資通安全法律案例宣導彙編

第九輯

行政院國家資通安全會報技術服務中心編印

中華民國 100 年 12 月

序

在社會高度資訊化的發展趨勢下，網路通訊科技的利用日益頻繁，網際網路成為資訊傳遞與交換的重要管道，民眾、企業與政府的行為方式亦隨之改變。由於雲端服務的興起、社群網站的風行、智慧型手機及平板電腦等行動裝置的蓬勃發展，在資訊安全議題上所面臨的威脅，更趨複雜與多元。尤其近年來個人資料外洩事故頻傳，在立法院於 99 年 4 月 27 日三讀通過個人資料保護法後，法務部亦於 100 年 10 月 27 日對個人資料保護法施行細則草案進行公告，使得個人資料保護的相關資安議題，廣受社會各界關注。此外，98 年 1 月行政院訂頒「國家資通訊安全發展方案（2009-2012 年）」，以達成「安全信賴的智慧台灣，安心優質的數位生活」為願景，並確立「強化整體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」及「建構資安文化發展環境」四大政策目標，以期使民眾、企業及政府在充分享受資通訊科技所帶來的便利之餘，亦能對日趨嚴重的資安威脅提出有效對策。

為提升政府與社會各界對網際網路應用安全議題的風險意識，「行政院國家資通安全會報技術服務中心」（以下簡稱技服中心）自 91 年起，已發行八輯「資通安全法律案例彙編」，希望藉由對近年來廣受社會矚目的實際案例，進行精要的說明解析，協助各界建立網路環境應有的法治觀念。此次 101 年編印之第九輯「資通安全法律案例彙編」，仍將內容概分為「資訊保護」、「資訊公開」、「資訊監察」及「資訊應用」四項主軸，持續委由「國巨律師事務所」蒐集近一年來發生之資安時事新聞與法院實際案例。內容除保持深入淺出的說明及專業法律觀點外，並與 CNS27001（資訊安全管理系統國家標準）之觀念宣導相結合，以期各界多關注管理系統的重要性。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

「行政院研究發展考核委員會」(以下簡稱「行政院研考會」)以及「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,戮力提昇國家整體資訊安全水準,甚為感佩。

值新修正後之「個人資料保護法」(新版個資法)持續受到各界專注之際,相關個人資料管理系統及標章制度陸續登場,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,有關本輯資訊安全管理之「管理 Tips」,特別商請資誠企業管理顧問股份有限公司梁亦民協理協助提供資訊,並為致謝。

第九輯除延續第八輯之作業模式外,在擷取新聞議題時間主要以民國(以下同)100 年 1 月到 12 月為主。同時,因為現行有效的法律仍然是「電腦處理個人資料保護法」(以下簡稱「現行法」),以致於在 100 年與 101 年間,新版個資法尚未正式施行之際且對應之施行細則草案,尚未通過行政院核定。是以,有關本輯個資議題的呈現有現行法,以及新版個資法與施行細則草案之對應說明。此一差異,為本輯有關「資訊保護」類中「電腦處理個人資料保護法」之特殊性,還請讀者注意。

在「資訊公開」類,主要以「資訊公開法」為介紹案例。「資訊監察」類還是以「通訊保障及監察法」為對象。有關「資訊應用」類,是以電子簽章在法院實務上認定之法律效力為介紹對象,可作為推動電子簽章制度之重要依據。此外,有關公司股東會線上投票制度亦為電子簽章之重要應用實例,輔以說明佐證雲端應用所涉法律制度之重要性。

整體案例分布,仍以「資訊保護」佔大宗,有 22 則案例。「資訊公開」則為 4 則。「資訊監察」2 則與「資訊應用」2 則。以上案例共計 30 則。

政府與企業各界正建立各種雲端運算服務提昇國家整體競爭力,是我們邁向全球資訊應用重鎮之重要指標。然對應搭配之法律與管理系統如能併同檢視,並形塑嶄新雲端面貌所需之整體法規與產業所需環境架構,應更可引導雲端服務可以更快成形,並引導資訊產業有更好的發展基石。

國巨律師事務所
朱瑞陽律師

凡　例

壹、本案例彙編分為以下類別：

一、資訊保護 (Security)

01 電腦處理個人資料保護法

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、本案例編碼共 8 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年份三碼及上述各小類之編碼兩碼，最後兩碼為該小類中之第幾篇案例。例如：S1000101，即代表資訊保護類 100 年度之電腦處理個人資料保護法第一則案例。

目　　次

壹、 資訊保護（Security）

一、電腦處理個人資料保護法

類別：資訊保護

【案號：S1000101】

房仲洩個資 5 千求職者受害

【資料來源：蘋果日報 100/08/17】

焦點話題

房屋仲介業者○○房屋總公司驚傳將 5000 筆求職者履歷資料，夾帶在電子郵件中寄出，已寄出 200 多封，求職者的姓名、性別、出生年月日及聯絡電話一覽無遺，有外洩求職者個資之嫌。對此，○○房屋總公司坦承，承辦人員誤將求職者資料夾帶在電子郵件中寄出，已立即停止寄發，並予懲處，依「個人資料保護法」之規定，民眾可請求損害賠償。

民眾王先生說，他 7 月初到○○房屋應徵工作，其後收到○○房屋寄出的未錄取通知電子郵件，開啟電子郵件夾帶的檔案，內容竟是近 5000 筆求職者的個人資料，其中也包含他的資料，讓他相當震驚，隨即向○○房屋反映，○○房屋總公司坦承是承辦人員疏失，內部第一時間發現後，立即停止寄發，並緊急聯絡收到夾檔的求職者，請他們刪掉相關檔案，也會懲處失職人員。

重點摘要

1. 企業應對個人資料採取適當的安全保護措施，以避免個人資料外洩。
2. 依新修正的個人資料保護法規定，發生個資外洩事件時，除非企業可以證明其無故意或過失，否則即應對受害人負損害賠償責任。

法律觀點

房仲業雖非電腦處理個人資料保護法(以下簡稱「現行個資法」)指定適用的

非公務機關，但依照新修正的個人資料保護法(以下簡稱「新版個資法」)的規定，未來只要是不屬於公務機關的自然人、法人或其他團體，都屬於新版個資法規範的非公務機關。因此對於求職者的個人資料，包含姓名、性別、出生年月日及聯絡電話等，都應該要採行適當的安全保護措施，防止所保有之個人資料被竊取、竄改、毀損、滅失或洩漏[1]，以保護個人資料，避免侵害他人的隱私權。

依照舉證責任之分配法則，一般民事案件當事人主張權利受到侵害時，請求方需負舉證責任，但在個人資料外洩之情況，受害人面對的往往是龐大的企業團體，證據資料往往係由企業保有，受害人難以取得相關資料，且因個資外洩導致受害人所受的損害通常不易舉證，造成當事人的個資外洩卻難以進行舉證。因此，新版個資法第 29 條特別規定[2]，除非非公務機關(即企業團體)可以舉證證明自己無故意或過失違反個人資料保護法之相關規定，否則發生個資外洩時，即須負損害賠償責任。

本案中○○房屋將 5000 筆求職者履歷資料，夾帶在電子郵件中寄出，明顯造成求職者履歷上的個人資料外洩，資料被外洩的求職者依新版個資法第 29 條的規定可向○○房屋請求損害賠償，依同條 2 項的規定，請求賠償的金額可以適用第 28 條第 3 項規定的方式計算[3]，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣 500 元以上 2 萬元以下計算，據此，除非○○房屋可以證明其沒有故意或過失外，○○房屋至少須負新臺幣 2,500,000 元到 100,000,000 元的損害賠償金額。

新版個資法通過後，所有行業均須遵循新版個資法的規定，將加重企業的法律責任，企業應該即早因應並對個人資料採取適當的安全保護措施，以

[1] 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。」

[2] 個人資料保護法第 29 條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。依前項規定請求賠償者，適用前條第二項至第六項規定。」

[3] 個人資料保護法第 28 條第 3 項：「依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。」

降低因個人資料外洩所帶來的法律風險。

管理 Tips

組織應針對存放個人資料之資料庫與資訊系統進行妥善之安全管理，並且應配置適當之監控機制及資料存取控管相關技術，例如限制可被存取之資料內容或數量，或是發現有大筆資料被存取時應進行之通報及處理程序。另外經由電子郵件等傳遞之資訊應有適切的保護機制，例如內容經過壓縮加密處理等。而平時應定期對組織人員進行相關之資訊安全教育訓練，使全員瞭解資訊安全及資料保護的觀念及可能面臨之法律責任。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.8.4　電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A.10.10.2　監控系統的使用

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000102】

新北監視全都錄 隱私不外露？

【資料來源：中央社 100/08/24】

焦點話題

新北市警局啟用「情資整合中心」，以監視器加強犯罪蒐證與偵防；民眾擔心隱私全都露，警方強調，透過權限認證及全程管制功能，將保障民眾隱私權。

有鑑於現有部分監視器影像品質不佳，市警局計畫民國 103 年底，在新北市特定路口建置 2 萬 7000 具百萬畫素高解析度監視器。「治安人口影像監控系統」透過民眾的即時臉部影像，與身分證等影像資料庫比對，將提升犯罪嫌疑人比對正確率，強化警方監控能力，並掌握犯罪人、車的動態及軌跡。不過，目前網路駭客技術高超，個人資料洩漏情形氾濫，部分民眾擔心，街頭到處都有攝錄器材，走到哪就拍到哪，雖有助犯罪偵防，但毫無隱私可言。

市警局表示，這套系統結合市警局既有的網域登入身分辨別系統，任何 1 名員警未經授權即無法登入；一旦登入，系統即全程自動記錄員警的使用紀錄，以防堵違法侵權，保障民眾隱私權。

這套系統由電腦自動擷取監視影像中的人物，自動分析治安人口影像資料庫，供警方辦案參考。

警方說，遠端監視系統結合光纖網路，整合鄰里監視系統，將所有監視畫面集中由警方管理，有利維護治安，保護隱私；透過開放權限管理，里長、派出所、警分局各有權限，可以調閱相關監視畫面。

重點摘要

1. 警政單位在公開場合設置「治安人口影像監控系統」是依據警察職權行使法的規定辦理。

2. 取自公開場合的拍攝資料不適用新修正個人資料保護法規定，但若公開場合的拍攝資料儲存進資料庫後進行人像資料比對結果，即屬個人資料保護法之保護範圍。

法律觀點

依照警察職權行使法第 10 條第 1 項的規定：「警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，為維護治安之必要時，得協調相關機關(構) 裝設監視器，或以現有之攝影或其他科技工具蒐集資料。」因此，本案例中，警方依照上開規定設置監視器，是具有法律依據的。

值得探討的是，依新修正個人資料保護法(以下簡稱新版個資法)第 2 條之規定，除了個人之姓名、出生年月日、國民身分證統一編號外，個人之特徵與社會活動亦屬個人資料保護法中所稱之「個人資料」。本案中「治安人口影像監控系統」是透過民眾的即時臉部影像，與身分證等影像資料庫比對，以提升犯罪嫌疑人比對正確率，因透過身分證影像資料庫的比對可以辨識個人身份，是以將涉及新修正個資法的相關規定。

依照新版個資法第 51 條第 1 項第 2 款的規定，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，不適用該法的規定。

因此本案例中「治安人口影像監控系統」所拍攝的民眾臉部及行蹤畫面，將不適用新修正個資法的規定，同時維護治安本屬於警方的法定職務範圍，且有前揭警察職權行使法作為蒐集資料之依據。

應注意的是，設置監視器必須符合警察職權行使法第 10 條第 1 項的要件，亦即須設置於可能發生犯罪案件之公共場所或公眾得出入之場所，否則仍

會有侵犯隱私權爭議，併予說明。

管理 Tips

本案例中之隱私議題主要源自於利用「治安人口影像監控系統」可透過攝錄到之即時臉部影像，與身分證等影像資料庫進行比對，民眾之行蹤會被清楚記錄。組織應評估蒐集民眾隱私資料，以及里長、派出所、警分局查詢該資料的合法性，並應建立完善之權限管理機制，避免存放有民眾個人隱私之資料庫等遭到未經授權的存取，並且應建立監控機制，當組織人員登入系統存取敏感資料時，即啟動監控系統進行側錄。針對與「治安人口影像監控系統」結合的網路連線，組織應予以保護，例如透過防火牆或入侵偵測系統等，降低經網路傳輸之資料被未經授權存取的機會。

相關標準

A.10.8.4　電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A.10.10.2 監控系統的使用

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A.11.2.2　特權管理

應限制與控制特權的配置與使用。

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000103】

在 itunes store 遭盜刷 蘋果不給資料

【資料來源：聯合報 100/11/27】

焦點話題

桃園縣某議員指出，他在蘋果 ipad 專屬 itunes store(線上軟體購物商城)的個人帳號與信用卡被盜用，向警方報案後，辦案人員要求蘋果公司協助調查，卻要不到盜用者身分和交易資料，警方最後發給他一張「至感歉意」的公文，讓他覺得無奈，也擔心消費者要活在帳號被駭客入侵的擔憂中。

該議員表示，日前用信用卡帳單有一筆買了 4 種 ipad 付費軟體共 1 萬多元的消費，購買地點在歐洲的盧森堡，他覺得匪夷所思。他說，雖在 itunes store 註冊，但很清楚不曾選購需付費的軟體，很可能是帳號遭駭客入侵，他向信用卡公司反映，獲得正面回應他不必付這筆消費。向桃園警分局報案後，希望揪出駭客，日前收到分局公文，表示向蘋果在台灣的代理商等團隊連繫，另外寄電子郵件連絡 itunes store，結果台灣的業者都說沒有權限，itunes store 更直接回信說不提供，警方追查碰壁，只能告訴他「至感歉意」。

桃園警分局表示，itunes store 總公司在國外，以前在這網站註冊，必須輸入電子郵件地址當成會員名稱，還會要求消費者留下信用卡卡號與密碼，事實上消費者不一定要輸入信用卡與密碼，在填寫信用卡資料時，可以點選「none」，已經填寫信用卡資料者，可以進入「我的帳號」更改。

重點摘要

1. 境外公司在中華民國領域外蒐集中華民國人民的個人資料時，亦須遵守新版個人資料保護法的規定。

2. 個人資料在境外外洩時，即使可以透過司法互助的方式調查證據，但可

能因諸多因素而難以行使權利，因此提供資料給境外公司時應特別小心。

法律觀點

本案例中，某議員的 itunes store 帳號疑似因駭客入侵，而有個人資料被盜用、信用卡被盜刷的狀況，但因為 itunes store 的總公司為境外公司，並在我國警方調閱時拒絕提供盜用者身分和交易資料，因此無法進一步偵辦。此部份會涉及境外公司在中華民國境外蒐集中華民國國民的個人資料，是否應遵守我國法律的相關規定。

電腦處理個人資料保護法(以下簡稱現行個資法)對於境外蒐集個人資料並沒有特別規定，因此在中華民國境外蒐集中華民國國民個人資料時，將不適用現行個資法的相關規定。有鑒於科技之進步與網際網路使用普遍，即使在我國領域外蒐集、處理或利用國人的個人資料，亦非常容易。為防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，以規避法律責任[1]，因此新修正個人資料保護法(以下簡稱新版個資法)新增第 51 條第 2 項規定[2]，在國外蒐集、處理或利用個人資料的行為，將有新版個資法的適用，相關行為必須遵守相關程序且應採取適當的安全維護措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，因此本案例中若是因為蘋果公司沒有採取適當的安全維護措施時，蘋果公司將會面臨民事求償與行政罰則。

新版個資法第 51 條第 2 項的規定雖然提高了對國人個人資料的保障，但實際案例發生時，相關資料的調閱可能須要透過國外政府的司法互助才能夠取得，而且即使獲得民事的勝訴判決，也可能會因為境外公司在中華民國境內沒有可以執行的財產，而無法獲得實質的賠償。因此，在網站上提供

[1] 參見新版個資法第 51 條修法理由。

[2] 新版個資法第 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。」

個人資料時，應該特別留意不要留下太多個人資料，否則一旦資料遭到竊取時，恐會有求償無門的情況。

管理 Tips

本案例可就以下兩方面討論之：

1. 對 itunes store：組織可考量以取得最少個人資料的原則，蒐集消費者的相關資料，並於消費者註冊時，適當地告知蒐集其個人資料的目的與消費者提供資料所須注意之相關事項與權益，確保盡善良管理者之責任。
2. 對消費者：應避免於網路上留存過多之個人資料，以降低因資料外洩所可能導致的風險與損失。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000104】

