義不容隱--個資法「通知義務」相關規定淺介

蔡柏毅 / 金融聯合徵信中心　法務室

一、前言

個人資料之蒐集、處理、利用通常發生在資料主體（當事人）所得控制範圍之外，其本質即易於被侵害，若資料之控管者刻意或消極隱匿事故的發生，不僅當事人無從得知其個資被侵害而置於危險處境之事實，無法及時彌補或防止損害繼續擴大。即令有監督管理之法定權限的主管機關，如未獲得控管者通報，往往僅能在事後進行裁罰，無法從源頭降低個資事件的潛在負面影響。因此，個資保護法規通常對資料之控管者課以對監管機關之通報義務，以及向資料主體所為之通知義務。

行政法上規範之通報義務並不少見，例如洗錢防制法規定就大額交易、可疑交易負有通報義務（第9條、第10條）；資恐防制法對特定金融事業及律師、會計師、記帳士等課予通報義務（第7條）；傳染病防治法規定發現法定傳染病之個案時，應向衛生主管機關通報（第39條）；其餘如性別平等教育法、家庭暴力防治法、兒童及少年性剝削防制條例等，亦均有通報義務之規定。究其性質與目的，不外乎使主管機關儘先得知相關事件之發生，以採取必要之監督管理作為，具有高度之公益性及規制性。

資料控管者蒐集資料主體的個人資料，其資訊流並非只有單向，而係雙向。個資保護法規課予控管者對資料主體至少負有三項資訊提供義務，包括蒐集資料前的告知義務（duty of disclosure）、個資侵害事故一旦發生後的通知義務（notification obligation）、以及賦予資料主體接近使用其所受蒐集之個人資料之資訊近用權（right of access）[1] 等，含括事前與事後、主動與被動等情況，亦即資訊透明原則（transparent information）[2] 的體現。

1　例如GDPR第15條規範資料主體得向控管者確認其個人資料是否被正確處理，得行使之接近使用權。或我國個資法第3條規定當事人就其個人資料依本法得行使之5項權利，包括：得查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除等。

2　資訊透明原則規範於GDPR第12條至第15條。

然而，普遍性的通報義務與通知義務，其執法成本（enforcement costs）與遵法成本（compliance costs）負擔相當高，況且過於頻繁的通知，反而容易造成「狼來了」效應（cry wolf effect），從而容易對早期預警失去應有的警覺與關注，對資料主體的保護不一定有正面效益。本文擬引介歐盟有關向監管機關通報與向資料主體通知之程序設計與相關機制，並與我國個資法相關制度與規範，及具體落實規定之要求等層面進行比較法的討論。

二、GDPR 中與通報義務及通知義務相關之條文

摘錄歐盟個人資料保護規則（General Data Protection Regulation，本文簡稱'GDPR'）前言（recitals）與法條本文中與「通報及通知義務」相關之條文如下：

（一）前言（85）：

「若未受到適當且及時（appropriate and timely manner）之處置，個人資料之侵害（personal data breach）可能造成當事人身體上、物質上或非物質上之損害（physical, material or non-material damage）。例如喪失對其個人資料之控制或對其權利之限制、遭受歧視、身分盜用或詐欺、金融損失、假名化之未經授權被還原（unauthorised reversal of pseudonymisation）、名譽損害、受職業性秘密保護個人資料之機密性喪失、或其他任何有關所涉及當事人之顯著經濟或社會性之不利益（economic or social disadvantages）等。因此，一旦控管者發現個人資料侵害已然發生，應即向監管機關通報，並不得無故遲延，且若情況許可，應於查覺或發現（become aware of it）後72小時內通報，惟控管者如得以證明依課責原則（accountability principle），該個人資料之侵害不可能造成當事人之權利或自由的風險者，不在此限。如該通報無法於72小時內到達時，遲延之原因應與該通報一併提交，並且不得有更進一步之無故遲延。」

（二）前言（86）：

「當個人資料侵害可能造成當事人權利或自由之高度風險時，為使其得以採取必要之防範措施（necessary precautions），控管者應通知資料主體個人資料之侵害，不得無故遲延。該通知應描述個人資料侵害之本質（the nature of the personal data breach）及對該當事人降低潛在不利影響（mitigate possible adverse effects）之建議。對資料主體之通知，應儘快、合理、可行，且與監管機關密切合作，控管者應遵循監管機關、或其他相關機關如執法單位（law-enforcement authorities）等之指導。此外，為降低損害之立即風險（mitigate an immediate risk of damage）之目的，必須即時與資料主體溝通，但執行適當措施以對抗繼續性或類似之個人資料侵害之需求，則得容許較長之通知時間。」

