個資法風暴襲捲下的企業生存之道

Openfind 產品經理 廖享進

對於新版個資法使用定出詳細規範，與舊法標準相比更為嚴格。此規範將對許多企業產生重大影響的隱私資料保護法案，由於詳盡規範個人資料蒐集與處理程序，不但將加重企業的相關控管責任，從今日起，企業更需嚴密注意外部公開資訊是否有觸法嫌疑，且必須小心內部員工對外流通的資訊，是否有不慎將個人資料公開的可能。否則輕者受罰，重者將可能面對受害者的團體賠償訴訟，面臨最高求償上限 2 億元的風險；同時，企業也肩負使用個人資料時的通知義務，若未盡完善告知或者使用過程上有瑕疵，也會面臨單一案件 2 萬至 50 萬的行政罰鍰風險。

新法三讀通過，行政院施行在即，一般企業也開始惶恐，尤其是面對網際網路訊息的控管，更是一時千頭萬緒，不知從何下手。由於網際網路的訊息流通快速，電子訊息傳播代價極低，再加上現今公共搜尋引擎技術的進步，許多員工不慎外洩的個資不但傳播速度超乎管理者想像，更容易在公眾搜尋引擎上留下紀錄，導致難以預料及掌控的後果，將嚴重影響企業商譽。

在個資法正式實施後，企業日常都會使用的 Web 及 Email，將會面臨到什麼風險呢？下述幾個使用情境，值得企業審慎思考。

(1) 某購物網將抽獎中獎名單公佈在網站上，不慎流露得獎者的身份證字號。
(2) 某公家機關自行建置網站搜尋引擎，沒想到在搜尋關鍵字內輸入「健保卡號」，便得到了許多姓名和健保卡號的對應清單網頁。
(3) 某銀行理專將客戶的電子開戶資料(帳戶號碼與姓名)寄給客戶的時候，未得客戶同意就順便轉寄給同集團的投信公司，導致客戶的個資外洩。
(4) 某會計師事務所會計師，被人指控使用 Email 流洩客戶的信用卡號與相關交易資訊，但公司卻無法提供檢調單位相關的電子郵件歸檔證據。
(5) 某竹科製造業主管，將擁有員工編號和薪資的個人資料使用 Email 轉寄給上層主管，事前未告知當事人，事後稽核單位也無主動機制追查此外洩事件。

以上幾個實境聽起來怵目驚心，但卻是已經發生在真實世界的確實案例，同時這些情形也都屬於觸犯個資法的規範範圍，將使企業受到行政罰鍰與相關控訴的風險。為了預防這類問題，建議從最基本的檢視開始 -- 從自身的網站和企業內部

收發的 Email 開始控管個資的外洩問題，以下提供一些必備的方法，讓管理者可以使用輕鬆、簡單的方式，制定並防範個資外洩的問題。

透過掃描引擎協助

在 Web 方面，管理者可以選購具備掃描個人隱私資訊(例如身份證字號、信用卡號、護照號碼、信用卡號、手機號碼等等)樣式的掃描引擎，定期掃描放置在公開網站上數以萬計、甚至百萬計的網頁、文件，一旦偵測到符合特定樣式的個人隱私資料，便提出警示，讓管理者方便檢視、確認後移除。通常企業的網站內容多由各子單位自行維護上傳，因此若不具備這樣的機制，而改用每次上傳就必須慎重檢查的方法，不但影響網站更新的效率，也無法即時有效的以「統一中控」的方式，攔阻隱含個人資訊內容的網頁和文件，也可以避免之前常耳聞的線上購物或公家機關網站不慎流洩個資的類似事件。

此外，更需要注意的是許多網站管理者購置了企業內的搜尋引擎方案，作為本身網站的內容搜尋引擎，如果您的網站不慎放置了個人隱私資訊，該搜尋引擎方案應也必須具備「暫時移除該筆搜尋資訊」的功能，避免有心人士直接藉由網站內建的搜尋引擎，使用「Search Hack」的方式取得該網站上的個人資料。同理，若您已經發現網站上有不當的個人隱私資料，不但需要立即移除，也應該立即到各大公眾搜尋引擎嘗試搜尋，若已被公眾搜尋引擎快取，應立即提出移除申請，並暫時修改網站本身的「公眾搜尋引擎存取限制檔」(robots.txt)，暫時針對出問題或者有個人隱私資訊露出風險的網頁或文件目錄做「拒絕出現在公眾搜尋引擎」的設定(註一)，避免相關災情繼續蔓延。

【圖說：可於系統內容管理選擇機敏資料檢測功能，以進行查找動作。】

【圖說：配合查詢結果，可針對機敏資料設定排外功能，避免發生個資外洩。】

郵件更重視前、後稽核機制

針對企業在因應個資法實行同時，在 Email 方面的因應之道，郵件發送的前、後稽核則是最大的重點，如同上述，管理者也應該挑選具備攔截或掃描個人隱私資訊能力的郵件安全解決方案，在郵件發送前預先攔截隱含個人隱私資訊的郵件，依照企業政策進行主管審核或者紀錄備查的動作；發送後的資訊也應該歸檔至歷史郵件庫，定期進行關鍵字追蹤，主動警示管理者隱含個人資訊的信件內容，讓管理者能主動地進行此類機敏信件的控管；如此搭配無論是在事前風險的控管，或事後蒐證需求，都能萬無一失的應對。

同時，為了降低使用者將隱含對方個人隱私資料的信件誤寄或者副本給不應接受的對象，也可以將 Email 的 Webmail 或 Email Client 的發信介面設定為送信前強制預覽狀態，以方便使用者發信前再度檢視收件人員是否正常，若一時發送錯誤，也應提供管理者立刻從伺服器上取消、收回郵件的功能，將誤寄郵件的傷害即時降低。同時，企業若有定期發送帳單、EDM、或者定期郵件的機制，也應加上免責聲明機制，對收件者闡述其個人隱私資訊的取得方式和來源，並針對信

件內容做「無償免責」相關說明，且警示非此信件收件人的收件者應立即刪除此信件。

【圖說：系統管理者可針對機敏資訊做稽核的參數設定，稽核規則設定後，即可依規定將機敏資訊傳送至郵件審核區進行稽核的動作。】

事實上，個人隱私資料保護的相關法令在許多先進國家(例如日本、美國、德國、俄羅斯、西班牙等)已行之有年，不管針對網站維運或者 Email 領域，這些國家都已經有成熟的機制和 IT 方案去應對，因此在挑選本土廠商的相關 IT 產品之時，也可以注意該廠商在此類市場的市占率和名聲，作為評選的保障項目之一。本文針對 Web 和 Email 所描述的許多簡單、實際的基本注意事項，是可以保障您的組織在現有個人資料保護法尚未實行前的未雨綢繆之策，能於山雨欲來風滿樓之際，便擁有萬無一失的準備，協助企業走過風雨，安然度過個人隱私資料外洩的危機。

註一：
http://www.google.com/support/webmasters/bin/answer.py?hl=b5&answer=156449