個資外洩，不能河蟹 －論個資外洩實務規範及處理

■第 58 期學習司法官 吳宜展*

■■■ 目　次 ■■■

壹、引言

我國自民國（下同）99 年 5 月 26 公布全文 56 條之「個人資料保護法（下稱個資法）」，於 101 年 10 月 1 日施行，取代 84 年所訂定之「電腦處理個人資料保護法」，並於 104 年 12 月 30 日進行修正個資法第 6 至 8、11、15、16、19、20、41、45、53 及 54 條，共 12 條條文，於 105 年 3 月施行。此次修法超過 20％以上的異動幅度，足見立法者對個資領域的高度重視。

事實上，隨著科技、金融、電子商務等社會型態的轉變，個資的蒐集與提供已不再是為了舉辦活動，毋寧已現代人的生活模式，從每日使用 Instgram、Facebook 等通訊軟體，至使用 Apple Pay、支付寶等行動支付 (Mobile Payment)、第三方支付 (Third-Party Payment) 工具，現代人幾乎不可能不提供資料予他人處理、利用。是以，如何一方面給予當事人生活便利，一方面便保障當事人資訊隱私權、資訊自主權，已不只是一般法律層次問題，更是涉及憲法上人性尊嚴[1]、

* 法務部司法官學院第 58 期學員。臺灣大學法律研究所畢業。曾任財團法人工業技術研究院律師、財團法人資訊工業策進會律師、個資推動秘書組成員。

1 參大法官釋字第 603 號解釋。

人權保障[2]之重大迫切問題。

而各大中小企業，往往掌握著員工及客戶等，少則數千筆，多則數百萬筆之當事人個資。是個資一旦遭受外洩，已非只是資料易受不法者濫用，或當事人將受詐騙，還將造成社會的動盪不安，甚至淪為國安危機[3]。

近日，Uber 於美國時間 2017 年 11 月 21 日，坦承於 2016 年 10 月曾遭駭客攻擊，竊走全球 5000 萬名乘客、700 萬名司機的個資，Uber 支付給駭客 10 萬美元贖金救回個資。而 Uber 表示，遭竊取的乘客個資包括姓名、電子郵件、電話號碼，司機的個人資料、駕照號碼也遭竊。但 Uber 強調，信用卡資料、乘車地點等訊息並未流出。惟消息披露後，已引起社會恐慌，紐約檢方也將介入調查[4]。

而日本，大型旅行社 JTB 於 2016 年 6 月間，遭到駭客標的型攻擊，最大約有 793 萬筆的個人資料流出[5]。無獨有偶，我國知名旅行社雄獅於 2017 年 5 月間，發現其伺服器流量異常，遭駭客登入抓取公司文件，外洩 36 萬筆個資，並受到客戶投訴，詐騙集團謊稱員工進行詐騙[6]；知名書商三民網路書店，於 2017 年 10 月底疑似個資外洩 2 週，108 人共被詐騙 500 萬元[7]。

基此，面對個資外洩造成的衝擊，不只是臺灣需面對的挑戰，亦是全世界須共同面對的課題，筆者將以 in-house 律師經驗，分享實務處理心得，期待透過現行法規分析、日本法比較及本文建議，能夠建立一套法規遵循 (Legal Compliance) 流程，亦期待能夠就此「藍海」領域，作出開拓。

---

2 Facebook 等通訊軟體被指出提供個資給國安單位。The New York Times，June 8 2013,How the U.S. Uses Technology to Mine More Data More Quickly, http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?pagewanted=all&_r=1&。

3 原為房仲之犯嫌所開發出「客戶開發搜尋系統 V5.0 專業版」系統，能破解「圖形辨識系統」，且能提供的個資多達 1 億 7000 萬筆，連總統蔡英文的個資也在內。自由時報，http://www.asahi.com/ business/reuters/CRBKCN0Z307R.html，2017 年 5 月 12 日 (最後瀏覽日：2017 年 12 月 15 日)。

4 聯合新聞網，https://udn.com/news/story/6809/2832776，2017 年 11 月 22 日 (最後瀏覽日：2017 年 12 月 15 日)。

5 朝日新聞，http://www.asahi.com/business/reuters/CRBKCN0Z307R.html，2016 年 6 月 17 日 (最後瀏覽日：2017 年 12 月 15 日)。

6 三立新聞網，http://www.setn.com/News.aspx?NewsID=255550，2017 年 5 月 23 日 (最後瀏覽日：2017 年 12 月 15 日)。

7 自由時報，http://news.ltn.com.tw/news/society/breakingnews/2222342，2017 年 10 月 14 日 (最後瀏覽日：2017 年 12 月 15 日)。

貳、我國實務規範及處理

本文目的固在於當個資外洩事件發生時，提供令個資保有者足資遵循之規範及處理，惟如何維護、管理個資，使個資不致外洩，亦為個資法實務之重要課題，故擬先從個資保有者應防止個資外洩之維護義務談起，循序切入個資外洩之通知義務、外洩後如何處理及相關損害賠償等法律責任，最後談及事件發生後，個資保有者就持有之個資，是否仍得利用，若不得利用，則該如何處理之問題。

一、個資保有者防止個資外洩之維護義務：

按我國個資法體系，將蒐集、處理及利用主體分為公務機關及非公務機關，而公務機關就個資之維護及防止外洩責任，僅有個資法第 18 條規定：「公務機關保有個人資料檔案者，應指定**專人辦理安全維護事項**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」而有關於安全維護事項內容，各公務機關大多自行參考以內部行政規則訂定，如：經濟部及所屬機關個人資料保護管理要點。

針對非公務機關，除須依中央目的事業主管機關指定相關處理方法，進行資料處理外，並須採取適當之安全措施，可見個人資料保護法第 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。」而若有違反該適當安全措施，主管機關可處非公務機關罰鍰，見同法第 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**：……四、違反第二十七條第一項或未依第二項訂定**個人資料檔案安全維護計畫**或業**務終止後個人資料處理方法**。」

實際上，除在非公務機關領取政府科技專案或能源專案等補助情形外，中央目的事業機關尚未就各行業均有指定處理方法，縱屬專案補助情事，政府單位亦多會以契約或投標須知文件之方式，約束非公務機關。故大多數的情況，都是要由非公務機關自行判斷，是否已採取適當之安全措施，以防止個資之外洩。

有關適當之安全措施，參個資法施行細則第 12 條：「……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。」

