個資保護兩大標準改版內容剖析

BS 10012:2017+A1:2018 個資管理系統標準與
ISO 29100:2011+Amd 1:2018 資安技術—隱私框架

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

為因應歐盟 2018 年 5 月正式實施的一般資料保護規則（2016/679 the EU General Data Protection Regulation，以下簡稱 GDPR），BSI 已於 2017 年 3 月正式頒佈新版 BS 10012:2017 標準（以下簡稱舊版 BS 10012 標準），並於 2018 年 5 月 GDPR 實施後正式作廢原 BS 10012:2009 標準；鑑於英國於同年 5 月在面對脫歐下所通過的 Data Protection Act 2018（以下簡稱 DPA）[1]，ISO 組織及 BSI 針對與個人資料保護相關的兩個標準，BS 10012 及 ISO 29100 分別進行微調與補充說明，而有 BS 10012:2017+A1:2018（以下簡稱新版 BS 10012 標準）[2]與 ISO 29100:2011+Amd 1:2018（以下簡稱新版 ISO 29100 標準）[3]等兩個「添加新意」的標準，以冀供使用上述標準做為遵循當前個人資料保護法規的組織做參考。

為方便使用者閱讀，上述新標準在撰寫過程中，特別將所異動部分以 A1 標示起迄處，本文即是將所標示處列出並加以說明。

BS 10012:2017+A1:2018 標準增修說明

新版 BS 10012 標準主要修正、微調了 2017 年 3 月所頒佈的舊版 BS 10012 標準方向，主要是針對：

1. 對特種個人資料的定義，整合 GDPR 第 9 條與第 10 條；

---

[1] 英國 Data Protection Act 2018 資料保護法全文請參見 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted （last visited Sept. 27, 2018）。

[2] BS 10012: 2017+ A1: 2018 個人資訊管理系統標準請參見 https://shop.bsigroup.com/ProductDetail/?pid=000000000303785748&_ga=2.17757369.1876182761.1538017659-1124287125.1510926445 （last visited Sept. 27, 2018）。

[3] ISO 29100: 2011+ Amd1: 2018 隱私保護框架標準請參見 https://www.iso.org/standard/73722.html （last visited Sept. 27, 2018）。

2. 對於以剖析方式處理個人資料時的權利行使；
3. 對設立或不設立資料保護長的要求；
4. 對個人資料去識別化的規範；
5. 對回應個人資料監管機關的要求；
6. 對當事人告知隱私權資料內容的調整；
7. 對資料主體行使法定權利的要求；
8. 對資料主體行使刪除權（被遺忘權）及可攜權的要求；
9. 資料侵害事件發生時通知的要求；
10. 對 GDPR 在從設計著手保護隱私，與隱私衝擊評鑑要求；及
11. 增加法律對資料處理者規範。

以下則進一步說明新版 BS 10012 標準增修部分：

0 前言

- 條款 0.3 通知

內容：一般資料保護規範並未有一般的通知，但英國政府已公布新的要求架構，請見 2017 年數位經濟法案。英國 2018 年資料保護法則許可資訊委員公署可進一步要求相關資訊。

說明：舊版 BS 10012 標準僅針對 GDPR 第 36 條要求，新版 BS 10012 標準則同步考量英國個人資料保護監管機關 ICO 的規範[4]，對受監管之組織仍有要求通知其之義務。

新版 BS 10012 標準異動處對台灣組織的影響：若無受英國 ICO 監管之組織，自無需考量條款 0.3 之要求，但若適用，或其海外經營據點適用當地國家個人資料監管機關要求時，則仍有適用之必要。

3 名詞定義與縮寫

- 條款 3.1.7 資料侵害

內容：侵害意指違反安全性導致傳輸、儲存或以其他方式處理之個人資料遭到意外或非法破壞、遺失、變更、未經授權之揭露或存取。

[4] ICO 對受管轄組織在個人資料保護通知義務下的說明請見 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/blog-ico-fee-and-registration-changesnext-year/ （last visited Sept. 27, 2018）。

說明：本條為新增條款，以因應 GDPR 第 4 條(11)與 DPA 定義。

- 條款 3.1.8 資料控制者

內容：決定個人資料處理之目的與方法的組織。

說明：本條為新增條款，以因應 GDPR 第 4 條(8)與 DPA 定義。

- 條款 3.1.9 資料處理者

內容：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。

說明：本條為新增條款，以因應 GDPR 第 4 條(9)與 DPA 定義。

- 條款 3.1.17 資料主體

內容：現存個人的識別符可被直接或間接識別，例如：姓名、身分證字號、位置資料、網路識別符碼，或生理、心理、遺傳、精神上、經濟、文化或是社會身分等來自處理的資訊或可能為提供組織處理的資訊。

