個資保護合規新挑戰—歐盟 GDPR

高額罰款 • 接觸歐盟公民個資即適用 • 採用國際標準助合規

隨著科技發展，個人資料更容易被儲存、運用及傳遞，大幅增加隱私權風險。歐盟執委會於是著手立法，在 2012 年提出一般資料保護規範（General Data Protection Regulation, GDPR）草案，整合隱私保護指令、電子通信隱私保護指令，及歐盟公民權利指令，歷經四年討論方於 2016 年 4 月 27 日經歐洲議會通過，並即將於 2018 年 5 月 25 日正式全面實施。

企業組織只要有來自歐盟的客戶、合作夥伴，就不能置身事外。首先須留意以下 GDPR 的重點：

1. **祭出高額罰鍰**
   - 第一階（Tier one）：最高罰 1 千萬歐元或年度全球營業額的 2%，擇金額較高者罰之
   - 第二階（Tier two）：最高罰 2 千萬歐元或年度全球營業額的 4%，擇金額較高者罰之

2. **個資刪除權**

   若個人想收回個資處理權限，而持有單位無正當理由繼續留存該資料，則須予以刪除，並且須由資料收集單位負責證明資料有留存必要，而非由個資當事人(個人)負責舉證。

3. **新法重新修訂同意權概念，以確保個資使用透明度**

   收集資料時須充分且明確告知個資當事人資料的所有用途，且個資當事人現在得基於任何理由隨時撤銷同意。

GDPR – 強化資料保護和隱私權

全新的歐盟一般資料保護規範（GDPR），預計將於 2018 年 5 月 25 日起正式實施。這項改革對企業來說影響深遠，不僅是歐盟境內公司，所有接觸、處理歐盟公民資料的企業組織也都將受到影響。

歐盟這項改革法規新制的目標在於：

- **強化**個人隱私權，透過設計符合需求的政策，從法規層面著眼
- **強化**歐盟內部市場，透過制定清楚、周密的新法規，賦予個人自由轉移資料的權利
- **確保**新法規實施的一致性
- **設定**全球資料保護標準
- **維護**各行各業資料保護的黃金標準

※ GDPR 各章節說明請詳**〈附錄一〉**

4. **資料若遭外洩，須依法告知**

現在若企業發現資料遭外洩，須於得知後 72 小時內回報主管機關及通知受影響的個資當事人。

5. **個資可攜權**

新法規規定，個資當事人應有權將個資從原本的資料持有單位（以常用電子格式）轉移至另一單位，原持有單位不得阻礙干涉。

6. **隱私權政策設計**

這是新法規的核心精神之一，旨在改變業界整體思維，以及企業制定資料保護政策的方式。根據第 23 條規定，企業應根據業務程序發展，制定符合需求的資料保護政策。

7. **指派資料保護長（DPO）**

企業現在必須指派 DPO，而 DPO 須為獨立職位，且須向主管機關負責，而非董事會。

三階段達成 GDPR 合規

為符合歐盟 GDPR 法規遵循，可以依「了解」、「執行」、「改善」三階段來逐步達成並維持合規狀態。

了 解

1. 董事會和高階主管的認知研討會
2. 繪製資料資產工作流程
3. 差異分析
4. 法律和法規要求評估
5. 資料保護風險評估
6. 訓練及員工教育

執 行

1. 資料保護長（DPO）
2. 隱私權法規遵循架構研發
3. 資料保護和隱私權執行
4. 隱私權設計─隱私權影響評估（PIA）及變更管理

5. 執行、運作和改善安全措施
   - ✓ 滲透測試
   - ✓ 加密使用審查
   - ✓ 事件管理和資料外洩
   - ✓ 安全控制
   - ✓ 當事人存取要求，包括電子蒐證（eDiscovery）

改 善

1. 法規遵循專業能力審查
2. 法規遵循和保證評鑑
   - ✓ 隱私權合規稽核
   - ✓ 內部稽核
   - ✓ 獨立第三方稽核
   - ✓ 主管機關稽核的準備
   - ✓ 驗證（例如：BS 10012、PCI DSS）

最佳個資管理實務–BS 10012 個人資訊管理系統標準

BS 10012 是國際認可的個人資訊管理系統標準，在 GDPR 制定的過程中，BS 10012 也依循 GDPR 的要求做改版，企業組織導入新版 BS 10012:2017 將能有效管理個資，以符合 GDPR 的規範。進一步了解 BS 10012:2017 請參考 BSI 專家文章(一)、專家文章(二)、研討會講義，及教育訓練課程。

By Royal Charter

bsi. 訓練學苑 Training Academy

bsi.

取得 BS 10012 標準

- BSI 網路商店
- BSOL 線上標準資料庫

BS 10012 稽核驗證

BS 10012 新版系列課程

- 稽核員轉版課程
- 建置課程
- 主導稽核員課程
- 基礎課程

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

〈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。