從新版 BS 10012: 2017 標準看資訊治理要求

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

前 言

英國 BSI 所發佈之 BS 10012:2017 版本個人資訊管理系統標準乃是源自於歐盟歐洲議會於 2016 年 4 月 27 日所通過的 2016/679 the EU General Data Protection Regulation （以下簡稱GDPR）一般資料保護規範而來，BSI在歐洲議會通過後即啟動標準修改撰寫的準備，在同年 9 月至 11 月於網路上對改版標準草案進行公開審閱[1]，在公開審閱的兩個多月期間中，共收到超過 150 件修改意見，後於 2017 年 3 月 31 日正式公布。

新標準在撰寫過程中，曾經參與討論BS 10012:2017 年版本個人資訊管理系統標準的外部機關，除英國個人資料的主管機關 Information Commissioner's Office （以下簡稱ICO）資訊委員公署外，尚包含 Barts and the London NHS Trust、BP、The Children's Society、Dorset County Council、Enterprise Privacy Group、Group 5 Training、IT Governance、Lexis Nexis UK、Lloyds Banking、Mosoco Ltd、NADPO、NHS Business Services Authority、Privacy Partners、Royal Mail、T-Mobile UK Ltd、Trunomi Ltd、TRUSTe、UK General Insurance 等來自不同領域的外部機關[2]。

與原 BS 10012:2009 版本個人資訊管理系統標準不同之處，除 BS 10012: 2017 版本個人資訊管理系統標準以 GDPR 為遵循個人資料保護法規依據外，

[1] 公開審閱乃於 BSI Draft Review 網站（http://drafts.bsigroup.com）進行，BSI Draft Review 係為對外公開網站，使用者於註冊後即可對近期所公布之新標準草案提供個人意見，於公開審閱期間所給予意見者，則囿於該所註冊之會員，並非限定組織身分，會員可以以個人身份參加，故於本文中未特別納入。

[2] 外部單位係以字母排序，係引用自 BSI 於 2017 年 4 月針對 BS 10012: 2017 年版本個人資訊管理系統標準所召開研討會中之簡報，<BS 10012:2017 Data Protection – Specification for a personal management information system> 內容。

BS 10012: 2017 版本個人資訊管理系統標準亦參考了 ISO 組織 Annex SL 對撰寫標準本文 Plan-Do-Check-Act（ 以下簡稱 PDCA)架構， BS 10012: 2017 版本個人資訊管理系統標準與其他 ISO 管理系統標準本文一致，例如： ISO 22301:2012 年版本營運持續管理系統標準、ISO 27001:2013 年版本資訊安全管理系統標準、ISO 9001:2015 年版本品質管理系統標準、ISO 14001:2015 年版本環境管理標準等，對於未來組織建立以多標準為依循的公司治理機制時，可以有共同架構的整合基礎。

簡介 2016/679 the EU General Data Protection Regulation 歐盟一般資料保護規範

欲瞭解 BS 10012: 2017 版本個人資訊管理系統標準，則勢必得從 GDPR 著手，而 GDPR 與過去歐盟於 1995 年所頒佈的 EU Directive 95/46/EC : the Data Protection Directive 隱私保護指令（以下簡稱隱私保護指令）又有何不同之處呢？

GDPR立法的動機，可回溯至 2012 年 1 月歐盟執委會所提出的一般資料保護規範草案，試圖整合隱私保護指令、EU Directive 2002/58/EC : Privacy and Electronic Communications 電子通信隱私保護指令，及 EU Directive 2009/136/EC，希冀透過管理強度的提升，從過去的管制層級而到全歐盟會員國均可直接適用的規章（Regulation），並調和各國分歧不一的現況[3]；該草案由於其嚴苛的規範撼動資訊科技界的巨擘於歐盟經營的根基，紛紛投入龐大的資源向歐盟當局進行遊說，歐洲議會共計收到四千多份相關修正意見，歷經四年的討論，方於 2016 年 4 月 27 日經歐洲議會通過，並於 2016 年 5 月 24 日生效[4]；但由於考量具體實施的可行性，GDPR計畫將於 2018 年 5 月 25 日正式全面實施；在正式實施之前，原隱私保護指令仍為適用，因此，歐盟Article 29 Working Party, WP29 第 29 條工作小組藉由提出Statement on the 2016 action plan for the implementation of the General Data Protection Regulation（ GDPR ） 2016 年關於因應 GDPR 施行之行動計畫，以階段性協助歐盟公務與非公務機關面對個人資料保護法規的變動[5]。