科大洩數百生個資 網路可輕易查到

【資料來源：蘋果日報 100/09/27】

焦點話題

有民眾反映兩科技大學，不慎將學生個資公布在網路上。對此，兩科大均坦承疏失，立即刪除相關資料，承諾加強教職員再教育。

新竹陳小姐說，她一時興起在入口網站搜尋自己名字，發現第一筆標示床位名稱的資料，竟詳細記錄她和另兩位學校宿舍室友的電話與地址，進一步搜尋，竟連結到她就讀的○○科大官網住宿生資料，包括她及室友在內，多達數十人的系所班級、聯絡電話及住家地址均一覽無遺。另名台北吳小姐則說，最近在網路搜尋自己姓名時，搜尋到○○科技大學 2004 學年度四技推甄錄取生報到名冊，內容包括姓名、身分證字號、生日、地址及電話等資料，且有數百名學生資料遭外洩。

對此，兩科技大學均坦承疏失，接獲反映後已立即刪除，並通知入口網站移除資料，會對職員再教育，未來將更注意資訊安全。

重點摘要

1. 學校蒐集學生的個人資料後，應採行適當之安全措施，以防止個人資料被竊取或洩漏。
2. 在網頁公布個人資料時，應避免揭露過多資訊，以保護個人資料。

法律觀點

現代社會網路資訊發達，搜尋網站功能日趨龐大，直接衝擊到的即為個人隱私之保護和個人資料之防護。透過搜尋網站可以將特定個人散落於不同

網頁的個人資料拼湊在一起，讓個人資訊無所遁形，民眾的隱私權越來越不受到保護。

本案中的兩所科技大學，基於學生宿舍管理或推甄活動的特定目的，而蒐集學生的姓名、身分證字號、生日、地址及電話等個人資料，乃具有特定目的，並由學生同意提供，因此對於此蒐集行為，應屬合法。但對於個人資料的蒐集、處理及利用行為並非毫無限制，依照新修正個人資料保護法(以下簡稱新版個資法)第 5 條[1]的規定，前述行為不得逾越特定目的之必要範圍，且應與蒐集之目的具有正當合理之關聯，否則將會違反新版個資法的規定[2]。另依新版個資料保護法 27 條的規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏[3]。本案例中兩所科技大學依照上開的規定，僅能在學生宿舍管理或推甄活動的特定目的之必要範圍內處理與利用個人資料，在入口網站讓任何人可以查到身分證字號、生日、地址及電話，顯然與宿舍管理或推甄活動的目的無關，是對個人資料沒有採行適當的安全維護措施，依法應負相關責任。

現今網路資訊雖然很發達，但是在揭露個人資料時必須要檢視揭露的內容及必要性，不要為了便利而違反法律規定。

管理 Tips

此案例主要發生原因係為組織對於資料之管控不確實，致學生個人資料被揭露於公開網路環境中。組織應透過教育訓練及宣導，讓組織內人員於處理機敏資料時更加謹慎，並應建立資料保護機制，避免此類資料被未經授權的揭露。

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

[2] 同現行電腦處理個人資料保護法第 6 條的規定。

[3] 學校屬於現行電腦處理個人資料保護法的適用主體，依照該法第 26 條准用第 17 條的規定，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.7.3　資訊處置程序

應建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用。

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000105】

校長搜教師置物箱 判國賠 50 萬

【資料來源：中國時報 100/09/20】

焦點話題

○○市○○國小校長○○，因搜索教師置物箱，教師認為隱私權受侵害提告，經台灣高等法院台中分院審理，認定校長○○侵犯教師隱私權，應給付損害賠償金額 50 萬元。

這起發生在 96 年 8 月的案件，當時李姓、廖姓兩名教師，因校長○○在同年 8 月 7 日要求兩人從教務處改調至輔導處，免兼行政職務，並限兩人當天立即搬行政辦公室，時間匆促，兩人只好先將私人物品裝箱搬到隔壁教室。校長○○在同年 8 月 10 日，和多名行政人員至輔導室旁教室搜查這兩名教師私人財物，教師認為已妨害教師隱私權，兩造對簿公堂，纏訟四年多。

校長○○表示，這兩名老師有的公文未移交，並且去查看置物箱時多人在場，只想找回公文書檔案，並無侵害兩人祕密。對被判國賠 50 萬，將委請律師提新事證，申請再審。

重點摘要

1. 翻閱他人之私人物品，除非法律有特別規定外，應得到物品所有人的同意，否則即屬侵害他人隱私權之行為，將會有民法損害賠償責任。
2. 公務員因執行職務而侵害他人之隱私權，公務機關會有國家賠償責任。

法律觀點

隱私權乃是憲法保障的權利，因此，若隱私權受到侵害時，依照具體個案，受害人可能可以依照刑法第 315 條以下妨害秘密罪章提出告訴，或依民法

第 184 條的規定請求損害賠償。

本案例中，○○為公立國小校長，屬於國家賠償法第 2 條第 1 項定義的「依法令從事公務之人員」[1]，因此校長○○執行職務若不法侵害他人權利時，依同條第 2 項規定[2]，國家應負損害賠償責任。因此，本案的爭議在於校長○○為找回未移交公文，是否屬於有正當理由，而非屬「不法侵害」。就此部分，法院認為校長○○應循刑事訴訟的規定聲請搜索及扣押，但校長○○沒有依法聲請搜索及扣押，且沒有取得李姓、廖姓老師的同意，即擅自搜查他們的私人物品，乃是侵害隱私權的行為，依照國家賠償法第 5 條[3]、民法第 184 條[4]及第 195 條[5]的規定，判決○○國小及校長○○應連帶賠償 50 萬元。

值得注意的是，隱私權的範圍包括個人資料，若案例事實有涉及到個人資料時，受害人將能依照電腦處理個人資料保護法(以下簡稱「現行個資法」)的規定向公務機關行使權利，差別在於一般隱私權的侵害，須由受害人對於損害事實及損害範圍負舉證責任，尤其精神損害部分，將會由法院衡酌兩造雙方的社會地位、學經歷等狀況認定精神賠償數額。但若是適用現行個資法，公務機關將負無過失責任，且每人每一事件會有 2 萬元以上 10 萬元以下的損害賠償責任，受害人將不負舉證責任，受害人求償相對較不困難。因此，公務員執行職務時，應注意個人隱私權的保護並遵守相關法律規定，否則將會使公務機關須負國家賠償責任。

管理 Tips

本案例中之校長應在其搜查教師之私人物品前，即針對所可能面臨的法律

[1] 國家賠償法第 2 條第 1 項：「本法所稱公務員者，謂依法令從事於公務之人員。」

[2] 國家賠償法第 2 條第 2 項：「公務員於執行職務行使公權力時，因故意或過失不法侵害人民自由或權利者，國家應負損害賠償責任。公務員怠於執行職務，致人民自由或權利遭受損害者亦同。」

[3] 國家賠償法第 5 條：「國家之損害賠償，除依本法規定外，適用民法規定。」

[4] 民法 184 條：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。故意以背於善良風俗之方法，加損害於他人者亦同。違反保護他人之法律，致生損害於他人者，負賠償責任。但能證明其行為無過失者，不在此限。」

[5] 民法 195 條：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

議題進行探討，清楚辨識其所需遵循的法令法規，以及所需擔負之法律責任，進而確認其行為的合法性，以避免違反相關法規及侵害他人隱私。

相關標準

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000106】

立院初審通過聯徵中心排除適用新版個資法

【資料來源：聯合晚報 100/11/16】

焦點話題

立法院財政委員會初審通過銀行法部分條文修正案，排除聯徵中心適用新修正個人資料保護法(以下簡稱新版個資法)適用，但增定聯徵中心必須設定內稽內控，以保護個人資料，若未落實內稽內控，最高可處 1000 萬元罰鍰。

依照新版個資法規定，聯徵中心蒐集、處理及利用個人資料，必須逐筆、逐案告知及取得當事人同意。

為避免聯徵中心蒐集、處理民眾個人資料必須逐筆、逐案告知，財委會審查多位立委所提的銀行法部分條文修正案，讓聯徵中心排除新版個資法適用範圍，但為加強信用資料報告機構之管制，聯徵中心和財金資訊必須建立內部控制和內部稽核制度，若聯徵中心和財金資訊未落實建立內稽內控，可處 200 萬元以上，1000 萬元以下罰鍰。

重點摘要

1. 依照新版個資法的規定，直接或間接蒐集個人資料，原則上須盡告知義務。
2. 機關於間接蒐集個人資料時，在法律有明文規定時，可以免除告知的義務。

法律觀點

「財團法人金融聯合徵信中心」(以下簡稱聯徵中心)負責銀行公會會員間授信資料蒐集、處理及交換，並建置全國性信用資料庫，以增進徵信功能，

並健全信用制度發展，以維護交易安全。金融業及徵信業為電腦處理個人資料保護法(以下簡稱現行個資法)之指定行業，依現行個資法第 23 條之規定，非公務機關於特定目的範圍外利用個人資料，除有「為增進公共利益」、「為免除當事人之生命、身體、自由或財產上之急迫危險」、「為防止他人權益之重大危害而有必要」的情形外，必須取得當事人書面同意。銀行提供民眾信用資料給聯徵中心，應屬於特定目的利用。

過去銀行都是在民眾申請金融服務時，透過定型化契約的約定，取得當事人同意，將申請人的信用資料登錄於聯徵中心，並讓申請人同意其他銀行可以向聯徵中心查調資料。不過，此方式在新版個資法施行後可能會產生很大的變化。因為，新版個資法第 9 條增加間接蒐集的告知義務[1]，也就是說蒐集非由當事人提供之個人資料時，除非符合免為告知的例外狀況外，否則蒐集者必須在處理或利用前，向當事人盡告知義務，對於平時即大量蒐集個人信用的聯徵中心，將產生極大的負擔。

必須補充說明的是，在直接蒐集個人資料時，亦須依新版個資法第 8 條[2]進行告知義務，因此，除非銀行符合得免為告知的例外事由，否則在蒐集資料時亦須向當事人進行告知，應特別注意。

本案中銀行法第 47 條之 4 的修正案，即是以增訂「依法律規定得免為告知」的規定，以免除聯徵中心於間接蒐集個人資料時應負的告知義務。未來上

[1] 新版個資法第 9 條：「公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。
有下列情形之一者，得免為前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人為告知。四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。
第一項之告知，得於首次對當事人為利用時併同為之。」

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

述銀行法修正案通過後，聯徵中心於取得當事人信用資料時，將可以不用逐一向當事人告知，但聯徵中心仍應對個人資料採取適當安全維護措施，若違反時，除會遭當事人依照新版個資法求償外，主管機關亦可能依銀行法規定進行處罰，不可不慎。

管理 Tips

依據銀行法及主管機關相關行政命令，聯徵中心可蒐集金融機構間信用資料。由本案例中得知，聯徵中心排除適用新個資法，但因所蒐集及傳遞之資料涉及民眾之機密個人隱私，需訂定適當之內稽內控制度以落實個人資料保護，並應考量與金融機構、銀行等跨單位資料傳輸的保護機制(例：資料加密或虛擬私人網路等)，以確保傳遞時的安全。

相關標準

A.10.8.1　資訊交換政策與程序

應備妥適當的正式交換政策、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交換。

A.10.8.2　交換協議

組織與外部團體間資訊與軟體的交換應建立協議。

A.10.8.4　電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000107】

銀行兩萬筆個資外洩　受害人每月接詐騙電話

【資料來源：蘋果日報 100/12/24】

焦點話題

警方破獲詐騙集團，查扣電腦中發現有大量甲銀行客戶個資，數量多達 2 萬筆，檔案夾以 A、B、C、D……等區分，並以身分證字號排序，滑鼠點入就可看到客戶填寫的現金卡申請書，填寫時間約在 2003 至 2005 年間。一名警官透露：「A 資料夾檔案，就是身分證 A 開頭，也就是台北市，B 就是台中市，每個資料夾都有上千筆內容，歹徒就像從銀行電腦裡直接把資料 copy 出來，實在離譜。」

這些外洩的個資被轉存影像檔，以方便不法集團轉賣牟利，資料詳載客戶姓名、卡號、身分證、電話及地址，甚至還有健保卡、戶籍及存摺。外流資料包括該銀行晶片現金卡轉換申請書，還有軍人辦貸款時，提供的軍人身分證或薪資單，也有員工訪查貸款者紀錄。

甲銀行個金執行長表示，外洩個資研判為 2008 年警方破獲駭客入侵案，當時受害包括多家銀行機構。甲銀行後續就電腦主機安全、使用者權限管制加強，也針對本案客戶資料集中管理，持續追蹤帳戶，迄今未接獲客戶反映異常。

金管會指出，甲銀行外洩個資全是現金卡申請資料，約 1.9 萬筆，已請各銀行加強個資保護，就算外洩也需確保客戶權益；金管會銀行局長表示：「甲銀行已監控外洩的客戶資料，目前沒交易異常，並要求甲銀行需提醒客戶防範詐騙。」

重點摘要

1. 銀行對於蒐集的個人資料應採取適當的安全維護措施。在新修正個人資料保護法(以下簡稱新版個資法)正式施行後，若發生個人資料外洩情事，銀行將依法負有通知當事人的義務。

2. 若欠缺適當的安全維護措施，銀行除須負擔民事損害賠償責任外，新版個資法並加重行政罰鍰的額度。

法律觀點

現行「電腦處理個人資料保護法」(以下簡稱現行個資法)第 3 條明文將金融業訂為適用現行個資法的行業主體[1]，因此，銀行蒐集個人資料應符合現行個資法規定。現行個資法針對保有個人資料檔案的機關，規定其有「指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」之義務[2]。因此，銀行對於客戶申辦各類金融業務所留存的個人資料，不僅應妥善保存，還需要訂定「電腦處理個人資料安全維護計畫」來防止資料被竊取或洩漏[3]，否則主管機關不僅可命其限期改正，如逾期不改正，更可按次課處負責人新台幣一萬元以上五萬元以下罰鍰[4]。

新版個資法為了防止個人資料被竊取、竄改、毀損、滅失或洩漏，針對保有個人資料檔案的機關，亦規定應「指定專人辦理安全維護事項」（公務機關）或「採行適當之安全措施」（非公務機關）[5]，所謂的「安全維護事項」或「適當安全措施」，法務部預告的新版個資法施行細則草案第 9 條則有詳細的定義和例示[6]。若銀行違反新版個資法之前述規定未採行適當安

[1] 現行個資法第 3 條第 7 款:「非公務機關：指前款以外之左列事業、團體或個人。……（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。」

[2] 參照現行個資法第 26 條準用第 17 條規定。

[3] 現行個資法施行細則第 35 條準用第 34 條:「(非)公務機關保有個人資料檔案者，應訂定電腦處理個人資料安全維護法令，其內容應包括資料安全、資料稽核，設備管理及其他安全維護等事項。」

[4] 參照現行個資法第 39 條第 1 項第 4 款規定。

[5] 參照新版個資法第 27 條規定。

[6] 新版個資法施行細則草案第 9 條:「(第 1 項)本法所稱適當安全維護措施、安全維護事項或適當之安全措施，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必要措施。(第 2 項)前項必要措施，應包括下列事項：一、成立管理組織，配置相當資源。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。

全措施，經主管機關限期改正，而屆期未改正時，新版個資法除將課予銀行之罰鍰額度，提高至新台幣二萬元以上二十萬元以下外[7]，如有致個人資料被竊取、洩漏、竄改或其他侵害者，並課予銀行「查明」事實和以適當方式「通知」當事人的義務[8]。

此外，當事人對於個資遭外洩一事，還可以向銀行主張民事損害賠償請求權。惟在提起損害賠償訴訟時，尚須注意「請求權時效」的規定。不論依現行個資法或新版個資法之規定，損害賠償請求權自請求權人「知」有損害及賠償義務人時起，因二年間不行使而消滅；而若損害「發生」已逾五年，該請求權亦會消滅[9]。本案個資外洩事件疑似是 2008 年警方破獲的駭客入侵案的延續，實際發生外洩事件的時間，仍待警方查證，受害人應於知悉其個資外洩時起（例如，受害者自新聞媒體得知）二年內請求損害賠償，否則若待本個資外洩事件發生經過五年後，縱令受害者事後知悉，亦將不得再行請求損害賠償。

管理 Tips

現今社會公司機構遭遇駭客侵入竊取個人資料的案例層出不窮，特別是擁有大量個人資料的金融機構，容易成為駭客或有心人士覬覦的目標，一旦資料外洩事件發生，不僅主管機關會究責處罰，更會影響一般民眾的信賴度。因此應有良好的安全機制控管資料庫與資訊系統，並且針對內、外部的資料傳輸均應配置適當之監控機制及資料存取控管相關技術，發現資料被不當存取時應立刻通報主管機關、即時處理，並通知個資當事人。

相關標準

A.10.10.2 監控系統的使用

九、資料安全稽核機制。十、必要之使用紀錄、軌跡資料及證據之保存。十一、個人資料安全維護之整體持續改善。」

[7] 參照新版個資法第 48 條第 4 款規定。

[8] 新版個資法第 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。」

[9] 參照現行個資法第 29 條、新版個資法第 30 條規定。

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A.11.2.4　使用者存取權限的審查

管理階層應定期使用正式過程審查使用者的存取權限。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000108】

