【PIMS 個資管理系列】之三〈電子報版〉

ISO/IEC 27701 隱私保護國際標準解析

──條款 7 和 8

撰文：BSI 英國標準協會
BS 10012 & ISO 29100 產品經理
章　鈺（Oscar Chang）

歐盟 GDPR 發布後，在可預見之未來各國在資料保護法架構上將予以參酌，例如：印度在 2018 年所擬定之資料保護法草案將個人資料之近用權、更正權、資料可攜權、包含被遺忘權的刪除權外，將 Privacy by Design and by Default 納入資料控制者與資料處理者責任範圍[1]；中國則於 2017 年擬定的個人信息保護法草案，除與我國個人資料保護法相同，將國家機關（公務機關）與非國家機關（非公務機關）區隔外，並於個人信息權將個人資料之近用權、更正權、資料可攜權及被遺忘權納入[2]。可見歐盟 GDPR 的立法模式，的確已如原先歐盟執委會所規劃，藉由該法之推動成為全球資料保護法制的參考模式。

ISO 組織為了因應歐盟 GDPR 以及各國資料保護法架構參酌歐盟 GDPR，新出爐之延伸資訊安全管理系統 ISO 27001 及 ISO 27002 標準、用來保障隱私管理之新資訊安全標準──ISO 27701，自然也與歐盟 GDPR 在結構上極其類似，這個結果並不令人意外。

ISO/IEC 27701 條款 7 與附錄 A 對資料控制者的控制要求說明

歐盟 GDPR 在第 4 條第 7 款定義了資料控制者為：『係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；依照歐盟法或會員國法決定處理之目的及方法，由歐盟法或會員國法律規定控管者或其認定之具體標準』。而 ISO 27701 則引用 ISO 29100 標準條款 2.10 之定義：『判定個人可識別資訊處

[1] 印度資料保護法草案說明請見 https://stli.iii.org.tw/article-detail.aspx?no=0&tp=1&i=0&d=8182 及 https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-bill-noexp.pdf（last visited Sept. 7, 2019）。

[2] 中國個人信息保護法法草案說明請見 http://www.sohu.com/a/203902011_500652 及 http://www.xinhuanet.com/politics/2019lh/2019-03/04/c_1210072739.htm（last visited Sept. 7, 2019）。

理之目的及方法的隱私權利害相關者，而非就個人目的使用資料的自然人』，相較之下，BS 10012 標準在條款 3.1.8 對於控制者定義為『決定個人資料處理之目的與方法的組織』其實更加接近歐盟 GDPR 對於資料控制者的定義。

在 ISO 27701 標準條款 7 對於資料控制者的要求，係架構於條款 6 從 ISO 27002 標準所延伸的控制，本文同時參照了條款 7 的控制要求 (尚有建置指南與其他資訊供導入時參照) 與附錄 A 的強制要求做為對比，並將過往 BS 10012 標準條款加入對照，部分舉例如下：

7 針對 PII 控制者在 ISO 27002 的額外控制指引

7.1 一般要求：基於條款 6 建立本條款做為資料控制者的指引，其具體建置方針則詳見附錄 A。

7.2 蒐集與處理資料的情況，包含：

7.2.1 識別並文件化目的

- 控制：宜識別並記錄處理 PII 具體的目的。
- 附錄 A：應識別並記錄處理 PII 具體的目的。
- BS 10012：8.2.7.1。

7.2.2 鑑別法律基礎

- 控制：依據所處理 PII 的目的，宜建立、書面化並符合法律基礎。
- 附錄 A：依據所處理 PII 的目的，應建立、書面化並符合法律基礎。
- BS 10012：6.1.3。

7.2.3 確認取得資料主體同意的方式與時機

- 控制：宜確定並書面化建立何時與如何取得 PII 資料主體同意的過程。
- 附錄 A：應確定並書面化建立何時與如何取得 PII 資料主體同意的過程。
- BS 10012：8.2.6.1、8.2.6.3。

7.2.4 取得並記錄資料主體的同意

- 控制：宜透過文件化程序取得並記錄 PII 資料主體的同意。
- 附錄 A：應透過文件化程序取得並記錄 PII 資料主體的同意。
- BS 10012：8.2.6.2。

7.3 對 PII 資料主體的義務

7.4 資料隱私設計及隱私預設

7.5 PII 分享、傳送與揭露

ISO/IEC 27701 條款 8 與附錄 B 對資料處理者的控制要求說明

歐盟 GDPR 在第 4 條第 8 款定義了資料處理者為：『代控制者處理個人資料之自然人或法人、公務機關、局處或其他機構』。而 ISO 27701 則引用 ISO 29100 標準條款 2.12 之定義：『代表個人可識別資訊控制者並依其指示，處理 PII 之隱私權利害相關者』，BS 10012 標準在條款 3.1.9 對於處理者定義為『僅遵照來自資料控制者的指示且具有安全義務（例如：侵害通報）的組織』，其實無論 ISO 29100、引用的 ISO 27701，或 BS 10012，對於處理者的定義與歐盟 GDPR 相比，均非常接近。

在 ISO 27701 標準條款 8 對於資料處理者的要求，係架構於條款 6 從 ISO 27002 標準所延伸的控制，本文同時列出了條款 8 的控制要求（尚有建置指南與其他資訊供導入時參照，但本文囿於篇幅所限無法逐項列出），與附錄 B 的強制要求做為對比，且由於過往 BS 10012 標準並未將控制者與處理者分別明列，故本文以適用之法律要求對照 BS 10012 條款舉例說明如下：

