歐盟「個人資料保護規則」導讀

蔡柏毅/金融聯合徵信中心 法務室*

壹、歐盟個人資料保護法制發展

歐洲聯盟基本權利憲章（Charter of Fundamental Rights of the European Union）第8條第1項及歐洲聯盟運作條約（Treaty on the Functioning of the European Union）第16條均規定，任何人均有保護其個人資料之權利。爰此，歐洲議會及歐盟理事會於1995年10月24日制訂歐盟指令第95/46/EC號，於施行逾十載後，再度領先世界潮流，於2016年4月27日通過歐盟規則第2016/679號「個人資料保護規則（General Data Protection Regulation）[1]」，取代前揭95/46/EC號歐盟指令，並自2018年5月25日起施行。

歐盟指令第95/46/EC號所揭示之宗旨及保護原則雖仍屬健全，惟僅係最低限度之保護規範，歐盟各會員國於歐盟指令第95/46/EC號基礎上所建立之個人資料保護制度，對當事人權利保護程度之差異，可能因此阻礙歐盟對於經濟活動之執行、造成不當競爭及妨礙機關根據歐盟法所應履行之職責。為確保對當事人一致且高度之保護，並排除個人資料在歐盟間流通之阻礙，本規則關於資料處理之個人權利及自由之保護程度於全體會員國間係一體適用，以建構強力且更一致之資料保護框架。

貳、歐盟「個人資料保護規則」章節一覽

第一章 總則（General provisions）

含：主旨與立法目的、適用範圍、用語定義等。

---

* 本文為財團法人金融聯合徵信中心「歐盟個人資料保護規則暨相關規定委外翻譯專案」，法規版本為歐盟網頁揭載之英文版條文，中譯部分委由萬國法律事務所提供。

1 歐盟「個人資料保護規則」之名稱為暫譯。如未特別標示，本文簡稱為「本規則」者，及直接引述之各條（項、款、目）號者，均係指涉此一歐盟規則而言。

第二章 原則（Principles）

含：個人資料處理之一般原則、合法性、特殊個資之處理等。

第三章 資料主體之權利（Rights of the data subject）

第一節 透明度及管道（Transparency and modalities）

第二節 個人資料之資訊與接近使用（Information and access to personal data）

第三節 更正及刪除（Rectification and erasure）含：資料可攜權（Right to data portability）

第四節 拒絕權及個人化之自動決策（Right to object and automated individual decision-making）

第五節 限制（Restrictions）

第四章 控管者及處理者（Controller and processor）[2]

第一節 透明度及管道（Transparency and modalities）

第二節 個人資料之資訊與接近使用（Information and access to personal data）

第三節 更正及刪除（Rectification and erasure）含：資料可攜權（Right to data portability）

第四節 拒絕權及個人化之自動決策（Right to object and automated individual decision-making）

第五節 限制（Restrictions）

第五章 個人資料傳輸至第三國或國際組織（Transfers of personal data to third countries or international organisations）

第六章 獨立監管機關（Independent supervisory authorities）

第一節 獨立地位（Independent status）

第二節 權限、職務及權力（Competence, tasks and powers）

第七章 合作及一致性（Cooperation and consistency）

第一節 合作（Cooperation）

第二節 一致性（Consistency）

第三節 歐洲資料保護委員會（European Data Protection Board）

第八章 救濟、義務及處罰（Remedies, liability and penalties）

2 依本規則第4條之定義，「控管者」（controller）係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；「處理者」（processor）指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構。

第九章 特殊處理之規範（Provisions relating to specific processing situations）[3]

第十章 授權法及施行法（Delegated acts and implementing acts）

第十一章 附則條款（Final provisions）

參、歐盟「個人資料保護規則」之規範重點

一、個人資料處理之一般性原則

個人資料保護之一般原則為尊重權利主體之基本權及自由，尤其是保護個人資料之權利，不問其國籍或住居所而有差異。然而，個人資料之保護並非絕對，必須考慮社會的機能與作用，依照比例原則，平衡兼顧其他基本權利，特別是尊重個人及家庭、住居、通訊、思想、良心及宗教自由、言論及資訊自由、職業自由、受有效之救濟及公正審判之權利，及文化、宗教及語言之多元性保障等。依本規則第5條之規定，個人資料處理應遵循之原則如下：