就上揭條文之安全措施事項，以個資外洩問題，最直接相關，且不可或缺的事項應是「四、事故之預防、通報及應變機制」及「十、使用之紀錄、軌跡資料及證據保存」。前者涉及個資法規應盡之通報義務，後者涉及事故的調查、資安漏洞的填補及將來訴訟之證據保存。其他部分雖非毫不相關，惟除「十一、個人資料安全維護之整體持續改善」，如何持續改善，內容較為空泛，姑不討論外，各中小企業就其他事項，亦未必均能實踐，本文參酌個資法就措施採擇係規定為「得」，且僅須符合比例原則，本文將僅就筆者認為，與個資外洩高度相關，**且實踐可能性較易之第一、二、四、六及十措施事項介紹**，以求使中小企業之事業主，均能盡基本之個資遵循義務：

（一）配置資料安全管理人員及人員管理

就上揭第一措施事項及第六措施事項，因有高度關聯性，故併同於此部分說明。個資保有者除應配置資料安全管理人員外，尚應就該人員**建立權限設定及異動管理程序**，防止未經授權或異常存取、破壞及個資外洩。而該管理人員應按其職責，並依業務功能所需，最小權限範圍內得以完成者為限，接受無權限同仁申請調閱個人資料，並留存軌跡資料於系統或檔案伺服器（file server）。此外，若該管理人員有異動，個資保有者應確認繼任者已完成個資保護認知，及相關交接程序，俾利個資外洩時，能確認應負責之人。

（二）界定個資種類並使用不同管理措施：

按個資法就個人資料之種類，分為自然人之姓名、出生年月日、國民身分證統一編號得以直接或間接方式識別之資料之一般個人資料，及個資法第 6 條之有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之特種個人資料，原則上依個資法第 6 條第 6 款規定，經當事人書面同意者，仍得蒐集。惟同條款後段又規定，其同意違反當事人意願者，不在此限。而在面試或工作場合，員工是否會事後抗辯，受迫於長官壓

力，實際上違反其意願，不得而知。是除有個資法第 6 條第 1 款至第 5 款事由外，**本文建議一般企業或政府機關內部仍應規範為不得蒐集特種個資**，若有部門有蒐集必要，內部程序亦應規範為經部門首長同意，以示慎重。

此外，特種個資因有其機敏性，建議與一般個資分開存放不同系統或檔案伺服器，至少應分放於同一系統或檔案伺服器之不同資料夾，並設定不同密碼。甚且，即使同為一般個資，亦有受違法利用程度較之高低不同，如：身分證字號、護照號碼、銀行帳號、信用卡號碼等，受違法利用程度較高。故建議**有關個人金融及財務狀況資料，應同特種個資，分開存放，分別設定密碼**，以分散外洩風險。

（三）事故之通報及應變機制：

此部分指的是當事故發生後，就企業或政府機關其自身之內部通報及應變程序。大致而言，個資保有者應分就識別與通報、處理及應變、檢討與管理三部分分別規範之。

1. 識別與通報：

企業或政府機關之員工發現個資外洩情事時，應先就個資事故影響範圍進行初步研判，然後填寫如通報單之書面紀錄，記錄事故發生地點、原因、影響範圍及目前處理情形，並判斷是否涉及資安事故，其後向直屬主管陳報。建議個資保有者可依個資外洩所涉及之個資種類及外洩筆數，斟酌規範員工陳報直屬主管之層級。

2. 處理及應變：

直屬主管收到個資外洩通報後，若涉及系統或檔案伺服器之資安事故，應聘請資安專家或顧問掃瞄並修復系統弱點，並研議資訊安全補強措施，以防止損害持續擴大。若未涉及資安事故，直屬主管可採取之應變措施有：(1) 尋求內、外部專家諮詢 (內部專家如通過 TPIPAS 認證之個資管理師、BSI 受訓人員；外部專家如於 TPIPAS 登錄之輔導機構)。(2) 發布新聞稿或召開記者會。(3) 依法令進行外部通報。

3. 檢討與管理：

直屬主管應指示個資外洩部門或員工，擬定矯正預防措施，並完成個資事故檢討報告，內容至少應包含背景說明、系統及網站說明、判斷及鑑識作業、影響範圍及損失評估、應變處理措施、通知當事人作業、矯正預防措施等事項，以臻完備。

（四）蒐集、處理及利用紀錄、軌跡資料及證據保存：

就蒐集資料而言，紀錄及保存應區分為紙本及電子文件而不同處理。

1. 紙本：

資料管理人員應以口頭說明或書面提示方式進行告知，請當事人簽署

「蒐集個人資料告知事項暨同意書」後，交由資料安全管理人員**存放於上鎖專櫃**，防止非執行業務或無權限人員取用，以避免個資外洩。

2. 電子文件：

若藉由電腦網站蒐集個人資料時，仍應先提供當事人閱讀「蒐集個人資料告知事項暨同意書」，並經當事人勾選「同意」後，始由當事人填寫個人資料。**而就蒐集之個資，亦應施以加密**，除資料管理者外，他人不應有接近 (access) 權限。另就當事人提供個人資料之過程，所留存**軌跡資料**，至少應包含**當事人資料 (如 IP、姓名或其他直接或間接得以識別當事人之資訊)、同意書版本、蒐集日期及時間。**

就處理及利用而用，若藉由系統或檔案伺服器者，亦應留存軌跡資料，其所稱軌跡資料，至少應包含**存取者** (如電腦名稱、IP、姓名或其他直接或間接得以識別存取者之資訊)、**存取日期及時間、執行之動作**（如新增、編輯、瀏覽、刪除、列印、匯出等）。若藉由紙本處理及利用者，若資料管理者與使用人並不相同，則資料管理者提供資料前，起碼應記錄何人、何時及為何特定目的而使用。確實作好上述之維護及管理，雖不能完全避免個資外洩，但至少能留存紀錄，讓個資取得人、使用人，得知個資一旦外洩，自己將被究責，產生嚇阻力。

另隨著個資保有者所持個資數量逐漸龐大，考量成立 IT 部門之人力、成本因素，個資保有者直接將所持個資委託外部廠商管理者，或將個資存放位置於外部廠商系統或伺服器者，亦比比皆是。此時，應區分情形為 1. 不涉個資業務之委外管理及 2. 涉及個資業務之委外管理[8]，適用不同個資法規定。