---

[3] 參見徐彪豪，<物聯網時代的資料保護防線 - 以歐盟 GDPR 為中心>，《科技法律透析》2016 年 10 月號，頁 56 至頁 58。

[4] 參見林思惟，<歐盟新規：個人資料保護規則 - 數位防護的新縱深>《聯徵論壇》，http://www.jcic.org.tw/main_ch/fileRename.aspx?fid=950&kid=1 (last visited Jul. 2, 2017)。

[5] 參見林其樺，<數位浪潮：由歐盟個人資料管理制度與英國匿名化探索資料合理利用>，《科技法律透析》2017 年 1 月號，頁 17 至頁 18。

GDPR的立法，對於歐盟會員國具有直接適用的法律效力，但各個會員國家仍可依照其特殊性，於各自國家的資料保護法中進行補充，例如德國聯邦內閣即於 2017 年 2 月 1 日通過Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 為調整資料保護法以符合歐盟一般資料保護規範與歐盟隱資料保護指令之法律修正草案，使德國國內法與GDPR趨於一致[6]。

法國亦於 2016 年開始著手進行修法，在République Numérique數位共和國法案中，欲修改現行關於資料保護之法律，如Loi Informatique et Libertes Act N°78-17 Of 6 January 1978 資料保護法，法國國民議會於 2016 年 1 月一讀通過，以符合歐盟對於個人資料保護水準要求[7]。

英國則有別於前述的德、法兩國，主要是因為英國的脫歐情況，英國ICO發言人認為，資料保護法是屬地主義，無關公投結果，若英國不再是歐盟的成員國，則GDPR也就不會直接適用於英國。然若英國希望在平等條件下與歐盟市場進行交易，則必須證明資料保護是充足的，亦即英國資料保護法須符合 2018 年的GDPR，因此，ICO會向政府提出建議修改英國的資料保護法[8]。**GDPR共 11 章 99 條[9]，各章節說明請參考〈附錄一〉。**

BS 10012: 2017 年版個人資訊管理系統標準介紹

BSI 於 2009 年為因應英國於 1998 年所公布的 Data Protection Act 資料保護法，發佈 BS 10012:2009 年版個人資訊管理系統，乃是希望藉由個人資訊管理系統的建立，作為整體資訊治理基礎設施的一部分，使得可符合個人資料保護法及產業之優良實務要求；BS 10012 標準與 ISO 29100:2011 隱私保護框架不同，BS 10012 標準非僅限於資通訊科技技術上之參考標準，而是可維運之管理系統標準，且管理系統標準自 2000 年 ISO 9001 標準改版後，已全面採用戴明

---

[6] 參見洪政緯，<德國政府通過聯邦資料保護法修正草案>，《科技法律透析》2017 年 2 月號，頁 2 至 3。

[7] 參見孫鈺婷，<法國參議院關於資料在地化(Data Localization)之修法提案>《資策會科技法律研究所》，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=156&d=7283 (last visited Jul. 2, 2017)。

[8] 參見孫鈺婷，<英國資訊專員辦公室關於退出歐盟後續個資保護回應與未來影響>《資策會科技法律研究所》，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=152&d=7533 (last visited Jul. 2, 2017)。

[9] 歐盟 GDPR 一般資料保護規範全文請參見，http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (last visited Jul. 2, 2017)。

博士所推廣之 PDCA 循環來擬定標準內容。

如前言時所提及，BS 10012: 2017 年版個人資訊管理系統標準已參照 ISO 組織 Annex SL 對撰寫標準本文 PDCA 架構來撰寫，當組織擁有重疊的管理系統時，例如：品質管理(ISO 9001)、環境管理(ISO 14001)、資產管理(ISO 55001)、資訊安全管理 (ISO 27001)，或營運持續管理 (ISO 22301) 等，可以透過此一共同架構適當整合。

一、資料保護原則的調整

BS 10012:2017 年版個人資訊管理系統標準與 2009 年版標準的差異，除了引用的法規改為GDPR、使用ISO組織Annex SL架構外，主要的變動尚包括引用的資料保護原則的改變，從原先的參考OECD於 1980 年所公布的Guidelines on the Protection of Privacy and Transborder Flows of Personal Data隱私保護與個人資料跨境傳輸指引 [10]第二部分的資料保護八大原則，改為 GDPR第 5 條的資料保護六原則，將跨境傳輸要求納入資訊安全議題，以及資料主體對其個人資料的近用權等法定權利成為獨立於資料保護原則範圍外，請見下〈表一〉：