員工保密義務與個人資料保護

【資料來源：臺北地方法院 99 年度勞訴字第 335 號判決】

焦點話題+

本案原告甲是 A 保險公司的員工，負責公文系統維護及文件歸檔的業務，某天甲被發現在電腦上查看含有其他員工個人資歷、身分證字號、職等及薪資組別等的機密人事檔案，明顯逾越甲之業務範圍及操作管理權限。A 公司稽核室調查後交由人事評議委員會議處，由董事長裁示核准免職。

甲表示自己是在處理公文系統異常時無意發現這些夾帶檔案，而私自下載留存，但從未洩漏，並未對 A 公司或其他員工造成損害，A 公司則主張甲之行為重大違反員工保密及作業守則，其免職處分應屬合法。法院判決認為，甲下載的人事資料筆數高達一千多筆，記載內容包括員工編號、單位、姓名、身分證字號、電子信箱、薪資組別、地址、學歷、年資等項，明顯涉及個人隱私。再者，甲的行為也違反受雇於 A 公司時，所簽署的「職務上電腦處理個人資料切結書」、「保密承諾書」等資安保密規定，縱使人事檔案未再對外洩漏，但已足以造成內部員工對於個資外洩或遭人不法利用的困擾，嚴重影響員工對於公司經營管理的威信。因此，甲的違約行為重大、損害勞雇雙方信賴關係，故 A 公司以違反工作規則達情節重大為由，依勞基法第 12 條第 1 項第 4 款，不經預告終止勞動契約，屬於合法有據。

重點摘要

1. 員工僅能在業務管理範圍內查看與留存個人資料，公司可以透過讓員工簽署保密契約的方式，約束員工遵守業務權限範圍。

2. 員工未經授權而查看、留存逾越其業務處理權限及範圍的個人資料，將

違反聘雇契約與員工保密的義務，可構成解僱事由。

法律觀點

本案原告甲主張是在處理公文系統異常時，發現信件附件夾帶有人事資料檔案，而逕自留存，並非從系統後台的人事資料庫擅自下載。但法院認為 A 公司中有權控管人事資料的人力資源部人員都無法私自持有這類資料，更遑論甲身為公文管理人員，本無查詢、增刪、維護人事資料權限，而且假若甲基於處理公文系統異常，而有排除異常公文、暫存該人事資料檔案的必要時，亦應於處理程序完畢後全數刪除，而不應逾越職務目的，將檔案儲存於個人電腦並變更檔名後自行查看。因此，甲未經 A 公司同意或授權，私自儲存具有機密性的人事資料檔案於個人電腦，嚴重違反勞工忠實提供勞務及保密義務。

A 公司為保險業，本有電腦處理個人資料保護法(以下簡稱「現行個資法」)之適用，而民國 99 年 5 月新修正通過的個人資料保護法(以下簡稱新版個資法)，更擴大個人資料保護範圍，並強化資料蒐集者的行為義務及相應的法律責任。行政院為順利推動新版個資法的施行，已於 100 年 11 月預告新版個資法施行細則修正草案，其中第 9 條明確界定公務機關及非公務機關保有個人資料時，為防止個人資料遭到竊取、竄改、毀損、滅失或洩漏，應採取技術上及組織上的必要措施，包含建立管理組織、個資蒐集處理內部管理程序、資料安全管理及人員管理、必要使用紀錄及軌跡資料保存等 11 項。

因此，新版個資法施行後，無論公務或非公務機關，對於內部資料安全管理機制的建立與運作，均負有義務，若無法控管內部人事資料庫的存取權限、查核人員使用紀錄，導致員工個人資料遭到洩漏或竄改，或逾越蒐集目的的非法利用，將面臨行政罰鍰及民事責任。此外，新版個資法雖廢除非公務機關的登記與執照制度，但銀行、電信、醫院、保險等行業因保有大量且重要的個人資料檔案，所負的安全保管責任應較一般行業重，故新

版個資法第 27 條第 2 項授權主管機關得指定特定之非公務機關，要求其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，以加強管理，確保個人資料之安全維護。是以，有蒐集、處理及利用個人資料需求者，應盡速配置相當資源建置內部個資風險的管理機制，諸如針對個資使用目的及機密類型，管理內部人員的存取權限，並定期稽核系統的防護程度與管理效能等，系統性提升對於個人隱私及資料的保護[1]。

另外，現行個資法第 5 條與新版個資法第 4 條均規定，受公務或非公務機關委託蒐集、處理或利用個人資料的團體或個人，於本法適用範圍內，視同委託機關。業者為避免因員工的違法行為以致需負擔民刑事或行政責任，亦可透過在員工聘僱契約中增訂保密義務及個資處理標準作業規則，強化對於個人資料內部使用的控管，並降低個資管理不當以致個資外洩或影響企業名譽的風險，以避免往後業務受到大幅影響，而增加運作成本及法規遵循風險。

管理 Tips

組織內員工應於簽署保密同意書前詳細閱讀內容，了解其需遵循之條款與條件，並於簽署後確實遵循。本案例中之甲簽署 A 公司之「職務上電腦處理個人資料切結書」、「保密承諾書」，即表示同意切結書與保密承諾書所規範之條款，但仍透過其職務之便不當下載、留存及查看其他員工之機密人事資料，不僅可能使 A 公司之商譽受損，更可能有意或無意的外洩員工的個人資料。組織除應要求員工確實依循政策及人員聘僱之相關條款，亦可透過存取控制與權限配置保護組織重要機密資料，例如僅授與員工執行業務最小權限並有適當的監控機制、避免員工一次可取得大量資料等，以降低公司機密檔案與個人資料外洩的風險。

[1] 新版個資法施行細則草案第 9 條第 2 項規定：「前項必要措施，應包括下列事項：一、成立管理組織，配置相當資源。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、必要之使用紀錄、軌跡資料及證據之保存。十一、個人資料安全維護之整體持續改善。」

相關標準

A.8.1.3　聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.8.2.1　管理階層責任

管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜。

A.10.10.2 監控系統的使用

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A11.1.1　存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A11.6.1　資訊存取限制

應根據所界定的存取控制政策，限制使用者與支援人員對資訊與應用系統功能之存取。

類別：資訊保護

【案號：S1000109】

銀行徵信紀錄與個人資料保護

【資料來源：臺灣高等法院 99 年度上易字 283 號判決】

焦點話題

A 銀行自民國 91 年 8 月起至 98 年 3 月止，與甲之間未具資金關係且未經甲的同意下，向財團法人金融聯合徵信中心(下稱聯徵中心)，查詢甲相關個人信用資料共計 17 次，甲主張 A 銀行違反電腦處理個人資料保護法。A 銀行則主張基於甲之姻親為該銀行內部職員，而為避免不當授信，有查詢甲信用資料之必要。

第一審法院認為在甲擔任董事、監察人或經理人的企業，與 A 銀行均未有借貸或資金往來關係下，A 銀行為確認授信限制對象，而先行向聯徵中心查詢甲之信用資料，顯然不是最小侵害手段，亦不具有必要性。因此認定 A 銀行於不同時期探知個人同一類型之資料共計 17 次，以每件侵害 2 萬元損害賠償額計算，A 銀行應賠償予甲共計 34 萬元。

第二審法院認為 A 銀行依銀行法規定，為避免不當授信，而建立相關授信限制對象之資料備查，以防範利害關係人利用銀行授信職務之便，承作不當授信，此符合電腦處理個人資料保護法第 18 條第 5 款依金融業相關法規有特別規定之情形，因此認定 A 銀行主張其向聯徵中心查詢原告甲之紀錄的行為應屬合法，廢棄第一審判決。

重點摘要

1. 銀行向聯徵中心查詢當事人的信用資料時，應注意符合法律規定的要件，並符合必要性與比例原則。
2. 銀行依銀行法規定，針對利害關係人向聯徵中心蒐集授信限制對象之個

人資料，符合現行個資法所定具有特定目的並符合法律規定的情形。

法律觀點

依電腦處理個人資料保護法(以下簡稱現行個資法)第 3 條第 7 款規定，A 銀行與聯徵中心均為適用現行個資法之非公務機關(金融業)，因此 A 銀行蒐集、處理個人資料時，必須合乎現行個資法第 18 條規定之「具有特定目的並符合其他法定要件」。本案第二審法院推翻第一審見解，認為 A 銀行依銀行法第 32 條第 1 項、第 33 條第 1 項規定[1]及財政部相關函釋[2]，金融機構依法應避免對利害關係人為不當授信、危及存款人權益，故 A 銀行向聯徵中心蒐集他人信用資料，具有法律明文規定，且合乎核貸與授信業務、授信業務管理之特定目的。再者，現行銀行法規對於銀行蒐集授信限制對象資料之情形及範圍已有明確規範，而聯徵中心提供個人授信資料予銀行業，亦屬於聯徵中心蒐集個人資料供作授信業務管理之必要範圍內，故 A 銀行查詢行為未違反現行個資法規定。

現行個資法及新修正個人資料保護法(以下簡稱新版個資法)第 1 條，均明揭個人資料保護法制目的在於「規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用」。因此，非公務機關須於特定目的下，依法律明文規定或其他法定正當事由，始得未經個人之同意，對個人資料進行蒐集處理。新版個資法將「蒐集」的定義，由現行個資法的「為建立個人資料檔案而取得個人資料」，擴大為「以任何方式取得個人資料」，以因應蒐集個資行為態樣的多樣性。

本案法院見解，對於有蒐集個人資料以建立潛在客戶名單、確認客戶資格

[1] 銀行法第 32 條第一項規定：「銀行不得對其持有實收資本總額百分之三以上之企業，或本行負責人、職員、或主要股東，或對與本行負責人或辦理授信之職員有利害關係者，為無擔保授信。」；同法第 33 條第一項規定：「銀行對其持有實收資本總額百分之五以上之企業，或本行負責人、職員、或主要股東，或對與本行負責人或辦理授信之職員有利害關係者為擔保授信，應有十足擔保，其條件不得優於其他同類授信對象，如授信達中央主管機關規定金額以上者，並應經三分之二以上董事之出席及出席董事四分之三以上同意」。

[2] 財政部 82 年 7 月 12 日台財融字第 821165024 號、85 年 12 月 17 日台融局(一)字第 85556881 號及 86 年 5 月 6 日台財融字第 86620894 號等函。

需求的機關或業者，影響不小。依法院見解反面推知，若公務機關或非公務機關不具有特定目的，並且在欠缺當事人同意或其他法律明文依據下，逕自蒐集他人的個人資料時，依現行個資法規定，被害人得以每人每一事件新台幣兩萬元以上十萬元以下計算損害賠償總額，請求損害賠償。惟基於有損害始有賠償之法理，當事人能證明之損害均得請求賠償，例外於當事人不易或不能證明其實際損害額時，始有規範賠償金額上、下限之必要。因此，新版個資法對於損害賠償總額之認定，即以實際損害額之認定為原則，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新台幣五百元以上兩萬元之金額酌定損害額[3]。

管理 Tips

組織於蒐集、處理及利用民眾之個人資料時，應符合法令法規要求的必要性以及最低限度。本案例中之 A 銀行，向聯徵中心蒐集甲之個人資料，是為防範內部員工利用銀行授信職務之便承作不當授信，符合個資法所定具有特定目的，惟 A 銀行應確保所蒐集之信用資料僅用於上述之特定目的，而不應另作他用。

相關標準

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

[3] 新版個資法第 28 條第 3 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 1 項）。……依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算（第 3 項）。」依同法第 29 條第 2 條規定，前條第 3 項規定於非公務機關亦適用之。

類別：資訊保護

【案號：S1000110】

未維護個人資料正確性的法律責任

【資料來源：臺灣士林地方法院 96 年度訴字第 1176 號民事判決】

焦點話題

本案原告甲曾為 A 銀行信用卡的持卡人，甲在民國(下同)94 年 5 月繳清消費款項後，即未再使用該卡，信用卡於 95 年 1 月到期後，也沒有再同意續發新卡。但 B 銀行於 95 年 2 月份概括承受 A 銀行信用卡之權利義務後，竟於 95 年 8 月間,以甲未依約繳納 95 年 4 月份通知的年費新台幣(下同)150 元為由，提報甲遲繳紀錄予財團法人聯合徵信中心（下稱聯徵中心），經甲告知銀行客服後亦未獲處理，造成甲在聯徵中心有事實上不存在之信用瑕疵紀錄，因而甲起訴請求名譽及信用受損的侵權損害賠償。

法院判決認為 B 銀行概括承受 A 銀行的信用卡業務,本應查證 A 銀行是否確於 95 年 1 月續發信用卡予原告甲，以及甲是否已收受並開卡使用，以確認 B 銀行對甲是否可以請求 150 元的會員年費。但 B 銀行未經詳查，貿然於 95 年 5 月向聯徵中心提報原告遲繳紀錄，自有過失，而聯徵中心蒐集金融機構間信用資料，建置個人與企業之正面與負面信用資料，因此聯徵中心的資料攸關個人信用及名譽。B 銀行因其過失，提報甲遲繳年費的訊息予聯徵中心，直接侵害及貶損甲之信用與名譽，並導致甲精神痛苦，因此判決 B 銀行應賠償甲 6 萬元。

重點摘要

1. 維護個人資料正確性為個人資料保護法賦予的義務，銀行因故意或過失，提供錯誤的個人信用資料給聯徵中心時，應負有民事侵權損害賠償責任。

2. 新修正個人資料保護法施行後，對於可歸責於銀行之事由，導致個人資料不正確時，應於更正或補充後，通知曾經提供利用之對象，即聯徵中心。

法律觀點

聯徵中心經財政部於民國 82 年指定為信用卡戶信用資料建檔機構，因此銀行及聯徵中心依現行「電腦處理個人資料保護法(以下簡稱「現行個資法」)」第 3 條，均為適用本法的金融業非公務機關，且銀行及信用報告機構對於個人財務資訊的蒐集、處理，均涉及個人姓名、身分證字號、信用卡號等足以識別特定個人的資料，其處理作業上應符合本法的相關規定。

本案當事人是依民法第 184 條第 1 項前段[1]侵權行為的規定，向 B 銀行請求損害賠償，但新修正個人資料保護法(以下簡稱新版個資法)亦課予資料蒐集機關維護個資正確性的義務，第 11 條第 1 項規定「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之」，且同法第 29 條規定「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限」。由於新版個資法對非公務機關違反本法規定致侵害當事人權利者，採推定過失責任，因此當事人若依新版個資法規定請求損害賠償，無須自行證明 A 銀行在業務處理上具有過失，而應由 A 銀行證明其維護客戶個資正確性及提報信用紀錄予聯徵中心的行為並無過失，始能免責。

再者，新版個資法第 11 條第 5 項規定，「因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象」。因此，新版個資法施行後，銀行若提供錯誤的個人信用資料予聯徵中心處理、利用，不僅對當事人負有民事損害賠償責任，銀行本身因有可歸責的事由，未主動或應當事人請求而更正、補充其個人資料時，銀行對於聯徵中心及其他利用該資料者，亦負有通知義務，否則主管機關

[1] 民法第 184 條第 1 項前段:「因故意或過失，不法侵害他人之權利者，負損害賠償責任。」

可依新法第 48 條規定，命其限期改正，未限期改正者，將面臨新台幣二萬元以上二十萬元以下的罰鍰[2]。銀行往後信用資料報送的業務運作，勢必須因應新版個資法規定，調整相關作業。

管理 Tips

新版個資法規定「公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之」，以及「因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象」。本案例中之 B 銀行應於甲告知銀行客服後即予以更正，並告知聯徵中心更正甲之信用瑕疵紀錄。B 銀行應於處理客戶之個人資料時更加謹慎，以避免稍有不慎即觸犯相關法律，造成商譽受損甚至是面臨罰責。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

[2] 新版個資法第 48 條:「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：.....二、違反第十條、第十一條、第十二條或第十三條規定。」

二、 國家機密保護法

類別：資訊保護

【案號：S1000201】

見習生疑似在網路上洩漏機密資訊 ○○部籲出面

【資料來源：中央社 100/09/01】

焦點話題

週刊報導，有○○部見習生藉處理外交機密文件之便，將獲取片段資訊張貼在社群網路上。關於此件○○部見習生疑似在網路洩漏機密資訊之事件，○○部表示這名見習生曾簽署「保密切結書」，呼籲他儘速出面說明；並會繼續清查文件，視結果決定是否採取法律行動。

這名見習生到○○部工作，時數共 100 小時，當初即簽署「保密切結書」，內容為「保證對因見習工作而知悉的檔案資料，均應負保密之責，絕無洩漏、盜取、破壞及利用電子媒體儲存等情事，並願負一切法律責任」。

