

BS 10012 : 2017個人資訊管理系統新版標準已發布



BS 10012:2009個人資訊管理系統近期轉版，英國標準協會已於2017年3月31日發布BS 10012:2017新版標準，此次修改主要係為遵循歐盟一般資料保護規則GDPR (General Data Protection Regulation)之規定。為了讓企業組織能更有效率整合內部已導入之多項標準，新標準採用ISO/IEC附錄SL之高階架構（High Level Structure），該架構為通用於各管理系統的規範框架。

2017新版架構由原本的6章變為為10章，新架構如下：

- 第1章 範圍
- 第2章 引用規範
- 第3章 專有名詞與定義
- 第4章 組織背景
- 第5章 領導統御
- 第6章 規劃
- 第7章 支援
- 第8章 營運
- 第9章 績效指標
- 第10章 改善

新標準主要修改內容如下：

1. 個資盤點單需增加「法規」盤點項目，且應載明個資流向(軌跡紀錄)。
2. 風險管理架構參酌ISO 31000:2009修改。
3. 組織增設資料保護官(Data Protection Officer, DPO)。
4. 個資蒐集、處理及利用：
 - (1) 蒐集前須先告知當事人並取得其同意。
 - (2) 蒐集應有必要性且最小化。
 - (3) 兒童個資蒐集、利用須先經監護人同意。
 - (4) 若個資利用目的為開放資料（Open data）須作去識別化。
5. 個資必須維持正確且最新。
6. 個資保存不超過處理目的存在必要之期限(保存期限)。
7. 增加個資完整性與機密性要求。
8. 預先諮詢與授權，例如：網頁有使用cookies需明確告知瀏覽。
9. 個資管理目標與量測，包括欲導入範圍、現況評估等有效性目標。
10. 增添文件管理規範。

BS 10012:2009版本將於2018年5月25日廢止，公司驗證轉版的過渡期為24個月，因此2019年3月末轉版者證書失效。

[British Standard Institution, BS 10012:2017 Data Protection - Specification for a Personal Information Management System \(2017\). Published the BS 10012:2017 on Personal Information Management System, VsiOn Platform](#)

[BS 10012:2017, bsi. shop](#)

你可能會想參加

- **【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
- 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
- 電商零售業法制宣導說明會暨產學研座談會
- 零售業個資保護宣導暨座談會
- 零售業個資保護及資訊安全教育講習
- 零售業個資保護及資訊安全教育講習

蔡馥如

法律研究員 編譯整理

上稿時間：2017年05月

資料來源：

British Standard Institution, BS 10012:2017 Data Protection - Specification for a Personal Information Management System (2017). Published the BS 10012:2017 on Personal Information Management System, VsiOn Platform, <http://www.visioneuproject.eu/?p=710> (last visited Apr. 27, 2017).

BS 10012:2017, bsi. shop, <http://shop.bsigroup.com/ProductDetail/?pid=000000000030339453> (last visited Apr. 27, 2017).

文章標籤

個資管理制度

個人資料保護與管理

 推薦文章