（三）前言（87）：

「應查明是否已實行所有適當之科技上之保護與組織化之措施（technological protection and organisational measures），以立即確認個人資料侵害是否發生，並儘速通報監管機關及通知資料主體。判斷該通報與通知非無故遲延

（without undue delay）之事實，尤須考量個人資料侵害之本質、嚴重性及其對資料主體之結果與不利影響等。監管機關接獲通報後，得依本規則所定之任務與權力，介入個人資料侵害事故之調查。」

（四）前言（88）：

「在訂定個人資料侵害之通報與通知所適用之形式及程序上之細節性規定時，應適當考量（due consideration）侵害之具體情形，包括：資料是否已受到適當技術措施之保護、是否已有效限制身分詐騙或其他形式濫用之可能性。此外，如過早之資訊揭露反而可能會對個人資料侵害情形之調查造成無謂之妨礙時，該等規定及程序應同時考量執法機關之正當利益（legitimate interests）。」

（五）前言（89）：

「歐盟指令第 95/46/EC號規範向監管機關通報個人資料處理之一般性義務。然而該義務造成了行政上與財政上過重之負擔（administrative and financial burdens），且並非所有情況下都對提升個人資料之保護有所助益。因此該未加區別（indiscriminate）之普遍通知義務應予廢除，改以注重依處理活動之本質（nature）、範圍（scope）、脈絡（context）與目的（purposes）等特徵，區分容易對當事人權利或自由造成高度風險之種類的加以取代。該處理活動之種類尤其可能涉及新技術之使用，或未曾由控管者實施資料保護影響評估，或隨著處理時間的經過而逐漸變得有必要通報之新類型處理活動等。」

（六）本文第4條「定義（Definitions）」：

.....

(12)「個人資料侵害」係指違反安全原則（a breach of security）導致傳輸、儲存或以其他方式處理之個人資料遭受意外的或非法的（accidental or unlawful）破壞（destruction）、遺失（loss）、變更（alteration）、未獲授權之揭露或接近使用（unauthorised disclosure of, or access to）等。

（七）本文第33條「向監管機關進行個人資料侵害之通報（Notification of a personal data breach to the supervisory authority）」：

1.於個人資料侵害發生時，控管者應即依第55條規定向各該監管機關通報，不得無故遲延，如可能，應於查覺或發現後72小時內通報，但個人資料之侵害對當事人的權利或自由不造成風險時，不在此限。如未於72小時內向監管機關通報，該通報應附帶說明遲延之事由。

2.處理者查覺或發現個人資料侵害後，應即通報控管者，不得無故遲延。

3.第1項之通報應符合下述規定：

(a)描述個人資料侵害之本質，如可能，應包括所涉及之資料主體類型（categories）及大致之數量（approximate number）、以及個人資料紀錄之類型及大致之數量；

(b)告知資料保護員（data protection officer）之姓名及其聯絡細節，或其他得以獲得更多相關資訊之聯絡窗口；

(c)描述個人資料侵害之可能結果；

(d)描述控管者已採取或預計採取用以處理個人資料侵害之措施，如適當，應包括得以降低可能不利影響之措施。

4.暫時無法提供應通報之全部資訊時，得分階段提供（provided in phases），惟不得有進一步之無故遲延。

5.控管者應記錄個人資料侵害，包括與該個人資料侵害相關之所有事實、其影響、及已採取之救濟措施（remedial action taken）。該等記載應得由監管機關事後查驗是否與本條規定相符。

（八）本文第34條「向資料主體為個人資料侵害之通知」（Communication of a personal data breach to the data subject）」：

1.於個人資料侵害可能導致當事人權利或自由之風險時，控管者應通知資料主體個人資料侵害之事實，不得無故遲延。

2.本條第1項所稱向資料主體之通知，應以清晰平易之語言（clear and plain language）描述前揭個人資料侵害，並至少包括第33條第3項第(b)、(c)、及(d)等各款資訊及相關措施。

3.本條第1項所稱向資料主體之通知，如有符合下列條件之一者，得無須被要求為之：

(a)控管者已執行適當之科技化與組織化之措施，並已適用於該次遭受資料侵害影響之個人資料時。特別在該等措施已足以使未獲授權接近使用之人無法識別該個人資料者，例如加密（encryption）；