說明：本條為修改後的條款，以因應 GDPR 第 4 條(1)與 DPA 定義。

- 條款 3.1.20 組織

內容：備註 2-組織可為資料控制者、資料處理者，或二者兼具，端賴所進行的處理而定。

說明：備註 2 為補充資料，以相應條款 3.1.8 與條款 3.1.9 角色定義。

- 條款 3.1.33 特種個人資料

內容：備註 2-犯罪前科資料雖非特種個人資料，但仍須以特種個人資料之方式處置。

說明：備註 2 為補充資料，以符合 GDPR 第 10 條對犯罪前科資訊的實際要求。

5 領導作為

- 條款 5.2 政策

內容：13) 在提供產品與服務給自然人，其為歐盟其他會員國家的居民時，應有適當的策略（見條款 8.2.11.11）。

說明：鑑於條款 8.2.11.11 為新版 BS 10012 標準所新增之條款，5.2 政策內容於 13)新增索引。

- 條款 5.3 組織的角色、責任與權限

內容：組織應指定管理高層中的一位成員承擔組織內部個人資訊管理的責任，如此才能證明組織對個人資料保護法及優良實務的遵循狀況（見條款 8.2.1.1 條款 8.2.1.2）。

說明：本條為新版 BS 10012 標準新增資料保護長的責任，故於本條款除援引 8.2.1.1 管理高層外，亦將 8.2.1.2 資料保護長納入。

6 規劃

- 條款 6.1.3 法律依據及/或規範基礎

說明：置換舊版 BS 10012 標準於條款 6.1.3.1 及 6.1.3.2 中『法源依據』一詞，改為新版 BS 10012 標準『法律依據及/或規範基礎』。

8 運作

- 條款 8.2.1.2 資料保護長

內容：

■ 備註 2- 當組織符合以下其中條件，需要指派資料保護長：

公務機關；

持有大規模監控資料主體資料；

持有大規模處理特種個人資料；或

處理與犯罪前科相關之資料。

■ 當組織決議不指派資料保護長，宜將決策制訂過程中的調節、授權與複核流程文件化。

說明：新增備註 2，以符合 GDPR 第 37 條(1)，及新增對組織決議不指派資料保護長應有的評估要求。

新版 BS 10012 標準異動處對台灣組織的影響：若需遵循 GDPR 組織且符合第 37 條(1)要求需設置資料保護長之組織，無論最終有無指派資料保護長，均需考量新版 BS 10012 標準條款 8.2.1.2 新增要求；若需遵循 GDPR 組織但不適用第 37 條(1)要求，或無需遵循 GDPR 之組織，自無影響。

- 條款 8.2.1.3 持續監督組織遵循個人資訊管理系統政策責任

內容：f) 核准個人資料處理程序，例如：
5) 管理資料侵害事件（見條款 8.2.11.7）；

說明：修訂資料安全事故為資料侵害事件，以符合 GDPR 第 4 條(12)之定義。

- 條款 8.2.6 公平、合法與透明化的處理

說明：置換舊版 BS 10012 標準於目標，及條款 8.2.6.1 中『法源依據』一詞，改為新版 BS 10012 標準『法律依據及/或規範基礎』。

- 條款 8.2.6.1 個人資料蒐集與處理

內容：d) 組織以適當的形式提供隱私權資訊予自然人，當中應明確溝通下列事項：

(1) 在適當情況下，提供控制者及其代表的身份與聯繫方式；
(2) 如果適用，資料保護長的聯繫方式；
(3) 所欲處理之個人資料之處理目的及該處理之法律依據；
(4) 處理個人資料是基於控制者或第三方的正當合法利益時，對該正當合法利益的描述；
(5) 當個人資料會分享時，接收方及其個人資料類型；
(6) 當個人資料移轉至歐洲經濟區外（特別是未經歐盟適當決議）地點、該處之安全防護措施，及取得是項安全防護措施的副本；
(7) 保存期限或是設定保存期限之準則；
(8) 關於自然人近用權、更正權、刪除權、限制處理權，以及資料可攜權的資訊；
(9) 當處理是基於當事人同意下，可以撤銷同意的權利；