1. 不涉及個資業務之委外管理：

因受委外管理之單位僅提供系統或伺服器，供個資保有者租用後置放個資，於此情形，尚無個資法第 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」等規定之適用。此時，故應由**委外管理之個資保有者，按上揭文章所述，依契約方式，要求受託管理之單位，符合個資法要求，**若發生個資外洩，亦應由個資保有者負賠償等最終責任。然實務上，個資

[8] 陳宏志，個資法修正後當事人同意及委外監督管理實務之因應，《科技法律透析》，第 28 卷第 10 期，2016 年 10 月 15 日，13-19 頁。

保有者至多只有選擇受委外管理之單位之權利，對於提供該巨型企業所提供之系統及平台，如 Amazon EC2、Google Cloud Platform（GCP）、Microsoft Azure，毫無監督能力，只能遵循該巨型企業所提供之定型化契約。**然個資法卻無就該提供系統及平台之單位，就如何防止個資外洩，有任何規範**，應屬不及跟上時代潮流之立法疏漏。

2. 涉及個資業務之委外管理

個資實務上常見之情形應分為下述三種，個資保有者即委託管理之單位、受託管理之單位均應依個資法負相關責任，惟受託管理之單位是否須依個資法第 9 條告知當事人，則有不同：

(1) 當個資保有者在蒐集個資時，向當事人明示日後欲將蒐集之個資「交付」受委託之單位，進行處理、利用，此時受託管理之單位形式上雖該當個資法第 9 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定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」，即間接蒐集規定之適用，惟因當事人受蒐集個資前已明知受託情事，故受託管理之單位應無需再依該條向當事人通知，個資保有者應依個資法施行細則第 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」，個資外洩時，除由委託者即個資保有者負最終責任外，受託管理之單位亦應有前揭個資法第 4 條、個資法施行細則第 7 條之適用，負擔個資法損害賠償等責任。

(2) 當受託管理之單位蒐集時明示，係受個資保有者之委託，以個資保有者名義進行蒐集、委託及處理。此時，應以蒐集名義人為個資保有者，同時為委託者，為實務上最典型、多數之委託案例，個資保有者應受個資法施行細則第 8 條規範，受委託管理之單位則受個資法第 4 條、個資法施行細則第 7 條規範，負個資外洩之相關責任。

(3) 比較特殊的情形，為個資保有者蒐集個資時，漏為告知將交付由他人進行處理、利用等管理，此時會產生問題的是，個資保有者將當事人個資交由他人處理及利用，是否會違反蒐集之「特定目的」？本文以為，除非在當事人簽署個資同意書時，個資保有者已明確告

知使用方式僅限於個資保有者使用，不得委託或交付他人。否則，特定目的通常較為概括，只要在同一性範圍內，個資保有者將個資交由受託管理之單位處理、利用並無不可，如委託單位為舉辦課程，蒐集參加者個資後，後續繳費、通知均由受託單位為之等情形。然鑑於個資當事人並未知悉，個資實際使用情形，及為免不知該向何人行使個資法第 3 條之當事人權利，此時，**得到當事人個資之受託管理單位應屬個資法第 9 條間接蒐集情形**，應由受託管理之單位，向當事人告知資料來源及個資法第 8 條第 1 款至第 5 款事項，個資外洩後，不論是間接蒐集 (受託人) 者，或是直接蒐集者 (委託人)，應直接按個資法負擔責任，無須再引用個資法第 4 條、個資法施行細則第 7 條規定。

二、個資外洩通知義務 — 時間、內容、對象及方式

按個資法第 12 條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」然就除通知方式，有個資法施行細則第 22 條規定外，就該通知時間、具體內容、對象是否包括主管機關及何種方式方為適當等實務問題，茲分述如下：

1. 查明後通知時限：

按個資法第 12 條規定，個資外洩事件應「查明後」通知當事人。誠然，若不經查明，逕為通知當事人個資遭外洩，徒增當事人之恐慌。惟若個資保有者一直在查明，不願公布或通知，又該如何？個資法及法務部函釋[9]均未規定查明時限，顯有不足。又個資保有者應查明事項為何？亦涉及通知當事人之內容，個資法未就此明文規定，亦有不足。本文認為，在談論查明時限之前，應先談論個資保有者於個資外洩後，能查明之手段及事項，再去判斷查明時限之合理性。

以舉辦活動為目的之報名網站，遭大陸烏雲網站公布有 SQL injection 漏洞為例，個資保有者自身若無 IT 相關部門，則可尋求民間提供資安鑑識

9 參法務部法律字第 10603503230 號函要旨：「如公務機關發現所蒐集個人資料有被竊取、洩漏、竄改或其他侵害等情事，即應查明事實，以適當方式迅速通知當事人，始符合個人資料保護法第 12 條立法目的，又公務機關違法責任確認，尚非構成通知義務之要件或前提。」雖有提及迅速通知，但仍未說明通知之時限為何。

服務之公司，進行事故鑑識作業，清查**網站主機資訊、涉及個資檔案及個資筆數、受駭客攻擊次數、外洩時間點、網站全面性弱點掃描及針對 SQL Injection 弱點的特定加強掃描**。若該個資是委外進行管理，得一併提供弱點掃描結果給受託管理之單位，作為為網站漏洞程式修補依據。又就查明時限而言，雖仍須依系統弱點多寡，民間公司就保全、管理、分析、報告所需時程而定，惟考量目前業界能力、當事人個資遭濫用之急迫性，本文認查明時限仍以不超過 1 個月為宜。

2. 通知具體內容：

按個資法施行細則第 22 條第 2 項規定：「依本法第十二條規定通知當事人，其內容應包括**個人資料被侵害之事實及已採取之因應措施**。」惟具體而言，若只簡述個資外洩事實，及未來將加強保護個資，而未向當事人敘明被外洩個資之種類、筆數及矯正預防等資訊，如此通知內容，是否已符合立法目的，則非無疑。

參美國加利福尼亞州政府所公布之「違反個人資料安全之通知實行事項」[10]（下稱通知實行事項），通知內容應包含 (1) 本次通知日期 (2) 事件之概略描述。(3) 特定個資種類。(4) 寄發信件之組織、承辦人及聯絡資訊。(5) 事件發生之期日或預估期日。(6) 免付費協助之電話號碼。(7) 已進行之矯正措施。(8) 能保護自己之方法及資訊。(9) 提供州政府保護個資之網站資訊。上揭事項內容相當詳實，值得參酌。