編號	2017 版標準	2009 版標準
1	對資料主體應合法、公平且透明的處理 (「合法、公平且透明」)。	受到公平合法的處理。
2	為具體、明確、合法的目的蒐集，且不符合前述目的不得進行更進一步的處理；但為公共利益、科學或歷史研究，或統計目的而進一步處理，則依據第 89 條第 1 項，不被視為不符合初始目的 (「目的拘束性」)。	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。
3	適當、相關且僅限於處理資料目的所需限制 (「資料最小化」)。	適當、相關且不過度。

[10] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 隱私保護與個人資料跨境傳輸指引全文請參見，http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm，該指引已於 2013 年更新，惟第二部分對於資料保護原則並未異動 (last visited Jul. 2, 2017)。

4	正確且於需要處保持更新，與處理目的不相符的資料，必須無任何延遲下以合理方式及步驟確保不正確的資料會被移除或更正 (「正確性」)。	正確且最新。
5	在不超過個人資料處理目的之必要情形下，允許以資料主體以可識別的形式儲存；為了保護資料主體的權利和自由，依據第 89 條第 1 項予以實施適當的技術上和組織上的措施；若個人資料因公共利益、科學或歷史研究，或統計的目的而處理時，個人資料能被長時間儲存 (「資訊保管期限」)。	保留時間不超過必要程度。
6	資料處理應以正當的技術或組織進行，以適當確保個人資料安全，例如：防範未經授權或不合法的處理、防範資料遺失、毀損或損壞 (「完整性及機密性」)。	處理方式符合法律賦予個人的權利，包括標的存取權。
7		獲得安全保障。
8		不在未受到適當保護的情況下被移轉到歐洲經濟區（European Economic Area, EEA）以外的國家。

表一：BS 10012: 2017 年版與 2009 年版標準資料保護原則對照表

二、調整對個人資料及特種個人資料的定義

BS 10012: 2017 年版個人資訊管理系統標準，在名詞解釋上基於資料主體已被識別或可以被識別的資料均屬於個人資料，包含對現存個人的姓名、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，此一定義乃係基於 GDPR 第 4 條第 1 項定義，與原 2009 年版對於個人資料的定義基於英國資料保護法第 1 條第 1 項所定義之『與可辨識存活之人有關的個人資料』，有更進一步的解釋。

對於特種個人資料，BS 10012:2017 年版個人資訊管理系統標準則參照 GDPR 第 9 條，包含種族或族群背景、政治理念、宗教或其他信仰、職業工會會員、基因資料、基於識別唯一自然人為目的的生物特徵資料，及與健康或自然人性生活或性傾向的資訊，與原 2009 年版對於特種個人資料的定義略有出入，差別在於排除『違反任何法規或有違反任何法規的嫌疑，包括個人涉及任何訴訟、對此等訴訟的處置，或在此等訴訟中因任何違反行為而被法院判刑，或被告發有違法的可能』的資料；惟對於近似我國個人資料保護法第 6 條第 1 項所言之犯罪前科類的特種個人資料，BS 10012:2017 年版個人資訊管理系統標準條款 6.1.4 隱私衝擊分析中要求將犯罪定讞、抗辯，或相關安全理由之個人資料與特種個人資料一併納入考量。

三、新版標準 PDCA 架構內的重要增修內容

- **Plan 規劃**

  - ✓ **條款 4 Context of the organization 組織全景：**本條款於 2017 年版個人資訊管理系統標準增加對於組織的瞭解要求，包含：

    - 條款 4.1 Understanding the organization and its context 瞭解組織及其全景，需要鑑別與個人資訊管理有關之內部外部議題

    - 條款 4.2 Understanding the needs and expectations of interested parties 瞭解關注方的需要及期望，需要辨識關注方以及其對組織個人資訊管理系統的期望內容。
      同時，在決定組織建立個人資訊管理系統範圍時，將條款 4.1 與 4.2 所確認之內部外部議題、關注方的期望納入評估個人資訊管理系統範圍的考量。