(b)控管者已採取之後續措施，足以確保第1項所稱對資料主體權利或自由之風險將不會實現；

(c)涉及不成比例之勞費（disproportionate effort）。惟於此情形，應有公共溝通（public communication）或類似措施取代，以使資料主體獲得同等有效之通知（in an equally effective manner）。

4.控管者尚未依本條規定通知資料主體有關個人資料之侵害前，監管機關得考量該個人資料侵害所可能導致之高度風險，要求控管者進行通知，或亦得逕行認定已符合本條第3項所定之任一要件。

三、向監管機關進行之通報與向資料主體所為之通知

GDPR與1995年歐盟個人資料保護指令（Directive EU 95/46/EC）相較，在向監管機關進行通報與向資料主體進行通知的規定部分略有不同。於個資侵害事故發生時，資料控管者應通報監管機關；如涉及跨國境之個資事故，則應通報首要監管機關，且在特定情況下應通知受影響的資料主體。惟本次刪除有關通報個人資料處理之一般性義務規定，控管者進行資料之蒐集、處理，原則上毋須通報。

控管者於個資侵害發生時，如未履行上述通報義務及通知義務，監管機關可依GDPR第58條之規定命其改正，如未改正者，即可能遭受第83條規定的相關裁罰[3]。個資侵害事故的發生，亦顯示控管者對於資料的安全維護措施未

3 可參閱本刊第38期「法規時論」專欄刊載之拙著<有過必悛–違反個資法的責任與罰則>，2021年6月。

盡周全，因此監管機關除了可以控管者未通報或通知個資侵害事故為由，而施以裁罰外（違反GDPR第33、34條），亦可能同時以控管者安全維護措施不當而予以裁罰（違反GDPR第32條）。

判斷個資侵害事故的「態樣」

個資侵害事故依其性質，可區分為以下三種樣態：

- 「機密性」侵害（confidentiality breach）：個人資料遭未經授權之存取、揭露、外洩或遺失（loss）；
- 「完整性」侵害（integrity breach）：個人資料遭未經授權之竄改或變更（alteration）；
- 「可用性」侵害（availability breach）：個人資料遭到未經授權之毀損或破壞（destruction），或因而導致無法存取。

上述個資侵害態樣並非絕對的分類，實際上可能單獨發生或同時併存。相對於「機密性」或「完整性」的侵害，「可用性」的侵害可能較不容易判斷。一般而言，當控管者無法從備份或藉由其他途逕取回資料，即構成「可用性」的喪失。例如當一個機構在正常營運期間遭斷電，或發生其他導致服務中斷之攻擊，而使所保管之個資無法取得，亦屬於暫時喪失可用性之情形。

「暫時性」可用性的喪失，是否會被認為構成GDPR所定義之個資侵害事故，而應通報監管機關及通知當事人呢？參照GDPR規定，個資蒐集與利用上的安全性係指採取「技術上及組織上的措施」來確保適當安全性，確認足以應付並處理相關風險，包括用來處理個資的系統與服務必須確保持續其機密性、完整性、可用性與快速復原（resilience）的能力等。如遇到相關物理上或技術上侵害事故，可即時回復對個人資料的可用性。因此在發生安全性事故（security incident）而造成一段期間內喪失資料庫的可用性，也可能構成個資侵害事故，因為資料即使是暫時無法取得，也可能對資料主體的自由或權利造成影響。

例如，醫院如有攸關病患醫療的重要資訊無法取得，即使只是暫時性，也將對病患人身或健康權利造成不可回復的重大風險，攸關生命的手術可能因此無法進行而影響生存。相對而言，媒體公司因斷電數小時而無法將播送新聞，則難以認為對個人權利及自由造成高度風險。因此，服務中斷是否構成「可用性」個資侵害，須與導致當事人權利或自由風險之可能性綜合判斷。

惟縱然不構成可用性的喪失，仍須評估是否構成其他應通報之事由。例如受勒索病毒（ransomware）影響，導致經營保管的資料庫被加密而鎖住，雖可透過完整的備份資料庫回復，僅暫時性喪失可用性，然而因系統被侵入之事實確然已經發生，入侵的駭客可能已經存取並竄改相關資料，甚至可能複製並傳輸資料庫內的個資，此時已屬構成「機密性」或「完整性」的喪失，對當事人權利及自由造成重大風險，於此情形則必須進行通報。

