歐盟 GDPR 一般資料保護規範章節說明

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

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。