罪，有事實足認通信紀錄及通信使用者資料於本案之偵查有必要性及關連性時，除有急迫情形不及事先聲請者外，應以書面聲請該管法院核發調取票。聲請書之應記載事項，準用前條第一項之規定。司法警察官因調查犯罪嫌疑人犯罪情形及蒐集證據，認有調取通信紀錄之必要時，得依前項規定，報請檢察官許可後，向該管法院聲請核發調取票。檢察官、司法警察官為偵辦最輕本刑十年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪防制條例等罪，而有需要時，得由檢察官依職權或司法警察官向檢察官聲請同意後，調取通信紀錄，不受前二項之限制。」

[3] 參見法務部 103 年 7 月 25 日新聞稿，救災救難不能陷入觸法爭議，法務部對於現行警察職權行使法、電信法或消防法等法規，是否已明確賦予相關權責單位調閱通信紀錄之權限，表示仍有疑義。檢索自 http://www.moj.gov.tw/public/Data/482195226440.pdf

[4] 民法第 803 條：「拾得遺失物者應從速通知遺失人、所有人、其他有受領權之人或報告警察、自治機關。報告時，應將其物一併交存。但於機關、學校、團體或其他公共場所拾得者，亦得報告於各該場所之管理機關、團體或其負責人、管理人，並將其物交存。前項受報告者，應從速於遺失物拾得地或其他適當處所，以公告、廣播或其他適當方法招領之。」

應得撥打給該手機持有人先前通話對象，或以其他適當方法聯繫手機所有人取回，惟警察機關保管期間應盡保管人義務，避免手機持有人隱私遭到外洩或遭竊取等侵害[5]；至於民眾報案手機遺失，通常僅涉及侵占或竊盜案件的偵查，並非重罪或通保法第 11-1 條規定得調閱通信紀錄之犯罪類型。警察職權行使法第 28 條雖規定，警察為排除現行危害個人財產之行為或事實狀況，得採取必要措施[6]，惟該規定係適用在即時強制的情形，因此警方調閱通信紀錄以追查手機下落，是否符合即時強制所要求之急迫性[7]，即有疑義。再者，依電信法與「電信事業處理有關機關查詢電信通信紀錄實施辦法」規定向電信事業查詢通信紀錄，亦限於「依法律規定查詢」之情形[8]。因此，目前已有立委提案修正通保法第 11-1 條規定，刪除第 1 項關於本刑 3 年以上之限制[9]。因此，關於警察機關基於偵辦手機疑似失竊或侵占案件之目的，能否向電信事業查詢實際使用者發話位址資訊，在主管機關進一步解釋釐清適用關係或修法解決前，實務上恐有困難。

## 【管理 Tips】

通訊保障及監察法修正施行後，警方對於民眾拾獲或報案遺失的手機，恐難以調閱通聯紀錄方式追查手機下落。為避免組織發生類似本案例在業務執行與資訊安全或隱私保護要求的兩難窘境，組織應盡可能兼顧二者，在資訊安全的要求上，儘量與組織業務執行效能的需求取得平衡，同時避免將資訊安全無限上綱到影響業務的正常執行。

---

[5] 法務部 103 年 6 月 25 日法律決字第 10303506290 號函要旨：「民法第 803、804、807 條、個人資料保護法第 11 條規參照，警察機關保管遺失物期間係居無因管理地位，應負保管義務，保管方法應與無因管理人同，須以善良管理人注意義務為之，故基於對遺失人人格權保護及隱私權維護，如遺失物含有個人資料部分，建議宜予移除或其他適當方式處理後，再行交付拾得人，以避免發生個人資料洩漏情事」。

[6] 警察職權行使法第三章「即時強制」第 28 條：「警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。」

[7] 行政執行法第 36 條：「行政機關為阻止犯罪、危害之發生或避免急迫危險，而有即時處置之必要時，得為即時強制。即時強制方法如下：一、對於人之管束。二、對於物之扣留、使用、處置或限制其使用。三、對於住宅、建築物或其他處所之進入。四、其他依法定職權所為之必要處置。」

[8] 電信法第 7 條第 1 項：「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。」第 2 項：「前項依法律規定查詢者不適用之；電信事業處理有關機關(構)查詢通信紀錄及使用者資料之作業程序，由電信總局訂定之。」

[9] 參立法院第 8 屆第 6 會期第 1 次會議議案關係文書，103 年 9 月 10 日，院總第 1407 號委員提案第 16981 號，查詢自 http://lci.ly.gov.tw/LyLCEW/agenda1/02/pdf/08/06/01/LCEWA01_080601_00055.pdf

鑑於政府、企業及民眾對於個人資訊之隱私及保護的要求越來越重視，組織也應主動蒐集及關注相關的資訊，視需求調整業務執行上必須注意的安全規範。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A18.1.1 適用之法規及契約的要求事項之識別

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法。

A.18.1.4 個人可識別資訊之隱私及保護

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。

# 檢察總長洩漏監聽譯文，判處徒刑

## 【焦點話題】

甲為最高法院檢察署檢察總長，指揮監督最高法院檢察署檢察官及高等法院以下各級法院及分院檢察署檢察官。甲明知全民電通更一審關說案仍在偵查中，卻仍將最高法院檢察署專案報告，內容包含全民電通更一審偽證案之研究、本案通訊監察譯文及全民電通更一審關說案的後續偵查方向等依法應秘密之資料(下稱專案報告)，洩漏並交付予總統，嗣後又向行政院長報告並交付與專案報告內容相同的資料。又甲明知該關說案未經承辦檢察官以犯罪嫌疑不足為由而為不起訴之處分，亦未以未涉有犯罪嫌疑為由簽結，卻為使外界知悉關說案論證依據，竟指示下屬將通訊監察譯文的通話時間與通話內容，製作為新聞稿並於記者會上公告，台北地檢署依刑法洩密罪、違反通訊保障及監察法起訴。

本案法院認為，甲分別向總統與行政院長報告，並交付偵查所得資料與監察通訊所得譯文，嗣後又召開記者會洩漏上開資料的行為，均已違反通訊保障及監察法第 27 條公務員洩漏、交付監察通訊所得應秘密資料罪，與刑法第 132 條第 1 項公務員洩漏國防以外機密罪，故判處甲執行刑 1 年 2 個月有期徒刑。

【資料來源：臺北地方法院 102 年度矚易字第 1 號判決】

## 【重點摘要】

1. 監聽對於人民的隱私權侵害嚴重，偵查機關實施通訊監察，應符合通保法對於監聽事由之限制，並就通訊監察所得資料依法採取保存與銷燬。
2. 通訊監察所得資料，原則上應僅能於監察之目的範圍內始能使用，縱有涉及行政調查之必要，亦僅能提供給具有調查或審議評鑑權限之機關。

【法律觀點】

憲法第 12 條規定：「人民有秘密通訊之自由」，保護人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾的權利。因此，國家採取限制手段時，除應有法律依據外，限制之要件應具體明確，不得逾越必要範圍，所採取的程序亦應合理正當，始符合憲法保護人民秘密通訊自由之意旨。而通訊保障及監察法(以下簡稱通保法)之立法，除為確保國家安全與維持社會秩序等目的外，亦在保障人民秘密通訊自由及隱私權不受非法侵害。對於人民不願公開的對話或資訊，在未得通訊當事人同意下即予以監聽，且實施監聽時蒐集的資訊內容與範圍亦不易控制，長時間監聽對於人民的隱私權侵害程度相當嚴重。因此，通保法明文限定實施通訊監察的事由，並規定通訊監察所得資料的保存與銷燬方式[1]，課與國家事後嚴格限制使用範圍的方式，以免通訊監察所得之內容遭不當濫用。

通保法第 18 條已明確限制通訊監察所得資料，原則上應僅能於監察之目的範圍內始能使用[2]，亦即原則上僅刑事偵查、審判機關於追訴第 5 條等規定列舉之犯罪，或監察院、檢察官評鑑委員會等具有依法調查、懲罰行政不法等責任之機關，為究責行政不法之目的，行使其調查權以取得通訊監察所得的資料，始能予以使用。本案所涉關說案，縱然已偵查終結並為不起訴處分，偵查機關仍有繼續維持保護證述內容的秘密性，以保護涉案當事人名譽，並避免妨礙後續行政調查之必要，故通訊監察所得資料，應僅能提供予具有調查或審議評鑑權限的機關。是以，本案法院認為甲分別將通