判斷個資侵害事故「知悉」的時點

資料侵害事故發生後，資料控管者應於「知悉侵害事故」後儘速（最遲不得晚於72小時）向監管機關通報，除非該侵害事故不太可能對個人之權利及自由造成風險（GDPR第33條）。所謂控管者對侵害事故的「知悉」（become aware of it）係指，控管者相當程度上確信已發生足以影響個人資料之安全事件。由於GDPR要求控管者應採取所有適當之安全維護措施以保護資料，包括運用科技上之保護與組織化的措施（technological protection and organisational measures）即時偵測是否發生侵害事故。控管者有義務確保其具有可即時發現侵害事故發生之設備與技術，不能諉為「不知」而脫免義務與責任，因為「不知」侵害事故發生，意味著安全維護措施確有不當，此亦為課責原則（accountability principle）的體現。

因應個資侵害事故的處理，控管者宜事先擬訂相關作業方針，制訂一套包括應變、通報、通知及預防的機制，即「整體個資侵害事故回應方案」（breach response plan），於知悉事故發生後，得以即時發現個資侵害、評估風險、確認是否必須通報主管機關及通知當事人，此種預備性回應方案，即控管者應對個資事故的標準作業流程（SOP, Standard Operation Procedure），有助於即時妥善因應個資侵害事故，避免遺漏，並可作為有效之安全維護措施的一環。

為偵測及決定如何處理個資侵害事故，控管者必須進行內部調查以找出資料處理過程是否有任何異常，控管者及處理者可透過各種技術，包括資料處理流程（data flow）及日誌分析（log analysis）來找出可能原因，並透過關聯紀錄檔案（log data）進行判讀。一旦確認為侵害事故，首先必須往上回報至管理階層，接著應通知至內部專責人員（如未設置專責資料保護員，則為法務、稽核及相關技術部門如資訊、資安人員等），該等人員應負責確認侵害事故、評估可能風險並採取必要措施，確認事故的性質及範圍，並進行適法之後續處理與通報。

在資料控管者進行內部調查確認是否發生個資侵害事故及蒐集證據的期間，尚不會被認定為已經「知悉」，但此項初步調查應及早完成，亦即，初步確認的時間不能過長。在完成調查，確認構成「知悉」事故發生之後，控管者即須接著評估對資料主體可能造成的風險，以確定是否須要通報監管機關並通知當事人，同時應採取適當的補救措施，以控制侵害事故的擴大，並以回復侵害之前的原狀為第一優先事項。最後，則應妥善記錄個資侵害事故的始末，並確實保留備查。

資料控管者雖已「知悉」有個資侵害事故，但可能尚未掌握所有資訊以確知並判斷影響程度，為避免延滯通報，GDPR允許分階段（in phases）通報。例如網路攻擊可能涉及技術層面複雜之個資侵害，控管者必須進行詳盡之鑑識及調查，才能瞭解受影響之內容及其可能的後果。此時控管者可先行通報監管機關，並於蒐集完整資訊後提交補充報告，亦即控管者亦應隨時更新通報之內容，並於事後說明事件之完整過程。

另外，如果個資侵害事故涉及數個資料控管者，應由各控管者推派負責履行義務之主要機構，負責履行包括向監管機關通報以及通知個人之義務，惟仍依其個別與資料主體的關係與所涉及的風險程度負責。如果控管者另有指派處理者（例如委外廠商）進行資料處理，處理者發現個資侵害事故後應儘速通知控管者。與控管者不同的是，處理者無須在通知控管者前先行評估風險，而應由控管者於知悉個資事故後進行評估。此時因為控管者係指派處理者進行資料的處理，因此當控管者受處理者通知有個資侵害事故發生當時，即構成前述的「知悉」。例如顧客通知銀行服務中心（call center），自稱未收到自己當月的對帳單，而係收到屬於其他客戶的對帳單，控管者經初步調查，認為確實發生影響資料安全之事件，可能是因為系統漏洞或人為因素，並可能還有其他客戶的個人資料也遭受影響，則應於72小時內通報監管機關，並視情況通知受影響之資料主體。此時控管者得於與處理者締結的合約中，要求處理者必須「儘速」將侵害事故通知控管者，使控管者得遵循規定於知悉後72小時內完成通報；如性質允許，亦得約定處理者如獲得控管者的授權，亦可代為進行個人資料事故之通報（通知）。