(10) 向監管機關提出申訴的權利；
(11) 當資訊的提供是依據法規或是合約要求時，提醒自然人為何必須提供與無法提供資訊之後果；
(12) 有關資訊可能用於任何自動化決策和/或剖析的資訊，包括所涉及的邏輯和對自然人的後果；
(13) 當組織欲進一步逾越原特定目的所蒐集之個人資料時，在處理前的其他目的及相關的資訊；
(14) 在網站上蒐集個人資料所使用的任何技術之細節，例如：cookies。

說明：調整隱私權資訊需對資料主體揭露之內容，以符合 GDPR 第 13 條(1)、(2)之要求。

- 條款 8.2.7.2 同意不相容的目的

內容：任何處理應與原來的目的相符，如果將個人資料用於任何目的，除原始指定目的之外，或不同於原特定目的，則新用途宜符合預期並公平。

個人資訊管理系統應確保任何新的目的同意皆可自由提供與通知。

個人資訊管理系統應確保下列措施：

(a) 獲得自然人同意於一個目的下使用其個人資料的正面表示；

(b) 維持為新處理目的獲得同意的紀錄。

說明：調整文字敘述。

- 條款 8.2.7.3 處理兒童的資訊

內容：備註- 在英國，資訊委員公署將兒童年齡定為 13 歲及其以下，唯此可能與其他國家法令相異。

說明：新增此項備註。

新版 BS 10012 標準異動處對台灣組織的影響：若需遵循 DPA 組織且持有未成年人個人資料之組織，需參考本新增項目；若無需遵循 DPA 之組織，自無影響。

- 條款 8.2.7.4 資料分享

內容：

■ *（節錄）*如不可能，組織應確保：
(1) 有法律依據及/或規範基礎的資料分享基礎；
■ 備註：進一步說明請詳一般資料保護規範第 28 條。

說明：
■ 置換舊版 BS 10012 標準於目標，及條款 8.2.7.4 中『法源依據』一詞，改為新版 BS 10012 標準『法律依據及/或規範基礎』。
■ 新增本項備註，對資料處理者要求以因應資料分享處置。

- 條款 8.2.7.5 開放資料

內容：當採取去識別化方式，應考慮能防止重新識別自然人的技術上與組織上的合理手段。

說明：移除舊版 BS 10012 標準條款 8.2.7.5 備註，並增加此要求，以控管資料去識別化可能衍生的風險。

新版 BS 10012 標準異動處對台灣組織的影響：對持有個人資料且會有資料經去識別化公開需求之組織，需定期評估其去識別化之技術與組織的方法，以避免被識別之風險。

- 條款 8.2.8 適當、相關且與資料最小化原則一致

內容：確保個人資料是適當、相關且僅限於處理目的相關之必要性。

說明：調整目標內容文字。

- 條款 8.2.8.2 相關且僅限於需要

內容：
■ 個人資訊管理系統應確保：
c) 檢討個人資訊處理的相關新系統及過程，以確保處理的資料是相關且僅限於需要。
■ 如個人資料對組織的合法基礎而言是不相關或不需要的，個人資訊管理系統應確保此等個人資料不會被處理。

說明：調整文字。

- 條款 8.2.9.1 正確且最新

內容：個人資訊管理系統應確保被處理之個人資料能維持完整和正確。
個人資訊管理系統應確保讓自然人能夠質疑其個人資料之正確性，並在需要時要求更正其個人資料。當個人資料為不正確且無法更正時，例如與歷史紀錄，個人資訊管理系統應記錄不正確處，並適當提供正確的個人資料。
個人資訊管理系統應具有已核准及文件化過程來檢查個人所聲稱的不正確資訊是否屬實。經過檢查後，若聲稱的不正確處是錯誤，而實際上資料是正確的，個人資訊管理系統應保留適當的證據。

說明：調整文字。

- 條款 8.2.11.4 資訊傳輸

內容：當以電子方式傳輸時，宜使用加密。

說明：將舊版 BS 10012 標準本條款備註改為條款內容。

- 條款 8.2.11.6 安全評鑑

內容：此評鑑應考量在資料侵害事件發生時，對自然人造成危害、損害及/或痛苦的風險。

說明：修訂資料安全事故為資料侵害事件，以符合 GDPR 第 4 條(12)之定義。

- 條款 8.2.11.7 管理安全事件

內容：個人資訊管理系統應：

a) 評估、管理和記錄所涉及個人資料安全事件，包括減緩任何安全事故所造成的損害的程序，應包含：
   (1) 評估事件符合資料侵害標準；
   (2) 量測對當事人的風險；
   (3) 決定個人資料侵害事件符合通報監管機關及/或受到影響的當事人；及
   (4) 決定適用的免除條款。
b) 任何有可能損害自然人的權利和自由的風險時，應在得知後 72 小時內通知主管機關此一安全事件。此類通知應包括下列事項：
   (1) 事件所涉及的個人資料；

