我國去識別化實務發展－「個人資料去識別化過程驗證要求及控制措施」

我國關於個人資料去識別化實務發展

財團法人資訊工業策進會科技法律研究所

2019年6月4日

壹、我國關於個人資料去識別化實務發展歷程

我國關於個資去識別化實務發展，依據我國個資法第1條立法目的在個資之隱私保護與加值利用之間尋求平衡，實務上爭議在於達到合理利用目的之個資處理，參酌法務部103年11月17日法律字第10303513040號函說明「個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍」，在保護個人隱私之前提下，資料於必要時應進行去識別化操作，確保特定個人無論直接或間接皆無從被識別；還得參酌關於衛生福利部健保署資料庫案，健保署將其所保有之個人就醫健保資料，加密後提供予國衛院建立健保研究資料庫，引發當事人重大利益爭議，終審判決（最高行政法院106年判字第54號判決）被告（即今衛福部）勝訴，法院認為去識別化係以「完全切斷資料內容與特定主體間之連結線索」程度為判準，該案之資料收受者（本案中即為衛福部）掌握還原資料與主體間連結之能力，與健保署去識別化標準不符。但法院同時強調去識別化之功能與作用，在於確保社會大眾無法從資料內容輕易推知該資料所屬主體，並有提到關於再識別之風險評估，然而應採行何種標準，並未於法院判決明確說明。

我國政府為因應巨量資料應用潮流，推動個資合理利用，行政院以推動開放資料為目標，104年7月重大政策推動會議決議，請經濟部標檢局研析相關規範（如CNS　29191），邀請相關政府機關及驗證機構開會討論，確定「個人資料去識別化」驗證標準規範，並由財政部財政資訊中心率先進行去識別化驗證；並以我國與國際標準(ISO)調和之國家標準CNS 29100及CNS 29191，同時採用作為個資去識別化驗證標準。財政部財政資訊中心於104年11月完成導航案例，第二波示範案例則由內政部及衛生福利部（105年12月通過）接續辦理。

經濟部標準檢驗局目前不僅將ISO/IEC 29100:2011「資訊技術－安全技術－隱私權框架」(Information technology – Security techniques – Privacy framework)、ISO/IEC 29191:2012「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」(Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication)，轉換為國家標準CNS 29100及CNS 29191，並據此制訂「個人資料去識別化過程驗證要求及控制措施」，提供個資去識別化之隱私框架，使組織、技術及程序等各層面得整體應用隱私權保護，並於標準公報(107年第24期)徵求新標準之意見至今年2月，草案編號為1071013「資訊技術－安全技術－個人可識別資訊去識別化過程管理系統－要求事項」(Management systems of personal identifiable information deidentification processes – Requirements)，主要規定個資去識別化過程管理系統(personal information deidentification process management system, PIDIPMS)之要求事項，提供維護並改進個人資訊去識別化過程及良好實務作法之框架，並適用於所有擬管理其所建立之個資去識別化過程的組織。

貳、個人資料去識別化過程驗證要求及控制措施重點說明

由於前述說明之草案編號1071013去識別化國家標準仍在審議階段，因此以下以現行「個人資料去識別化過程驗證要求及控制措施」（以下簡稱控制措施）[1]說明。

去識別化係以個資整體生命週期為保護基礎，評估資料利用之風險，包括隱私權政策、隱私風險管理、隱私保護原則、去識別化過程、重新識別評鑑等程序，分別對應控制措施之五個章節[2]。控制措施旨在使組織能建立個資去識別化過程管理系統，以管理對其所控制之個人可識別資訊(personal identifiable information, PII)進行去識別化之過程。再就控制措施對應個人資料保護法（下稱個資法）說明如下：首先，組織應先確定去識別化需求為何，究係對「個資之蒐集或處理」或「為特定目的外之利用」（對應個資法第19條第1項第4、5款）接著，對應重點在於「適當安全維護措施」，依據個資法施行細則第12條第1項規定，公務機關或非公務機關為防止個資被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施；而依據個資法施行細則第12條第2項規定，適當安全維護措施得包括11款事項，並以與所欲達成之個資保護目的間，具有適當比例為原則。以下簡要說明控制措施五大章節對應個資法：

