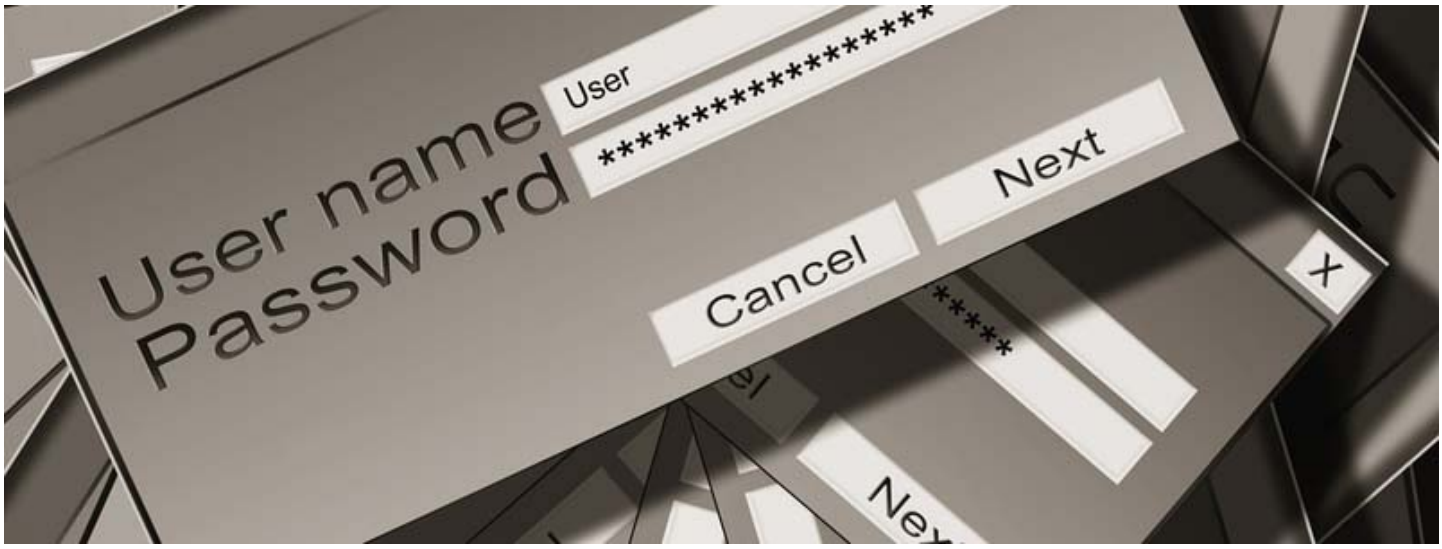
歐盟資料保護工作小組修正通過個人資料侵害通報指引



歐盟資料保護工作小組修正通過「個人資料侵害通報指引」

資訊工業策進會科技法律研究所
法律研究員　李哲明
2018年3月31日

壹、事件摘要

因應歐盟「通用資料保護規則」（The General Data Protection Regulation，或有譯為一般資料保護規則，下簡稱GDPR）執法即將上路，針對個人資料侵害之通報義務，歐盟資料保護工作小組（Article 29 Data Protection Working Party, WP29）特於本（2018）年2月6日修正通過「個人資料侵害通報指引」（Guidelines on Personal data breach notification under Regulation 2016/679），其中就GDPR所規範個資侵害之定義、對監管機關之通報、與個資當事人之溝通、風險及高風險評估、當責與紀錄保存及其他法律文件所規定之通報義務等，均設有詳盡說明與事例。

貳、重點說明

一、何謂個資侵害？個資侵害區分為哪些種類？

依據GDPR第4條（12）之定義，個資侵害係指：「個人資料因安全性之侵害所導致意外或非法之毀損、喪失、修改、未經授權之揭露、存取、個資傳輸、儲存或其他處理。」舉例來說，個人資料之喪失包括含有控制者（controller）顧客資料庫的備份設備之遺失或遭竊取。另一例子則為整份個資的唯一檔案遭勒索軟體加密，或經控制者加密，但其金鑰已滅失。依據資訊安全三原則，個資侵害之種類區分為：