再參實際發生個資外洩情事之 JTB[11] 案例，所包含之通知項目為 (1) 被侵害之事實及經過。(2) 被侵害之個人資料項目。(3) 免付費聯絡電話及相關窗口。(4) 已採取之現在及未來因應措施。JTB 所通知的內容，均大致與上揭通知實行事項相符。差異點在於是否提供保護自己之資訊，及提供政府保護網站資訊。惟相較於美國加州設立隱私保護辦公室 (California Office of Privacy Protection)，並於網站提供相關資訊，我國目前就個資外洩並無統一處理之主管機關，自無須提供政府保護網站資訊。然就提供保護自己資訊之部分，乃針對個資外洩提醒，係指告訴當事人如何防範未來利用個資之詐騙，在個資外洩包含當事人網站帳號密碼情形，建議可提醒當事人如：「為防詐

[10] California Office of Privacy Protection, Recommended Practices on Notice of Security Breach Involving Personal Information, Rev.January 2012, 8-14

[11] rocketnews24，https://rocketnews24.com/2016/06/14/761411/，2016 年 6 月 14 日（最後瀏覽日：2017 年 12 月 15 日）。

騙，建議檢視您的金融帳號密碼與註冊該網站之帳號密碼是否相同。」

實務上，有些組織或單位會選擇於個資外洩後，在網站上提醒當事人防範詐騙。然若只是提醒防範詐騙，而未告知上揭事項，應認不符合個資法之通知義務。末參法務部法制字第 10502506140 號函要旨：「各中央目的事業主管機關應針對轄下所有特許行業，依個人資料保護法第 27 條規定訂定相關個資檔案安全維護計畫及辦法，而相關辦法就業者對於當事人通知義務事項，應明定通知內容包含**『個資外洩之事實、業者所採取之因應措施及所提供之諮詢服務專線』**。」雖不及上揭美國之通知實行事項，然亦可作為我國通知法律遵循之參考。

3. 通知對象是否包括主管機關：

按個資法第 12 條規定，因個資持有者違反個資法管理義務，致個資外洩事件發生時，個資持有者須以適當方式通知當事人，此部分自不生疑問，惟實務運作上，是否須一併通知主管機關備查，以符合個資法第 27 條之中央主管機關指定之安全維護計畫？

我國各部會如中央銀行、內政部、交通部、金管會、勞動部、經濟部、財政部、教育部等，迄今已陸續發布 20 多項法規命令，如「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」(下稱金融安全維護辦法)、「票據交換所個人資料檔案安全維護計畫標準辦法」等[12]，從上揭既有辦法中，有規定須通報主管機關者，如金融安全維護辦法第 6 條規定：「……非公務機關遇有重大個人資料安全事故者，應即通報本會。」，然大部分辦法並無規定須通報主管機關，以致法務部第 27 條訂定辦法之參考事項所規定，須通報有關單位之意旨[13]，難以實現。

參民國 104 年 2 月 10 日，行政院所屬部門就「消費者個資外洩事件處理機制」研商會議紀錄[14]，本文整理要旨略以：「一、各中央目的事業主管機關應盡速按個資法第 27 條規定訂定相關辦法。二、上揭辦法應明訂業者通報主管機關義務，內容包含外洩事實、因應措施、諮詢服務專線等。」足見，目前實務就個資外洩，雖未有辦法明文規定，各單位及組織均有通報主管機關

[12] 財團法人資訊工業策進會，《個資解碼：一本個資保護工作者必備的工具書》，五南，2015 年 11 月，初版，149-260 頁。

[13] 法務部，中央目的事業主管機關依個人資料保護法第 27 條第 3 項規定訂定辦法參考事項，收錄於：《個人資料保護法規及參考資料彙編》，2013 年 8 月，146-152 頁。

[14] 參行政院發文經濟部，中華民國 104 年 2 月 16 日，院臺消保字第 1040125073 號函附件。

之義務，惟未來明確成立辦法，通報主管機關，應為實務之趨勢。甚且，本文以為，就個資外洩比數達到一定程度以上情形，應由統一之主管機關或政府單位，監督個資外洩後續處理情形，而非僅是備查。

4. 通知方式評估及送達：

(1) 適當通知方式評估

按個資法施行細則第 22 條第 1 項前段規定：「本法第十二條所稱適當方式通知，指即時以**言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之**。但**需費過鉅者**，得斟酌技術之可行性及當事人隱私之保護，**以網際網路、新聞媒體或其他適當公開方式**為之。」足見，就通知方式，除言詞方式無法留下紀錄，較不合適外，只要能使當事人知悉，一切方式皆無不可，惟網際網路、新聞媒體方式，依現行法律須要需費過鉅，方得為之。然網路公告方式，實際上有代替無法通知當事人、迅速發布之功能，實務上即使大部分能以電子郵件或簡訊方式通知當事人，而無須費過鉅情形，仍會考慮併行網路公告方式，進行通知，惟網路公告亦有新聞媒體得自由瀏覽，若有不慎，反而造成公司不名譽，擴大外洩危機的風險。為便利實務考量，就網路公告和個別通知之優、缺點，整理下述表 1：

本文以為，鑑於當事人提供個資時，所留存者未必全部皆為正確資料，除非個資外洩情形確屬輕微，網路公告反而引起外界不必要誤會外，否則建議併同網路公告，以便依當事人所留個資，無從聯絡當事人時，即得主張因需

表 1：適適當通知方式評估

	網路公告	個別通知 (含簡訊、信函及電話)
優　點	1. 執行費用較低。 2. 可迅速於網路發佈。 3. 可適用於無法個別通知當事人之情形。 4. 可展現道歉誠意。	1. 符合個資法查明後通知之規定。 2. 只有內部同仁得瀏覽通知。
缺　點	1. 非內部同仁及新聞媒體均得瀏覽公告。 2. 不易判斷是否符合個資法施行細則規定，網路公告須需費過鉅方得為之要求。	1. 執行時間及費用均較多。 2. 簡訊聯絡容易表達不清楚，致生誤會。 3. 電話聯絡易被誤為詐騙電話，若回答不清楚，易生新的糾紛。 4. 信函聯絡須考量地址正確性，否則信函將被退回而無法送達。

費過鉅，故已按個資法進行適當通知。

(2) 適當通知方式送達

按個資法所規定之通知方式，具有多種，若採某一方式送達，送達至何處才是合法送達？送達時間為何？當不採傳統書面以雙掛號為送達，無法院實務可參酌時候，則有討論必要。因進行通知時，在實務基於成本、留存證據資料考量，鮮有以言語、電話進行通知，故本文以實務進行通知時，最常使用的電子郵件為例，其他簡訊、傳真等非傳統書面類推適用之。