得免除通報義務之例外情形

倘若個資侵害事故經過調查，確認不足以造成個人權利或自由之風險，則尚毋需通報主管機關。舉例而言，如果涉及的個人資料為已經公開之資料，對當事人不致於造成風險。又如，控管者將個人資料檔案分為主資料庫及備份資料庫，並將備份資料庫之個人資料以密鑰加密儲存，該實體密鑰因駭客攻擊或入侵而被盜用或竊取，如嗣後發現密鑰完好未受到侵害，且備份資料庫使用之加密技術得以確保資料無法被未授權之人讀取（機密性、完整性未被侵害），且備份資料庫之資料可以透過主資料庫即時恢復（可用性不會喪失），初步研判不致於對資料主體產生不利影響，則毋須通報。惟事後若發現實體密鑰可能已被侵入，或發現資料庫之加密功能已被破解，則因會對資料主體造成可能之不利影響，此種情形於發現後則必須儘速進行補通報。因此技術層面的掌握有其重要性，資料控管者必須留意慎選加密軟體或相關服務提供者（如廠商），並熟知其功能，例如部分裝置於關機時會自動加密，但在待機狀態（standby mode）則無此功能；或部分產品有預設金鑰（default key），必須由使用者變更後才能有效運作，此時控管者若誤以為有加密，事實上資料並不存在有效加密功能，如因此而誤判未進行通報，仍可能違反通報義務。因此，雖經控管者初步判斷屬於毋需通報監管機關之個資侵害事故，資料控管者仍必須留存相關紀錄（軌跡），備供主管機關複核。

對於資料主體的通知

與通報監管機關之要件相較，對資料主體的通知義務之門檻較高，亦即，須對個人造成不利影響之程度較高，具有「高風險」時，才須要通知受影響之個人。至於通知時間，亦無如前述通報監管機關有72小時內規定之限制，僅須視個案情形「儘早通知」即

可。必須通知的對象為經調查確認受到事故影響之當事人，如經確認不受該次事件影響之當事人，則毋需通知。另如受個資侵害事故影響的資料主體有二位以上，原則上仍應個別通知各該資料主體，除非涉及不符比例之勞費（disproportionate effort），此時則應以公告（或其他替代方式）確保資料主體受到告知相關訊息。此種通知應單獨寄送，相關訊息應獨立、清楚、透明，且不得與其他例行性的帳單、廣告、或動態等合併提供。惟可行之通知方式並不限於後郵件方式發送之紙本信函，包括電子郵件（email）或簡訊（SMS, Short Message Service）等均無不可。至於公告的方式，可選擇於網站顯著位置公告，或在報章顯著位置刊登廣告等。然而，如果只透過新聞媒體進行相關報導，或僅有在網站「內文」中提到該等事件，則未能滿足獨立、清楚、透明的要求，可能難以構成對資料主體之有效通知。

以前述銀行誤寄對帳單事件為例，若經後續調查發現有更多客戶的資料受到影響（即大規模的發生帳單寄送的錯誤），除必須個別通知受影響的客戶外，也可以在銀行網站顯著位置加以公告，或者在報章顯著位置刊登啟事等。另對帳單的寄送係委由其他廠商提供相關服務，則因客戶已熟悉相關流程，除非該次事故的發生確與負責寄送對帳單的委外廠商之疏失有關，且尚未改善者外，則對資料主體的通知，自得繼續委由該廠商為之。

