

臺北市政府資料治理委員會個資保護組第 4 次會議紀錄

時間：110 年 6 月 30 日 15 時

地點：視訊會議

主席：個資保護組沈杏霖副組長

紀錄：陳宜霞

出席(列席)人員：詳簽到單

壹、主席致詞 (略)

貳、討論事項：本府個資保護規範共通範本之研議(含盤點及機關間資料交換相關規定)

一、背景及處理程序說明(略)

二、臺北市政府所屬機關訂定個人資料保護管理要點參考範本及指引(訂定草案)說明(本府法務局)
(略，詳現場簡報)

三、執行臺北市政府資訊局個人資料保護管理要點實務之補充說明(本府資訊局)
(略，詳現場簡報)

四、綜合討論

余若凡委員

(一)第 14 點有關未成年人之當事人同意，無論本人或法定代理人均明定應以書面為之，有何特殊考量？在實務執行上會否造成困難？若無其他法規明確之限制，得否增加處理彈性？建議考量。

(二)建議第 18 點於指引中，就我們處理案件的經驗，對於各單位間個資之交換、利用增加合規機制、流程之說明，以利機關執行。

王琍瑩委員

(一)條文規範得很完善，建議可以有案例的提供及內部訓練課程。

(二)贊同第 44 點要隨時為滾動式的修正，因為在規範訂定時可能會有很多情境是沒有到的，而且科技是與時俱進的，新科技會

蒐集的資料及狀況是隨時在改變的，所以歐盟有很多指引是針對新的科技、新的演化。

蔡玉玲委員

- (一) 規範非常完整，所以僅需確認得否執行；如可執行，則對於個資的保護很完備。關於個資的蒐集、處理及利用一定是以「符合法定職務之必要範圍」為核心，現在的規範架構，似乎是將法定職務區分為各個局處，則有關告知與同意亦應以各個局處為之，若此，則法定職務之必要範圍亦必須以局處為界，連結後面的不得恣意連結、不得濫用的規定。則在局處之間的資料交換，每一個連結每一個利用，都要受到這一套流程的管控，所以提醒注意可執行性。
- (二) 第 16 點第 2 項，關於特定目的外利用，規定有給予退出之選擇機會，這樣對當事人來說保護確實非常周全，但也要考量機關執行面的困難，個人從行政管理的角度，建議除了有這樣原則性的規定，也要協助機關設想執行面的問題。
- (三) 有關所提到政府資訊公開法、檔案法及個資法的關係，個人很贊同法務局的論述，每部法都有其體制上、本質上規範的重點，不是單純特別法與普通法的關係。
- (四) 委外監督的部分也是非常重要的規定，在實務上個資外洩遭受侵害的案例很大一部分是發生在委外的廠商，個人建議，與其盡可能去規定，不如未來在委外的招標文件或契約上，讓委外的廠商依照委託機關的要求去說明如何以科技的方式落實執行個資保護，重要的是最好能使用最新技術，但新技術的導入往往涉及成本問題，處理的方式是可以將之列入評選廠商的條件，科技產生的問題以科技來解決會更有效率些。
- (五) 軌跡紀錄檔對於查詢有沒有造成個資的侵害是非常重要的，但在草案第肆章有關個人可以調閱資料之相關規定中，似乎未包含本項，建議增加之，會成為個資保護的亮點。

曾韵委員

- (一)第 18 點是一個重要的規定，但我個人比較擔心單位知不知道如何適用。
- (二)第 34 點有關個人資料盤點作業之檔案清冊算是列的很詳細了，第 35 點則是規定風險評估之必要項目，經比對這兩點規定的項目，因為實務上在做風險評估時，是會跟清冊所列的項目有所連結，目前此二點規定的項目存有落差，會造成第 34 點所提到的項目有漏未納入評估之虞，執行風險評估時要求評估的個資數量也未明定於第 34 點，是否會產生操作之困難？為了保留執行的彈性及空間，有些規定可以斟酌簡略一點。
- (三)第 41 點至第 43 點是有關個資安全事故之相關應變及通報機制，第 41 點規定知悉時起多少小時內要進行處理，但在資通安全事件通報及應變辦法中其實是規定「一定時間內」要完成處理，所以個人認為第 41 點規定儘速處理即可；第 43 點規定亦採一定時間內完成通報，其中第 2 項提到應依資通安全事件通報及應變辦法等辦理，個人認為是否直接依照該辦法規定即可，不需要另訂時間？可再審酌。