「通知」在法理上屬準法律行為，應適用或類推適用民法規定。而電子郵件屬非對話意思表示，按民法第 95 條第 1 項規定，係以書面達到相對人時發生效力。所謂達到，係指意思表示達到相對人之支配範圍，置於相對人隨時可了解其內容之客觀狀態而言 (最高法院 58 年台上字第 715 號判例參照)。若表意人以書信為意思表示 (或意思通知)，該書信達到相對人，相對人無正當理由而拒絕接收，或相對人已受郵局通知往取書信 (郵件)，該書信既已達到相對人之支配範圍內，相對人隨時可以了解其內容，依上說明，應認為已達到而發生效力 (最高法院 86 年台抗字第 628 號判決參照)。

是故，依個資法規定進行通知時，若以**電子郵件寄至當事人指定並「有效」信箱，即屬已達到相對人之支配範圍內，該通知之送達應為有效**。惟若當事人所留信箱無效，受系統退回時，即未到達相對人可支配範圍，實務該如何處理？本文以為，此時應考慮上揭以網路公告方式通知當事人，作為代替性通知方式。

另就送達時間部分，按電子簽章法第 2 條第 2 款：「電子文件：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，而供電子處理之用者。」、同法第 7 條第 2 項第 1 款前段：「電子文件以下列時間為其收文時間。但當事人另有約定或行政機關另有公告者，從其約定或公告。 一、如收文者已指定收受電子文件之資訊系統者，以電子文件進入該資訊系統之時間為收文時間。」基此，所謂電子郵件係該當為電子簽章法之電子文件，而**當事人的收件時間，則應以該電子文件寄至當事人之信箱系統為準**。

5. 通知具體作業：

當個資外洩事件發生時，公司擁有並得進行通知之資料，通常為當事人信箱、電話及地址。而公司在選擇通知方式時，除網路公告外，亦以寄電子郵件為大宗、電話簡訊次之、書面通知再次之。惟有些當事人只留電子郵件、有

些只留簡訊、有些只留地址、或雖皆有留存，但寄出後發現有誤，實際情形，不一而足。是本文為建立完整之法規遵循，擬同時選擇三種通知方式，並區分為三個階段如圖 1，**於第一階段進行電子郵件發送通知與第一次郵局雙掛號通知，第二階段進行簡訊通知與網站公告，第三階段進行第二次郵局雙掛號通知**。

詳細而言，第一階段電子郵件發送，以密件副本的方式發送給個資當事人兩次，如果第一次發送成功並取得郵件讀取回條者，則不會再發送第二次；若電子郵件發送失敗及含有行動電話號碼者，會以簡訊方式作第二階段第二波簡訊通知，簡訊通知也會發送給個資當事人兩次，如果第一次發送成功者，則不會再發送第二次；而無電子郵件信箱者但，若有正確地址，則會在第一階段第一波以郵局雙掛號通知個資當事人；若是電子郵件發送及簡訊通知都失敗但有正確地址者，則在第三階段會依規劃進行郵局雙掛號通知作業。