○○部表示經初步清查，發現週刊所刊載的資訊屬於早已註銷機密等級的檔案，影響不大；○○部除呼籲這名見習生針對週刊所引述的資料，儘速出面說明是否屬實，也正繼續清查文件，會依據結果來決定是否採取法律行動。

重點摘要

1. 公務的機密資訊可以分成國家機密及一般公務機密。
2. 機密資訊經註銷後，雖然就不受國家機密保護法的保護，但依法令或契約負有保密義務時，仍應負有保密的義務，否則仍會有相關刑責。

法律觀點

公務人員於公務上會接觸到的機密資訊，可以分為國家機密與一般公務機

密，前者是指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經國家機密保護法核定機密等級者，後者指政府機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者，二者性質與法令依據均有不同[1]，必須予以區分。

本案例中，遭到外洩的機密資料經清查結果，屬於已註銷機密等級的檔案。所謂「註銷」機密等級，乃適用於國家機密核定有無效或得撤銷的情形，例如違反國家機密保護法第 5 條第 2 項，基於違法目的而核定者，該機密的原核定機關或其上級機關有核定權責人員可以依職權或依申請，予以註銷[2]。因此，已註銷機密等級的資料即不受到國家機密保護法的保護。另本案中的見習生有簽署「保密切結書」，會因此產生契約上的保密義務，因此如案例中外洩的資料具備機密性，可能會涉及刑法第 132 條第 3 項的罪責[3]，恐會面臨 1 年以下有期徒刑的法律責任。

機關對於保有的資料，若有保密的需求時，除了應該依照國家機密保護法核定機密等級以外，更應簽署保密協議書，以增加所屬人員應遵守保密義務的基礎，減少機密資料外洩的風險。

管理 Tips

組織內員工應於簽署保密同意書前詳細閱讀內容，了解其需遵循之條款與條件，並於簽署後確實遵循。本案例中之見習生簽署了○○部之保密同意書，即表示同意保密同意書所規範之內容，但卻將因見習工作而知悉的檔案資料張貼於網路上。組織除應要求員工確實依循政策及人員聘僱之相關條款，亦可透過就職前教育訓練，使即將到職之人員更加了解組織應保護之資訊，及其工作職務應注意與遵循之事項。

[1] 參照法務部 94 年 4 月 8 日法政字第 0940006733 號函釋。

[2] 參照法務部 95 年 1 月 11 日法政字第 0940044083 號函釋。

[3] 刑法第 132 條第 3 項：「非公務員因職務或業務知悉或持有第 1 項之文書、圖畫、消息或物品，而洩漏或交付之者，處 1 年以下有期徒刑、拘役或三百元以下罰金。」

相關標準

A.8.1.3　聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.8.2.1　管理階層責任

管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜。

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

三、 營業秘密法

類別：資訊保護

【案號：S1000301】

營業秘密之保護與競業禁止

【資料來源：臺灣高等法院民事判決 100 年度上易字第 175 號】

焦點話題

甲公司乃以從事 IC 設計及高密度記憶體產品為主要業務，並以快閃記憶體（Flash Memory）為主要產品。上訴人廖○○前任職於甲公司擔任快閃設計部經理，並曾簽署「智權歸屬暨保密合約」（以下簡稱保密合約），對甲公司負有一年競業禁止義務。嗣甲公司終止其與廖○○間之勞動契約，廖○○隨即至甲公司競爭對手乙公司任職。甲公司主張廖○○任職甲公司期間每月薪資新台幣(下同)95,000 元，並享有紅利與員工認股權外，甲公司尚發給廖○○100 萬元簽約金。且依保密合約之約定，如限制競業期間內，廖○○因遵守競業禁止條款而受有損失或喪失利益時，甲公司將提供相當於其離職時基本月薪之補償金，即設有適當之補償方式予廖○○，廖○○對甲公司負有競業禁止義務與保密義務，乃起訴請求廖○○按其違反期間於新職所得薪資之兩倍與因新職所得之所有期約利益計算之違約金，總計 2,112,200 元。地方法院及高等法院審理後，均認為廖○○違反競業禁止約定，判決應賠償 40 萬元。

重點摘要

1. 競業禁止是為了保護雇主市場上競爭的公平地位，因此，只要當事人同意，且符合一定的條件時，競業禁止約定即屬有效。

2. 競業禁止的約定，對於勞工就業之對象、期間、區域或職業活動範圍，應有合理的範疇及合理代償措施存在。

法律觀點

公司從事經濟活動，營業秘密乃是重要資產，為維護市場秩序，使公司保持市場競爭力，鼓勵公司持續研究並不斷進步，營業秘密即成為法律應該保護的客體。但是要成為法律保護的營業秘密，必須符合具機密性與有實際或潛在之經濟價值，且營業秘密所有人已採取合理之保密措施等要件[1]。因此，公司要依營業秘密法主張相關權利時，必須先舉證證明保護標的符合上開要件，且其營業秘密確實受到侵害，對於權利人保護常有不足。為了避免舉證責任帶來的不利益，公司往往會與接觸核心業務的員工約定競業禁止條款，亦即要求員工於離職後一定期間內，不可以到競爭對手的公司任職，以避免離職員工洩漏機密，產生市場上的不公平競爭。基於契約自由原則，雇主與員工間固可自由約定競業禁止條款，但因為競業禁止往往涉及到員工的工作權議題，因此在審視競業禁止條款時，即必須在兩者間取得平衡。

本案法院認為競業禁止有效要件，必須雇主的固有知識或營業祕密確有保護必要，且須視勞工或員工在原雇主或公司之職務及地位，如無特別技能、技術且職位較低，非企業之主要營業幹部、係處於弱勢之勞工，縱使員工離職後至相同或類似業務之企業任職，亦不會侵害原雇主的營業秘密。而競業禁止限制勞工就業之對象、期間、區域及職業活動的範圍，不可以逾越合理的範疇，並有填補勞工因競業禁止之損害之代償措施。由於甲公司確存有應保護的營業秘密，且甲乙兩公司主要營業項目相同，產品均為 Flash IC，互為競爭對手，且廖○○於兩家公司均是從事 Flash IC 設計，其到乙公司任職，將使甲公司秘密洩漏可能性急遽升高。而廖○○與甲公司競業禁止之限制僅有 1 年，且限制之工作對象僅為與甲公司所營業務有直接或間接競爭關係之事業，以廖○○的專業學識與工作經驗，仍可以從事競

[1] 營業秘密保護法第 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。」

業禁止業務以外的其他工作，同時若因保密合約之約定，導致生計受有重大影響，而有必要受僱於與甲公司的競爭者時，廖○○於就職前 20 日內，可以檢附書面錄取證明影本，以存證信函通知甲公司。甲公司若收到通知後，認為廖○○就任新職將影響甲公司的競爭力，可以在 14 日內以書面禁止廖○○就任新職，但應該提供廖○○自預定新職就任日起，至競業禁止期間期滿、解除或廖○○覓得其他不違反競業禁止規定的新職時為止，按照廖○○離職時基本月薪的補償金。因此本案例中競業禁止之約定，屬合理範圍內之競業禁止限制，廖○○依約未通知雇主係屬違約。法院因此判決廖○○應賠償 40 萬元。

管理 Tips

組織內員工應於簽署保密同意書前詳細閱讀內容，了解其需遵循之條款與條件，並於簽署後確實遵循。本案例中之上訴人簽署甲公司之保密合約，即表示同意保密合約所規範之條款，但仍於離職後選擇任職於為甲公司競爭對手之乙公司，此行為不只違反保密合約之競業禁止約定，也可能導致甲公司之業務機密外洩。組織除應要求員工確實依循政策及人員聘僱之相關條款，亦可透過存取控制與權限配置保護組織重要業務機密，例如僅授與員工執行業務最小權限並有適當的監控機制、避免員工一次可取得大量資料等，並且應確保於員工離職時確實移除其存取權限，降低業務機密外洩的風險。

相關標準

A.8.1.3　聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.8.2.1　管理階層責任

管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜。

A.8.3.3　存取權限的移除

所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

A11.1.1　存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A11.6.1　資訊存取限制

應根據所界定的存取控制政策，限制使用者與支援人員對資訊與應用系統功能之存取。

類別：資訊保護

【案號：S1000302】

醫療診所的病患個人資料與營業秘密

【資料來源：臺灣高等法院 99 年度上字第 807 號判決】

焦點話題

甲為 A 診所的負責人，他與 B 公司簽訂合作契約書（以下簡稱「K1 契約」），約定 B 公司提供 A 診所所需的各項軟硬體設施，包括儀器設備及電腦網路軟硬體設備，上開合作契約書並約定 B 公司提供的儀器設備電腦檔案內所留存的所有資料都是 B 公司的營業秘密，甲於契約終止後不得使用。

B 公司為了控制利益，乃由 B 公司旗下診所負責人乙與 A 診所的受雇醫師丙簽訂合作契約（以下簡稱「K2 契約」），雙方約定在合作期間丙應於 A 診所服務，且丙於 K2 契約終止時起，不得使用其所持有或知悉診所及 B 公司的營業秘密、商標或服務標章，或以任何形式標示丙為 A 診所之合作醫師，且自 K2 契約終止起 2 年內，丙不得於天母地區從事上開競爭行為。

嗣後甲於 K1 契約到期後沒有與 B 公司續約，因此搬離原地址，丙隨即於原地址開立 C 診所，並於開幕前寄發載有：「雖然稍有遲延，經過兩個月的裝修後，我們回來了！」等內容之開幕通知前 A 眼科診所的患者。乙即依照他與丙簽訂的 K2 契約，主張丙違反營業秘密及競業禁止的約定，向法院請求損害賠償。高等法院審理後，判決丙應賠償 50 萬元。

重點摘要

1. 對於可能會接觸營業秘密者，至少應簽署保密契約，賦予其保密義務並有保密措施，同時可以透過競業禁止的約定，確保相關人員不會以利用所悉機密從事競爭行為。

2. 有效的競業禁止約定，必須有值得保護的利益存在、約定的競業期間及

地區具合理性，且不危經濟生存能力。

法律觀點

本案件的主要爭點在於 A 診所病患個人資料是否屬於營業秘密，以及雙方競業禁止約定是否有效。所謂營業秘密，依營業秘密法第 2 條[1]規定，係指方法、技術、製造、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「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」。除了上述營業秘密法的規定外，企業於經營活動中，為保護自身之營業秘密，對於可能接觸營業秘密之人，可以另外簽署保密契約約定接觸者之保密義務，而其所約定應遵守之保密義務，本於契約自由原則，無須與營業秘密法所定義之營業秘密完全一致，惟仍應具備明確性及合理性。

法院認為根據甲與 B 公司簽署的 K1 契約,B 公司提供的儀器設備電腦檔案內所留存的所有資料為營業秘密，而甲於契約終止後即不可以使用。A 診所所蒐集的病患個人資料，是病患於就診時經診所人員登入 B 公司提供的電腦系統後，由 B 公司授權相關人員依權限登入使用者密碼才能讀取，丙是因為到 A 診所服務才能登入軟體系統取得病患個人資料，因此病患個人資料屬於丙與乙簽署 K2 契約中的「營業秘密」。

至於競業禁止部分，法院認為一般人在大都會就醫會有區域性，乙為確保他在天母地區經營診所的優勢，有與丙約定競業禁止的利益存在，且依照社會一般觀念與商業習慣，約定 2 年的競業期間應屬合理適當，且沒有危及丙的經濟生存能力。丙在原 A 診所地址開立 C 診所，並向原 A 診所病患寄發開幕通知，顯然是利用 A 診所與其病患間的醫病關係來開發 C 診所的病患，有違誠信。

[1] 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。」

法院基於上述理由，判決丙應賠償乙 50 萬元。由此案例可知，透過契約的約定及對營業秘密的管控措施，例如權限控管，可以賦予所屬人員對營業秘密負保密義務。同時，為避免所屬人員利用其於職務所悉機密從事競爭行為，應同時約定競業禁止條款，使營業秘密可以獲得更周全的保護。此外，本案例中涉及的病患資料，乃是 A 診所基於醫療目的所蒐集，屬於受到個資法的客體，因此丙利用病患資料必須符合個資法得蒐集、處理或利用之情況，並應依法盡告知義務，併予說明。

管理 Tips

組織應於員工到職時要求其簽署保密同意書，使其了解所需遵循之條款與條件，並確保其於簽署後確實遵循。本案例中之丙與乙簽訂 K2 契約，即表示同意合作契約所規範之條款，但卻違反 K2 契約內之競業禁止約定，同時還利用在 A 診所任職時獲悉之 B 公司營業秘密及客戶資料。組織除應要求員工確實依循政策及人員聘僱之相關條款，亦可透過存取控制與權限配置保護組織重要業務機密，例如僅授與員工執行業務最小權限並有適當的監控機制、避免員工一次可取得大量資料等，並且應確保於員工離職時確實移除其存取權限，降低業務機密外洩的風險。

相關標準

A.8.1.3　聘僱條款與條件

身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.8.2.1　管理階層責任

管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜。

A.8.3.3　存取權限的移除

所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

A11.1.1　存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A11.6.1　資訊存取限制

應根據所界定的存取控制政策，限制使用者與支援人員對資訊與應用系統功能之存取。

類別：資訊保護

【案號：S1000303】

智慧財產案件與秘密保持命令

【資料來源：最高法院 99 年度台抗字第 133 號民事裁定】

焦點話題

A 公司在對 B 公司的假處分程序中，對外發布 B 公司涉嫌侵害其智慧財產權的言論，B 公司認為 A 公司的行為已違反公平交易法，向智慧財產法院提起損害賠償訴訟。在訴訟過程中，B 公司基於訴訟的需要，於民事陳報狀中提出了所販售產品的規格、品質及客戶名稱等資訊，並主張該等資訊涉及 B 公司的營業秘密。為了避免該營業秘密被開示，或作為訴訟以外其他目的使用，導致妨害 B 公司的事業活動，B 公司聲請對 A 公司及其律師甲、法務人員乙、工程師丙及產品經理丁等人核發秘密保持命令。除此之外，B 公司還向法院聲請限制產品經理丁閱覽相關資料，並禁止甲、乙、丙及丁等四人影印、抄錄及攝影相關資料。

在本案中，法院雖核准秘密保持命令，但認為並無另外限制甲、乙、丙及丁等人閱覽、影印、抄錄及攝影的必要，所以否准 B 公司這個部分的請求。

重點摘要

1. 在智慧財產案件審理過程中，為防止書狀內容記載或證據涉及的營業秘密被公開揭露，或被用於訴訟以外之其他目的，當事人或第三人可以向法院申請核發「秘密保持命令」。
2. 法院在審理是否准予核發秘密保持命令時，聲請人必須自行向法院釋明核發秘密保持命令的理由，再由法官依法審酌聲請是否確實必要。

法律觀點

依照智慧財產案件審理法第 11 條第 1 項的規定，若當事人書狀的內容，記載有當事人或第三人之營業秘密，或已調查或應調查之證據，涉及當事人或第三人之營業秘密者，為避免上述營業秘密因訴訟程序採公開審理程序而被公開揭露，或被使用於該訴訟進行以外之目的，妨害該當事人或第三人基於該營業秘密從事之事業活動，而有限制其揭露或使用的必要時，當事人或第三人可聲請法院對相關訴訟關係人核發「秘密保持命令」。受秘密保持命令之人，不得將該營業秘密用於該訴訟以外之目的，或是對未受秘密保持命令的人揭露該營業秘密；如違反秘密保持命令，將可處三年以下有期徒刑、拘役或併科新台幣十萬元以下的罰金[1]。

A 公司主張 B 公司所提出的資料具有專業性，A 公司需要指派專利工程師、法務人員、產品經理及律師一同聲請閱覽研究處理，始能解析 B 公司所提出的資料是否真實。法院認為 A 公司及甲、乙、丙及丁等人接觸上揭訴訟資料後，可能會將之用於訴訟以外之目的、或對未受秘密保持命令之人揭露，故核准 B 公司聲請對上述人等核發秘密保持命令。

然而，本案涉及營業秘密的資料不僅內容複雜而具專業性，並且和產品行銷有關，其中涉及產品規格及品質之行銷數據內容繁多，若要求甲、乙、丙及丁等人在短時間內閱覽相關訴訟資料並即時查證其真實性，實為強人所難。再者，法院既已准許對甲、乙、丙及丁四人核發秘密保持命令，他們即不得將相關資料用於該訴訟以外之其他目的，或對未受秘密保持命令之人揭露，如此已足夠保護 B 公司的營業秘密，實毋須再限制甲、乙、丙及丁等人閱覽、影印、抄錄及攝影相關資料，否則反而侵害當事人平等訴訟的權利。因此，最高法院駁回 B 公司的抗告。