[1] 通訊保障及監察法第 17 條：「監察通訊所得資料，應加封緘或其他標識，由執行機關蓋印，保存完整真實，不得增、刪、變更，除已供案件證據之用留存於該案卷或為監察目的有必要長期留存者外，由執行機關於監察通訊結束後，保存5年，逾期予以銷燬。通訊監察所得資料全部與監察目的無關者，執行機關應即報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長許可後銷燬之。前二項之資料銷燬時，執行機關應記錄該通訊監察事實，並報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長派員在場。」

[2] 通訊保障及監察法第 18 條：「依本法監察通訊所得資料，不得提供與其他機關（構）、團體或個人。但符合第 5 條或第 7 條規定之監察目的或其他法律另有規定者，不在此限。」同法第 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。」及同法第 7 條第 1 項：「為避免國家安全遭受危害，而有監察下列通訊，以蒐集外國勢力或境外敵對勢力情報之必要者，綜理國家情報工作機關首長得核發通訊監察書。」

訊監察所得監聽譯文交付總統與行政院長，甚至以召開記者會公布新聞稿的方式洩漏，均非向權責機關為追訴或究責該關說案行政不法責任之用，顯與上開通保法 18 條規定的使用範圍有別，均已構成犯通保法第 27 條公務員洩漏、交付監察通訊所得應秘密資料罪[3]與刑法第 132 條第 1 項公務員洩漏國防以外機密罪[4]，從一重論以通訊保障及監察法第 27 條之罪而，判處執行刑 1 年 2 個月有期徒刑。

## 【管理 Tips】

就資訊保護的角度，從此一案例組織應體認到，對於組織所擁有、管理的資料及其內容，相關的權責機關或特殊關注方（如政府單位、目的事業主管機關、合作夥伴、民眾等），皆可能對與其有關的資訊內容應受到適當保護有合理的期待。

因此組織對於資訊及資訊處理設施除應有適當的保護措施之外，對於資訊的合理使用，應在不逾越法律、法令、法規及契約的要求下，訂定明確的使用規則，以避免資訊被誤用及濫用。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.8.1.3　資產之可被接受使用

對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。

A.18.1.1 適用之法規及契約的要求事項之識別

[3] 通訊保障及監察法第 27 條：「公務員或曾任公務員之人因職務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處三年以下有期徒刑。法官或檢察官執行本法而有法官法第 39 條第 2 項或第 89 條第 4 項各款情事者，應移送個案評鑑。公務員或曾任公務員之人違反第 18 條之 1 第 2 項、第 3 項規定，將本案通訊監察資料挪作他用者，處三年以下有期徒刑。」

[4] 甲明知全民電通更一審關說案並未依法予以不起訴處分，亦未依實務行政簽結方式結案，又已於其指揮下針對該案發動刑事偵查作為予以調查並蒐集證據資料，仍應受偵查不公開原則之拘束，對於犯罪嫌疑不足或不明之犯罪偵查所得資訊應予以保密，而不能逕行自認無刑事不法即予以公開，故甲此舉亦屬違反偵查不公開原則，而成立刑法第 132 條第 1 項之洩漏國防以外秘密之罪。

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。

# 肆、資訊應用（Application）

# 一、電子簽章法

**類別：資訊應用【案號：A1030101】**

## 證交所重申禁止證券營業員以手機接單

### 【焦點話題】

臺灣證券交易所(以下簡稱證交所)券商輔導部日前接獲投資人檢舉，指出某證券商營業員未依照其電話指示買進股票，經派員前往證券商瞭解並調聽相關交易錄音內容，發現除部分電話委託未留存錄音紀錄外，另有部分電話委託係由營業員撥電話給客戶，向其確認委託買賣之股票名稱、數量及價格等，與一般由客戶撥打營業員電話委託下單的模式不同。

證交所進一步查證，得悉該營業員與客戶為方便聯繫，故互留手機號碼，客戶偶爾會撥打營業員手機下單，或利用 line 或 facebook 等通訊軟體傳遞下單訊息，再由營業員打電話跟客戶確認交易資訊後下單。

證交所表示考量到現行設備及技術，尚無法確保手機接單相關紀錄之不可竄改性，恐難以保障投資人權益，亦容易衍生交易糾紛，故重申依法禁止營業員以手機接單。【資料來源：工商時報 103/5/14】

### 【重點摘要】

1.電話委託紀錄屬證券委託買賣之交易憑證，應儲存於無法修改與消除之電子儲存媒體，並於成交當日製作完成，以確保交易紀錄事後均可追蹤稽查。

2.證券商若欲以電子文件取代紙本委託書，應確保錄音紀錄之內容可完整呈現，並可於日後取出供查驗。

### 【法律觀點】

為便利客戶買賣證券，並維護交易秩序暨保障投資人權益，臺灣證券交易所營業細則已明訂證券經紀商得以非電子式交易型態，例如當面或電話委託，以及以電子式交易型態接受委託，包含透過語音、網際網路等方式委託買賣。若客戶係以電話方式委託營業員買賣有價證券，營業員依規定須以書面或電子方式填具委託書，以留存業經客戶委託之紀錄，而若證券經紀商係以電子方式填具委託書，在符合分層負責且能確認該筆委託所歸屬之營業員下，證券經紀商得無庸逐一列印委託書，以減免紙本作業成本，但電話紀錄須儲存於無法修改與消除之電子儲存媒體，並於成交當日製作完成[1]，以確保交易紀錄事後均可追蹤稽查，而強化有價證券市場的交易安全。此外，臺灣證券交易所營業細則規定客戶電話委託紀錄視為交易憑證，證券經紀商應同步錄音，將電話錄音紀錄置於營業處所並至少保存一年[2]。

是以，證券經紀商雖得以電子方式填具委託書並免逐一列印委託書，但參酌電子簽章法關於文書得以電子文件保存之規定[3]，證券經紀商若欲以電子

[1] 臺灣證券交易所股份有限公司營業細則第 75 條第 8 項：「證券經紀商不得以電腦設定群組方式受託買賣有價證券，委託書與委託紀錄應記載事項依主管機關之『證券經紀商受託買賣有價證券製作委託書買賣報告書及對帳單應行記載事項準則』第 4 條、第 12 條規定，並應依下列規定製作：（一）非電子式交易型態：1.當面委託：委託人或其代理人或被授權人當面委託買賣有價證券者，應填寫委託書並簽章。2.電話、書信、電報或其他經本公司同意之方式委託：委託人或其代理人或被授權人以上開方式委託買賣有價證券，應由受託證券經紀商之受託買賣人員以書面或電子方式填具委託書；除電話委託外，應將函電或相關文件附於委託書後。證券經紀商以電子方式填具委託書者，如能執行受託買賣分層負責暨確認該筆委託歸屬之受託買賣人員，得免逐一列印委託書，惟應使用無法修改與消除之電子媒體儲存。（二）電子式交易型態指委託人以語音、網際網路、專線、封閉式專屬網路及其他經本公司同意之電子式委託買賣方式，證券經紀商應依下列規定辦理：1.以電子式交易型態委託者，證券經紀商得免製作、代填委託書。2.以網際網路委託者，另應記錄其網路位址（IP）及電子簽章；以語音委託者，應配合電信機構開放顯示發話端號碼之功能，記錄其來電號碼。（三）證券經紀商受理非電子式交易型態之委託買賣且採電子方式填具委託書，或受理電子式交易型態之委託買賣，應依時序別列印買賣委託紀錄，並於收市後由受託買賣人員簽章。但買賣委託紀錄儲存作業符合下列規定者，得免列印及簽章：1.使用無法修改與消除之電子儲存媒體，並於成交當日製作完成。2.建立完整目錄及管理程序。3.專人管理負責，並可隨時將電子媒體資料轉換成書面格式。」