  - ✓ **條款 5 Leadership 領導作為：**本條款於 2017 年版個人資訊管理系統標準調整高層次的管理議題，包含：

    - 條款 5.1 Leadership and commitment 領導及承諾，將管理高層需要負責的責任增加，例如：確保以建立個人資訊管理系統目標，以與組織的策略方向一致、確保個人資訊管理系統的要求事項整合進組織的營運過程，及當適用其他相關管理角色的職責範圍時，予以支持以展現其領導力等。

- 條款 5.2 Policy 政策：對於政策必要時提供予關注方，以及政策內容對於內部外部議題、關注方要求的增加。

✓ **條款 6 Planning 規劃：**本條款於 2017 年版個人資訊管理系統標準在規劃層面較為顯著的變動，包含：

- 條款 6.1.2 Data inventory and data flow 資料盤點與資料流向：由於 GDPR 將資料控制者、資料處理者、協同資料控制者、第三方，以及委外廠商等均有不同的法律責任與規範，2017 年版個人資訊管理系統標準在盤點個人資料時，除原有在鑑別出個人資料後需辨識目的、類別及說明個人資料的流向外，尚須確認資料控制者、資料處理者、協同資料控制者、第三方，以及委外廠商等角色，以及所使用的關鍵系統、存放位置，及個人資料保留時間表等資訊。

- 條款 6.1.3 Legal basis 法源依據：2017 年版個人資訊管理系統標準要求組織需確認蒐集、處理、利用個人資料與特種個人資料的法源依據，可與我國個人資料保護法第 15 條、第 16 條、第 19 條，及第 20 條第 1 項要求銜接。

- 條款 6.1.4 Privacy impact assessment（PIA）隱私衝擊分析及條款 6.1.5 Privacy risk treatment 隱私風險處置：2017 年版個人資訊管理系統標準要求組織建立隱私衝擊分析方法論以符合 GDPR 第 35 條個人資料衝擊分析要求，隱私衝擊分析方法論需辨別可接受風險水準、識別包含法律遵循、對資料主體權利及自由意志和生理、心理、人身安全、財務損害，以及對組織可能造成聲譽、財務、市場等可能之威脅，並辨識風險發生的可能性與嚴重性等；2017 年版個人資訊管理系統標準並要求組織所辨識之風險，於處置時需經由風險擁有者核可處置計畫及對殘餘風險審核的機制。

- 條款 6.1.6 Prior consultation and authorization 事前諮詢與授權：2017 年版個人資訊管理系統標準為符合 GDPR 第 36 條第 3 項要求，要求組織建立該機制，惟目前以我國現行法律法規，此要求尚未有任何主管機關要求其轄下事業機構需予以遵循。

- 條款 6.1.7 Privacy by design and by default 從設計著手保護隱私：2017 年版個人資訊管理系統標準為符合 GDPR 第

25 條要求，組織於設計重大變更時須適當的以組織化與技術程序實現從設計著手保護隱私控制要求，並留存相關紀錄。

- 條款 6.2 PIMS objectives and planning to achieve them 個人資訊管理系統目標與達成之規劃：2009 年版個人資訊管理系統標準條款 3.2 要求組織應建立文件化之個人資訊管理系統目標，惟對於目標的要求並未明文規範；2017 年版個人資訊管理系統標準則進一步要求組織除應文件化個人資訊管理系統目標外，目標應盡可能可被量測，並規劃量測的頻率、時間、評估量測的方法、執行量測的人員，以及所需的資源等。

✓ **條款 7 Support 支援：**2017 年版個人資訊管理系統標準於條款 7.5 將 ISO 9001、ISO 27001 標準所要求的文件化資訊納入。

● **Do 實施**

✓ **條款 8.2.1 Key appointments 重要人員之指派：**

- 條款 8.2.1.2 Data protection officer（DPO）資料保護官：2017 年版個人資訊管理系統標準為符合 GDPR 第 37 條至第 39 條要求，規範組織應選定資料保護官，並明訂資料保護官的責任與工作。

✓ 移除 2009 年版個人資訊管理系統標準條款 4.6 對主管機關的通知要求。

✓ **條款 8.2.6 Fair, lawful and transparent processing 公平、合法與透明化的處理：**

- 條款 8.2.6.1 Collection and processing of personal information 個人資料蒐集與處理：2017 年版個人資訊管理系統標準將對資料主體直接或間接蒐集個人資料所為之告知要求，從原有的 privacy notice 隱私權公告或 online privacy statement 線上隱私權聲明，統一改為 privacy right information 隱私權資訊；隱私權資訊告知的內容具體化『讓處理過程公平與透明的任何其他資訊』，例如：保存期限的準則、資料主體向主管機關申訴的權利，且對於有關資訊可能用於任何自動化決策和/或剖析時，包括所涉及的邏輯和對資料主體的影響等。