管理 Tips

本案例中 B 公司擔憂因訴訟使其營業秘密被揭露，導致其權益受損，而提出限制 A 公司人員閱覽、影印、抄錄及攝影相關資料之要求。惟法院已核

[1] 參照智慧財產案件審理法第 35 條第 1 項規定。

准 A 公司受到秘密保持命令之限制，不得將 B 公司的營業秘密洩漏予未受秘密保持命令限制之人，或作為訴訟以外其他目的使用，故即便 A 公司人員將相關資料影印攜出，仍不可作產品設計或開發等之用，保障了 B 公司之權益。

相關標準

A.6.1.5　機密性協議

宜識別與定期審查反映組織對資訊保護之需求的機密性或保密協議要求。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

四、 刑法

類別：資訊保護

【案號：S1000401】

洩邱○○個資　前銀行襄理被判六月

【資料來源：自由時報 100/05/07】

焦點話題

某銀行襄理沈○○被控洩密，私自下載某機關前秘書長邱○○的銀行帳戶個資，被懷疑與某黨籍立委在巴紐案爆發期間開記者會，所公布邱○○信用卡刷卡帳單有關，最高法院依妨害電腦使用罪，判處沈○○六月有期徒刑確定、可易科罰金。

庭訊時，沈○○辯稱，97 年 6、7 月間下載邱○○等客戶個資，安裝在自己硬碟中，是為了方便開發建置的系統進行壓力測試，測試後他就把資料刪除，並非刻意下載邱○○個資，也無意非法取得客戶的電腦資料。

合議庭不採信沈○○辯辭，認為沈下載邱○○等客戶信用卡資料，轉檔為樂曲的 MP3 檔案，並將檔案命名為「牧笛.mp3」、「冬季下雪.mp3」，如沈○○真為測試而下載個資，不須將檔案存為 MP3 格式，顯示沈○○確有掩飾非法下載意圖，沈○○的行為嚴重損害該銀行商譽和信用，犯後還推卸責任，雖已被該銀行開除，仍應予判刑。

重點摘要

1. 無故取得他人電腦內的電磁紀錄，導致他人受到損害時，將觸犯刑法妨害電腦使用罪章之無故取得電磁紀錄罪。
2. 員工有類此行為，不但構成勞動基準法所規定的解雇事由，雇主也可能與員工承擔連帶民事賠償責任。

法律觀點

所謂電磁紀錄[1]，是指電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄，因此存放在電腦裡的資料，例如文字檔、虛擬寶物等，均屬於刑法規範的電磁紀錄。

刑法第 359 條[2]之立法目的係防範一般人在沒有正當理由之情況下，取得、變更或刪除他人電腦或其相關設備的電磁紀錄，導致公眾或他人受到損害之情形。若違反前述規定，將面臨 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。

以本案為例，該銀行襄理利用維護銀行系統之便，而無故取得銀行系統中之客戶金融資料並提供予第三人且從媒體上被揭露，其行為除符合前揭刑法規定行為外，並造成客戶損害。

該銀行襄理職務上不法行為，於民事責任上，除符合勞動基準法第 12 條第 1 項第 4 款[3]雇主得予解雇外，並因此對該客戶有民事賠償責任。同時，銀行因該銀行襄理之行為並有連帶賠償責任[4]。至於，銀行是否得主張其已盡監督管理責任而得免負連帶賠償責任，則需由銀行負舉證責任。

管理 Tips

金融機構擁用大量個人資料，稍有不慎即可能被誤用或遭有心人士利用，一旦造成損害，不僅主管機關會究責處罰，更會影響商譽。因此在資料庫

---

[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 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 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

[3] 勞動基準法第 12 條第 1 項第 4 款：「違反勞動契約或工作規則，情節重大者」雇主得不經預告終止契約。

[4] 民法第 188 條規定：「受僱人因執行職務，不法侵害他人之權利者，由僱用人與行為人連帶負損害賠償責任。但選任受僱人及監督其職務之執行，已盡相當之注意或縱加以相當之注意而仍不免發生損害者，僱用人不負賠償責任。
如被害人依前項但書之規定，不能受損害賠償時，法院因其聲請，得斟酌僱用人與被害人之經濟狀況，令僱用人為全部或一部之損害賠償。
僱用人賠償損害時，對於為侵權行為之受僱人，有求償權。」

與資訊系統均應有妥善之安全管理，並且應配置適當之監控機制，發現資料被不當存取時應立刻通報，即時處理。而平時定期的資訊安全教育訓練亦不可或缺，應使全員瞭解資訊安全觀念及可能面臨之法律責任。在資料存取控管之相關技術與管理，應具備組織整體安全規劃之全景，以達成有效管理之目標。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.10.2 監控系統的使用

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A.11.2.4　使用者存取權限的審查

管理階層應定期使用正式過程審查使用者的存取權限。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000402】

屋主槓上社區 裝 12 支監視器擾鄰

【資料來源：東森新聞 100/05/26】

焦點話題

在花蓮某社區，有一別墅之屋主在自家牆上掛滿了布條，上面寫了辱罵字眼，底下箭頭畫左又畫右。而原因漆在車庫鐵門上，是因為某天深夜鄰居故意製造噪音，還出口辱罵自己。除掛布條外，屋主還裝了監視器，監視鄰居一舉一動。一間房子裝了 12 支監視器，其中有 4 支分別裝在大門二和三樓左右邊，監視鏡頭就正對著左右鄰居的窗戶，主機裝在自家客廳裡，公然侵犯他人隱私，鄰居抗議，卻不見改善。

監視器一裝就是兩年，弄得鄰居住不下去，告上法院，雖然屋主向法官表示，是因為房子被潑漆破壞，才裝監視器保護自己，還是被依妨害秘密罪章中之無故竊錄非公開活動罪，判刑 2 個月。

重點摘要

1. 居家生活屬於個人非公開的活動，沒有正當理由而侵犯時，應該負相關法律責任。
2. 為了保護自己權利而不得不侵害他人隱私時，手段必須在一般合理客觀的社會通念所能夠忍受的範圍，否則仍將負有相關刑事責任的風險。

法律觀點

隱私權雖非憲法明文列舉之權利，但基於人性尊嚴、保障個人生活私密領域免於受到他人侵擾及個人對於自身個人資料之自主控制，應受憲法第 22 條之保障，此可以參考大法官釋字第 603 號解釋之意旨。刑法第 315 條以

下之妨害秘密罪章，即為隱私權保護之具體法規範，目的是為了保護個人自我事務的秘密性，防止他人使用不當侵入方法而侵犯個人秘密事務，因此若故意侵犯他人之隱秘、獨處及私人事務，如侵犯行為已經超越一般合理客觀之社會通念所能忍受的範圍時，即屬於無正當理由侵犯隱私，均為法律所禁止。

本案例中屋主架設 12 支監視器對著鄰居拍攝，其中 4 支監視器正對著鄰居的窗戶，可以拍得鄰居之生活起居狀況，因此屋主的行為可能涉嫌觸犯刑法第 315 條之 1 第 2 款之妨害秘密罪[1]。此罪名是以「無故」竊錄他人「非公開行為」為要件，因此若是行為人具有正當理由或涉及的內容屬於他人的公開活動時，即不會構成犯罪。

首先，依照一般社會通念，個人的居家生活並非公開行為，而且案例中鄰居曾多次向屋主抗議，可見鄰居並無公開自己室內居家生活的意思。其次，所謂「無故」即指無正當理由，理由是否正當應依照日常生活經驗法則，從客觀事實上加以判斷，本例中屋主抗辯是「為了保護自己」而主張架設監視器具有正當理由，但如此一來，監視器應該是對著曾被潑漆破壞的外圍屋牆，並非可以拍到鄰居起居生活的窗戶，屋主的行為明顯逾越保護自身及住家安全之程度，顯非一般社會通念所能接受，因此屋主的行為不具正當理由。

基於以上理由，法院認為屋主之行為違反刑法 315 條之 1 的妨害秘密罪，並判處 2 個月有期徒刑。因此，若為了保護自己的權利而不得不侵害他人隱私時，手段必須在一般合理客觀的社會通念所能夠忍受的範圍，否則仍將負有相關刑事責任的風險。

管理 Tips

[1] 刑法第 315 條之 1：「有下列行為之一者，處 3 年以下有期徒刑、拘役或 3 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。」

自從個人資料保護法通過後，個人相關資訊與資料之保護已涵蓋全國所有機關、組織與民眾，個人居家生活之影音資料亦屬個人資料，不可被不當蒐集、處理及利用。本案例中除了架設監視器攝錄鄰居行動時未注意已觸犯法令，須負擔刑事責任外，在被拍攝的一方亦可考慮如何強化安全措施以保護個人資訊。

相關標準

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000403】

疑妻外遇 送手機監控行蹤

【資料來源：蘋果日報 100/07/14】

焦點話題

許○○婚後見妻子時常與不明對象通話，認為她有外遇，決定掌握她日常行蹤及交往對象，遂在聖誕節前，買一支全新手機後再請通訊行改裝，設定新手機每次只要一撥話，就會同時發送一則簡訊到其手機，再買衛星定位追蹤裝置裝在妻子車內。

許○○自以為神不知鬼不覺，卻多次在掌握妻子密集通話給同一對象後，忍不住試探其妻口風，致妻子起疑，向電信公司調閱通聯紀錄才揭發。許妻也懷疑自己車子可能也被動手腳，檢查後發現被裝衛星定位追蹤裝置，憤而提告。

檢方調查認為，雖是夫妻但也不能利用設備窺視妻子非公開活動，考量許○○坦承犯行後，處以一年緩起訴，但須向指定的公益或自治團體捐款三萬元。

重點摘要

1. 對於他人非公開之活動，未經當事人同意且沒有正當理由的情況下利用工具或設備竊聽、窺視或竊錄，將觸犯刑法 315 條之 1 妨害秘密罪。
2. 配偶權之行使，必須注意隱私權的界線，以免觸法。

法律觀點

刑法第 315 條以下的妨害秘密罪章，為隱私權保護之具體法規範，目的乃是為了保護個人自我事務的秘密領域範疇，防止他人使用不當的手段及方法侵犯個人秘密事務。

本案中，許○○先購買改裝的手機給妻子，設定手機一撥話就會同時發送一則簡訊到許○○的手機裡，另外購買衛星定位追蹤裝置裝在妻子的車內，以掌握妻子的通話及行蹤。當妻子手機撥話時，系統會自動發送訊息到許○○的手機，許○○即可藉此得知妻子撥出的電話號碼，以掌握妻子以電話常聯絡之對象。由於一般大眾使用手機撥打的電話號碼與通話對象，僅有撥打方與受話方可以知悉，因此應該屬於非公開的活動，而應受到法律的保護。另外除非法律有特別規定外，個人享有行動的自由，許○○將衛星定位追蹤裝置裝設在妻子車內，無異可以隨時掌控並追蹤其從事的非公開活動，應屬於以電磁紀錄竊錄他人非公開之活動，因此在沒有正當理由的情況下，依刑法第 315 條之 1 規定[1]， 最重可處 3 年以下有期徒刑、拘役或 3 萬元以下罰金。

另我國刑事訴訟法考量司法資源的有效利用與犯罪情節的刑罰必要性，於該法第 253 條之 1 規定被告所犯為死刑、無期徒刑或最輕本刑三年以上有期徒刑以外之罪，經檢察官斟酌認為案情輕微且被告有悔意時，可為緩起訴之處分，亦即被告只要在緩起訴期間沒有故意犯罪的行為，檢察官即不會起訴被告。本案檢察官衡量犯罪情節與許○○坦承犯行之情況，給予一年期間的緩起訴處分，但須向指定的公益或自治團體捐款三萬元。

值得注意的部分在於，配偶之間依法雖然互負忠誠義務，但是並非即可以作為監控或追蹤他方活動的正當理由，因此，在行使配偶權利時，亦應注意隱私權的界線，避免惹禍上身。

管理 Tips

本案例中之許○○透過裝設竊錄或定位追蹤設備窺視妻子的非公開活動，明顯侵害妻子之個人隱私。許○○應在其裝設竊錄或定位追蹤設備前，即針對所可能面臨的法律議題進行探討，清楚辨識其所需遵循的法令法規以及所

[1] 刑法第 315 之 1 條：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：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。」

需擔負之法律責任，進而確認其行為的合法性，以避免違反相關法規及侵害他人隱私。

相關標準

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000404】

冒名上網爆料 國防部前官員被訴

【資料來源：中國時報 100/08/21】

焦點話題

前國防部整合評估室 A，因不滿國防部對於上校 B 擅將有極機密資料的公務筆電攜出營區，懲處太輕，涉嫌多次冒用他人名義上網向行政院長電子信箱爆料，經憲兵隊查獲送辦，台北地檢署依偽造文書罪起訴。

國防部整合評估室上校 B，將公務用筆電攜出營區，事後國防部雖懲處 B，但不久，就有人到公館郵局寄掛號信給國防部長，控訴 B 與包商員工共謀違規將筆電攜出營區，甚至十七次以電子郵件寄至總統府、行政院長信箱爆料。爆料內容指稱 B 將有建軍計畫、兵力部署及反登陸作戰等極機密資料的筆電，偷攜出營區，拿到醫院、餐廳等公共場所展示、複製，機密資料恐遭網路攔截。

國防部總政治作戰局軍事安全總隊指示憲兵隊調查，經調閱公館郵局監視器畫面，發現 A 當天曾進郵局寄信，比對掛號信上的字跡，認與 A 相符，以及部分電腦 IP 地址亦與他有關，認定是 A 所為，依偽造文書、妨害名譽將 A 移送北檢。

重點摘要

1. 冒用他人名義寄發掛號信及電子郵件，將觸犯刑法偽造文書的罪名。
2. 國家機密保護法為刑法的特別規定，若行為同時違反者，將優先以國家機密保護法論處。

法律觀點

本案例中 A 冒用他人的名義，以掛號信及電子郵件進行爆料，乃屬於無製作權而冒用他人名義製作文書的狀況，且因電子郵件屬於刑法定義的「準文書」[1]，因此 A 偽造掛號信及電子郵件的行為，涉嫌違反刑法第 210 條的偽造私文書罪，依法可以處 5 年以下有期徒刑[2]。另外 A 將爆料信件寄送給國防部長、總統府及行政院長信箱等處爆料，乃是散布給特定多數人，若 A 無法證明其爆料內容為事實時[3]，將會構成刑法第 310 條第 1 項誹謗罪[4]。

在 B 的部分來說。若 B 確有將建軍計畫、兵力部署及反登陸作戰等極機密資料的筆電攜出營區，拿到公共場所展示並複製時，若上開資料經過國家機密保護法核定機密等級，且保密期限未屆至或解密條件未成就時，B 的行為將違反國家機密保護法第 32 條[5]的規定，恐有 1 年以上 7 年以下有期徒刑的刑責。另外刑法第 109 條「洩漏交付國防秘密罪」[6]，其保護的客體為「關於中華民國國防應秘密之文書、圖畫、消息或物品」，因此上述建軍計畫、兵力部署及反登陸作戰亦屬於國防應秘密文書，因此 B 洩漏該等資料的行為亦涉嫌違反刑法第 109 條第 1 項的規定，但因國家機密保護法為刑法的特別法，所以 B 同時違反二者規定時，將優先以國家機密保護法論處。

管理 Tips

本案例中之爆料者除涉及誹謗他人，更冒用他人名義進行不法事宜，爆料者應需針對其行為，清楚地辨識其所需遵循的法令法規。個人之言論自由應被限制在合法的範圍內，針對他人的文字應避免誹謗或捏造事實等，不

[1] 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。」

[2] 刑法第 210 條：「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。」

[3] 刑法第 310 條第 3 項前段：「對於所誹謗之事，能證明其為真實者，不罰。」

[4] 刑法第 310 條第 1 項：「意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處 1 年以下有期徒刑、拘役或五百元以下罰金。」

[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 1 年以上 7 年以下有期徒刑。」

[6] 刑法第 109 條第 1 項：「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 1 年以上 7 年以下有期徒刑。」

應隱身於網路匿名性的保護傘下，而踰越法律的規範。

相關標準

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000405】

市府洩密 民眾投訴遭嗆

【資料來源：蘋果日報 100/10/05】

焦點話題

民眾爆料投訴台中市府市長信箱○○局李姓官員執行電梯檢查時，態度不佳，結果隔了三天後李姓官員竟來電指責並嗆要對質，痛批市府根本沒有保障投訴人權益及人身安全。市府坦承投訴案未以密件控管，確實有疏失，將進行內部檢討，對李姓員工的不當行為，也會予以懲處。

投訴民眾指出市府大樓申請電梯檢查，李姓官員一來就猛打官腔，不斷對其它等非檢查項目挑毛病，口氣和態度都很差。他氣不過到市長信箱留言投訴，但過了三天，卻接到李姓官員來電，指他投訴內容不是事實，還嗆說要找當時也在場的設備廠商來對質；民眾質疑，市長信箱明明寫著「檢舉郵件之檢舉人資料將採保密方式處理」，為何他的資料會洩漏，讓對方打電話來嗆聲，造成二度傷害。