[2] 臺灣證券交易所股份有限公司營業細則第 80 條規定：「證券經紀商接受委託買賣，應由登記合格之業務人員承辦之。前項登記人員執行受託買賣有價證券，應佩帶本公司發給之登記證，接受委託買賣時，應依第 75 條第 8 款規定填具委託書並編號，依委託順序處理之。證券經紀商於買賣申報成交後，應製作買賣報告書，其格式及應行記載事項依主管機關之規定。證券經紀商對電話委託應同步錄音，並將電話錄音紀錄置於營業處所。前項電話錄音紀錄，證券經紀商應至少保存一年。但買賣委託有爭議者，應保存至該爭議消除為止。如證券經紀商發生設備故障或作業疏漏時，應於事實發生之日起二日內將其原因事實及改善情形向本公司申報。依前項所保存之電話錄音紀錄，視為交易憑證之一種，如證券商有規避或拒絕檢查情事者，依違反第 25 條第 2 項之違規處理規定暨『證券商規避、拒絕檢查之認定標準及處理程序』辦理。」

[3] 電子簽章法第 6 條：「文書依法令之規定應以書面保存者，如其內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。前項電子文件以其發文地、收文地、日期與驗證、鑑別電子文件內容真偽之資料訊息，得併同其主要內容保存者為限。」

文件取代紙本委託書，應確保錄音紀錄之內容可完整呈現，並可於日後取出供查驗。鑒於營業員若以手機、其他通訊軟體或網路電話服務，提供客戶委託買賣，通訊工具本身縱能同步錄音，但能否保存相關發話資訊恐有疑慮，亦無法確認是否遭到竄改、變更或消除，致未來恐無法確認客戶委託內容之真正性與完整性而衍生交易糾紛。因此，證券交易所依其營業細則，再次重申禁止營業員以手機接受客戶委託。

## 【管理 Tips】

本案例中證券商營業員未依規定程序處理客戶之委託下單，以致衍生交易糾紛；另一方面，證券業者對客戶電話委託之交易錄音紀錄亦有所遺漏。由於行動設備與通訊軟體之日益普遍與方便性，基於提供客戶服務並爭取交易時效，上述行動設備與通訊軟體確實提供另一便捷的管道，但對證券業者、營業員以及客戶而言，也存在著如身分冒用、否認交易內容等可能的潛在風險。

為保障彼此權益，證券業者對於交易過程及內容應予以確實記錄，並確保其完整性，以便交易發生爭議時可以提供佐證；同時亦應規範新興科技於執行業務上的使用限制，並教育員工應以合於規定的程序執行業務，對違反規定者之懲處，亦應有明確的規範及宣示。

## 【相關標準】

**ISO 27001：2013（CNS 27001）**

A.6.2.1　行動裝置政策

應採用政策及支援之安全措施，以管理使用行動裝置所導致之風險。

A.7.2.2　資訊安全認知、教育及訓練

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、教育與訓練，並定期更新。

A.7.2.3　懲處過程

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。

A.12.4.1 事件存錄

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。

A.18.1.1 適用之法規及契約的要求事項之識別

對每個資訊系統及組織，應明確識別、文化件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。

類別：資訊應用【案號：A1030102】

# 警被控竄改 MSN 對談，栽贓性侵

## 【焦點話題】

○○市政府警察局刑事警察大隊(以下簡稱市刑大)於民國 100 年間偵辦妨害性自主案件時，搜索並扣押被告 20 歲張姓男子的筆記型電腦。未料，市刑大警員遭控利用張男偵訊期間，刪除張男與被害人原始對話紀錄，再以相同檔名的對話紀錄檔案覆蓋，進而出現被害人表示「但有一件事我真的會怕，那就是脫褲子」云云的關鍵對話，成為檢方起訴有力證據。

經張男委任律師聲請調查局鑑定後，證實電磁紀錄的確遭到竄改，故一、二審法院認為無積極證據證明女方於 16 歲前與張男發生性關係，而作出無罪判決。目前張男已對該女子與市刑大警員提出誣告罪與妨害電腦使用罪告訴，遭指恐竄改電磁紀錄的市刑大警員表示，覆蓋檔案是從電腦資源回收筒複製出來，並無竄改。【資料來源：工商時報 103/5/14】

## 【重點摘要】

1.數位資料具有無差異複製、易於增刪修改、製作人不易確認，以及無法直接以感官知覺等特性，使用此類資料作為證據應注意避免更動或毀損。

2.蒐集數位證據時，應採取適當鑑識工具進行保全、隔離及記錄，以確保與原始內容間具有同一性。

## 【法律觀點】

隨著科技發展進步，可作為犯罪事實認定基礎的資料，資料來源與呈現型態產生極大變化，不同於一般物證與書證，新型態證據可能為監視錄影畫面、電腦相關程式執行的軌跡紀錄或通訊軟體對話紀錄等，讓司法機關於進行證據能力認定與調查時，面臨新的挑戰。是以，我國刑事訴訟法即明

文規定[1]，具「與文書相同之效用」之電磁紀錄，準用「文書」之證據方法，以概括地規範將來可能新生的各種新型態證據。

然而，原始數位資料具有無差異複製、易於增刪修改、製作人不易確認及無法直接以感官知覺等特性，且在儲存、轉檔或移動過程中，均可能發生資料流失或毀損的情形。因此，無論是人為或檔案處理過程中所無法避免的失真，均足以影響資料原貌。我國法院刑事訴訟實務上，在判斷該數位資料得否採為證據時，首要前提即在確認電磁紀錄是否與輸入或建立時內容具有同一性，若無法證明該資料未遭到任何竄改或變更，則該資料能否作為認定法律構成要件事實的依據，即有疑義[2]。

本案員警扣押被告電腦與執行取證之過程，即未採取適當鑑識工具進行保全、隔離及記錄，以確保其移動、複製或還原相關檔案或電磁紀錄的各作業環節，並未更動該資料內容或其他附屬資料註記。是以，若電磁紀錄已無法證明與原始內容間具有同一性，即恐影響法院採為證據與否之心證。是以，建議若有採集數位證據作為訴訟上舉證之需求時，資料蒐集過程應採取適當保全程序，以確保其同一性與完整性，而能成為法庭攻防上的呈堂證供。

## 【管理 Tips】

隨著新興犯罪型態與工具及其所衍生的數位證據課題，執法人員亦應提升對數位證據、數位鑑識的必要知識，以及瞭解處理數位證據的責任與方法，相關單位亦應提供必要的訓練。而在證物保全的管理上，亦應納入數位證據，對於數位證據之保全，應考量其保管、存取的安全要求，確保數位證據之完整性與符合證據監管鏈原則。

[1] 刑事訴訟法第 165 條第 1 項：「卷宗內之筆錄及其他文書可為證據者，審判長應向當事人、代理人、辯護人或輔佐人宣讀或告以要旨。」同法第 165 之 1 條：「前條之規定，於文書外之證物有與文書相同之效用者，準用之。錄音、錄影、電磁紀錄或其他相類之證物可為證據者，審判長應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。」

[2] 例如我國最高法院 99 年度台上字第 3988 號判決即指出：「儲存電腦系統內之記憶，須經由一定程序，以文字、圖片、影像或符號予以重現。惟因儲存過程，具有潛在偽造、變造或修改之危險，是將電腦儲存資料列印後提出為訴訟上之證明，應確認電磁紀錄是否與輸入時之資料相合，若以列印資料之影本為某項事實之證明，尤以證明影本與原本之內容具有一致性為必要。」

【相關標準】

**ISO 27001：2013（CNS 27001）**

A.7.2.2　資訊安全認知、教育及訓練

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。

A.18.1.3　紀錄之保護

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。

# 建立健保雲端藥歷，提升用藥品質

## 【焦點話題】

隨著雲端科技日趨成熟，衛生福利部中央健康保險署(以下簡稱健保署)決定結合網路科技朝建立雲端資料庫發展，初步規劃以民眾的用藥歷史檔案為首要對象，設置「雲端藥歷檔」資料查詢系統。雲端藥歷檔主要以病患為中心，將病患即全民健康保險對象最近 3 個月內，至各醫院門、住診及用藥明細等就醫紀錄，以人為單位進行歸戶，彙集整理成即時的就醫紀錄。民眾就醫時只要透過全民健康保險保險憑證(以下簡稱健保 IC 卡)，就可請醫師或藥師協助查詢過去 3 個月的用藥紀錄，包括處方來源及處方主要診斷、藥品藥理作用、成分名稱、藥品健保代碼、藥品名稱、藥品規格及用量等資料，提供醫師處方開立或藥師藥物諮詢參考。