萬幼筠委員

- (一)在第 2 點名詞定義的部分，有些機關是直接把電子簽章法排除適用，但如果排除了電子簽章法的適用，則當事人同意的部分就一定要回歸書面，如此可能會造成業務推動的困境。我個人鼓勵盡量朝著電子簽章法的精神，在智慧的環境下利用科技帶來便利，不要被細節的科技面問題阻礙；只是要如何突破，可能還有待大家一起研議。
- (二)有關去識別化的問題，我們沒有引用歐盟的匿名化跟假名化規定，在實務上，很多是統計型的資料，並不會那麼容易洩漏個資，只需要做到假名化即可；針對匿名化，我們沒有很嚴謹的

要求也沒有規範，所謂達到無法識別個人資料的程度，目前法院的判決也是指不要跟其他資料做連結而得被再識別，但這個連結的範圍究竟多大？我個人在擔任顧問時會建議，原則上應達「窮盡所有可能避免得以被再識別」之程度，但這會讓機關產生很大的壓力，因為實務上常發生廠商已盡可能去做去識別化，但被人利用海量資料去連結而被再識別，這是否應歸責於廠商？我認為在風險評估上，應該適度的引進歐盟的規定，提供明確的規範及依循。

(三)第貳章個人資料保護管理組織有指定專人之規定，我個人最常被問到的問題就是應否專職或專責，這會涉及執行上的問題，例如編制員額問題，所以在國內常見的是採專責而非專職，但只要專責人員業務異動，或者其兼辦業務繁多，則對於此業務之落實就會產生問題。建議就此規定可以進一步去指引機關在何種情境或條件下應設置專職/專責人員，或者是表明清楚專職或專責人員皆可；以歐盟的規定為例，某一類的人員是規定一定要專職，這當然都有其規範意涵，我們可以去探討，也要考量我們現存的制度及成本問題。

(四)有關委託執行職務，受委託機關依個資法第 4 條既應視同該委託機關，其責任與權利亦應相同。第五章所提到的委外，與上述委託是否相同？第 13 點第 1 項第 3 款有依法受委託執行職務之規定，但其安全管理義務僅第 2 項規定有疑義時應即通知委託人，在這種情況之下，其是否亦受到委外監督規定的規制？解讀上容有疑義。另實務上，有很多資料的委外是存在複委託，而且很多情況不是因為能力問題，而是為了分散個人資料的風險；在多層次複委託的情況下，可能會讓採購單位或政風單位在出問題時無法追溯到最源頭，委託管理的責任權利也因為分級複委託變得非常複雜，這是業界常發生的狀況，最後只能依靠保險或其他模式去處理，甚至無法處理，並隨著時間經過及委託關係結束，無主的運用可能會越來越多。所以關於委外的

管理機制一定要健全，不是委託機關去幫受委託的廠商管理，而是受託廠商要自己提出一套管理計畫，並由委託機關或政風單位去進行稽核。此外，廠商所提出管理計畫中，委託機關在審查上要注意：系統開發(執行業務)與資安稽核必須是互相獨立，始能有效發揮稽核功能。

(五)通知當事人的目的應係為了控制損害，個人對於通報的時間沒有特別的感知或堅持，所以對於要規定幾個小時沒有意見。但關於讓當事人「知道發生這樣的事件及如何能降低損害」這點，我認為應該更明確規定；個資法規定「查明後」告知當事人，因所謂「查明」需要經歷一段時間的調查，實務執行上反而會阻礙通知，且很多情況是真的無法查明行為人；換個角度說，或許有沒有確認是什麼人，似乎也不影響通知當事人所欲達成之目的。