市府人員指出，這起個案是未列為密件，可能在公文處理流程中，被李姓員工發現，才會發生打電話給投訴人對質的不當行為，但絕無透露投訴人的資料。研考會則表示，投訴人的資料應嚴格保密，發生這種事情確實非常不當，將會進行檢討。

重點摘要

1. 對於陳情人之姓名及電話，為避免危及陳情人之安全，並衍生不必要困擾，行政機關應有保密義務[1]。此一保守機密義務，不因該陳情案件處

[1] 本案中為台中市府之案例，依臺中市政府及所屬機關處理人民陳情案件作業要點第 5 條：「民眾檢舉或陳情案件有保密必要者，應以保密方式處理，不得公開。」

理完畢而結束。

2. 人民陳情函等文件之內容若涉及政府機關職掌必要範圍，是否有公開之必要雖屬行政裁量之範圍，但是對於陳情人本身之個人資料應予以保護。

法律觀點

民眾投書政府機關，該投書之內容雖屬政府機關職掌之範圍，但是為了保障陳情人之權益與避免陳情人因投書而受到不利之對待，政府處理民眾投訴之信箱多會註明「檢舉郵件之檢舉人資料將採保密方式處理」，明示會確保陳情人之個人資料不會因此外洩與因此受到不利之對待，有此保障方能使民眾暢所欲言，勇於表達對於政府機關之意見。

依照刑法第 132 條之規定[2]，公務員洩漏或交付國防以外應秘密之文書、圖畫、消息或物品，將處三年以下有期徒刑，若是過失洩漏或交付，亦將處一年以下有期徒刑。因此，本案例應探討的是「檢舉人之資料」是否屬於前述刑法第 132 條規定之應秘密事項。依行政程序法第 170 條第 2 項[3]即規定機關受理人民陳情案件有保密之必要時，應不予公開。另依照行政機關訂定的處理人民陳情案件要點[4]，均規定對於人民陳請案件若有保密之必要者，應以保密方式處理。因此，對於人民陳情案件有必要時，公務員依法負有保密義務。有問題者在於，「檢舉人之資料」是否有保密的必要。由於是否必要，乃屬於不確定法律概念，因此在個案上將會有行政裁量的空間。若在個案的案件事實中，若「檢舉人之資料」負有保密之必要時，將屬於上述刑法第 132 條所指的應秘密事項，相關公務員因故意或過失洩漏

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

[3] 行政程序法 170 條第 2 項：「人民之陳情有保密必要者，受理機關處理時，應不予公開。」

[4] 如：行政院暨所屬各機關處理人民陳情案件要點第 18 條：「人民陳情案件有保密之必要者，受理機關應予保密」、臺中市政府及所屬機關處理人民陳情案件作業要點第 5 條：「民眾檢舉或陳情案件有保密必要者，應以保密方式處理，不得公開」等。

或過失交付資料時，即可能會面臨刑事責任。

綜上所述，公務人員在處理人民陳情案件時，應特別注意陳情資料是否有保密的必要，若有保密的必要時，應注意採取保密措施，否則可能會有刑事責任的風險。

管理 Tips

組織應依據法令法規或實務所需，評估資料對於組織之價值以及其受到侵害或被揭露等，對組織的風險及衝擊，並建立適當之分類分級以及管控機制，保護組織內所持有之民眾個人資料，例如與民眾隱私相關之資訊，應列為敏感或機密文件。在處理與他人隱私相關之資料時應更加謹慎，避免因組織人員之疏失或管理機制的不足，導致民眾之隱私受到侵害，進而影響民眾對組織之觀感及信賴度。

相關標準

A.7.2.1　分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000406】

天才駭客破解悠遊卡 盜刷 39 元

【資料來源：蘋果日報 100/09/28】

焦點話題

警方調查，嫌犯吳○○是○○科技公司資訊安全顧問，獨自在北市租屋，他破解悠遊卡加值系統並盜刷消費，新聞披露後，他未到公司，也沒回租屋處。

悠遊卡公司報案，指稱悠遊卡疑遭竄改儲值於超商盜刷，立即將消費紀錄及疑似歹徒的監視器畫面交給警方。警方循線鎖定吳嫌，隔天趁吳○○進入超商刷悠遊卡買早餐時將他逮捕。

吳○○供稱，悠遊卡設計四道加密防護機制，發行公司曾號稱「絕對不可能被破解」，他為了挑戰不可能，歷經四個月埋首研究、重寫程式，終於破解成功，可用自製讀卡機為悠遊卡竄改加值。吳○○以自製讀卡機加值 300 元，陸續持悠遊卡盜刷消費 6 次、共 608 元，扣除他卡片中原本的 569 元，不法所得僅 39 元。

吳○○隨後被依違反《電子票證發行管理條例》、詐欺等罪嫌移送偵辦，最重恐面臨十年徒刑。由於吳○○向檢方認罪，坦承只是為了試卡挑戰，絕無販售牟利意圖，遭請回候傳。

重點摘要

1. 電子票證乃是以電子、磁力或光學形式儲存金錢價值，並含有資料儲存或計算功能之晶片、卡片、憑證或其他形式之載具，以作為多用途支付之使用工具，悠遊卡即屬於電子票證之一種。
2. 破壞悠遊卡防護機制而進行加值，可能會構成電腦詐欺罪而有刑事責

任。

法律觀點

依電子票證發行管理條例第 3 條之規定，電子票證是指以電子、磁力或光學形式儲存金錢價值，並含有資料儲存或計算功能之晶片、卡片、憑證或其他形式之載具，作為多用途支付使用之工具。悠遊卡可以晶片方式儲存金錢價值，並且在台灣已可普遍用於便利商店、特定商店、台北捷運系統以及特約停車場作為支付工具，故具有多用途支付之功能，屬於電子票證之一，適用電子票證發行管理條例之規定。

悠遊卡的儲值系統，一般而言有四道關卡，即：所有的票卡都有防護的金鑰密碼、每張票卡皆有獨一性之金鑰、交易當下有防偽的驗證碼以及交易後可經由後台判斷是否異常等四個關卡。本案中吳○○乃是透過改寫程式破解悠遊卡的金鑰密碼，再以自己之讀卡機作加值的動作。

電子票證發行管理條例第 30 條[1]雖然對於偽造或變造電子票證有刑責規定，但該條是以「電子票證」為客體，因此著重電子票證之形式更改，強調「無中生有」的財產價值或以「改變外型」為必要，因此單純修改程式或破解密碼所造成之機器判讀錯誤，應不構成電子票證發行管理條例第 30 條的要件。

依照刑法第 339 條之 3 第 1 項之規定：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處七年以下有期徒刑。」此案例中，吳○○為破解悠遊卡防護系統自行撰寫程式，使其可使用自製讀卡機為悠遊卡竄改加值，因此成功盜刷 6 次共消費 608 元，扣除自己儲值之金額，不法所得為 39 元，應屬於以不正方法將虛偽資料輸入電腦設備，不法取得儲

[1] 電子票證發行管理條例第 30 條 1 項：「偽造、變造或未經主管機關核准發行本條例所規定之電子票證者，其行為負責人處一年以上十年以下有期徒刑，得併科新臺幣一千萬元以上二億元以下罰金。其犯罪所得達新臺幣一億元以上者，處七年以上有期徒刑，得併科新臺幣二千五百萬元以上五億元以下罰金。」

值金額，並成功使用悠遊卡完成盜刷而取得財物，應會構成上開刑法第 339 條之 3 第 1 項之電腦詐欺罪。值得注意的是，吳○○辯稱寫程式破解之目的在於挑戰悠遊卡，想把破解經驗當作資安教材，此部份會涉及其是否有「不法所有之意圖」，由於吳○○於破解悠遊卡後乃持卡片進行消費，仍取得不法財物，因此能否抗辯其無不法所有意圖，可能須視吳○○的舉證狀況。另外吳○○為提升駭客技術，和同伴常入侵大小公司系統，將會違反刑法第 358 條以下的妨害電腦使用罪的相關罪名，併予說明。

管理 Tips

悠遊卡之儲值系統共有四道防護機制，本案例之破解者乃針對防護機制中的金鑰密碼進行破解，而悠遊卡發行公司係於結算後將交易資料回傳後台查核時，發現破解者消費的異常交易量。

故本案例可就以下兩方面討論之：

1. 對悠遊卡發行公司：外來之惡意攻擊或破解難以防範，組織應有更強大的保護措施加以防堵。未來可評估票卡之防護金鑰密碼及卡片基碼數目，並於進行變更或新票卡開發時加強金鑰管理，降低金鑰被破解的風險以及其可能對組織營運造成的影響。
2. 對案例中之破解者：應需針對其行為，清楚地辨識其所需遵循的法令法規，避免因個人因素導致觸犯法律之行為。

相關標準

A.12.1.1　安全要求分析與規格

新資訊系統或現有資訊系統提升的營運要求聲明中，應詳述安全控制措施的要求。

A.12.3.2　金鑰管理

應備妥適當的金鑰管理，以支援組織使用密碼技術。

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

五、 醫師法

類別：資訊保護

【案號：S1000501】

護士將病患剖腹照發布上網 被罰 1 萬 2 停業 1 個月

【資料來源：中廣新聞網 100/07/13】

焦點話題

新北市○○醫院傳出有護士將剖腹受傷民眾的照片發布在社交網站上，還加註好久沒看到她喜歡的人體，甚至寫上「自行拉出腸子酷」等不當字句，引發網友圍剿她沒有職業道德，消息一出○○醫院馬上展開調查，找到這名護士。醫院表示該護士對自己的行為相當後悔，○○醫院公關主任也說，根據醫院的倫理規範，會對她予以重懲。

新北市衛生局表示，這名護理人員在未尊重病患隱私情況下，逕自將照片及對病患狀況的敘述放置在個人社交網站上，已經涉及違反護理人員法第 28 條洩漏秘密的規定，衛生局心理衛生及長期照顧科科長黃○○表示，將對她處以 1 萬 2 的罰鍰，另外針對該護士違反同法的第 35 條業務上的不正當行為部分，衛生局給予停業一個月的處分。

重點摘要

1. 護理人員對於因業務而知悉或持有的他人秘密，不得無故洩漏。
2. 護理人員有洩漏因業務知悉或持有他人秘密之不當行為時，最重恐會面臨廢止執業執照的處分。

法律觀點

一般人的醫療病歷紀錄通常是屬於隱密性且不欲人知的敏感資料，為建立醫病間之信賴關係，醫療從業人員除須遵守相關職業倫理規範外，相關法

令皆有保密義務之一般規定，例如醫師法 23 條[1]、護理人員法 28 條[2]及刑法 316 條[3]等，均對醫療從業人員作出保密的要求，醫師或護理人員對於因業務所知悉或持有的秘密資料，例如病情或健康資訊，只有在病人明示同意或法律有明文准許的情況下，始可被公開，否則恐會因為違反保密義務，而受到行政懲處，並負相關法律責任。

本例中，護士在沒有經過當事人同意，或符合法律明文規定之情況下，逕自將病患剖腹受傷的照片公布在個人的社群網站上，是屬於洩漏因業務持有他人秘密的行為，違反護理人員法第 28 條的規定，且此行為屬於違法的不正當行為，依護理人員法 35 條之規定[4]可處一個月以上一年以下之停業處分，情節重大者，得廢止其執業執照。據此，主管機關即對護士作出罰緩 1 萬 2 千元暨停業 1 個月的處分。

醫師及護理人員的保密義務，乃是為了保障病患就診隱私，並藉以建立雙方信賴機制，如此一來，病患才能放心透露完整的個人資訊，並接受必要的診療行為，進而健全我國醫療體制。因此，醫療人員必須確實遵守保密義務，並注意自身言行，避免不當行為，否則最嚴重可能會面臨廢止執業執照的處分。

管理 Tips

在此案例中法令已有明確地規定病歷內容屬於應保密的範圍，所以就管理面而言，組織應在初期便對其人員可能接觸的所有資料進行機密等級之判定，尤其針對受法令規範部分，並將判定結果清楚宣達予所有可能接觸資料的人員，使所有人員瞭解其所應擔負之責任；另在案例中有提及實體病

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

[2] 護理人員法第 28 條:「除依前條規定外，護理人員或護理機構及其人員對於因業務而知悉或持有他人秘密，不得無故洩漏。」

[3] 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。」

[4] 護理人員法第 35 條：「護理人員於業務上有違法或不正當行為者，處一個月以上一年以下之停業處分；其情節重大者，得廢止其執業執照；其涉及刑事責任者，並應移送該管檢察機關依法辦理。」

歷出現於記者會中的部分，組織應可就實體文件的保存再行加強。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：S1000502】

病歷當便條紙 ○○醫院洩隱私

【資料來源：聯合報 100/08/05】

焦點話題

一名民眾到台北市立○○醫院服務台，詢問就醫資訊時，志工給他的便條紙背面竟有另一名病患在眼科的就醫資料，姓名、年齡、體重、病歷號、就診科別及診斷結果等，資訊都清清楚楚，病患隱私「全都露」。

消息一出，引起各界譁然，○○醫院清查所有服務台的便條紙後，副院長初步研判這張洩漏病情的便條紙，可能是從眼科門診候診室的服務台流出，診間人員將本應銷毀的廢棄表單，重新回收使用。副院長並表示這一份記載著批價序號的病情資料，可能是誤將批價單當成便條紙使用所造成之個案情形，並非整批病情資料外洩。通常批價單正本給民眾，副本貼在病歷上保存，不過有時因電腦列印錯誤，造成多印或重印，就會被當成廢棄表單，歸類為機密文件。

台北市衛生局醫護管理處長表示，這份資料連名字、診療過程及診斷都有，已違反醫療法，可罰新台幣(下同)5 萬元以上、25 萬元以下。

重點摘要

1. 就醫資料涉及病人病情或健康資訊，醫療機構及其人員應負保密義務。
2. 紙本資料屬於新版個資法保護的客體，資料遭外洩的當事人可以請求損害賠償。

法律觀點

就醫資料涉及個人的身體及健康狀況，屬於敏感性資料，並為隱私權保護

之核心，因此醫療法第 72 條即規範醫療機構及其人員之保密義務[1]，違反時，依同法第 103 條第 1 項及第 107 條第 1 項規定，可對醫療機構及行為人處 5 萬元以上、25 萬元以下之罰緩，且若為無故洩漏時，可能將面臨 1 年以下有期徒刑[2]。

值得探討的部分在於，當事人可否向醫療機構或行為人請求損害賠償。案例中外洩資料包括就醫診斷結果，應屬於病歷而為個人資料，如該病歷是電腦處理列印，係屬於現行「電腦處理個人資料保護法」規範的客體。如該病歷為手寫而非電腦處理，則當事人只能主張隱私權受到侵害，而依照一般民法規定請求損害賠償，亦即當事人必須證明受到的損害及範圍，如此一來，將會因為舉證程度而影響可請求的範圍。

有鑑於個人隱私保護日益受到重視，總統於 99 年 5 月 26 日公布新修正的個人資料保護法(以下簡稱新版個資法)，將保護客體擴大至非經電腦處理的人工資料。因此，案例中，便條紙因載有個人資料，依新版個資法的規定，○○醫院應負損害賠償責任，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件以 500 元以上 2 萬元以下計算，○○醫院最高應承擔 2 億元之損害賠償上限。此外，新版個資法對於醫療及健康檢查等較為敏感的資料有特別規定，除了法律規定的情況外，原則上不得蒐集、利用及處理。因此，醫療機構除了應該對醫療及健康檢查等資料進行更嚴密的保護外，更應該加強對醫療從業人員、聘僱員工及志工等的教育訓練，以避免病人的敏感性資料外洩，並承擔高度的法律風險。

管理 Tips

本案例主要發生原因係為組織內員工教育訓練之缺乏，致使本應作廢之資料遭誤用。新版個人資料保護法第 6 條提及「有關醫療、基因、性生活、健康

[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。」

[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。」

檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」，本案例中之敏感個人資料基於醫事人員法律規定，組織可加以蒐集、處理或利用，惟組織內部人員應謹慎保護業務所知悉或持有的秘密資料。組織可透過教育訓練及宣導，使內部人員更清楚瞭解保護業務機密資料之重要性和資料保存、報廢等程序，及其所應擔負之法律責任，避免因不知情或不熟悉的情況下違反該遵循之法令、法規。