健保雲端藥歷系統的建置，除能為病患用藥安全把關之外，更能減少醫師重複處方，降低醫療資源浪費，以及減少醫療費用經審查後遭到核刪的問題。

【資料來源：全民健康保險雙月刊第 106 期 102 年 11 月號】

## 【重點摘要】

1. 雲端藥歷系統配合憑證登入機制，可有效確認查詢者身分與其存取權限範圍，同時兼顧資訊安全與促進用藥品質提升。
2. 憑證為個人在電子環境中之身分識別方式，民眾應妥善保管自身憑證，以避免遭到他人竊取後從事不當利用。

## 【法律觀點】

健保 IC 卡是民眾就醫時的重要憑證，在晶片中留有保險對象最近就醫的登錄資料，醫師可經由醫事憑證的認證程序，讀取 IC 卡上的相關就醫資

訊。不過，健保 IC 卡容量相當有限，且查詢回應速度較慢，卡片晶片內僅能記錄民眾用藥及檢驗檢查等代碼，須進一步對照資訊系統中的健保支付標準檔或藥品檔，才能將代碼轉為臨床資料或用藥資訊。隨著醫療管理與服務需求的日益增加，單以健保 IC 卡恐無法即時協助醫師參考病患當時或先前曾使用之藥品，以開立更符合病患治療疾病所需的處方。再者，醫療診所與醫師對於因業務而知悉或持有的病人病情或健康資訊，負有保密義務[1]，且除經病患或其家屬同意以外，原則上並無權限閱覽病患於其他醫療診所之就醫或用藥紀錄[2]，以致於醫療實務上容易發生重複用藥情事。

因此，健保署為突破健保 IC 卡實務作業的限制，建置雲端藥歷查詢系統，該系統提供醫師以醫事憑證登入系統，並在病患同意下插入病患健保 IC 卡，登入健保資訊服務系統，線上即時查詢健保署已收載的病患近期用藥資訊。鑒於醫事憑證與健保 IC 卡均為衛生福利部核發的憑證，可作為憑證持有者在電子環境的身分識別機制。雲端藥歷查詢系統要求醫師須將其醫事憑證與病患健保 IC 卡同時插入，才能讀取該病患近期用藥資料。亦即，該系統以憑證登入機制，即時確認查詢人員為有權存取及其權限範圍，並留存必要的查詢紀錄，更能同時兼顧資訊安全與促進用藥品質提升。

惟就未來管理層面，應確保醫師以其個人醫事人員憑證登入系統，經告知病患有查詢其用藥紀錄必要，並經病患同意後，始能持病患健保 IC 卡查詢，以避免發生他人冒用醫事憑證，或病患對於醫師使用其健保 IC 卡的用途有所誤會等情事，確保事後追查課責。

## 【管理 Tips】

本案例係衛福部健保署為提升民眾用藥安全，並減少健保支出，因此擬以「健保雲端藥歷」系統，提供醫院就診民眾近 3 個月的完整用藥病史，作

[1] 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。」醫師法第 74 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。」

[2] 醫療法第 74 條：「醫院、診所診治病人時，得依需要，並經病人或其法定代理人、配偶、親屬或關係人之同意，商洽病人原診治之醫院、診所，提供病歷複製本或病歷摘要及各種檢查報告資料。原診治之醫院、診所不得拒絕；其所需費用，由病人負擔。」

為醫師處方參考，避免發生病人重複用藥情形。其立意良好，惟因系統內含機敏資料，事涉民眾之個人健康隱私，針對民眾用藥紀錄的資料存取，應考量相關的存取控制安全要求，包括建立及施行存取控制政策，並嚴格限制其所能存取的內容，依其職責提供必要的最小權限需求，同時對使用者之查詢活動應予以記錄。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.9.1.1　存取控制政策

存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。

A.9.1.2　對網路及網路服務之存取

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。

A.12.4.1 事件存錄

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。

A.18.1.4 個人可識別資訊之隱私及保護

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。

類別：資訊保護【**案號：A1030104**】

## 行動購物平台攜手銀行，大學生享受行動購物

### 【焦點話題】

看好龐大的學生消費商機，○○銀行與行動購物平台業者合作，整合影城、餐廳、音樂及藝文展演等服務，提供無法申辦或未持有信用卡的學生新的行動購物與支付工具，讓大學生透過手機應用程式，就能在平台上購票或享受折扣。目前已和多所大專院校合作，學生只需在線上申請開通帳戶，即可預存現金，並於行動購物平台上消費使用，一指輕鬆付款。

目前該行動購物平台已經與餐飲集團與電影院等洽談合作，共同推出多項學生會員專屬的優惠，例如透過行動購物平台所屬 App 購買電影票，除行動購物、線上劃位免排隊外，還有專屬優惠價格，其他校園內外活動也可透過線上購票，憑 QR Code 快速進場。

【資料來源：蘋果日報 103/8/1】

### 【重點摘要】

1. 為因應電子商務金流儲值服務需求，銀行公會已規範銀行受理客戶以網路方式開立儲值支付帳戶之作業審核程序，及其配套管理措施。

2. 線上儲值支付帳戶之開立與交易額度，係由銀行依客戶提供個人資料之身分認證強度，而設有不同金額限制。

### 【法律觀點】

為提供消費者更多元與更安全的支付工具，第三方支付服務逐漸興起。第三方支付是指在交易雙方當事人間，建立一中立的支付平台，買方可透過超商繳費、銀行帳戶轉帳、線上儲值帳戶或信用卡扣款等多種支付方式，將貨款預存至賣方虛擬帳戶中，由平台為買賣雙方提供款項代收代付服

務。此項服務對於未申請成為信用卡特約商店的微型商店或個人賣家，提供便利的收付款項機制，有助於電子商務環境的活絡。惟第三方支付通常須使用者預先儲值一定金額，而儲值涉及吸收不特定人資金，恐衍生帳戶安全、消費者權益保護及洗錢防制等議題。因此，行政院專案會議業已擬定長期目標為制訂電子商務第三方支付服務管理專法，短期目標則由銀行以存款方式預先收取客戶款項，以盡快提供客戶進行網路交易支付[1]；非銀行的第三方支付服務業者若欲提供儲值交易服務，須依電子票證發行管理條例提出申請，或與電子票證發行機構合作[2]。

因此，為因應電子商務金流儲值服務需求，金融監督管理委員會就中華民國銀行公會提出之「銀行受理客戶以網路方式開立儲值支付帳戶作業範本」，已於 102 年 8 月 30 日完成備查[3]，以規範銀行受理客戶以網路方式開立儲值支付帳戶之作業審核程序，及其配套管理措施。依該作業範本，儲值支付帳戶採實名制，銀行依客戶、業務關係或交易種類之風險，留存客戶提供的身分基本資料，並經由一定認證程序核對客戶身分。此外，儲值支付帳戶的儲值金額，係依客戶身分的認證強度而設有不同額度，例如客戶使用行動電話與電子郵件的雙重認證模式，即可在 1 萬元範圍內儲值與進行交易，若是使用自然人憑證或工商憑證等能驗證有效性的簽章，辦理線上申請開立儲值帳戶，則帳戶最高可儲值 20 萬元。在本案例中，學生族群若無自然人憑證，仍可透過連結至其他銀行存款帳戶，或使用手機號碼雙認證等方式，開立線上儲值支付帳號，並由銀行提供款項代收代付服務，享受行動購物的便利。

## 【管理 Tips】

[1] 網路交易代收代付服務指獨立於商品或服務之交易雙方以外，由交易雙方委任，接受付款人將交易款項交付予銀行，或提供該服務之網路平台業者於銀行所開立之專用存款帳戶內，並逐筆於付款人取得商品、獲得服務、一定期間屆滿或一定條件成就後，將該交易款項轉付予受款人之服務。

[2] 行政院即時新聞，江院長拍板「第三方支付服務」之管理短期以「電子票證發行管理條例」作為非銀行第三方支付儲值服務管理法源、中長期應制定專法，102 年 8 月 7 日，檢索自 http://www.ey.gov.tw/News_Content2.aspx?n=F8BAEBE9491FC830&sms=99606AC2FCD53A3A&s=E7A51BA28056D303

[3] 金融監督管理委員會 102 年 8 月 30 日金管銀票字第 10240002940 號函，准予備查訂定發布「銀行受理客戶以網路方式開立儲值支付帳戶作業範本」，檢索自 http://www.rootlaw.com.tw/LawHistory.aspx?LawID=A040390041059200-1020830