8 針對 PII 處理者在 ISO 27002 的額外控制指引

8.1 一般要求：基於條款 6 建立此本條款做為資料控制者的指引，其具體建置方針則詳見附錄 B。

8.2 蒐集與處理資料的情況，包含：

8.2.1 客戶協議

控制：宜確認在處理 PII 時強調提供協助符合客戶的責任時組織所扮演的角色（例如：處理的性質及組織可用的資訊）。

附錄 B：應確認在處理 PII 時強調提供協助符合客戶的責任時組織所扮演的角色（例如：處理的性質及組織可用的資訊）。

BS 10012：6.1.3、8.2.7.1。

8.2.2 組織的目的

控制：宜確認代表客戶處理 PII 僅針對客戶書面指南中所表示的目的。

附錄 B：應確認代表客戶處理 PII 僅針對客戶書面指南中所表示的目的。

BS 10012：8.2.7.1

8.2.3 行銷與廣告的利用

控制：根據合約所處理的 PII，在未事前取得 PII 資料主體同意時，不宜用在行銷及廣告所用。且不宜將 PII 主體的同意用來做為接受服務的前提。

附錄 B：根據合約所處理的 PII，在未事前取得 PII 資料主體同意時，不應用在行銷及廣告所用。且不應將 PII 主體的同意用來做為接受服務的前提。

BS 10012：6.1.3、8.2.7.1。

8.2.4 侵權指令

控制：於客戶指令違反適用的法律及 / 或法規時，宜通知客戶。

附錄 B：於客戶指令違反適用的法律及 / 或法規時，應通知客戶。

BS 10012：由於 BS 10012 標準並未針對處理者擬定此類條款，惟於條款 8.2.11.10 要求於委外於簽訂合約時，合約應包含要求受託廠商通知義務而適用。

8.3 對 PII 資料主體的義務

8.4 資料隱私設計及隱私預設

8.5 PII 分享、傳送與揭露

保護個人資料是全球一致的共同目標

與個人生活相關的資料及商業服務日益全球化的發展，各項 PIMS 國際標準及法令法規順應時勢承先啟後陸續頒布。無論是面臨本國個資法、歐盟 GDPR 又或是國際間的各項個資管理規範或要求，確保個人資料被妥善處理與保護，不僅是資料主體的權力，也是組織的責任與義務。

政府機關或企業組織面臨的個人資訊管理弱點與衝擊不盡相同，這與您所處的產業、領域及業務內容有緊密關聯，確實瞭解組織所面臨的個資風險，合理的將業務流程納入管控範圍，讓個資管理系統 (PIMS) 落實的更加完善，才是遵循法規並增強外部信賴的關鍵。●

本〈電子報版〉文章節錄自〈完整版〉內容

請點此前往下載〈完整版〉

【PIMS 個資管理系列】文章

1. ISO/IEC 27701 隱私保護國際標準新登場

BSI 網路安全及雲端個資保護產品經理花俊傑（Jack）撰文｜本文為 PIMS 個資管理系列文章的第一篇，介紹於 2019 年 8 月發布的 ISO/IEC 27701 隱私保護國際標準，它是第一個兼顧隱私保護和個資安全管理的 ISO 標準，其內容結構讓隱私資訊管理可以被視為現有 ISMS 資安管理系統要求和控制措施的擴展。它的重點主要在於提供隱私保護的要求和實務指引，並不強調要去取代任何一個標準，而是希望藉由與 BS 10012、ISO/IEC 27018、ISO/IEC 29100、ISO/IEC 29151、GDPR 或其他標準的對應互補，讓組織能夠將隱私保護落實的更加完善，並且更進一步展現組織在隱私保護的實施成果。點此閱讀>

2. ISO/IEC 27701 隱私保護國際標準解析—條款 5 和 6

BSI 客戶經理孫文良（Sunny Sun）撰文｜本文為 PIMS 個資管理系列文章的第二篇，介紹 ISO 27701 隱私保護國際標準的條款 5 和 6。ISO 27701 遵循管理系統持續精進改善的精神，在既有的資訊安全管理系統（ISMS）之上，延伸補充個人資料管理的要求和實務指引。本文從 ISO 27001 的標準架構開始，到比較 ISO 27001 附錄 A、ISO 27002 與 ISO 27701 條款 6 之間的對應關係，並舉例說明 ISO 27701 條款 5 和 6 對 PIMS 的特定要求。點此閱讀>

3. ISO/IEC 27701 隱私保護國際標準解析—條款 7 和 8（本篇）

BSI BS 10012 & ISO 29100 產品經理章鈺（Oscar）撰文｜本文為 PIMS 個資管理系列文章的第三篇，介紹 ISO 27701 隱私保護國際標準的條款 7 和 8。包含 ISO 27701 對「資料控制者」與「資料處理者」的控制要求，及與歐盟一般資料保護規範（GDPR）、ISO 27001 資安管理、ISO 27002 資安管理實行細則、ISO 29100 隱私框架等標準的關聯，並逐條比較條款 7 與附錄 A、條款 8 與附錄 B 的要求，及所對應之 BS 10012 個資管理標準條款。點此前往下載完整版>

BSI英國標準協會
T: +886 2 2656 0333 | E: infotaiwan@bsigroup.com | www.bsigroup.tw