相關標準

ISO27001 本文 4.3.2 (i)防止作廢的文件被誤用

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

貳、 資訊公開（Disclosure）

一、政府資訊公開法

類別：資訊公開

【案號：D1000101】

網路上公布具名陳情文 ○○部判賠

【資料來源：蘋果日報 100/05/30】

焦點話題

退役教官○○不滿○○部少發一天薪水而陳情，○○部回覆後卻將陳情書及其姓名、職稱、電子郵件地址，也公布在○○部網站，退役教官認為隱私權遭侵害，請求國賠 20 萬元，台北地院日前判退役教官可獲國賠 5000 元，創下公務機關侵害隱私判賠的罕見案例。

退役教官於 2007 年 10 月退伍，因○○部付薪少給一天，隔年 10 月陳情到總統信箱，總統府移給○○部處理，○○部之後竟將陳情書連同退役教官的姓名及其電子郵件地址，公布在○○部網站的常見問題集。○○部辯稱，是為避免類似案件再發生才公布上網，此屬行政裁量權。但法官認為沒必要公布退役教官的個資去達到業務宣導目的，○○部已逾越裁量權、侵害隱私權，判退役教官應獲賠 5000 元。

重點摘要

1. 政府資訊雖以主動公開為原則，但若資訊的公開會侵害人民隱私權時，即應限制公開。

2. 人民陳情函等文件內容若涉及政府機關職掌必要範圍，是否有公開之必要雖屬行政裁量之範圍，但仍應符合個人資料保護法與政府資訊公開法之限制，才不會發生逾越裁量權之瑕疵。

法律觀點

為了保障人民知的權利，讓人民可以共享及公平利用政府資訊，政府機關應依政府資訊公開法之規定公開政府資訊，本案例中，○○部將退役教官之陳情書、姓名、職稱及電子郵件地址公布於網站，即是為了避免日後其他人民對於退伍薪給發放時點計算及是否剋扣薪資等情事，產生類似爭議，並為有效正確發放薪給，而認為有必要將陳情函公布於網站，以達業務宣導的行政目的，法院認為在前述行政目的範圍內，○○部可以對陳情書之內容加以利用，且此部分涉及薪給發放標準之資訊公開，對於公共利益有其必要性，是以尚難認為對退役教官隱私權造成不法的侵害。

但退役教官的姓名、職稱及電子郵件屬於個人資料，同時也受到現行電腦處理個人資料保護法的保護，如何在政府資訊公開及保護個人資料取得平衡，將會產生法律適用上的疑義。就此問題，依政府資訊公開法的規定，政府資訊之公開或提供有侵害個人隱私時，應限制或不予公開[1]，法院認為個人資料與薪給發放標準並非不可以分離，○○部若認陳情函內容具公益性，可以遮蔽退役教官個人資料，而僅就薪給發放標準部分予以公開，即足以達成業務宣導的行政目的。因此，○○部在沒有取得退役教官同意的情況下，將其個人資料併予公開，有逾越行政裁量的瑕疵且具有過失，趙○○的個人資訊隱私權確實受到侵害，依國家賠償法第 5 條[2]及民法第 195 條第 1 項規定[3]，判決○○部應賠償新台幣 5,000 元。

由此案例可知，公務機關雖然依法應公開政府相關資訊，但應特別注意政府資訊公開法對於其他應保護的權利，例如個人隱私，乃是採取應限制或不予公開之立場，因此在揭露資訊時，應注意須在法定職務的必要範圍內，若不慎將不具必要性且受到其他法律保護的資料公開，將可能須依國家賠

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

[2] 國家賠償法第 5 條：「國家損害賠償，除依本法規定外，適用民法規定。」

[3] 民法第 195 條第 1 項：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」

償法負損害賠償責任，不得不慎。

管理 Tips

以往一般民眾對於個人資料與隱私之權利主張較不注意，但是在新版個資法引起社會關注後，擁有大量個資的公務機關將立刻面臨比以前更嚴格之檢視，因此公務機關對於個人資料應建立完整的管理制度，以正確的方式蒐集、處理和利用個人資料。如此應可降低法律訴訟、損害賠償之風險，更重要的是可提高民眾對於公務機關之信任感，使相關業務能順利執行。

相關標準

A.15.1.1　識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊公開

【案號：D1000102】

健保局可否拒絕公開所持有的免抽查診所名單

【資料來源：臺北高等行政法院 100 年度訴字第 662 號判決】

焦點話題

甲（醫事機構，獨資）於民國(下同)96 年 11 月 26 日與行政院衛生署中央健康保險局(以下稱「健保局」)簽訂「全民健康保險特約醫事服務機構合約」（以下簡稱系爭健保合約），由甲提供全民健康保險之保險對象醫療服務，承辦全民健康保險醫療業務。甲於 99 年 8 月 3 日以函文方式請求健保局應公布申復案件相關數據資料。經健保局於 99 年 10 月 12 日函覆，說明其已依政府資訊公開法第 3 條與第 7 條規定，於全球資訊網公布其已持有並製作之全民健保統計資料，並有提供特約院所醫療費用申報資料初核及申復後之核減統計。嗣甲復請求健保局公布免抽查診所名單；經健保局於 100 年 1 月 17 日函覆依政府資訊公開法第 18 條第 1 項第 4 款規定認應限制公開，而駁回其請求。甲不服，遂向法院提起行政訴訟。

重點摘要

1. 政府資訊雖以公開為原則，但若屬於政府資訊公開法規範應限制或不予提供之政府資訊時，則不在此限。

2. 政府機關為實施監督、管理、檢(調)查、取締等業務所取得之相關資料以及涉及營業秘密時，均屬於應限制或不予提供的政府資訊。

法律觀點

我國針對政府資訊公開之規範，分別定有行政程序法、政府資訊公開法以及檔案法，上述法律的規範內容、權利主體、權利存續期間及救濟方法均有不同。本案中，所爭執之問題為健保局是否應公開其職權範圍內所製作之資訊，即申復案件總數及通過比例暨免抽查診所名單，予特定醫療機構

甲。

依照政府資訊公開法之規定，政府資訊雖以公開為原則，但並非沒有限制，同法第 18 條[1]即針對政府資訊公開之限制作出相關規範，如：公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者，或有關個人、法人或團體營業上秘密或經營事業之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。故由此可知，人民知的權利固然應該受到保障，但並非毫無限制，在達成增進人民對公共事務之瞭解、信賴以及監督之目標同時，亦須兼顧個人、法人以及團體之隱私或商業秘密。

本案中，甲基於其與健保局簽署的健保合約，向健保局請求公布申復案件總數與通過比例暨免抽查診所名單[2]，但法院認為甲以行政契約作為請求依據，除不符合法律規定外，並認為若准許甲的請求，無異公布其他醫療院所申報醫療費用件數、成長率、單價等執業與營業秘密資料，也將影響健保局未來抽查醫療費用是否浮濫作業之進行，因此健保局依政府資訊公開法第 18 條第 4、6 及 7 款之規定拒絕公開，並未違反法律規定。

管理 Tips

在政府資訊公開法的規定，政府機關單位應可全面重新檢視組織內的資

[1] 政府資訊公開法第 18 條第 1 項：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制禁止公開者。二、公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。四、政府機關為實施監督、管理、檢 (調) 查、取締等業務，而取得或製作監督、管理、檢 (調) 查、取締對象之相關資料，其公開或提供將對實施目的造成困難或妨害者。五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資料，其公開或提供將影響其公正效率之執行者。六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。八、為保存文化資產必須特別管理，而公開或提供有滅失或減損其價值之虞者。九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。」

[2] 99 年度「西醫基層總額執行委員會南區分會共管會」提案決議通過，符合：A.總件數≦300 件、B.每件單價（含部分負擔）≦400 點、C.每件單價成長≦5%、D.件數成長率≦5%者，始得免審。健保局業已於網站上公布「西醫基層診所經檔案分析免除專業抽樣審查原則」，提供轄區內西醫基層診所參閱，甲乃請求健保局依政府資訊公開法規定公開免抽查診所名單。

訊，適當的標註其公開狀況，如主動公開、公開但需經申請或不可公開等，更進一步針對不可公開之部分，清楚敘明相關理由供民眾參考。

相關標準

A.7.2.1　分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2　資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

類別：資訊公開

【案號：D1000103】

訴願書之公開與個人資料保護

【資料來源：臺北地方法院 99 年度重國字第 22 號判決】

焦點話題

民眾龍○○參加 93 年專門職業及技術人員之外語導遊普通考試,嗣後因為不服考選部將聽力改成口試與筆試的新聞稿與考試須知公告而提起訴願，雖經訴願審議委員會作成駁回訴願的訴願決定書，惟龍○○認為，倘認為前開應考須知等公告內容非行政處分，依訴願法第 77 條第 8 款規定，訴願審議委員會自應為不受理之決定，但訴願審議委員會逕將案由欄記載為「『不服考選部未予及格之處分』提起訴願」、事實欄記載「不服第二試口試所評定之成績」,理由欄記載「不服未獲及格，提起訴願」,使人誤以為龍○○對口試委員成績評定不服之錯誤印象，理由欄又故意援引與本件情形不同之行政判例，比喻他對口試成績不服係無理取鬧。

又訴願審議委員會基於職掌，雖得接觸考試評分資料，但典試法第 28 條並未允許將考試評分資料涉入系爭訴願決定書，考試院依同法條規定，亦有保密義務而不得公開。龍○○認為他的姓氏特殊,在觀光業界已有多年經驗，相關單位公開載有其姓氏的訴願決定書，不僅嚴重侵害他的名譽權、隱私權及姓名權，更有違反電腦處理個人資料保護法之虞，請求國家賠償。法院審理後認為龍○○的隱私權及名譽權沒有受到侵害，因此判決駁回訴訟。

重點摘要

1. 依政府資訊公開法的規定，訴願書以主動公開為原則。
2. 訴願書的內容涉及個人資料時，若已作適當的處理與隱匿，即沒有侵害個人隱私的問題。

法律觀點

本案例中，龍○○主張考試院公開訴願書的內容，含有他的姓氏，而他的姓氏特殊在業界易於辨認，此舉侵害他的名譽權、隱私權及姓名權，因此本案爭議在於考試院公布訴願決定書內容的適法性。依政府資訊公開法第 5 條的規定，政府資訊以主動公開為原則，且同法於第 7 條[1]亦明確規定訴願決定應主動公開。關於公開之方式，同法第 8 條[2]則開放「利用電信網路傳送或其他方式供公眾線上查詢」的方式，因此考試院公布訴願決定書乃是基於政府資訊公開法的義務，並無違法。

有關訴願決定書的內容，依照訴願法 89 條的規定，訴願決定書除須載明主文、理由及事實外，尚必須載明訴願人之姓名、出生年月日、住居所及身分證明文件字號等個人資料。法院認為考試院在公開訴願決定書時，除保留龍○○的姓氏外，並沒有公布他的名字、出生年月日、住所地等足以識別龍○○的個人資料，已經採取適當的安全維護措施，且屬於法令明文規定可以為特定目的利用之情形，並沒有違反電腦處理個人資料保護法的規定。

至於典試法第 28 條的保密義務[3]，法院則認為龍○○的考試成績已因複查結果與原評定分數相同而確定，龍○○仍有疑問並提起訴願，評分過程自屬訴願所審酌的重點，龍○○是否享有考試評分過程不受公開之權，亦值得商榷，況且此是訴願及行政訴訟攻擊與防禦所需，訴願審議委員會將評分過程作為系爭訴願決定書之理由，並沒有造成隱私的侵害。

管理 Tips

在政府資訊公開法的規定，政府機關單位應可全面重新檢視組織內的資訊，適當的標註其公開狀況，如主動公開、公開但需經申請、不可公開等，

[1] 政府資訊公開法第 7 條第 1 項第 7 款：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：...七、請願之處理結果及訴願之決定...」

[2] 政府資訊公開法第 8 條 1 項第 2 款：「政府資訊之主動公開，除法律另有規定外，應斟酌公開技術之可行性，選擇其適當之下列方式行之：...二、利用電信網路傳送或其他方式供公眾線上查詢。...」

[3] 典試法第 28 條：「典試委員長、典試委員、命題委員、閱卷委員、審查委員、口試委員、實地考試委員及其他辦理考試人員應嚴守秘密，不得徇私舞弊、潛通關節、洩漏試題；違者依法懲處，其因而觸犯刑法者，加重其刑至二分之一。」

並清楚敘明相關理由供民眾參考。

相關標準

A.7.2.1 分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

類別：資訊公開

【案號：D1000104】

市府資料平台　交通、房產一把抓

【資料來源：自由時報 100/11/10】

焦點話題

台北市政府辦理「Data.Taipei」專案，推廣市府公開資料加值運用服務，由資訊處跨局處協調，未來將適度上網公布犯罪案件、交通事故的熱區，以及房地產成交價、租金行情等，提供民眾實用且便利的生活訊息。

台北市哪一條街巷頻傳飛車搶奪、性侵害等案件，哪一個路口容易發生車禍傷亡？某筆土地、房屋買賣或租賃價格是多少？這些民眾有興趣知道的事情，公部門長期掌握相關資訊，罕見完整、定期對外揭露。

資訊處指出，英國倫敦、美國紐約與奧克蘭等城市，警方上網公開刑案發生地點、時間、類型、處理情況等基本資訊，「模糊化」被、加害人身分訊息，有業者引用、整理並開發 App 應用軟體，提供民眾查詢最新治安狀況，規劃改走其他路徑，或結伴同行。

資訊處表示，「資訊不透明」對市民生命財產的保障、生活需求的滿足構成障礙，資訊處依政府資訊公開法，建置「台北市政府公開資料平台」（http://data.taipei.gov.tw/），正與警察局、交通局、地政處等，討論治安斑點圖、交通事故熱點、房地產交易資訊等資料公開事宜。

此平台已彙整公廁、旅館、停車場、文化場館等 131 項資料，無償開放個人、團體或企業，進行公益、學術、商業、研發等使用。

重點摘要

1. 除非法律有特別規定外，政府資訊應以公開為原則。

2. 政府機關在公開或提供政府資訊時，應「模糊化」當事人的身分訊息，

避免侵害當事人隱私權。

法律觀點

政府資訊公開法的制定，是為了便利人民共享與公平利用政府資訊，以保障人民「知」的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與。凡是政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物與其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息，都是政府資訊公開法所稱的「政府資訊」的範疇[1]。原則上，與人民權益攸關之施政、措施及其他有關之政府資訊，政府應適時主動公開之。但根據政府資訊公開法第 18 條[2]，如果政府資訊的公開或提供有「侵害個人隱私、職業上秘密或著作權人之公開發表權」，則應限制公開或不予提供；除非是對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，才能公開或提供。

台北市政府規劃將適度上網公布犯罪案件、交通事故的熱區，以及房地產成交價、租金行情等，應該可以提供民眾實用且便利的生活訊息，並可以讓民眾的人身安全與財產權獲得更進一步保護。但上述擬公開的資訊，可能會涉及個人資料，例如犯罪案件或房地產成交資訊，除非符合法律規定可以公開或提供的情況，否則在公開或提供內容時，除了參考國外模糊化

[1] 參照政府資訊公開法第 3 條。

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

身份訊息的作法外，並要注意是否會構成新個資法之「間接識別」，以致因特徵或部分事實揭露還是有可能知悉個人資料而違反保護個人資料之意旨。個資法施行細則草案第 3 條3規定的「間接識別」，是指該資料不能直接識別個人，尚須與其他資料對照、組合、連結等，才能識別該特定個人，但特定個人有查詢困難、需耗費過鉅或耗時過久的情況時，即屬於無法識別個人的資料。依此標準處理，除符合保護個人資料外也保護隱私權，同時兼顧民眾知的權利。

管理 Tips

未來民眾在「台北市政府公開資料平台」將可查詢到台北市犯罪案件、交通事故的熱區，以及房地產成交價、租金行情等。台北市政府資訊處應有適當之作業程序及控制措施，針對犯罪案件及交通事故之當事人身份資料進行去識別化，以避免在提供大眾便利的生活訊息時，洩漏或侵害部份民眾之個人隱私及資料。另台北市政府資訊處應對於「台北市政府公開資料平台」上提供之資訊的完整性加以保護，確保公開予大眾之資訊均為正確且未有非授權的修改。

相關標準

A.10.9.3　公眾可用的資訊

應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改。

A.12.2.4　輸出資料確認

應用系統資料輸出應經確認，以確保所儲存資訊的處理正確且合乎實際情況。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

[3] 新版個資法施行細則草案：「本法第 2 條第 1 款所稱得以間接方式識別該個人之資料，指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。」

參、 資訊監察（Monitors）

一、通訊保障及監察法

類別：資訊監察

【案號：M1000101】

比連環叩恐怖 手機 App 追蹤男友

【資料來源：自由時報 100/09/02】

焦點話題

日本手機軟體公司推出一款應用程式「男友追蹤器」，並且開設「男友記錄」網站，標榜可以協助女性利用智慧型手機的 GPS 功能，隨時鎖定男友的行蹤，推出後網站爆紅，不過卻引發侵犯隱私權的爭議。