電子商務的產值規模快速成長，即將成為下一個兆元產業，相較於真實世界銀貨兩訖的交易模式，網路交易首要建立信賴基礎，並且克服其中諸多挑戰，包括建立方便且可信賴的交易與支付模式、保護交易資料、以及確保平台安全等。

於本案例中，銀行欲搶攻第三方支付商機而與行動購物平台合作，提供客戶方便與優惠的服務。惟欲提供一個方便且可信賴的交易與支付模式，無論是銀行或行動購物平台業者，都應確保交易資料受到適當的保護，使其不被未經授權存取、惡意修改或損壞，並且確保交易服務能時刻正常運作。另一方面，對於交易過程中的對象，也必須有適當的身分認證機制，確保交易是由經授權的使用者發出，以及交易完成後用戶不能否認交易之執行。

因此，針對營運的作業平台或應用程式，於開發之初即應納入各方面的安全要求事項，如系統安全或程式安全要求等，並於日常維運中，持續進行資訊系統脆弱性的檢測與修補，以避免系統或程式存在安全漏洞而造成客戶、業者權益損失或資料外洩。針對交易資訊的完整性，也應透過適當的措施，例如加密或使用憑證簽發等，確保資訊正確性，並在登入的程序上規劃以適當機制核對確認用戶身分，評估採用雙因素認證的機制以強化身分的驗證與識別。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A.9.4.2 保全登入程序

當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。

A.12.6.1 技術脆弱性管理

應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

A.14.1.1 資訊安全要求事項分析及規格

資訊安全相關要求事項，應納入新資訊系統或既有資訊系統之強化的要求事項中。

A.14.1.2 保全公共網路之應用服務

應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。

A.14.1.3 保護應用服務交易

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

# 金管會保險局開放部分產險保單免簽名

## 【焦點話題】

金融監督管理委員會保險局(以下簡稱保險局)將開放產險業五類保單免經要保人、被保險人簽章。鑒於強制車險保單一年有 1,791 萬件，而住宅火險續保保單一年亦有 258 萬件，可望大幅降低保險業務作業成本。

由於保險法相關要求保險契約應留存保戶簽名，造成保險公司必須額外透過業務員或服務處通路，完成保單親簽，但隨著網路或電話投保盛行，保險局採納保險業者建議，逐步簡化投保程序。

開放部分產險保單免簽名的同時，保險局亦規定三項配套措施。一是產險業者對於要保書未經要保人、被保險人簽章或簽署的部分，未來若發生爭議，應作有利要保人或被保險人的解釋與處理；第二是保險業務員從事招攬與核保人員執行評估時，均須依金融消費者保護法第 9 條規定，確保金融商品或服務適合消費者；最後，保險局要求產險業者應在保單正面，以顯著字體載明個資蒐集告知事項供保戶參閱，以維護保戶權益。

【資料來源：中時電子報 103/7/30】

## 【重點摘要】

1. 因應行動投保需求，保險局開放部分產險保單無需要保人或被保險人書面簽名，以簡化投保程序。
2. 保險業者雖無需取得要保人簽章，但仍應保留證明要保人投保意願之證據，以利事後發生爭議時，得舉證保險契約當事人意思合致。

## 【法律觀點】

依我國保險法規定，除特定保險應經被保險人書面同意或承認[1]以外，只要保險契約當事人雙方意思一致即為成立[2]。金管會為保護消費者權益並防範道德危險，於「保險業辦理電話行銷業務應注意事項」要求保險業辦理電話行銷業務，應經要保人及被保險人於要保書簽名[3]。

金管會為因應行動化、網路化趨勢並簡化作業，業於民國 103 年 8 月 29 日金管保產字第 10302525791 號令公告「財產保險業者辦理特定保險業務時，得以取具足資證明要保人投保意願之相關證據，取代由要保人及被保險人於要保書簽章」，因此財產保險業者辦理包括法人業務財產保險招標業務、配合法令要求須投保之財產保險業務、進出口貨物運輸保險業務、住宅火災保險續約業務、強制汽車責任保險業務等五類業務，即無必要取得要保人或被保險人書面簽名，作為保險契約成立之證明。保險業承辦上開保險業務，雖無庸提出經要保人簽名之紙本保險單，或以數位簽章或其他憑證簽署之電子保單，但若事後就保險契約成立與否發生爭議，保險業者即須提出得以證明招攬當時要保人確實有投保意願之證據，例如要保人同意投保之電話錄音檔案，或要保人回覆投保之電子郵件發送紀錄等證據，惟須注意，保險業對此類電磁紀錄，應確保其內容可完整呈現，並至少留存至承保後一定期間，以利事後就投保有無或電磁紀錄內容真正與否發生爭議時得取出查驗。

**【管理 Tips】**

隨著網路投保或電話行銷盛行，為簡化投保程序，保險局採納業者建議，就較無投保爭議的產險業部分保單，逐步開放部分保單不必保戶簽章。此一措施實行後，原有的紙本簽名要求將被電話行銷錄音或網路投保紀錄等電子紀錄所取代。對許多組織而言，其日常營運作業在資訊化的過程中，電子紀錄已取代大多數的紙本作業紀錄，然為符合法令、法規、契約及營運要求，以及紀錄保護的要求，組織除應確認相關紀錄有被確實存錄外，亦應對紀錄提

[1] 保險法第 105 條：「由第三人訂立之死亡保險契約，未經被保險人書面同意，並約定保險金額，其契約無效。

供必要的保護，如存取控管、備份、完整性驗證等，以避免當發生投保爭議時，無法提出佐證紀錄的情況發生。

**【相關標準】**

**ISO 27001：2013（CNS 27001）**

A18.1.1 適用之法規及契約的要求事項之識別

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。

A.18.1.3 紀錄之保護

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。

# 自我評量

# 7 月分自我評量

## 是非題：(每題十分)

1. ( X )若政府機關係執行法定職務而蒐集、處理或利用當事人個資，是否完全無庸採取遮蔽措施?

2. 【資料保護 S1030101】

> 解析：公務機關因執行法定職務而蒐集處理及利用個人資料，仍應依個人資料保護法 5 條規定，合乎比例原則。

3. ( X )民眾地址無法送達時，公務機關為便於民眾即早知悉退稅結果，在官方 Facebook 粉絲頁公告民眾姓名、身分證字號及退稅方式，屬於辦理公示送達所必要? 【資料保護 S1030101】

> 解析：在 Facebook 粉絲網頁公告並非公示送達方式，且公告民眾完整身分證字號，亦有逾越識別身分之必要範圍而洩漏個資之疑義。

4. ( X )公務機關為促進民間加值運用，委託廠商將公務機關保有之個人資料進行分析與去識別化，因資料隨後均已遮蔽，因此公務機關對於受託廠商應無庸採取任何監督? 【資料保護 S1030101】

> 解析：公務機關委託廠商處理個人資料，應依個人資料保護法施行細則第 8 條進行監督。

5. ( X )警察人員於凱道反核活動現場，為犯罪偵查之公共利益，利用 M-Police 人臉辨識系統，拍攝每個參與者臉孔並比對其身分資料，是執行法定職務，故符合比例原則。【資料保護 S1030103】

> 解析：公務機關蒐集、處理或利用個人資料，應符合個資法第 5 條及行政程序法第 7 條比例原則之要求，於執行法定職務之必要範圍內為之，且不得逾越特定目的之必要範圍。

6. ( O )為達到政府資料最大加值利用可能性，政府以政府資料發展各項行動

化應用服務時，若有涉及個人資料時，仍應符合個人資料保護法之規定?【資訊公開 D1030101】

解析：政府機關行動化服務發展作業，仍應遵循個人資料保護法相關規定。

7. ( X ) 錄音檔案須透過機械設備播放，無法以個人知覺直接認識，因此不得作為電子文件? 【資訊應用 A1030101】

解析：依電子簽章法第 2 條規定，電子文件係指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄。

8. ( X )我國法院實務上目前禁止電磁紀錄，例如通訊軟體 Line 的對話紀錄或 Facebook 訊息作為證據? 【資訊應用 A1030102】

解析：我國刑事訴訟法或民事訴訟法均未禁止以電磁紀錄作為證據。

9. ( O )依我國法院實務，電磁紀錄及其複製本若能經一定鑑識方法，證明與其原本內容相同並無遭到竄改或更動，得作為認定法律構成要件事實的證據?【資訊應用 A1030102】