另就時程規畫部分，可參考圖 2 所示，電子郵件發送、簡訊通知、及網站公告的通知作業部份為時一週，郵

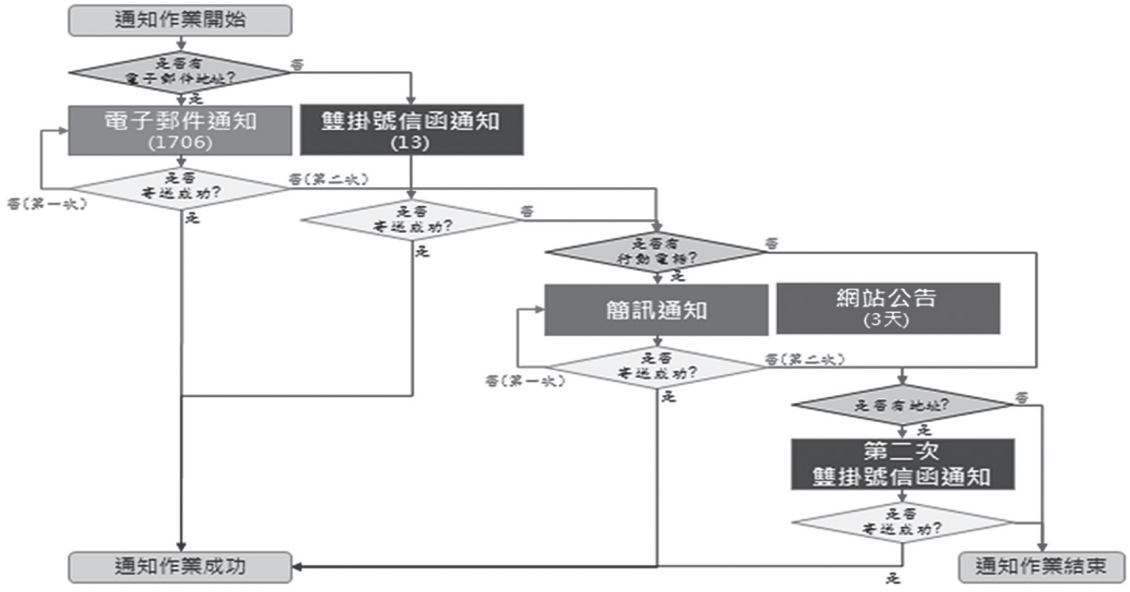

圖 1　通知作業流程圖

資料來源：資策會個資秘書組

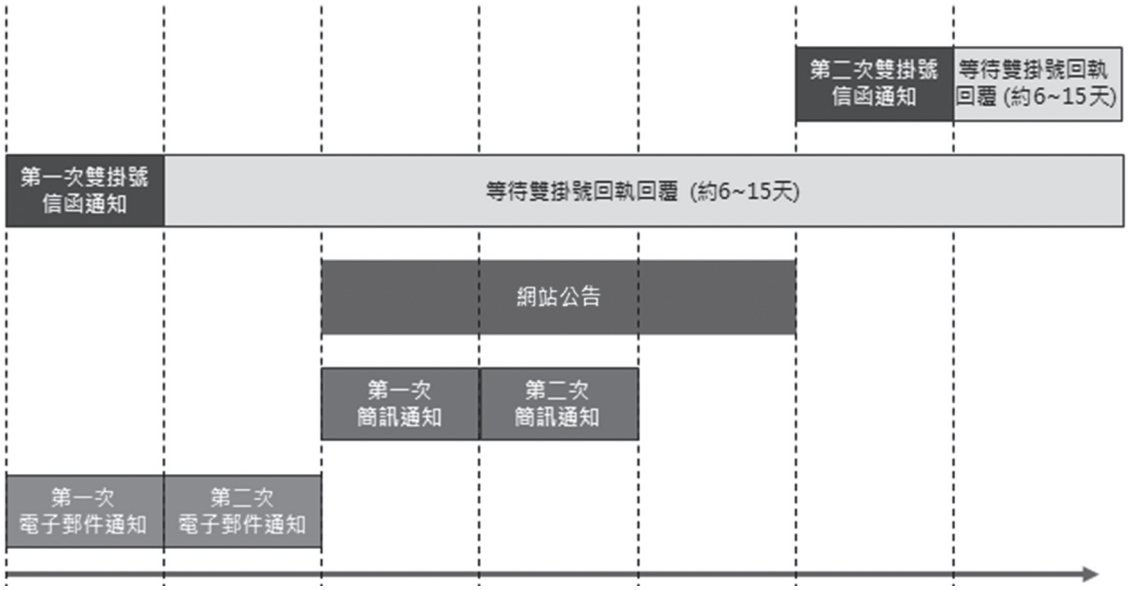

圖 2　通知作業時程規畫

資料來源：資策會個資秘書組

局雙掛號信函通知因有賴於郵局作業時程，因此預估為期兩週，總共時程預計於一個月內通知完畢。

三、個資外洩之後處理義務

按現行個資法規定，個資外洩事件，除了通知當事人外，並沒有明確規定後續該如何矯正、預防及應刪除當事人個資。本文擬就矯正、預防部份及應刪除當事人個資部分分述之：

（一）矯正、預防：

對內就該外洩之系統平台執行弱點掃描，並清查個資，進行個資盤點，並定期稽核；對外就有報名等服務管理功能之網站，判斷有無繼續經營之必要，或是停用繼續蒐集當事人個資之功能，並建立單位及組織內之對外網站管理規範。

（二）刪除當事人個資：

按個資法第 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。」惟現行實務，都是以定型化契約，採「概括目的」之蒐集方式，蒐集之目的及得處理、利用之方式，可謂包山包海，如當事人辦理信用卡，簽訂信用卡契約時，契約內通常約定單位及組織得基於「業務目的」使用，甚至提供保險、基金或其他子公司

使用，亦無明定使用期限，致使個資法之按特定目的蒐集、處理及利用之立法意旨，幾近無法達成，當單位或組織又無明顯提供當事人行使權利之資訊時，當事人往往不堪其擾。

本文以為，個資法第 11 條第 3 項規定，當事人得「事前」書面「概括同意」特定目的或特定目的消失、期限屆滿後，單位或組織仍得使用，應屬錯誤立法，至少在特定目的消失或期限屆滿後，單位或組織應「事後」再取得當事人同意。

另所謂基於業務目的使用，參個資法施行細則第 21 條：「有下列各款情形之一者，屬於本法第十一條第三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。」第一款情形，若當事人係依法令規定或契約定有保存期限，則為保有而留存，則本可解釋為特定目的並未消失；第二款情形，即使查詢立法理由，亦殊難想像有何謂刪除足認侵害當事人利益；第三款情形為其他不能刪除之正當事由，亦非判斷業務所必須之標準。

基此，在個資外洩後，很重要的一部分，應再判斷所外洩之個資，是否還有留存必要，是否屬特定目的早已消失，如辦理信用卡之消費者已剪卡，信用卡銀行當應刪除該當事人個資，而非使其他業務單位或子公司繼續使用；另既已發生個資外洩，仍留存個資，反而屬不刪除將侵害當事人值得保護之利益，故依個資法意旨，自應主動刪除當事人個資。

誠然，在這大數據的時代，各單位及組織莫不致力於蒐集個資，並加以類型化分析，進行資料探勘 (data mining)。惟在個資法定有高額賠償的情況下，擁有大量個資，與其是種利益，倒不如說是一種負擔、責任。故本文以為，個資外洩後，應檢視該外洩及其他個資是否確仍有留存必要，若無留存必要，建議即刪除該外洩之個資，並通知當事人，以降低當事人請求賠償之風險。

四、個資外洩之法律責任

按個資法第 28 條第 1 項至第 4 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。被害人雖非財產上之損害，亦得請求賠償相當之金額**；其名譽被侵害者，並得請求為回復名譽之適當處分。依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以**每人每一事件新臺幣五百元以上二萬元以下計算**。對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求

損害賠償者，**其合計最高總額以新臺幣二億元為限**。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。」、同法第 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。」

基此，當公務機關或非公務機關違反第 27 條規定訂定相關個資檔案安全維護計畫及辦法，或個資法 12 條之適當通知義務時，若造成當事人損害，當事人得以新台幣五百元以上二萬元以下計算賠償金額，總額以 2 億元為限。惟在實務上，當事人因個資外洩，接到詐騙集團電話，進而財物遭到詐騙之情形，得否依個資法第 29 條向個資保有者請求損害賠償？

此部分目前雖無相關判決可資參考，但本文以為，參個資法第 28 條、第 29 條，當事人固無庸證明個資保有者係基於故意、過失而導致個資外洩，惟當事人仍須證明其損害是因個資保有者所造成，亦及當事人仍須證明其損害，與詐騙集團之來電有因果關係。縱然當事人得依個資法第 28 條第 2 項規定請求非財產上的損害，然詐騙集團得到個資的來源則有多端，甚至當事人亦在不同的地方留下個人資料，故除詐騙集團假冒個資保有者名義，對個資集團進行詐騙外，當事人如何證明詐騙集團是自個資保有者取得個資，並因個資保資有者疏未通知當事人，而導致當事人受騙而有損害，顯有困難。

本文認為，實務上我國單位或組織於個資外洩而受求償之風險並不高，故目前尚無實務判決可參，也導致我國個資法遵推行之不暢。是以，本文認為，個資法條文應規定為：「公務或非公務機關於違反個資法規定，致第三人取得個資時，應負損害賠償責任，但公務或非公務機關如能證明無故意過失，或當事人所受損害與違反個資法規定無因果關係時，不在此限。」**以主觀及舉證責任倒置方式，鼓勵當事人提起損害賠償訴訟，以促進個資保有者就個資之保管及維護**。