(2) 個人資料類別的詳情和涉及的大致總數；
(3) 組織資料保護長或其他聯絡窗口的聯繫方式；
(4) 此一安全事件可能的影響；及
(5) 描述為解決此一安全事件而採取或提出的措施，並減輕任何可能的不利影響；

備註 1：見一般資料保護規範第 33 條第 3 項。

c) 如果安全事件可能導致自然人權利和自由受到高風險影響，避免不當拖延、通知有顧慮的自然人下列事項：

(1) 侵害事件；
(2) 侵害事件的類型；
(3) 為減輕任何不利風險的行動的任何建議；

d) 記錄每個安全事件，包括評估如何發生、採取的矯正行動，以及可以從中得到的教訓；

e) 決定是否將安全事件通知主管機關（例如：金融監督管理委員會）；

f) 記錄任何核發的通知。

說明：新增 a)要求，及文字調整 b)至 f)。

新版 BS 10012 標準異動處對台灣組織的影響：組織可參考條款 8.2.11.7 a) (1)至(3)要求擬定減緩安全事故減緩程序。

- 條款 8.2.11.9 依第三方請求揭露

說明：置換舊版 BS 10012 標準於目標，及條款 8.2.6.1 中『法源依據』一詞，改為新版 BS 10012 標準『法律依據及/或規範基礎』。

- 條款 8.2.11.10 委外處理個人資料

內容：刪除原 c)。

說明：舊版 BS 10012 標準本條款 c) 要求對資料處理者執行盡責調查，新版 BS 10012 標準仍保留 d) 合約中要求對資料處理者執行安全查核。

- 條款 8.2.11.11 營運遍及歐盟

內容：當組織提供產品或服務予歐盟一個或多個會員國的公民時，個人資訊管理系統應確認並文件化適當的主要監管機關。

備註：一般來說，主要監管機關為組織在歐盟建立的會員國的監管機關。

說明：本條款為新增，主要為當組織營運不僅限單一歐盟國家時，需確認所應遵循的主要監管機關，以確保法律遵循情形。

新版 BS 10012 標準異動處對台灣組織的影響：對需遵循 GDPR 及/或 DPA 之組織，可參照條款 8.2.11.11 要求確認需遵循的個人資料監管機關。

9 績效評估

- 條款 9.3 管理審查

內容：管理審查應包括對下列事項之考量：
k) 已發生的侵害事件/安全事件。

說明：修訂資料安全事故為資料侵害事件，以符合 GDPR 第 4 條(12)之定義。

10 改善

- 條款 10.3 持續改善

內容：組織應運用申訴抱怨、資料侵害事件、標的存取請求、技術演進及其他議題，來協助改善個人資訊管理系統的有效性。

說明：修訂資料安全事故為資料侵害事件，以符合 GDPR 第 4 條(12)之定義。

ISO 29100:2011+Amd:2018 標準增修說明

新版 ISO 29100 標準主要係因應修正、微調了 2011 年所頒佈的舊版 ISO 29100 標準，ISO 組織雖於官網並未進一步說明變動原因，但本次變動除與 GDPR 接軌外，同時與 ISO 29134: 2017 標準定義整合，其異動處包含：

Introduction 介紹：將 International Standard 國際標準，調整為本文件 Document。

2 名詞與定義

- 條款 2.6 識別

內容：移除本名詞定義。

- 條款 2.7 身份識別

內容：移除本名詞定義。

- 條款 2.9 個人可識別資訊

內容：所有資訊其

(a) 能用以識別此類資訊所涉之自然人，或

(b) 係或得以直接或間接連結至自然人。

備註 1：自然人的定義為個人可識別資訊的原則，為判定自然人是否為可識別，宜將能由持有資料之隱私權利害相關者或他人，合理使用的所有手段納入考量，以連結該自然人。

- 條款 2.20 隱私衝擊評鑑

內容：關於個人可識別資訊處理之風險識別、分析、評估、徵詢、溝通及對潛在隱私衝擊規劃處置的整體過程。
【來源：ISO 29134:2017[5]將隱私風險評鑑改為此通用術語】

說明：原標準為隱私風險評鑑，鑑於歐盟隱私工作小組於 2017 年 4 月公布之 WP248 Data Protection Impact Assessment[6]指引，ISO 組織亦於 2017 年 6 月公布此一指引。