解析：電磁紀錄及其複製本若經證明與原本內容相同，且與待證事實具有關連性、調查之可能性，得法院認定事實適用法律之基礎

## 選擇題：(每題十分)

1. ( 4 )公務機關受理民眾行使當事人權利，公務機關在以下何種情形下，得拒絕刪除?(1)該資料仍在法定保存期限內；(2)刪除將影響當事人重大權益；(3)公務機關對該民眾具有公法上請求權，須以該資料作為證據；(4)以上皆是。【資料保護 S1030102】

解析：公務機關是否依使用者請求，即應刪除含有其個人資料之檔案文件，仍應視有無符合個資法第 11 條第 3 項「因執行職務或業務所必須」之情形。

2. ( 4 )若依法得以電子文件保存相關交易紀錄時，應考量要項不包含以下何者?(1)內容可完整呈現；(2)可日後取出供查驗；(3) 發文地、收文地、日期與驗證等相關資訊須併同文件主要內容保存；(4)電子儲存設備使用年限。【資訊應用 A1030101】

解析：依電子簽章法第 6 條規定，若法令或公務機關公告並無排除電子簽章法之適用，如文書內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。惟該電子文件以其發文地、收文地、日期與驗證、鑑別電子文件內容真偽之資料訊息，得併同其主要內容保存者為限。

## 自我評量檢測成果評分說明

| 得分 | 溫馨提醒 |
|---|---|
| 100 分 | 資安小博士非您莫屬 |
| 80 分~90 分 | 小粗心，別灰心 |
| 60 分~70 分 | 釐清觀念，滿分到手 |
| 40 分~50 分 | 再接再厲，繼續努力 |
| 20 分~30 分 | 牛刀小試，再來一次 |

# 8 月分自我評量

## 是非題：(每題十分)

1. ( X )政府開放資料平臺提供的資料集內容僅提供民眾查閱，並未開放民眾進一步利用，因此亦無提供民眾意見回饋機制的必要? 【資料公開 D1030102】

> 解析：各機關設立網站提供政府資料開放服務者，應建立意見回饋機制、資料正確性回報及問題諮詢管道，並應綜整使用者意見，持續精進服務內容。

2. ( X )我國政府開放資料平臺僅提供民眾檢索國家發展委員會本身的資料集，無法查閱其他機關釋出的開放資料? 【資料公開 D1030102】

> 解析：中央二級機關統籌規劃其所屬機關資料集之管理，並集中列示於政府資料開放平臺(data.gov.tw)。

3. ( X )行政機關依法律授權訂定行政命令蒐集個人資料時，為達到行政效能最大化，應不受比例原則與授權明確性原則拘束? 【資料保護 S1030104】

> 解析：公務機關執行法定職務而有蒐集、處理及利用個人資料時，就個人資料蒐集之必要性與其範圍，仍應注意是否符合比例原則。

## 選擇題：(每題十分)

1. ( 4 )醫師須經病患同意並插入病患健保 IC 卡至讀取器後，始能查詢病患在雲端藥歷系統的資料，請問以下何者是以憑證登入查詢系統的效益?(1)識別憑證持有者身分；(2)確認存取權限與範圍；(3)有助系統保存必要軌跡資料；(4)以上皆是。【資料應用 A1030103】

> 解析：公務機關是否依使用者請求，即應刪除含有其個人資料之檔案文件，仍應視有無符合個資法第 11 條第 3 項「因執行職務或業務所必須」之情形。

2. （4）以下何者行政機關依法律授權訂定行政命令，作為蒐集、處理及利用時，應考量的原則?(1)比例原則；(2)正當合理關聯性；(3) 符合法律授權範圍；(4)以上皆是。【資訊保護 S1030104】

解析：公務機關執行法定職務而有蒐集、處理及利用個人資料時，就個人資料蒐集之必要性與其範圍，仍應注意是否符合比例原則，避免有逾越職權範圍過度蒐集而侵害民眾資訊自主權之疑義。。

## 自我評量檢測成果評分說明

| 得分 | 溫馨提醒 |
|---|---|
| 100 分 | 資安小博士非您莫屬 |
| 80 分~90 分 | 小粗心，別灰心 |
| 60 分~70 分 | 釐清觀念，滿分到手 |
| 40 分~50 分 | 再接再厲，繼續努力 |
| 20 分~30 分 | 牛刀小試，再來一次 |

# 9 月分自我評量

## 是非題：(每題十分)

1. ( X ) 公務機關委託業者辦理個人資料蒐集、處理及利用業務後，應信賴該業者的執行能力，無須再進行監督，以節省行政成本。【資料保護 S1030107】

> 解析：依個資法施行細則第 8 條規定，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，其監督事項，包括蒐集、處理或利用之範圍、類別、特定目的及其期間；適當安全維護措施；受複委託者；事故通知與補救措施；委託關係終止或解除後之返還或刪除事宜等。

2. ( O ) 政府機關於捷運等公開場所提供影片予民眾點選觀看，除屬合理使用之情形外，仍應先取得著作權人的授權，避免發生爭議。【資料保護 S1030603】

> 解析：著作人於著作完成時享有著作權，包括重製等著作財產權，未經授權擅自利用著作，可能涉及侵害著作財產權，但如屬合理使用之情形，則不構成著作財產權之侵害。

3. ( X ) BD 科技公司受安心市交通局委託辦理公共自行車租借業務，蒐集個人資料時，縱已逾越安心市交通局指示範圍，只要營業上有需要，即可蒐集與租借自行車無關之學歷、收入、婚姻狀況等個人資料。【資料保護 S1030107】

> 解析：BD 科技公司受公務機關委託蒐集個人資料時，視同公務機關，其於蒐集個人資料時，除須符合比例原則外，尚應於安心市交通局指示之範圍內為之，不得逾越特定目的之必要範圍，並應與蒐集目的具正當合理關聯，以符合個資法第 5 條及個資法施行細則第 8 條之規定。

4. ( X )公務員只要攜帶公務文件回家處理，就違反國家機密保護法之規定，而負有洩漏國家機密的刑責。【資料保護 S1030402】

解析：公務文件若未依國家機密保護法核定之絕對機密、極機密及機密文件，或依該法應報請核定之國家機密，即無適用國家機密保護法。

5. (O) 我國現行銀行受理客戶以網路方式開立儲值支付帳戶作業，銀行須留存客戶提供之真實身分基本資料，並經由一定認證程序核對客戶身分。【資料應用 A1030104】

解析：依「銀行受理客戶以網路方式開立儲值支付帳戶作業範本」，儲值支付帳戶採實名制，銀行依客戶、業務關係或交易種類之風險，留存客戶提供之身分基本資料，並經由一定認證程序核對客戶身分。

6. (X)我國金管會基於保護消費者個資安全，迄今仍全面禁止本國銀行將涉及消費者個資之金融系統委託國外廠商建置維護。【資料保護 S1030105】

解析：依「金融機構作業委託他人處理內部作業制度及程序辦法」關於跨境委外風險管理機制的相關要求，本國銀行應就受委託機構對客戶資訊之使用、處理及控管情形，確認符合我國個人資料保護法相關規定，且本國銀行對資訊系統的資安檢測標準不得低於我國規範。

7. (X)我國某銀行委託馬來西亞廠商統一處理客戶帳單清算事宜，該銀行只要監督馬來西亞廠商遵守當地法律與相關資安檢測標準即可，不需要符合我國主管機關要求。

解析：因應我國加入「跨太平洋夥伴協定」與「推動區域全面經濟夥伴關係協定」的需求，金管會修正「金融機構作業委託他人處理內部作業制度及程序辦法」，以放寬本國銀行跨境委外辦理的資格條件與風險管理機制，並於 103 年 5 月 9 日發布施行。

## 選擇題：(每題十分)

1. ( 1 )盜用他人身分線上填寫遊戲帳號註冊資料，是否構成偽造文書?(1)是，電磁紀錄亦屬於準文書，因此以他人名義提交網頁註冊資料，屬於偽造文書；(2)是，只要不是實質名義人，無論是否得到授權，均構成偽造文書；(3)不是，因為盜用者自己使用遊戲服務，實質名義人並未受到任何損害；(4)不是，因為電磁紀錄不屬於具有形體的文書。【資料保護 S10300402】