- 條款 8.2.6.2 Records of privacy information（such as notices and statements）隱私權資訊告知或聲明的紀錄：將原 2009 年版個人資訊管理系統標準條款 4.7.2 要求組織應保存告知的紀錄外，2017 年版尚須保留告知的隱私權資訊內容或隱私權資訊版本等資訊，作為未來解決告知爭議的參考。

- 條款 8.2.6.3 Timing of privacy information 隱私權資訊的時機及條款 8.2.6.5 Collection from third parties 自第三方蒐集：2017 年版個人資訊管理系統標準為符合 GDPR 第 14 條要求，於間接蒐集時告知資料主體隱私權資訊的期限為一個月內。

✓ **條款 8.2.7 Processing for specific legitimate purposes 為具體指明合法的目的處理：**

- 條款 8.2.7.3 Processing children's information 處理兒童的資訊：2017 年版個人資訊管理系統標準為符合 GDPR 第 8 條要求，將組織於處理兒童個人資料時，需額外考量其父母或監護人的同意要求，除非為提供專業諮詢與預防性服務的情況例外。

- 條款 8.2.7.5 Open data 開放資料：2017 年版個人資訊管理系統標準將開放資料的運用上，要求組織應建立去識別化機制，使資料無從識別其資料主體，除非有公開個人資料的基礎或法律要求。

✓ **條款 8.2.10.1Retention schedules 保留時程：**2017 年版個人資訊管理系統標準為符合 GDPR 第 5 條第 1 項第 e 款要求，組織如因公共利益、學術研究等目的，需將個人資料轉為給長時間保存，則應採取適當的技術上和組織上措施，維護自然人的權利和自由。

✓ **條款 8.2.11 Security issues 安全議題：**

- 條款 8.2.11.3 Storage and handling 儲存與處理：為因應新興科技所衍生之問題，2017 年版個人資訊管理系統標準將雲端儲存空間及個人自備裝置（BYOD）等議題納入控管要求。

- 條款 8.2.11.5 Access controls 存取控制：為因應資訊安全邏輯存取問題，2017 年版個人資訊管理系統標準將使用者存取個人資料監督機制，納入組織應實施的控管要求範圍。

- 條款 8.2.11.7 Managing security breaches 管理安全事件：2017 年版個人資訊管理系統標準為符合 GDPR 第 33 條要求，於發生安全事件時，組織應於 72 小時內通報主管機關，並依照 GDPR 第 34 條要求，於發生安全事件時，組織應沒有延遲下通知資料主體；同時，標準並明訂通報主管機關及通知資料主體的內容。

- 條款 8.2.11.8 Transfer of personal information outside the border 個人資料移轉到國境外地區：囿於歐盟執委會於 2015 年對 Facebook 資料跨境傳輸案宣布與美國的 U.S.-European Union Safe Harbor Framework 安全港協議無效，且英國並於 2016 年 6 月 24 日脫歐公投通過，因此在跨境傳輸議題上 2017 年版個人資訊管理系統標準要求也就相形複雜，但仍是以傳輸之所在地國家是否已有適當安全評估、國家（主管機關）是否已對所在地國現行法律法規健全情形予以評估、合約保護，以及專責人員適當評估等作為控制要求的考量。

✓ **條款 8.2.12 Rights of natural persons 自然人權利**

- 條款 8.2.12.1 Responding to rights 回應其權利：2017 年版個人資訊管理系統標準為符合 GDPR 第 12 條要求，當資料主體提出權利行使時，需於一個月內回應，必要時得以延長一個月，此條款要求類似我國個人資料保護法第 13 條要求。

- 條款 8.2.12.2 Access to information 個人資料近用權：2017 年版個人資訊管理系統標準將資料主體對其近用權行使查詢內容種類明文列出，包含：處理目的、類別、資訊揭露的接收者，尤其接收者為第三國或國際組織（利用的對象）、個人資料被儲存的期間或準則、有權要求更正或刪除個人資料，限制處理關於該自然人的個人資料、存在向主管機關提出申訴的權利、間接蒐集時個人資料的來源、在自動化決策含剖析，和涉及邏輯上有意義的資訊，該處理對自然人的意義和後果，以及將個人資料轉移到第三國或國際組織時的防護措施等資訊。