1. 機密性侵害（Confidentiality breach）：未經授權、意外揭露或獲取個人資料。
2. 完整性侵害（Integrity breach）：未經授權或意外竄改個人資料。
3. 可用性侵害（Availability breach）：在意外或未經授權之情況下，遺失個人資料存取權限或資料遭銷燬。

二、何時應為通知？

按GDPR第33條（1）之規定，當個資侵害發生時，在如果可行之情況下，控制者應即時（不得無故拖延）於知悉侵害時起72小時內，依第55條之規定，將個資侵害情事通報監管機關。但個資侵害不會對自然人之權利和自由造成風險者，不在此限。倘未能於72小時內通報監管機關者，應敘明遲延之事由。

三、控制者「知悉」時點之判斷標準為何？

歐盟資料保護工作小組認為，當控制者對發生導致個人資料侵害的安全事件達「合理確信的程度」（reasonable degree of certainty）時，即應視為其已知悉。以具體事例而言，下列情況均屬所謂「知悉」：

1. 在未加密個人資料的情況下遺失USB密鑰（USB Key），通常無法確定是否有未經授權者將獲致存取資料權限。即使控制者可能無法確定是否發生機密性侵害情事，惟仍應為通知，因發生可用性侵害之情事，且已達合理確信的程度。

故應以控制者意識到該密鑰遺失時起為其「知悉」時點。

1. 第三人通知控制者其意外地收到控制者的客戶個人資料，並提供該揭露係未經授權之證據。當侵害保密性之明確證據提交控制者時，即為其「知悉」時點。如：誤寄之電子郵件，經非原定收件人通知寄件者之情形。
2. 當控制者檢測到其網路恐遭入侵，並針對其系統進行檢測以確認個人資料是否遭洩漏，嗣後復經證實情況屬實，此際即屬「知悉」。
3. 網路犯罪者在駭入系統後，聯繫控制者以索要贖金。在這種情況下，控制者經檢測系統並確認受攻擊後，亦屬「知悉」。

值得注意的是，在經個人、媒體組織、其他來源或控制者自我檢測後，控制者或將進行短暫調查，以確定是否發生侵害之事實。於此調查期間內所發現之最新侵害情況，控制者將不會被視為「知悉」。然而，控制者應儘速展開初步調查，以形成是否發生侵害事故之合理確信，隨後可另進行更詳盡之調查。

四、共同（聯合）控制者之義務及其責任分配原則

GDPR第26條針對共同控制者及其如何確定各自之法遵義務，設有相關規定，包括決定由哪一方負責遵循第33條（對主管機關通報）與第34條（對當事人通知）之義務。歐盟資料保護工作小組建議透過共同控制者間之契約協議，約明哪一方係居主要地位者，或須負責盡到個資侵害時，GDPR所定之通知義務，並載於契約條款中。

五、通報監管機關與提供資訊義務

當控制者通報監管機關個資侵害情事時，至少應包括下列事項

（GDPR第33條（3）參照）：

1. 敘述個人資料侵害之性質，包括但不限於所涉之相關個資當事人、個資紀錄及其類別、數量。
2. 傳達資料保護長（DPO）或其他聯絡人之姓名與聯絡方式，俾利獲得進一步資訊。
3. 說明個資侵害可能之後果。
4. 描述控制者為解決個資侵害業已採取或擬採行之措施，在適當情況下，酌情採取措施以減輕可能產生之不利影響。

以上乃GDPR要求通報監管機關之最基本事項，在必要時，控制者仍應盡力提供其他細節。舉例而言，控制者如認為其處理者係個資侵害事件之根因（root cause），此時通報並指明對象即可警示委託同一處理者之其他控制者。