解析：網頁資訊等電磁紀錄屬於準文書，故盜用他人身分資料開立申請遊戲帳號，侵害實質名義人權益，並影響遊戲公司對遊戲點數儲值資料管理之正確性，恐構成刑法上偽造文書罪。

2. ( 3 )假設某公司以軟體自動回傳方式，蒐集開啟服務功能的使用者門號與註冊帳號，以比對確認使用者身分，請問該公司是否涉及蒐集使用者個資?(1)不是，因為門號與註冊帳號無法直接識別使用者身分，所以不屬於個資；(2)不是，因軟體自動回傳是系統自行作業，並非人為作業，故不是個資蒐集行為；(3) 若該公司能夠以使用者門號與註冊帳號識別特定使用者，即屬蒐集個資；(4)不是，因為個資法只適用於人工處理之個人資料檔案。【資料保護 S1030106】

解析：蒐集者如能將使用者電子郵件信箱、註冊帳號與其他資料對照、組合、連結而得識別特定個人，屬於本法所稱之個人資料而有本法適用。因此公司以任何方式取得間接識別資料，即屬蒐集個資。

3. ( 1 )外國手機製造廠商在國外蒐集台灣用戶個資，是否適用我國個資法?(1)外國製造商只要蒐集中華民國人民個資，仍應符合我國個資法規定；(2) 不適用，個資法並不適用於在我國領域外蒐集中華民國人民個資的情形；(3)適用，只要涉及到個人資料，無論目的或對象為何，都應該符合我國個資法；(4)要看外國手機製造廠商是否在我國辦理公司設立登記。【資料保護 S 1030106】

解析 : 我國個人資料保護法(以下簡稱個資法)第 51 條第 2 項規定 :「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」而所謂中華民國領域外，依法務部函釋係指我國政府法權未及之地域。再者，若自然人為單純個人或家庭活動之目的而蒐集個資，不適用個資法。

## 自我評量檢測成果評分說明

| 得分 | 溫馨提醒 |
|---|---|
| 100 分 | 資安小博士非您莫屬 |
| 80 分~90 分 | 小粗心，別灰心 |
| 60 分~70 分 | 釐清觀念，滿分到手 |
| 40 分~50 分 | 再接再厲，繼續努力 |
| 20 分~30 分 | 牛刀小試，再來一次 |

# 10 月分自我評量

## 是非題：(每題十分)

1. ( X ) A 為新聞媒體工作者，對於 B 牙醫看診時打了某名病患一巴掌的事件，縱使 B 牙醫於報導前受訪時，已要求報導須以匿名方式，但為確保民眾之的權利，A 仍得於報導內容中揭露 B 牙醫的姓名、診所名稱及地址。【資料保護 S1030109】

解析：B 受訪前已要求須以匿名方式進行報導，係已行使個資法第 3 條所定請求停止蒐集、處理或利用之當事人權利，如 B 並非公眾人物，事件內容亦與公共利益無關時，A 於報導時不得揭露 B 的個人資料。

2. ( X ) B 公司為搶搭 iPhone 熱賣風潮，乃推出 Bbox 雲端備份程式，供我國使用者將其照片等資料上傳至雲端保存，B 公司實際上已有蒐集個人資料之行為，但因 Bbox 雲端主機設置於美國加州，位於中華民國境外，故 B 公司不受我國個資法規定之拘束。【資料保護 S1030108】

解析：個資法第 51 條第 2 項規定：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」是以，B 公司於境外蒐集中華民國人民之個人資料時，亦適用我國個資法規定。

3. ( O ) 我國偵查程序應遵循偵查不公開原則，是以，參與偵查庭訊活動之人主觀上均期待該活動具有隱密性，客觀上偵查庭亦禁止與案件無關之人參與，故其性質上屬於非公開活動，在未經參與者同意之情況下，即使是當事人也不得擅自竊錄偵查庭之活動，否則可能因違法而面臨刑責。【資料保護 S1030403】

解析：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：...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。」是以，未經參與者同意，無故竊錄屬非公開活動之偵查庭庭訊狀況，已有違反前開規定而恐負有刑事責任。

4. (O) 網路駭客利用軟體破解他人雲端系統帳密，於登入後取得他人私密照片，此行為不但已屬違法蒐集個人資料，尚可能涉及我國刑法第 358 條所定「入侵電腦或相關設備罪」、第 359 條所定「無故取得、刪除或變更電磁紀錄罪」等罪，而須面臨刑責之處罰。【資料保護 S1030108】

解析：本題駭客行為涉及無故以軟體破解他人帳密之行為，在我國將可能構成刑法第 358 條「入侵電腦或相關設備罪」。其次，駭客取得 iCloud 伺服器中他人之私密照片之行為，則可能構成刑法第 359 條「無故取得、刪除或變更電磁紀錄罪」，且因屬違法蒐集個人資料之行為，而有違反個資法第 41 條第 1 項規定之虞。

5. (X) 員工於任職期間基於業務權限範圍內取得之公司機密資料，屬於合法持有，因此就算離職後繼續利用，也沒有任何侵害公司營業祕密的法律責任。【資料保護 S1030301】

解析：營業秘密法修正新增第 13-1 條，擴大構成侵害他人營業秘密之行為類型，以強化對營業秘密的保護。例如，原本具正當理由持有營業秘密之員工，如離職後經原公司要求刪除、銷毀該營業秘密，而故意不為刪除、銷毀或有隱匿情事時，即可依營業秘密法課予刑責。

6. (O) 要保人投保特定險種，得無庸親自在要保書上簽名，只要保險業者有留存證明雙方成立保險契約合意的相關證據即可。【資料保護 A1030105】

解析：保險局於民國 103 年 8 月 29 日公告財產保險業者辦理進出口貨物運輸保險業務、住宅火災保險續約業務、強制汽車責任保險業務等保險業務時，得以取具足資證明要保人投保意願之相關證據，取代由要保人及被保險人於要保書簽章。

7. ( X) 通訊保障及監察法修正施行後，檢察官與警方調閱通訊使用者資料與通信紀錄，均須向法院事先聲請，以確實維護人民秘密通訊自由。【資料保護 M1030101】

解析：新修正通保法第 11-1 條規定檢察官、司法警察官為偵辦最輕本刑十年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪防制條例等罪，而有需要時，得由檢察官依職權或司法警察官向檢察官聲請同意後，調取通信紀錄。

## 選擇題：(每題十分)

1. ( 4 ) 廠商推出具儲存功能之系統，供使用者以帳密登入後，將照片上傳備份時，下列何者是廠商可採取避免資料外洩之適當安全維護措施?(1)以字母大小寫、字元長度等要求，加強密碼複雜度；(2)設置帳號、密碼登入錯誤次數上限之防護機制；(3)偵測異常登入紀錄；(4)以上皆是。【資料保護 S1030108】

解析：依我國個資法施行細則第 12 條規定，適當安全維護措施係包括事故之預防；通報及應變機制；資料安全管理及人員管理；資料安全稽核機制；使用紀錄、軌跡資料及證據保存等。而以帳密登入之系統易遭暴力破解軟體攻擊，為確保使用者隱私及資料安全，應採取加強密碼強度、設置登入錯誤防護機制及相關安全防護機制，達到維護資料安全之目的。

2. ( 4) 以下何種行為，屬於我國新修正營業秘密法認定侵害他人營業秘密之行為類型?(1)盜取主管帳號密碼登入特定資料夾，瀏覽限制閱覽的機密資料；(2)未依主管指示於業務交接後刪除機密資料，而仍自行留存研究；(3)同事盜取前東家機密檔案給公司同仁使用；(4)以上皆是。【資料保護】S1030301】

解析：營業秘密法第 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」。

3. ( 3) 以下何種情形，警方可向電信業者調閱手機使用者通聯紀錄?(1)民眾請警察確認丈夫與外遇對象的交往頻率；(2)提供債務人發話所在位址給討債集團參考；(3)為偵辦兒童綁架案件，報請檢察官同意後向電信業者調取；(4)民眾遭到不明來電捉弄騷擾，想要知道來電者身份。【資料保護 M1030101】