- 資料主體依據條款 8.2.12.4 Erasure 刪除權、8.2.12.5 Restriction of processing 限制處理權、8.2.12.6 Data portability 個人資料可攜權、8.2.12.7 Objection 反對權，以及 8.2.12.8 Automated decision-making, including

profiling 自動化決策，包括剖析等權利時，適用的前提與要求，以符合 GDPR 第 17 條、第 18 條、第 20 條至第 22 條要求。

- **Check 檢查**

  - ✓ **條款 9.1 Monitoring, measurement, analysis and evaluation 監督、量測、分析及評估：** 2017 年版個人資訊管理系統標準參考 ISO 22301:2011 營運持續管理系統、 ISO 27001:2013 資訊安全管理系統、ISO 9001:2015 品質管理系統，要求組織除應文件化個人資訊管理系統績效量測紀錄外，並規劃量測的頻率、時間、評估量測的方法、執行量測的人員，以及所需的資源等。

  - ✓ **條款 9.3 Management review 管理審查：**相較於 2009 年版個人資訊管理系統條款 5.2 管理審查， 2017 年版個人資訊管理系統標準參考 ISO 22301:2011 營運持續管理系統、ISO 27001:2013 資訊安全管理系統、ISO 9001:2015 品質管理系統，要求組織於管理審查時需額外討論內部外部議題的變動，以及對個人資訊管理系統績效之回饋與趨勢分析。

- **Act 行動**

  相較於 ISO 22301:2011 營運持續管理系統、ISO 27001:2013 資訊安全管理系統、ISO 9001:2015 品質管理系統，2017 年版個人資訊管理系統標準仍保留 10.2 Preventive actions 預防措施，作為處理潛在不符合事項的因應措施。

BS 10012: 2017 年版驗證時程說明

如前所言， BS 10012: 2017 年版個人資訊管理系統標準是以 GDPR 的遵循所撰寫的國際標準，而 GDPR 將於 2018 年 5 月 25 日全面施行，因此，BS 10012:2017 年版個人資訊管理系統標準即於前言明文說明 2009 年版將於 GDPR 正式實施當天作廢，因此，在 2018 年 5 月 25 日前，BSI 仍可以對新申請驗證的客戶完成以 BS 10012:2009 年版個人資訊管理系統標準進行驗證，並於 2018 年 5 月 25 日前發驗證證書，惟於 2018 年 5 月 25 日後，即無法在對新客戶以 2009 年版執行首次驗證、發證。

對於已經取得通過以 BS 10012:2009 為驗證準則的個人資訊管理系統客戶，

則於 2017 年版標準正式發佈日起（2017 年 3 月 31 日），有兩年的時間進行準備，屆時客戶可於備妥後的追查稽核或重新驗證時一併執行，但請提早準備，若於 2019 年 3 月 31 日前尚未完成轉版驗證，將會影響到既有證書的效力。

開課中

BS 10012 :2017 新版個人資訊管理系列

更多課程請按此>

■ 主導稽核員/稽核員轉版訓練課程

8/03 – 8/04 (台北班)
9/18 - 9/19 (高雄班)
10/12 - 10/13 (台北班)

■ 新版主導稽核員課程

8/21 - 8/25 (高雄班)
9/18 - 9/22 (台北班)
11/6 - 11/10 (高雄班)

我們的專業師資：

章鈺（Oscar Chang）

BS 10012 & ISO 29100 產品經理

BS 10012、ISO 29100 課程專任講師

朱志偉（Justin Chu）

ISO 27001、BS 10012 主導稽核員

BS10012、ISO29100 課程專任講師

課程洽詢：

BSI 訓練學苑 02-26560333 分機 116 吳小姐 Jessie.Wu@bsigroup.com

轉版驗證洽詢、索取報價：

BSI 行銷部 02-26560333 分機 122 黃小姐 tracy.huang@bsigroup.com

〈附錄一〉歐盟 GDPR 一般資料保護規範章節說明

第1章　總則(General provisions，第 1 條至第 4 條)，主要為說明修法之目的、個人資料適用之範圍、適用區域，及 GDPR 所引用名詞的各項定義，定義各項名詞包含個人資料、處理、限制處理、剖析、擬匿名化、資料控制者、資料處理者、資料接收端、第三方、資料外洩、遺傳基因、生物特徵等。