(六)有關第 36 點規定之「不當」究為何指？建議予以例示。

(七)第 37 點規定之紀錄或證據，其中第 4 款之軌跡資料檔，建議把可能包含的類型都列入，使執行時無逸脫之可能。

賴文智委員

(一)有關 PDCA 循環，PLAN 的部分似乎比較沒有被放在範本裡。以本次的疫情為例，對很多局處來說這都是一個新的事件，在面對這樣的情況，誰來決定什麼樣的資料可以為了因應疫情而使用？這可能會與公務員在既定的法定職務、依照過去的作業模式去處理之一般事務有所不同。所以我會期待在這個範本裡去規定：當發生與過往經驗不一樣的事件，又涉及個資議題時的評估程序，否則當個資事件發生要去善後或是做輿情的回應，都是很複雜且要耗費很多成本，建議能增訂這樣評估的程序規定，或有將其精神凸顯出來的規定。

(二)對於非公務機關，比較重要的是個資的蒐集及利用；對公務機關而言，「處理」這個階段則是非常需要被控管的。從個資安

全維護管理的角度來看，公務機關向民眾蒐集個資，民眾為了使該項需求獲得滿足，幾乎都是非給不可，沒有選擇的餘地；這也回應到我剛剛提到評估程序的重要性，雖然已經揭示必要性、最小限度等個資法的原理原則，但並沒有明確的評估程序規定，以及明定誰有這樣的決策權限，應補充之。又資料蒐集後的處理，尤其是跨局處的資料調閱，不管是個別的或是系統的調閱，建議可以在範本裡說明處理原則及流程。

(三)有關紙本資料與數位資料的處理程序一定有很大的差異，前面提到的軌跡紀錄，就是帶入數位的概念，很多個資事件都是當事人在讀取相關紀錄時發現自己的資料被不當地存取利用。因應資料數位化的趨勢，建議應將資料數位化後較特殊或特別需要考量的部分亦納入規定，例如：個別公務員調閱來的數位化個人資料，一般會直接存放在電腦上，這就可能要有禁止攜出的規定；考量未來作業資料均已數位化，要怎麼去做因應的處理，可以在指引的部分去做更細節性的說明，解決在數位化的過程中可能遇到的問題。又在紙本部分，有關當事人權利之行使，實務上，非公務機關常常遇到的問題是，當消費者來要資料時，到底可以給什麼資料？還有可以給到什麼程度？這都是讓他們非常困擾的。至於公務機關面對這個問題，應該考慮不同的處理方式：當事人來申請行使個資法上的權利時，可以更進一步詢問其所欲調閱者是何種資料，而非單純告知可以調閱資料，如此機關在相應的提供資料上也會比較安全，不會被認為提供不完整。再者，因為我們的資料可能同時存在紙本與數位，調閱的難度也可能不一樣，例如有些比較舊的紙本，要調閱可能會有困難，要如何處理，亦應思考。

(四)關於資料的保存期限，我在非公務機關比較常遇到的問題是：能不能以自訂的保存期限到了，遇到有人來調閱資料，即答覆因保存期限屆滿業予刪除，無法提供？公務機關對類此情形，將如何處理？又本草案在第 37 點雖有證明紀錄文件「至少保

存 5 年」之規定，所屬機關得否提前銷毀之？另保存除了期限的規定，是否亦應有銷毀等相應的處理作業規定？因為紙本資料與數位資料在處理的各個環節，有可能均有差異，建議在指引中可以給予更多細節性的指導與說明。

(五)範本提供了很完整且具體的條文，我這邊會擔心是否限縮了執行的彈性，造成機關執行的困難？這個部分有待各機關依照自己的需求針對範本提出建議時加以處理。另外呼應萬委員，公務機關並不是依照個資法第 18 條設置一個專人，就完成其責任，甚至往往這個專人，會被設定成有責任，卻沒權力、資源，所以我在思考有沒有可能就這個專人的層級可以在範本中訂得更明確，並賦予其資源，以推動及落實相關業務。

五、結論

今天很感謝委員們提供許多寶貴意見，使法務局所草擬之範本及指引更加完整；後續按委員意見修正後，法務局將發函徵詢本府各機關意見，再予以彙整及評估，其後再提報本工作組會議，就擬訂之規定正式逐條討論，屆時再請委員協助。

參、臨時動議

肆、散會(16 時 50 分)