解析：檢察官、司法警察官為偵辦最輕本刑十年以上有期徒刑之罪、強盜、搶奪、詐欺、恐嚇、擄人勒贖，及違反人口販運防制法、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、組織犯罪防制條例等罪，而有需要時，得由檢察官依職權或司法警察官向檢察官聲請同意後，調取通信紀錄。

## 自我評量檢測成果評分說明

| 得分 | 溫馨提醒 |
| --- | --- |
| 100 分 | 資安小博士非您莫屬 |
| 80 分~90 分 | 小粗心，別灰心 |
| 60 分~70 分 | 釐清觀念，滿分到手 |
| 40 分~50 分 | 再接再厲，繼續努力 |
| 20 分~30 分 | 牛刀小試，再來一次 |

# 11 月分自我評量

## 是非題：(每題十分)

1. ( O ) 作品如係作者獨立創作而非抄襲所得，且具有少量足以表達出作者個性或獨特性之創意時，即可認已具原創性，應受著作權法之保護。【資料保護 S1030604】

> 解析：我國著作權法所保護的著作，是指屬於文學、科學、藝術或其他範圍之創作，而創作係指具原創性之精神上創作，包含原始性與創作性的概念，前者是指著作人獨立創作，未抄襲他人著作；後者所稱創作性，雖無須達到完全獨創的地步，但至少須少量創意，以表現出作者之個性或獨特性。

2. ( O ) A 為了縮短上班時間，就以因職務知悉的門禁與考勤系統帳密，登入系統修改、刪除自己的出缺勤紀錄的行為，可能涉及刑法偽（變）造私文書罪與刑法破壞電磁紀錄罪。【資料保護 S1030404】

> 解析：由於電腦的使用日趨普遍，並漸以取代紙本文書，刑法即明文規定，電磁紀錄係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，亦屬文書。A 行為除因刪除退勤時間及更改到勤時間之偽造、變造行為，構成偽造、變造私文書罪外，其擅自刪除、變更電磁紀錄之行為，亦構成破壞電磁紀錄罪。

3. ( X ) A 看好房市，準備出售名下的房產，但為了提高交易機會，決定同時委託 3 家仲介業者處理銷售事宜，並給予 3 家不同的實際委託銷售總價額，因 A 所提出的實際委託銷售總價額，已授權多家業者，屬一般人得輕易知悉的資料，已不具秘密性。【資料保護 S1030302】

> 解析：A 雖基於成本等考量，委託數家業者處理銷售事宜，並提供予各家不同的實際委託銷售總價額，但該售價因涉及利潤或磋商空間等因素，仲介業者不會輕易揭露，一般人亦無法得知，仍屬工商秘密的範疇。

4. ( X )檢察機關因偵查貪瀆案實施監聽時，若發現涉案公務員有不務正業、

道德操守問題時，應依法將通訊監察所得資料送交該公務員所屬服務單位作為舉發。【資料保護 M1030102】

解析：通保法第 18 條已明確限制通訊監察所得資料，應僅能於法定的監察目的範圍內始能使用，亦即除法律另有規定外，原則上僅刑事偵查、審判機關於追訴犯罪始能予以使用。

5. ( X ) 電信公司於客戶申辦門號等時，依法蒐集其個人資料，為各部門業務需求，將客戶資料公告於內部建置的討論區中。由於該討論區僅供內部使用，無須採取權限管控，亦無必要進行遮蔽，以利公司人員方便使用。【資料保護 S1030110】

解析：依我國個資法施行細則第 12 條規定，適當安全維護措施係包括事故之預防；通報及應變機制；資料安全管理及人員管理；資料安全稽核機制；使用紀錄、軌跡資料及證據保存等。縱使屬公司內部使用之討論區，須考量網路易受到攻擊、駭客入侵、系統漏洞等因素，採行適當的安全維護措施，以避免發生任何人可透過網路搜尋功能，取得個人資料之情形。

6. ( X )檢察機關於偵查程序終結並為不起訴處分後，對於實施通訊監察所得資料已無保密之必要，故涉案當事人對話內容均得以新聞稿方式公開。【資料保護 M1030102】

解析：對於同時涉及刑事與行政不法的案件，縱然已偵查終結並為不起訴處分，偵查機關仍必要繼續維持保護證述內容之秘密性，以保護涉案當事人名譽並避免妨礙後續行政調查。

## 選擇題：(每題十分)

1. ( 2 )以下何者不是公務機關就檔案得辦理銷毀之事由?(1)已屆保存期限且經機關核准銷毀；(2)機關倉儲空間不足，無法繼續收納；(3)檔案已變質、散發有毒物質而嚴重危害人體；(4)檔案因遭遇戰爭、暴動或事變，為保護國家安全或利益而須即時銷毀。【資料保護 S1030201】

解析：機關就業已歸檔之文件應依檔案法規定加以管理，且定期保存之檔案，於法定保存年限內應妥善保存，除非有變質、散發有毒物質而嚴重危害人體，或是遭遇戰爭、暴動或事變，為保護國家安全或利益而須即時銷毀之緊急情形外，尚不得任意銷毀。

2. ( 4 ) 以下何種不是公務機關依機關檔案保存年限及銷毀辦法之規定，辦理銷毀事宜時應執行之事項?(1)訂定銷毀計畫；(2)檔案若仍有保存價值，應先經電子儲存；(3)機關首長親自勘驗銷毀設備；(4)製作檔案銷毀目錄後送會相關業務單位表示意見。【資訊保護 S1030201】

解析：公務機關依機關檔案保存年限及銷毀辦法之規定辦理銷毀事宜，包含製作檔案銷毀目錄後送會相關業務單位表示意見，並訂定銷毀計畫，且執行銷毀時應由檔案管理單位會同相關單位派員全程監控 。若經核定銷毀之檔案尚有保存價值之必要，仍應先經電子儲存。

3. ( 3 ) A 任職於大房屋不動產經紀公司，並與公司簽訂保密協議，卻利用須以公司電腦登入之查詢系統，獲知客戶委託銷售的不動產銷售總價額，包括底價、物件編號與地址等資料後，透過發送簡訊方式，傳送給同業的 B，試問 A 的行為已涉犯構成下列何罪?(1)侵占罪；(2)偽造文書罪；(3)洩漏工商秘密罪；(4)竊盜罪。【資料保護 S1030302】

解析：刑法第 317 條規定，行為人依依法令或契約有保守工商秘密之義務，卻無故洩漏時，構成洩漏工商秘密罪而負有刑責，但並未對工商秘密加以定義，實務認為應參酌營業秘密之定義加以判斷之。
而客戶委託仲介買賣不動產實際委託銷售總價額，因涉及利潤或磋商空間等因素，仲介不會輕易揭露予買方，且其秘密性具有實際或潛在的經濟價值，又公司已採取合理保密措施，足認該價額屬工商秘密範疇，A 未經公司同意，無故洩漏予他人，已構成刑法第 317 條之洩漏工商秘密罪。

4. ( 4 )A 電信公司為擴大服務範圍，乃與台北市各區通訊行簽約，委由各通訊行可代辦手機門號申辦、續約等電信服務，並蒐集用戶之姓名或地址等資訊，試問下列敘述何者正確？(1)通訊行是受委託蒐集個人資料，應依 A 電信公司指示範圍為之；(2)通訊行因屬委託關係，仍須遵守 A 電信公司應適

用的個人資料保護法規；(3)A 電信通司對於通訊行負有委託監督義務，並應定期確認執行狀況；(4)以上揭是。【資料保護 S1030110】

解析：由於 A 電信公司委託各通訊行辦理電信服務業務，通訊行即屬受委託蒐集客戶個人資料之情形，依個資法施行細則第 7 條規定，通訊行應適用 A 電信公司須遵循之規定外，復依同細則第 8 條規定，通訊行僅得於 A 電信公司指示範圍內，蒐集、處理或利用個人資料，且 A 電信公司必須對通訊行負監督義務，包括通訊行應採取之適當安全維護措施、事故發生之通知及補救措施等，並須定期確認通訊行的執行狀況。

## 自我評量檢測成果評分說明

| 得分 | 溫馨提醒 |
|---|---|
| 100 分 | 資安小博士非您莫屬 |
| 80 分~90 分 | 小粗心，別灰心 |
| 60 分~70 分 | 釐清觀念，滿分到手 |
| 40 分~50 分 | 再接再厲，繼續努力 |
| 20 分~30 分 | 牛刀小試，再來一次 |