BS 10012 個資管理系統標準即將改版

改版緣起

歐洲議會於 2016 年 4 月 14 日正式通過「一般資料保護規範[1]」，並預計在 2018 年 5 月 25 日生效。由於與過往歐盟的《個人資料保護指令[2]》要求會員國需透過該指令要求，在考量因地制宜的彈性下，制訂其國內的資料保護法律不同，「一般資料保護規範」於實施後各會員國無需另行制訂其國內之資料保護法律，而得以直接適用，但在 2018 年 5 月生效前的過渡期間，歐盟各國仍為因應新修正規則而預作準備。

BSI英國標準協會於 2009 年所發佈之BS 10012 個資管理標準[3]，乃是架構在符合《英國資料保護法》（The Data Protection Act of 1998）及《個人資料保護指令》下，因此，為與未來將實施的一般資料保護規範相符，而著手進行 BS 10012 標準之修訂。

修訂方向

BS 10012 標準修訂的草案版已於 2016 年 11 月 7 日完成線上公眾意見徵詢，目前修訂的方向包含：

- 修訂版採用 ISO/IEC 指令附錄 SL 的高階結構(High Level Structure) 格式編寫，更易於未來與其他管理系統，包含 ISO 9001、ISO 27001 等標準做整合。
- 參考第四條及第九條、第十條，進一步定義個人資料與敏感性個人資料與規範
- 參考第五條，將原 BS 10012 標準所引用的八大原則改為六大原則，包含：

[1] General Data Protection Regulation, GDPR，文中簡稱一般資料保護規範。
[2] Data Protection Directive，95/46/EC，文中簡稱個人資料保護指令。
[3] BS 10012 資料保護 - 個人資訊管理系統規範（Specification for a personal information management system），文中簡稱 BS 10012 標準。

- ✓ 受到公平合法的處理
- ✓ 僅為具體指明的目的取得，且不會受到不符合此等目的的方式處理
- ✓ 適當、相關且不過度
- ✓ 正確且最新
- ✓ 保留時間不超過必要程度
- ✓ 獲得安全保障

- 參考第六條，對向當事人徵詢同意作業的新要求
- 參考第十五條、第十七條、第二十條，修改個人資料當事人對其資料行使近用權，包含：
  - ✓ 資料刪除權（即被遺忘權）
  - ✓ 資料可攜權
- 參考第二十二條，對運用個人資訊剖繪的限制
- 參考第二十五條、第二十八條及第三十條，對資料處理者的規範
- 參考第三十二條，對擬匿名化個人資料的使用與處理
- 參考第三十三條，對發現安全漏洞時的通知，及對發現安全事件在時限內通知當事人的要求
- 參考第三十五條，要求實施隱私衝擊分析
- 參考第四節，需符合對個人資料主管機關要求，以及廢除通知、登錄的規範
- 移除國際傳輸時原安全港協議

撰文：

BSI 英國標準協會

BS 10012 & ISO 29100 產品經理

章鈺（Oscar Chang）

BS 10012 個人資訊管理系列課程

- ■ 基礎課程
- ■ 建置課程
- ■ 主導稽核員課程

課程詳情請按此>