六、分階段通知

鑒於個資事故之性質不一，控制者通常需進一步調查始能確定全部相關事實，GDPR第33條（4）爰設有得分階段通知（notification in phases）之規定。凡於通報時，無法同時提供之資訊，得分階段提供之。但不得有不必要之遲延。同理，在首次通報後之後續調查中，如發現該事件業已受到控制且並未實際發生個資侵害情事，控制者可向監管機關為更新。

七、免通報事由

依據GDPR第33（1）條規定，個資侵害不會對自然人之權利和自由造成風險者，毋庸向監管機關通報。如：該遭洩露之個人資料業經公開使用，故並未對個人資料當事人構成可能的風險。

必須強調的是，在某些情形下，未為通報亦可能代表既有安全維護措施之缺乏或不足。此時監管機關將可能同時針對未為通報（監管機關）或通知（當事人），以及安全維護措施之缺乏或不足，以違反第33條或（及）34條與第32條等獨立義務規定為由，而依第83條4（a）之規定，併予裁罰。

參、事件評析

一、我國企業於歐盟設有分支機構或據點者，宜指派專人負責法遵事宜

揆諸GDPR前揭規定，當個資侵害發生時，控制者應即時且不得無故拖延於知悉時起72小時內，將個資侵害情事通報監管機關。未能履踐義務者，將面臨最高達該企業前一會計年度全球營業額之2%或1千萬歐元，取其較高者之裁罰。我國無論金融業、航運業、航空運輸業、電子製造業及進出口貿易業者等，均或有於歐盟成員國境內或歐洲經濟區（European Economic Area）當地設立子公司或營業據點。因此，在GDPR法遵衝擊的倒數時刻，指派具瞭解GDPR規定、當地個資隱私法遵規範、擅長與隱私執法機構溝通及充要語言能力者專責法遵業務實刻不容緩。蓋此舉可避免我國企業母公司鞭長莫及，未能及時處置而致罹法典之憾。

二、全面檢視個資業務流程，完備個資盤點與風險評鑑作業，掌握企業法遵現況

企業應全面檢視業務流程，先自重要核心業務中析出個資作業流，搭配全面個資盤點，並利用盤點結果進行風險評鑑，再針對其結果就不同等級之風險採行相對應之管控措施。此外，於全業務流程中，亦宜採行最小化蒐集原則，避免蒐集過多不必要之個人資料，尤其是GDPR所定義之敏感個資（如：種族、民族血統、政治觀點、宗教信仰、哲學信仰、工會會員資格等個人資料，及遺傳資料的處理，用於識別特定自然人之生物識別資料、健康資料、性生活、性取向等）或犯罪前科資料，俾降低個人資料蒐集、處理、利用、檔案保存及銷燬之全生命週期流程中的風險。此舉亦契合我國個人資料保護法第5條所揭櫫之原則。

三、立法要求一定規模以上之企業須通過個資隱私法遵第三方認（驗）證，並建置認證資訊公開平台

鑒於國際法遵衝擊以及隱私保護要求之標準線日漸提升，我國企業除自主導入、建置並維運相關個資保護與管理制度以資因應，更有賴政府透過法令（如：修正個人資料保護法）強制要求一定規模以上之企業通過第三方專業驗證，俾消弭風險於日常準備之中。蓋我國具一定規模以上企業，無論其係屬何種業別，一旦違反國際法遵要求，遭致鉅額裁罰，其影響結果將不僅止於單一企業，更將嚴重衝擊該產業乃至於國家整體經貿發展。職是，採法律強制要求企業定期接受獨立、公正及專業第三方認（驗）證，咸有其實益性與必要性。

你可能會想參加

→ 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
→ 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
→ 供應鏈資安國際法制與政策趨勢分享會
→ 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 商業服務業個資保護宣導說明會
→ 個人資料保護新思維企業法遵論壇
→ 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座

→ 智慧港灣/休憩/育樂面面觀–跨界在地合作新商機
→ 中部場–商業服務業個資保護工作坊
→ 南部場–商業服務業個資保護工作坊
→ 北部場–商業服務業個資保護工作坊
→ 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

李哲明
法律研究員 編譯整理

上稿時間：2018年03月

文章標籤

推薦文章