一、隱私權政策

涉及PII處理之組織的高階管理階層，應依營運要求及相關法律與法規，建立隱私權政策，提供隱私權保護之管理指導方針及支持。對應個資法施行細則第12條第2項第5款適當安全維護措施事項「個人資料蒐集、處理及利用之內部管理程序」，即為涉及個資生命週期為保護基礎之管理程序，從蒐集、處理到利用為原則性規範，以建構個資去識別化過程管理系統。

二、PII隱私風險管理過程

組織應定期執行廣泛之PII風險管理活動並發展與其隱私保護有關的風險剖繪。直接對應規範即為個資法施行細則第12條第2項第3款「個人資料之風險評估及管理機制」。

三、PII之隱私權原則

組織蒐集、處理、利用PII應符合之11項原則，包含「同意及選擇原則」、「目的適法性及規定原則」、「蒐集限制原則」、「資料極小化原則」、「利用、保留及揭露限制」、「準確性及品質原則」、「公開、透通性及告知原則」、「個人參與及存取原則」、「可歸責性原則」、「資訊安全原則」，以及「隱私遵循原則」。以上原則涵蓋個資法施行細則第12條第2項之11款事項。

四、PII去識別化過程

組織應建立有效且周延之PII去識別化過程的治理結構、標準作業程序、非預期揭露備妥災難復原計畫，且組織之高階管理階層應監督及審查PII去識別化過程之治理的安排。個資法施行細則第17條所謂「無從識別特定當事人」定義，係指個資以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者，組織於進行去識別化處理時，應依需求、風險評估等確認注意去識別化程度。

五、重新識別PII之要求

此章節為選驗項目，需具體依據組織去識別化需求，是否需要重新識別而決定是否適用；若選擇適用，則保留重新識別可能性，應回歸個資法規定保護個資。

參、小結

國際上目前無個資去識別化驗證標準及驗證作法可資遵循，因此現階段控制措施，係以個資整體生命週期為保護基礎，評估資料利用之風險，使組織能建立個資去識別化過程管理系統，以管理對其所控制之個人可識別資訊進行去識別化之過程，透過與個資法對照個資法施行細則第12條規定之安全維護措施之11款事項，內化為我國業者因應資料保護與資料去識別化管理制度。

控制措施預計於今年下半年發展為國家標準，遵循個資法與施行細則，以及CNS 29100、CNS 29191之國家標準，參照國際上相關指引與實務作法，於技術上建立驗證標準規範供產業遵循。由於國家標準無強制性，業者視需要評估導入，仍建議進行巨量資料應用等資料經濟創新業務，應重視處理個資之適法性，建立當事人得以信賴機制，將有助於產業資料應用之創新，並透過檢視資料利用目的之合理性與必要性，作為資料合理利用之判斷，是為去識別化治理之關鍵環節。

[1] 參酌財團法人電子檢驗中心，個人資料去識別化過程驗證，https://www.etc.org.tw/%E9%A9%97%E8%AD%89%E6%9C%8D%E5%8B%99/%E5%80%8B%E4%BA%BA%E8%B3%87%E6%96%99%E5%8E%BB%E8%AD%98%E5%88%A5%E5%8C%96%E9%81%8E%E7%A8%8B%E9%A9%97%E8%AD%89.aspx（最後瀏覽日：2019/6/4）財團法人電子檢驗中心網站所公告之「個人資料去識別化過程自評表_v1」包含控制措施原則、要求事項與控制措施具體內容，該網站並未公告「個人資料去識別化過程驗證要求及控制措施」，故以下整理係以自評表為準。

[2] 分別為「隱私權政策」、「PII隱私風險管理過程」、「PII之隱私權原則」、「PII去識別化過程」、「重新識別PII之要求」。

相關連結

個人資料去識別化過程驗證

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
→ 【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）
→ 數位發展部數位產業署113年資訊服務業安維計畫常見問題分享說明會
→ 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
→ 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

孫鈺婷
專案經理 編譯整理

上稿時間：2019年07月

文章標籤

推薦文章