參、日本法規範及處理

有關日本個人情報保護法制的體系，有所謂的個人情報保護關係 5 法，分為屬於基本法部分之個人情報保護法 (1 章 ~3 章)、屬於民間一般法部分之個人情報保護法 (4 章 ~7 章)、規範公的部門法人之行政機關個人情報保護法、獨立行政法人之個人情報保護法、規範地方公共團體之個人情報保護條例。其立法的特色，在於歐洲式跟美

國式立法的折衷，與歐洲個人資料保護指令，區分公的部門及民間部門，異其規範不同，日本的個人情報保護法是以綜合規範 (omibus) 方式，兼以公的部門及民間部門為整體規範對象，而再就有需要特別規範的民間、公的部門分別片斷化的立法規範[15]。而本文主要以日本之個人情報保護法 (含基本法及民間法) 為主，對照上文所討論的個資法議題，分別介紹日本法規範及處理如下：

一、對應個人情報保護法之系統

按日本之個人情報保護法所規定的三個原理，分別是 (1) 個人同意目的範圍之控制。(2) 利用主體的限定，亦即禁止提供第三人之安全措施確保。(3) 向情報主體之權利行使的對應。而為滿足上揭日本個資法原理，企業即應於內部作出能符合上揭原理之系統，並符合使用者之特殊性，此包括保有期間確定 (原則上只能短期持有)、削除、消去、廢棄時期的明示等[16]。

而就企業或組織內部的情報管理，包含所有個人情報、資料進行一元化管理之系統管理設計。特別是現在隨身碟、USB 等小型可搬運硬碟的興盛，即使非惡意洩漏，員工為了在家工作，亦可能將資料攜出，或接觸了不當的軟體而受到病毒感染，以致資料被竄改、破壞及削減。是以，通過分析風險，控制硬碟就顯得重要，如阻塞外部硬碟的接口及連接埠，為了避免硬拷貝 (hard copy)，而不採影印驅動程式 (copy driver)，在影印時對操作者作特定記號、影印時點及版本之記號、企業電腦的攜出禁止、設定密碼、log 記錄保管等情報安全對策[17]。

二、初動調查

所謂初動調查，是指企業從查知個人情報流出的可能性到對本人的通知及對媒體的公布，即相當於我國的查明後通知。其查明目的在於 (1) 把握企業或組織發生了什麼事，及對於該事件之風險測定。(2) 進行是否對本人通知或媒體公布之判斷材料。(3) 通知或公布之際，事實說明及原因究明之材料。(4) 發現並修復安全上缺陷。而調查項目包含 (1) 是否確定流出。(2) 流出個人情報項目。(3) 流出的件數、規模。

---

[15] 宇賀克也，《個人情報保護法の逐条解説》，2016 年 11 月 25 日，有斐閣，五版，26-28 頁。

[16] 田中克幸、大塚和成、竹内朗、鶴巻暁，《個人情報流出対応にみる実践的リスクマネジメント》(別冊 NBL (No.107))，商事法務，2006 年 2 月，7-9 頁。

[17] 稲垣隆一，《個人情報保護法と企業対応》，清文社，2003 年 10 月 25 日，74-76 頁。

(4) 流出的範圍、原因及期間。(5) 防止再發生的可能性[18]。

三、本人通知

本人通知的目的在於傳達當事人個資流出、道歉等第一次受害的事實；並提醒注意當事人，不再遭遇第二次被害。有關於通知時期，如電氣通信事業指導方針第 22 條第 1 項規定：「應盡速地將個資外洩的事實通知本人」，亦即日本也僅有盡速通知的努力規定，但一般實務也認為，事實確認後，若為免於非難，應先於媒體報導前先行通知。而有關通知內容，應包括 (1) 事實關係 (2) 道歉 (3) 提醒注意 (4) 原因究明 (5) 詢問窗口。另在通報主管機關方面，各產業指引綱領 (guideline) 大多有規定須通報主管機關，如：金融領域綱領第 22 條第 1 項規定：「個資外洩發生的場合，須向金融當局直接報告。」而在通知當事人方面，則著重於向大眾公布，迴避造成當事人第二次損害，不論以媒體、網路公告、新聞記者會形式均可，如金融領域綱領第 22 條第 2 項規定：「就洩漏之事實關係及再發防止對策，應盡早公布」[19]。

四、法律風險

日本個人情報保護法第 20 條至第 22 條，賦予企業在個人資料的利用上，有為安全管理加上適切措施的義務。而就違反該義務，所應承擔的法律風險，分述如下[20]：

（一）損害賠償

按日本個人情報保護法第 20 條意旨，個人情報處理及利用之企業，居有個人資料的安全管理義務。情報主體基於契約 (附隨義務) 或法律上義務，安全措施不備，以致個人資料外洩時，即應對當事人的一次被害，負損害賠償責任。作為個資外洩而受損害賠償責任的事件，考參考「宇治市情報外洩事件」(詳細報導可參 http:// www.kyotonews.org/uji-juki/index.html)。又上揭宇治市情報外洩事件中，當事人流出的個資包含姓名、性別、出生年月日、住所外，還包含戶籍等資料，而這些資料不只向名簿販賣業者流出，並被作成廣告上網販賣。然法院認為，此等不安、精神上苦痛尚難稱巨大，並考量宇治市已致力回收資料、對市民公布並說明並擬定防止對策等情事，認就此一

---

[18] 田中克幸、大塚和成、竹內朗、鶴巻暁，《個人情報流出対応にみる実践的リスクマネジメント》(別冊 NBL (No.107))，商事法務，2006 年 2 月，7-9 頁。

[19] 田中克幸、大塚和成、竹內朗、鶴巻暁，《個人情報流出対応にみる実践的リスクマネジメント》(別冊 NBL (No.107))，商事法務，2006 年 2 月，19-21 頁。

[20] 稲垣隆一，《個人情報保護法と企業対応》，清文社，2003 年 10 月 25 日，71-81 頁。

次被害情事，當事人得請求之精神賠償慰撫金，以 1 萬日圓為適當，可供我國實務借鏡。

另在一次被害之賠償請求場合，固無問題，然在被害者個資遭他人濫用，而有二次被害之情形，則應視被害者方過失責任有無、程度的差異，而有過失相抵之適用。然原本在討論二次被害之賠償時，就個人情報流出跟當事人損害間，是否具有相當因果關係就有極大的討論。縱承認有相當因果關係，亦須討論被害者有無過失，而被害者有無注意義務之違反，則須視基礎事實而定，被害者接受到個資外洩企業之通知，並提醒防範個資遭濫用，被害者即應自行提高注意義務，以免被害。即使被害人確實遭受恐嚇、詐欺的時候，仍應視受恐嚇及詐欺的情節，討論被害者是否應適用過失相抵，減低其損害賠償請求[21]。