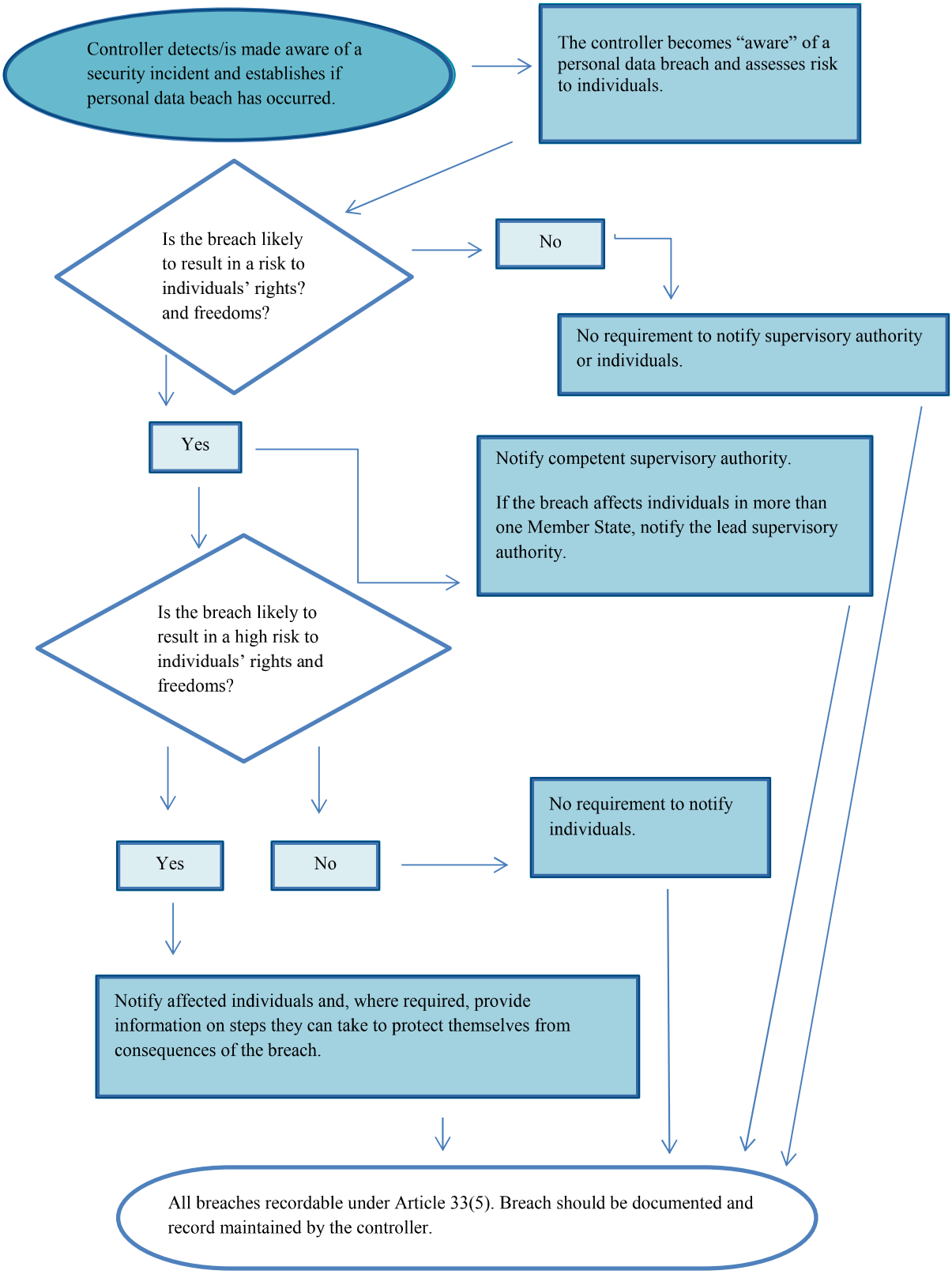
資料控管者應確保依受眾的不同，前述通知或公告的內容應該以不同的型式和語言加以呈現，以使資料主體得以順利接收並清楚瞭解其內容。例如個資侵害事故之通知所使用之語言，應使用與先前雙方往來之相同語言。如控管者未曾與資料主體往來，屬於間接蒐集資料的類型；或與控管者位於不同國家，而屬境外法人或自然人的情形，則應以當地語文進行通知。其判斷重點在於足使資料主體清楚瞭解該次個資侵害事故，以保障其自由權利。如對通知方式及內容有疑義，亦可考慮尋求監管機關的意見與協助。

小結：個資侵害事故之處理流程

資料控管者確認「知悉」個資侵害事故發生後，首先依資料蒐集、處理活動的本質、範圍、脈絡與目的進行分析調查，確認個資侵害的態樣，研判個資侵害對資料主體自由、權利的影響程度與風險高低，據以確認須通報監管機關及通知受影響之資料主體。個資事故對資料主體的自由權利如可能產生不利影響，則應通報監管機關；對資料主體的自由權利可能產生高度風險者，除通報監管機關外，並應通知受影響之資料主體，其內容應至少包括：描述個人資料侵害之可能結果，告知處理或降低不利影響之措施，並提供可以取得更多相關資訊之聯絡方式等（併請參閱附圖：個資侵害事故處理流程圖[4]）。