第2章　原則（Principles，第 5 條至第 11 條），主要為說明個人資料處理的六大原則、處理合法性的成立條件、當事人的同意要件、處理兒童、特種個人資料，及犯罪紀錄等個人資料處理原則，以及經控制者處理不允許識別自然人之去識別化要求等。

第3章　資料主體法定權利(Rights of the data subject，第 12 條至第 21 條)，並分為以下五節：

第1節　Transparency and modalities 透明性和形式。

第2節　Information and access to data 資訊與資料主體近用權，包含：直接或間接蒐集時對其個人資料之近用權。

第3節　Rectification and erasure 限制處理與刪除之要求，包含：第 17 條 Right to erasure 刪除權、第 18 條 Right to restriction of processing 限制處理權、第 19 條 Notification obligation regarding rectification or erasure of personal data or restriction of processing 通知資料主體限制處理或刪除權要求，及第 20 條 the data subject's right to data portability 資料可攜權。

第4節　Right to object and profiling 反對權與剖析，包含：第 21 條 Right to object 反對權、第 22 條 Automated individual decision-making, including profiling 對資料主體的自動化決策分析，包含剖析之反抗權。

第5節　Restrictions 限制權。

第4章　控制者與處理者（Controller and processor，第 24 條至第 43 條)，本

章再行細分為以下五節：

第1節 General obligations 一般性義務：針對資料控制者、不在歐盟境內之資料控制者、協同資料控制者、資料處理者及委外處理者等規範，並要求記錄處理個人資料之情形，與第 25 條 the principles of data protection by design and by default 從設計著手保護隱私原則及與主管機關配合等要求。

第2節 Security of personal data 個人資料安全：包含對處理個人資料安全保護要求、個人資料外洩通知主管機關與資料主體責任等。

第3節 Data protection impact assessment and prior consultation 個人資料保護衝擊分析與事前向主管機關諮詢與授權要求

第4節 Data protection officer 資料保護官設計及其責任。

第5節 Codes of conduct and certification 行為準則與認證或標章驗證機制。

第5章 個人資料傳輸至第三國或國際組織（Transfer of personal data to third countries or international organizations，第 44 條至第 50 條），本章主要為說明個人資料於傳輸至歐盟以外之第三國或國際組織時之要件，包含傳輸時的一般性限制、事前之評估、傳輸過程之保護等。

第6章 獨立監管機構（Independent supervisory authorities，第 51 條至第 59 條），本章主要在於說明各會員國所設立之個人資料監督管理專責機構之功能、權責、與要求，為保護歐盟境內有關個人資料處理和促進個人資料的自由流通的自然人之基本權利和自由，歐盟會員國需成立至少一個專責機構負責監督一般個人資料保護規章之落實情形，且各會員國間之專責機構及與歐盟執委會間亦需保持相互合作關係。

第7章 監督管理機構的協同合作與一致性（Co-Operation and consistency，第 60 條至第 76 條），本章主要在確保一般個人資料保護規章具備實施的可行性及在實施上的一致性，各個會員國所設立之個人資料監督管理專責機構需互相提供重要資訊和協同合作，並定義一般個人資料保護規章之實施及說明歐洲資料保護委員會之組成。

第8章　法律救濟、損害賠償與罰則（Remedies, liability and sanctions，第 77 條至第 84 條），本章說明依照一般個人資料保護規章向各會員國所設立之個人資料監督管理專責機構的申訴權利、與個人資料監督管理專責機構或控制者、處理者對抗時的司法救濟、損害賠償及相關刑責與行政裁罰等。

第9章　對特定資料處理情形（Provisions relating to specific data processing situations，第 85 條至第 91 條），本章針對個人表意自由、醫療、勞工雇主雇傭關係、學術研究及宗教等議題下之個人資料處理規範。

第10章　授權法和施行法（Delegated acts and implementing acts，第 92 條與第 93 條），說明一般個人資料保護規章之授權行使及執委會之定位與程序。

第11章　附則（Final provisions，第 94 條至第 99 條），說明對原隱私保護指令及電子通信隱私保護等指令之廢止、歐盟執委會之考核，及 GDPR 之公告生效與公告後兩年正式施行等。