是以，在日本於各種綱領均規範，於個資外洩的場合，為防止二次被害發生，故有向被害者通知及公布之規定，而從減免損害賠償之觀點來看，這樣的措施顯有重要性。

（二）禁止請求權、假處分

個人情報保護請求權係以日本憲法第 13 條作為基礎，對於有侵害之虞時，可對侵害行為的假處分或對行為組成物作出廢棄請求。如 1997 年 2 月 12 日神戶地方裁判所即作出假處分，禁止對造成隱私權侵害之雜誌出版、販賣及公布；又如 1991 年 9 月 26 日東京高等裁判所即針對未經授權而登載藝人姓名及相片之月曆，作出該行為組成物的廢棄請求。

（三）委託者作為被害者之行動

在企業委託外部廠商處理及利用的場合，當外部廠商發生個資事故，則委託者則亦與被害者基於相同地位。在委託者企業受到主管機關要求，進行矯正對策、損害填補等適切行為時，為查明外部廠商之故意、過失，及外洩原因事實，自得對外部廠商之系統及平台，作禁止請求權及假處分之請求。

（四）行政規制

日本個人情報保護法第 32 條至第 34 條規定，於企業欠缺安全管理措施時，除了向主管機關報告，並接受終止、改正勸告，在產生個人急迫重大利益場合，則應接受緊急命令。甚至在個資法規定以外法領域，如針對金融監督機關等行政機關就個人資料的檢查，企業也有配合義務，可參 2002 年

[21] 田中克幸、大塚和成、竹內朗、鶴巻暁，《個人情報流出対応にみる実践的リスクマネジメント》（別冊 NBL (No.107))，商事法務，2006 年 2 月，55 頁。

6 月 19 日瑞穗事件，日本金融廳對於瑞穗集團，即按銀行法第 26 條規定，以業務改善命令，命迅速提出個資之改善、對應策略 (詳細報告可參 http://www.mizuho- co.jp/release/2002/news/news_ 020619_1.html)。

肆、結語

歐洲議會歷經 4 年的討論後，在 2016 年 4 月 27 日通過 GDPR（EU General Data Protection Regulation，GDPR），於 2016 年 5 月 25 日生效，並給歐盟各國 2 年的緩衝過渡期，**預計在 2018 年 5 月 25 日正式實施。是近年來，影響全球資料保護最大的法規**。不管法人或自然人，不論公司規模大小，擁有的歐洲民眾個資多寡，只要你的網站或服務提供歐盟民眾瀏覽使用，或者是會搜集、處理和利用歐盟公民資料的企業或組織，到明年 5 月之前，都必須從內部程序至資安系統加以調整，以便能夠符合 GDPR 對於個資保護的規範和要求。

規範中，其個資保護之範圍，包含所有個人可識別資訊（Personally Identifiable Information，PII），甚至包含網路瀏覽器中的 Cookie、網路 IP 位址。一旦爆發個資外洩，不論是資料控制者 (Data Controller) 或是資料處理者（Data Processor），**必須要在 72 小時內，即刻通報給資料保護主管機　關**（Data Protection Authority）；但是，**若外洩資料對於當事人會造成重要危害時，也應該要及時通知當事人**，惟對於應在多久期間內，將個資外洩情事通知當事人，則沒有明確規定，亦可以公告形式通知當事人。另依外洩情結輕重，**可罰款 2 千萬歐元（新臺幣 7.2 億元）或全球營業額 4% 作為罰款（取其金額較高者，作為罰款）**[22]。

是以，在這波個資法的全球化的浪潮下，臺灣面對個資外洩事件，如何提高自身法律規範，以符合 GDPR 要求，是當前刻不容緩的問題。如 2010 年個資法修正時，雖於第 12 條新增個資外洩通知義務，惟卻未規定須通知主管機關，造成主管機關無法及時處理個資外洩情事，此即不符合 GDPR 的要求。然我國目前並無統一且獨立之主管監督機關，就企業界個資外洩之監督、法令解釋及法遵要求、安全維護及標準、跨國個資傳輸

[22] Home Page of EUGDPR，https://www.eugdpr.org/key-changes.html，最後瀏覽日：2017 年 12 月 15 日。

等問題，如何符合國際化標準，殊有疑義[23]。本文僅以實務處理經驗，供作目前參考，亦盼望國內主管機關盡早成立統一且獨立之個資監督機關，正視我國個資外洩情事，並提昇國內法規遵循標準。

參考文獻

California Office of Privacy Protection, Recommended Practices on Notice of Security Breach Involving Personal Information, Rev.January 2012, 8-14.

宇賀克也，《個人情報保護法の逐条解説》，2016 年 11 月 25 日，有斐閣，五版，26-28 頁。

田中克幸、大塚和成、竹內朗、鶴巻暁，《個人情報流出対応にみる実践的リスクマネジメント》(別冊 NBL (No.107))，商事法務，2006 年 2 月，7-23 頁。

稲垣隆一，《個人情報保護法と企業対応》，清文社，2003 年 10 月 25 日，71-81 頁。

陳宏志，個資法修正後當事人同意及委外監督管理實務之因應，《科技法律透析》，第 28 卷第 10 期，2016 年 10 月 15 日，13-19 頁。

法務部，中央目的事業主管機關依個人資料保護法第 27 條第 3 項規定訂定辦法參考事項，收錄於：《個人資料保護法規及參考資料彙編》，2013 年 8 月，146-152 頁。

經濟部工業局，《個人資料法規遵循參考指引暨宣導手冊》，2013 年 10 月 22 日，14-21 頁。

財團法人資訊工業策進會，《個資解碼：一本個資保護工作者必備的工具書》，五南，2015 年 11 月，初版，149-260 頁。

法務部，《歐盟及日本個人資料保護立法最新發展之分析報告》，受託單位：東海大學，2016 年 12 月 30 日，169-170 頁。

[23] 法務部，《歐盟及日本個人資料保護立法最新發展之分析報告》，受託單位：東海大學，2016 年 12 月 30 日，169-170 頁。