4 P. 30, Article 29 Working Party, 'Guidelines on Personal Data Breach Notification of the Regulation 2016/679', WP250(Rev.01)。

圖 1：個資侵害事故處理流程圖



四、我國個資法有關通報及通知之規定

我國個人資料保護法並未明文規定個資事故的通報機制，僅在個人資料保護法施行細則第12條第2項第4款，規定「事故之預防、『通報』及應變機制」為個資法本文[5]所稱：「為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取之技術上及組織上之適當安全維護措施」。因此我國有關向監管機關通報及向資料主體通知之細節性規定，係由主管機關以行政命令等方式補充之。

依行政院110年2月3日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，為強化非公務機關個人資料外洩之通報機制，決議增訂「個人資料外洩之通報時點」、「應通報事項」及「後續行政檢查」等規定。為強化各部會（即我國個人資料保護法所定各目的事業主管機關）依個人資料保護法第27條授權各部會訂定之「主管之非公務機關個人資料檔案安全維護辦法」，爰建立院層級之個資外洩聯繫機制，於110年8月11日訂定發布「行政院及所屬各機關落實個人資料保護聯繫作業要點」。

為使中央目的事業主管機關即時掌握所轄非公務機關資料外洩情形，依前述會議決議及「作業要點」第6點規定，各主管機關所訂「主管之非公務機關個人資料檔案安全維護辦法」中，有關通報事項之內容應包括：非公務機關應於發現個資外洩後72小時內通報個資安全事故；中央目的事業主管機關接受通報後，應於72小時內，通報國家發展委員會。

以受高度監管之金融機構為例，如發生重大之個人資料侵害事故，金融監督管理委員會原僅要求金融業者「應儘速通報」、「應即通報」。惟為配合行政院對安全維護辦法之一致性要求，於「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」增訂：非公務機關遇有重大個人資料事故者，應依規定格式於72小時內通報；如其他法令另有規定時（如「金融機構通報重大偶發事件之範圍申報程序及其他應遵循事項」），除應於72小時內通報外，同時亦應依各該法令之規定辦理。並明定接受非公務機關通報重大個人資料外洩事故後，金管會得依個人資料保護法第22條至第25條等規定，為適當之監督管理措施，如派員檢查、沒入或命銷毀違法蒐集之個人資料、公布非公務機關之違法情形及其名稱與負責人姓名等等。

5 包括個資法本文第6條第1項但書之第2款及第5款所稱蒐集、處理、利用特種個資之「適當安全維護措施」、第18條所稱指定專人辦理之「安全維護事項」、第19條第1項第2款及第27條第1項所稱「適當之安全措施」等。

五、結論

資料控管者於個資侵害事故發生後對監管機關有通報之義務，並通知受影響之當事人，為一傳統而基本的監理要求。較為理想的制度設計可能是：通報義務人宜設有專屬之「資料保護員」，並確保其成為與監管機關對口的稱職聯絡人。並由「專責主管機關」受理個資事故通報，並賦予該機關對違反通報義務的對象直接裁處行政罰或移送相關單位懲戒之法定權力。

有關通報義務的規範內容部分，宜就通報監管機關與通知資料主體的內容、時間、方式等作出詳盡規範，並將需要現代化科技、技術輔助進行的部分，如：確認個資侵害態樣、研判個資侵害對資料主體自由權利的影響程度與風險等程序及內容，明確納入規範中。

以我國現行個人資料保護法相關規定為例，有關「適當安全維護措施」僅是一種評估規定，尚非適用於各種情況下的強制性要求，欠缺具體落實的要件規定，仍待行政命令補足，此可能不利於資料主體自由、權利的保護。爰此，GDPR中有關個資侵害事故處理流程之詳盡規定，應有值得我國個資法制未來修正增補時加以借鑒之處。

參考文獻

1.張陳弘、莊植寧，新時代之個人資料保護法制：歐盟GDPR與臺灣個人資料保護法的比較說明，新學林，初版，2019年6月。

2.葉志良，因應物聯網發展資料保護法制的革新—歐盟法制的發展與啟示，中原財經法學，第40期，2018年6月。

3.Article 29 Working Party, 'Guidelines on Personal Data Breach Notification of the Regulation 2016/679', WP250(Rev.01), last retrieved on 2022/06/02, from https://ec.europa.eu/newsroom/ article29/items/612052。