這套手機應用程式，只要安裝後就能隨時透過「男友記錄」網站，追蹤手機持有人現在的位置、通話紀錄以及正在使用的 App（應用程式）一覽表等資訊，甚至連手機電池剩餘量都能一清二楚。

手機軟體公司表示，「男友追蹤器」可以協助女性在遇到男友以「手機沒電」為由不接電話又不回電時，能馬上驗證他是否說謊，就算男友想「搞失蹤」，透過手機 GPS 定位，也能馬上找到他的行蹤。不過，想利用這套服務，除了會費之外，網站也規定，必須先取得被追蹤者的同意，若對方不同意安裝軟體，或是安裝後未進行確認，仍無法啟用追蹤程式。

重點摘要

1. 在取得他人同意的情況下進行通訊監察，屬於通訊保障及監察法所列的不罰情況。
2. 個人手機常有機會被他人持有，故追蹤程式除應得當事人的「真正同意」外，應有「確認同意者身分」之雙重保障機制存在，方可確保使用者之隱私權，避免受到他人之侵害。

法律觀點

依通訊保障及監察法的規定，「通訊」的定義包括「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信」[1]，因此本案例中的「男友追蹤器」，透過 GPS 功能，可以鎖定男友的行蹤，應構成通訊監察的行為，依照通訊保障及監察法的規定，須由執法機關取得通訊監察書後才可以進行，否則將屬於違法監察他人的通訊，依法會有 5 年以下有期徒刑的刑責[2]。但若監察者已取得通訊之一方事先同意，而非出於不法目的時，將不會受到處罰[3]。因此本案例中，若女性在取得男友事先同意且非基於不法目的之情況下，即不會因為違反通訊保障及監察法受到處罰。

另外，因為「男友追蹤器」可以從網站上追蹤安裝者之現在所在位置、通話紀錄以及手機電池剩餘量等資訊，該等資訊均屬於他人非公開活動，亦將涉及刑法第 315 之 1 條[4]的規定，但因該條的規定都是以「無故」作為要件，是以若男友同意女友可以透過「男友追蹤器」掌握行蹤時，即屬於男友願意將其隱私曝露給女友，此時女友即有正當理由而非屬於無故，亦不會構成刑法第 315 之 1 條的罪責。

綜上所述，此類可以追蹤的應用程式，若在使用前可以取得被追蹤者的同意時，應屬於法律允許的範圍，但因個人手機的使用者有時不僅止於手機之擁有者，因此如此取得「當事人」的「真正同意」，將為重要課題。手機應用程式之開發廠商，在設計上應確保應用程式之執行，必須先取得被追蹤者的真正同意且須有確認同意者身分之雙重保障機制存在。若對方不

[1] 參照通訊保障及監察法第 3 條第 1 項第 1 款規定。

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

[3] 通訊保障及監察法第 29 條第 3 款：「監察他人之通訊，而有下列情形之一者，不罰：…三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

[4] 刑法第 315 之 1 條；「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：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。」

同意安裝或無法有效進行身分確認，則不應允許追蹤程式之執行，以避免讓手機使用者之私密生活受到他人之追蹤，造成手機使用者隱私權之侵害。

管理 Tips

本案例可就以下兩方面討論之：

1. 對應用程式開發商：應於開發應用程式前，評估並確認該應用程式是否可能被作為違反法令或侵犯他人隱私之使用。例如本案例中指出，只要安裝應用程式「男友追蹤器」，即可蒐集到手機持有人現在的位置、通話紀錄、正在使用的 App 及手機電池剩餘量等之資料，上述資料將使被蒐集人的隱私受到侵害。應用程式開發商應確認該應用程式所蒐集之相關資料，以及網站所呈現之內容，均不違反法令法規之規範。
2. 對應用程式使用者：應需針對其行為，清楚地辨識其所需遵遁的法令法規。應用程式使用者應在其裝設監控或定位追蹤設備前，即針對所可能面臨的法律議題進行探討，避免踰越法律的規範及侵害他人隱私。

相關標準

A.12.1.1 安全要求分析與規格

新資訊系統或現有資訊系統提升的營運要求聲明中，應詳述安全控制措施的要求。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊監察

【案號：M1000102】

周刊記者遭監聽　提國賠敗訴

【資料來源：中央通訊社 100/11/16】

焦點話題

某週刊溫姓記者因報導前總統家務事，遭國安局監聽長達 11 月，向法院控告國安局侵犯隱私權，求償國賠 1 元並登報道歉。台北地院審理後，認定國安局監聽合法，判決溫姓記者敗訴。

根據法院判決，溫姓記者因多次報導前總統私密家務事，事後接獲法院通知，才知遭國安局監聽長達 11 個多月。

溫姓記者不滿國安局為追查新聞消息來源，濫權監聽，侵害隱私權，向法院請求國家賠償新台幣 1 元，並刊登道歉啟事。國安局指出，當時以確保國家安全、維護社會秩序為由，向法院聲請監聽票，監聽未違法。

法官審理認為，原告隱私權雖於監聽期間遭受侵害，但國安局向臺灣高等法院聲請通訊監察書，並依法向高院專責法官回報監聽結果，全程屬合法監聽，判決原告敗訴。全案可上訴。

重點摘要

1. 國家情報單位向高等法院聲請通訊監察書時，高等法院除須審查程序要件外，並須判斷是否具備「監察理由及其必要性」的實體要件。
2. 監聽行為雖然侵害受監察人的隱私權，但在取得通訊監察書的情況下，即符合法定程序，構成阻卻違法事由。

法律觀點

自由民主憲政秩序之核心價值是「維護人性尊嚴」與「尊重人格自由發展」。隱私權雖然不是我國憲法明文列舉之權利，但基於人性尊嚴、維護個人主體性及人格發展的完整，並且為了保障個人私密生活免於受到他人侵擾，以及保障個人對自己資料的自主控制，大法官認為隱私權是受到憲法第 22 條所保障的權利（參照大法官釋字第 585 號）。然而即便隱私權是憲法保障的權利，憲法對個人隱私權的保障也並非絕對，國家基於公益的必要，可以在不違反憲法第 23 條的範圍內限制之，但限制須符合「正當法律程序」和「比例原則」。

本案，國安局依照通訊保障及監察法第 7 條的規定，向高等法院聲請通訊監察書[1]。承審法院認為依照通訊保障監察法施行細則第 12 條[2]規定，高等法院專責法官於受理國安局聲請同意核發通訊監察書時，即應先就程序要件為審查，再就該法所定之實體要件，即「監察理由及其必要性」為審查，因此高等法院專責法官在同意核發通訊監察書案件之審查上，不僅須為形式審查，還須就「是否為確保國家安全、維持社會秩序所必要」（必要性原則），「有無逾越所欲達成目的之必要限度」、「是否為侵害最少之適當方法」（比例原則）等實體要件為審查。由於高等法院已進行實質審查才核發通訊監察書，國安局據以對溫姓記者進行通訊監察，客觀上固然侵害溫姓記者的隱私權，但此監聽是依法定程序所為的行為，構成阻卻違法事由，並無不法。

管理 Tips

國安局應可透過公開宣導，使一般民眾了解監聽之合法性以及何種資料會

[1] 通訊保障及監察法第 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。一、外國勢力、境外敵對勢力或其工作人員在境內之通訊。二、外國勢力、境外敵對勢力或其工作人員跨境之通訊。三、外國勢力、境外敵對勢力或其工作人員在境外之通訊。」、第 2 項：「前項各款通訊之受監察人在境內設有戶籍者，其通訊監察書之核發，應先經綜理國家情報工作機關所在地之高等法院專責法官同意。但情況急迫者不在此限。」

[2] 通訊保障及監察法施行細則第 12 條：「綜理國家情報工作機關依本法第七條第二項及第三項規定，通知高等法院專責法官同意通訊監察者，應備聲請書並記載下列事項：一、案由。二、監察對象及其境內戶籍資料。三、監察通訊種類及號碼等足資識別之特徵。四、受監察處所。五、監察理由及其必要性。六、監察期間。七、監察方法。八、執行機關。九、建置機關。」

被蒐集或使用等，以期降低民眾對於隱私被侵犯、外洩或暴露的疑慮，並減輕反彈。其中國安局如有蒐集及保存較隱私之資料，且因業務需要而須檢查或播放錄音時，應有適當的核准及授權機制，並留存相關活動或操作紀錄，以避免未有正當理由而侵犯個人隱私。

相關標準

A.8.2.2　資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.11.1.1　存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.15.1.4　個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

肆、 資訊應用（Application）

一、電子簽章法

類別：資訊應用

【案號：A1000101】

電子簽章代表同意簽署電子文件內容

【台灣台北地方法院 99 年度訴字第 5265 號】

焦點話題

A 公司與 B 公司簽訂「商品寄售契約書 」（下稱系爭契約），約定由 B 公司提供商品或服務，並委由 A 公司於電視及其他媒體或通路行銷被告商品，並針對寄售之醫療美容商品以電子簽章方式簽署「美容服務性票券商品增補協議書」(下稱系爭協議書)。嗣後 A 公司依照系爭協議書之相關約定向 B 公司請求給付 4,765,220 元。B 公司抗辯 A 公司提出之系爭契約、系爭協議等文件，B 公司並未簽署，是 A 公司單方所提出之文件，沒有拘束 B 公司的效力，不得作為 A 公司請求的依據。

法院認定系爭契約及系爭協議書有 B 公司的工商憑證作為電子簽章，可以認定雙方對於系爭契約及系爭協議內容達成意思表示一致，因此認定 B 公司依約必須給付 A 公司 4,765,220 元。

重點摘要

1. 依照電子簽章法的規定，電子簽章可以發生依法令應簽名或蓋章之法律效力。
2. 進行電子交易時，利用電子簽章進行電子文件簽署會有很強的證據力，可以證明雙方對於契約內容有達到意思表示的一致。

法律觀點

依照民法第 153 條第 1 項規定，當事人互相表示意思一致者，無論其為明示或默示，契約即為成立，且契約的成立並不以簽名為要件。因此當事人

在締結契約時，若書面的形式不完全，但可以用其他方法證明雙方的意思已經合致時，契約仍依法成立。

本案例中，B 公司否認該公司有簽署任何文件，因此不受到系爭契約與系爭協議書約定的拘束。但 A 公司主張雙方是以電子簽章方式簽署系爭契約及系爭協議書，雙方應受到契約的拘束。是以本案爭點在於電子簽章的法律效力。

為了推動電子交易的普及運用，並確保電子交易安全，促進電子化政府及電子商務之發展，因此我國制定了電子簽章法，以規範相關法律效力。依據電子簽章法第 9 條第 1 項的規定，依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章之。因此若契約當事人均同意使用電子簽章以代簽名或蓋章者，可認定該電子簽章即為契約當事人表示意思的方法。本案經函詢經濟部鑑定後，經濟部工商憑證管理中心函覆 A 公司提出之光碟內容，確實與經濟部核發予 B 公司的工商憑證相符，B 公司使用電子簽章於系爭契約及系爭協議書上，可認定雙方的意思表示達到一致，法院因此判決 A 公司勝訴。

企業向經濟部申請的工商憑證，其性質等同於企業的網路身分證及公司大小章，以工商憑證之電子簽章簽署後，即等同於實體簽名或蓋章，並可據此推定簽章者具有同意簽署之意思表示，此部分乃經過法院判決的肯認。因此在網路科技發展的現代，若擬從事電子交易，應妥善利用憑證進行電子簽章，以發生等同簽名或蓋章的效力，以在日後對契約內容產生爭議時，能進行相關舉證。

管理 Tips

工商憑證的使用如同公司章一樣，具有相同法律的效力。企業可使用憑證的正卡申請多張附卡，惟企業應針對附卡之使用權限有適當控管機制，避免未經授權使用之風險。使用工商憑證須考量正卡與附卡的實體卡片保

護、卡片密碼的持有及憑證使用的授權等，企業應有妥適的規劃以及控管機制，以期能避免因憑證被未經授權使用時所遭致的損失及糾紛。

相關標準

A.11.2.1　使用者註冊

應有適當的正式使用者註冊與註銷註冊程序，以對所有資訊系統與服務核准和撤銷存取。

A.11.2.2　特權管理

應限制與控制特權的配置與使用。

A.11.3.1　通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

類別：資訊應用

【案號：A1000102】

保障小股東 啟動電子投票

【資料來源：經濟日報 100/01/05】

焦點話題

金管會初步決定，資本額逾 100 億元的上市（櫃）公司及金融機構，自民國(下同)101 年起股東會強制採取電子投票，電子投票不得以委託書委託他人，小股東自主性提高，但大股東慣用選戰策略「委託書徵求」難度大增，經營權掌控不確定性增加。

公司法修正案已於 101 年 1 月 4 日公布實施，其中第 177 條之 1 授權證券主管機關視公司規模、股東人數與結構及其他必要情況，命其將電子方式列為表決權行使管道之一。據了解，金管會規劃重點是參考獨立董事強制設立門檻，明訂資本額在 100 億元以上的上市（櫃）公司和金融機構，須率先強制推動電子投票，以落實股東行動主義。這次公司法修正增訂強制電子投票規定，但公司法本身並沒有相關罰責，金管會官員表示，未來在推動上，會透過要求公司在章程中訂定，並由財團法人證券投資人及期貨交易人保護中心要求公司落實資訊揭露等方式，督促公司依規定辦理。

電子投票方式對公司影響重大，例如改選董監時採電子投票，小股東可參與表達意見，大股東掌控經營權及重大議案的變數也相對增加，因此上市櫃公司非常關注強制推動的門檻。官員表示，公司除可選擇透過臺灣總合股務資料處理股份有限公司、臺灣集中保管結算所股份有限公司的股東會通訊投票平台外，也可以自己設計平台，供股東採用電子投票方式。

重點摘要

1. 101 年 1 月 4 日公布實施之公司法第 177 條之 1，授權金管會訂定強制

實施電子投票的範圍。

2. 實施電子方式投票時，應使用電子簽章之憑證機制在網路上確認股東身份及其行使意思表示內容的完整性。

法律觀點

公司法第 177 條之 1 第 1 項規定：「公司召開股東會時，得採行以書面或電子方式行使其表決權；其以書面或電子方式行使表決權時，其行使方法應載明於股東會召集通知。但證券主管機關應視公司規模、股東人數與結構及其他必要情況，命其將電子方式列為表決權行使管道之一。」此規定過去都是由公司自行選擇，但甚少公司採用，有鑑於近年來上市上櫃公司之年度股東會日期，有過度集中現象，致股東無法一一出席股東會行使其表決權，影響股東權益甚鉅，且電子投票平台已由行政院金融監督管理委員會協助集保結算所建置完成，為落實電子投票制度，鼓勵股東參與公司經營，強化股東權益之保護，因此修法明定證券主管機關應視公司規模、股東人數與結構及其他必要情況，命公司將電子方式列為表決權行使管道之一。

以電子方式投票時，因使用電子投票無法核對股東證件，因此首要克服的問題即是股東身分的辨識，以防止冒名投票或一人多投等情況的發生。再者，必須於電子投票傳輸過程中確保資料完整性及真實性。為達到上述目的，集保結算所建置之股東會電子投票平台即「股東 e 票通」，股東應使用該平台認可的「CA 電子憑證」行使表決權。所謂的「憑證」係指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明[1]。電子簽章之憑證猶如使用者的網路身分證，其功能在於確認使用者身分、以確保電子文件傳輸安全性、可歸責性及文件內容完整性，且在發生爭議情事時，得以提出經電子簽章簽署之電子文件作為證據資料，以釐清責任。因此，針對電子投票內容進行電子簽章，即可證明是由該股東本人親自行使及確保其意

[1] 參照電子簽章法第 2 條第 6 款規定。

思之真實性及內容完整性，未來應可讓股東行使股東權利更加便利，進而更充分表達股東之意志。

管理 Tips

就此案例而言，可從下面 2 個層面來檢視：

1. 股東身分識別：憑證的使用為數位環境證明持有者身分及簽署數位文件之用，組織應可要求股東於使用電子投票平台進行投票行為時，使用該平台認可之電子憑證作身份辨識之用以達成識別性與不可否認性。
2. 確保訊息完整：組織應有適當之保護措施確保電子投票的傳輸過程不會有未經授權的竄改。另外組織應保護電子投票平台資料儲存及輸出的完整性，避免後續因完整性被破壞導致的爭議。

相關標準

A.10.8.4　電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A.11.5.2　使用者識別與鑑別

所有使用者應有僅限其個人使用的唯一識別符(使用者 ID)，並應選擇適切的鑑別技術，以證實使用者宣稱之身分。

A.12.2.3　訊息完整性

應識別應用系統內為確保鑑別性與保護訊息完整性的要求，並識別與實作適當的控制措施。

A.12.2.4　輸出資料確認

應用系統資料輸出應經確認，以確保所儲存資訊的處理正確且合乎實際情況。