新版 BS 10012 標準異動處對台灣組織的影響：無，但如需遵循 GDPR 且需依照 GDPR 第 25 條及第 35 條之組織，可參考 ISO 29134:2017 指引執行隱私衝擊評鑑。

4 隱私權框架之基本元件

- 條款 4.5 隱私保全要求事項

內容：隱私保全要求事項之識別為整體隱私風險管理過程之一部分，其受下列因素所影響：
契約因素，如：數個不同參與者間的協議、公司政策，及行為守則；

[5] ISO 29134: 2017 隱私衝擊評鑑指引請參見 https://www.iso.org/standard/62289.html （last visited Sept. 27, 2018）。

[6] 歐盟隱私工作小組所公布之 WP248 DPIAs 指引內容請參見 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 （last visited Sept. 27, 2018）。

說明：增加企業守則以因應 GDPR 第 40 條行為守則要求。

- 條款 4.5.2 契約因素

內容：原則上，有 PII 存取權之任一方宜由各自的 PII 控制者以正式方式使其意識到其義務，例如：藉加入第三方協議。該協議可能包括數個第三方（PII 接收者）必須考量的隱私保全要求事項。在某些管轄權國家及地區主管機關可能已建立法律及契約文書使 PII 能夠傳送至第三方。

說明：將新版 ISO 29100 標準將舊版 ISO 29100 標準所提及之 PII 接收者，改為第三方，以呼應 GDPR 第 4 條(10)之定義。

- 條款 4.5.3 營運因素

內容：因此，許多營運因素對隱私保全要求事項並無直接衝擊。所設想之 PII 利用可能影響組織於隱私權政策之實作及隱私控制措施之選擇，但其不宜影響組織同意之隱私權原則。例：提供某種服務可能需要服務提供者蒐集額外的 PII，或允許其更多員工存取某些型式之 PII。然而，此並非意謂贊同本框架包含原則之 PII 控制者不需再詳細評鑑僅需哪些型式之 PII 以提供服務（蒐集限制原則），以及限制需具存取權以履行其職責之員工對關注之 PII 的存取（資料最小化原則）。

說明：本條款修改處有二，除調整語法外，並將舊版 ISO 29100 標準中『或允許其更多員工存取某些型式之 PII』移除。

5 ISO 29100 隱私權原則

- 條款 5.1 隱私權原則概觀

說明：將舊版 ISO 29100 標準所提之『states』移除。

- 條款 5.5 資料極小化

內容：堅持資料極小化原則，意指以下列方式設定及實作資料處理程序與 ICT 系統：

- 將處理之 PII、隱私權利害相關者及 PII 揭露對象或可存取 PII 之人員的數目最小化；
- 確保採用『僅知（need-to-know）』原則，亦即於 PII 處理之合法目的框

架下， 宜僅對執行正式職務所必要之人員賦予 PII 存取權限。

- 使用或提供視為預設選項，只要不涉及 PII 當事人之識別的互動及交易，儘可能降低其行為之可觀察性並限制所蒐集 PII 的可連結性。
- 一旦 PII 處理之目的終止，無法定要求保有 PII，或是實務上需如此做時，即刪除或廢棄 PII。

說明：僅調整語法。

- 條款 5.8 公開、透明及告知

內容：此外，PII 處理之目的宜足夠詳盡，以便使 PII 當事人瞭解下列事項：具體的 PII 保存及廢棄要求。

說明：移除舊版 ISO 29100 標準於本條款中的 PII『Data』語法。

- 條款 5.9 個人參與及存取

內容：堅持個人參與及存取原則，意指下列事項：
於知悉對方之情況下，對 PII 處理者及 PII 揭露對象之第三方提供所有修訂、更正或移除資訊；

說明：移除舊版 ISO 29100 標準於本條款中的『personal data』為『PII』。

結語

新版 BS 10012 與 ISO 29100 標準既然當初是針對所有類型的組織所撰寫，做為各個組織目前或可預見的未來在不同情況下有遵循法律要求的需要時的參考方向，本文所列乃是針對兩大標準新舊差異作出比較，唯使用的組織除了參照標準設計作法外，也需考量法律與主管機關在個人資料保護上的實質要求，以及切實的可行性作出符合比例原則的執行作法，因此，對於需要遵循本國法、歐盟 GDPR、英國 DPA，甚或日本個人情報保護法、韓國資料保護法，或未來中國的個人信息保護法，也可透過此一模式建立。