- 蒐集目的特定、明確且合法（specified, explicit and legitimate purposes）原則；
- 蒐集方式合法、公正及透明（lawfulness, fairness and transparency）原則；
- 資料最少蒐集（data minimisation）原則，即蒐集個人資料應以適當、相關且必要（adequate, relevant and limited）者為限；
- 正確性（accuracy）原則，即應採取一切措施，以確保不正確之個人資料立即被刪除或更正；
- 儲存限制（storage limitation）原則，即保存個人資料時不得長於處理目的所必要之期間；
- 整全與保密（integrity and confidentiality）原則：即處理個人資料之方式應具安全性，以有效防止未經授權或非法之處理、遺失、破壞或損壞；
- 課責（accountability）原則，即個人資料之控管者應遵守上述原則，並就其符合相關原則負舉證責任。

二、例外不適用本規則之情形

本規則要求歐盟各會員國應調和其內國法包括新聞、學術、藝術及或文學表達等表意自由、資訊自由與個人資料保護之權利。在必須調和個人資料受保護之權利與表意與資訊自由時，專為新聞、學術、藝術或文學表達目的所為之個人資料處理，應得除外或豁免於本規則之規定，尤適用於視聽領域、新聞檔案及媒體資料庫之資料處理。依本規則第2條第2項之規定，下列個人資料處理無本規則之適用：

3 本章規範各種特殊類型個人資料處理，包括：處理與言論及資訊自由、官方文件之處理與公衆接近使用、識別證字號之處理、僱傭關係下之處理及為實現公共利益、基於科學或歷史研究目的或統計目的所為處理之保護措施及例外規定等等。

- 歐盟法以外治權領域之活動（outside the scope of Union law）；
- 當事人所為單純之個人或家庭活動（purely personal or household activity）；
- 為預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的（包括為維護及預防對於公共安全造成之威脅）所為之個人資料處理。

三、個人資料處理之特定目的

個人資料處理之特定目的應具明確性（explicit）及合法性（legitimate），且應於蒐集個人資料時告確定（determined at the time of the collection）。個人資料應適當、相關及限於處理目的之必要範圍內（adequate, relevant and limited to what is necessary for the purposes），並確保個人資料之儲存期間在最小限度範圍。當個人資料之處理係以直接行銷為目的時，資料主體應有權在任何時間且毋需任何費用拒絕該處理，包括在與直接行銷有關之範圍內建檔，且不問係原始處理或進階處理。

為符合公共利益、達成科學或歷史研究目的或統計目的所為個人資料之處理，應受本規則所定適當保護措施之拘束。該等保護措施應確保備妥技術上及組織上之措施，特別是資料最少蒐集原則之落實。前述統計目的意指資料處理結果不是個人資料，而係總體資料（aggregate data），且該結果或個人資料並非用於支持關於任何特定當事人之措施或決定。

四、同意之合法要件

同意之給予必須是資料主體依其意思決定就其個人資料處理所為具體、肯定、自由、明確、受充分告知及非模糊之指示，如：口頭或書面之聲明，包括以電子方式為之者[4]。如單純沉默、預設選項為同意（pre-ticked boxes）或不為表示等，均不構成同意。同意須涵蓋基於相同之一個或多個目的所為之全部處理活動，如資料之處理具有多重目的時，全部目的均應取得同意。

個人資料處理係基於資料主體之同意者，控管者應舉證證明資料主體之同意，確保資料主體知悉同意之事實及範圍。事先擬定之同意聲明書，應以易懂（intelligible）且便於取得（easily accessible）之格式為之，並使用清晰易懂（clear and plain）之文字。資料主體應知悉控管者之身分及其個人資料處理所欲達成之目的。於資料主體並非出於真意；無從自由選擇；無法於不損及其權益之情況下得隨時撤銷其同意；不允許就不同個人資料處理方式分別同意；非屬必要而將契約之履行或服務之提供依存於該同意時，上述情形其同意應推定

4 依本規則第4條之定義，「同意」（consent）係指資料主體基於其意思，透過聲明（statement）或明確肯定之行動（clear affirmative action），所為具自主性（freely given）、具體（specific）、知情（informed）及明確（unambiguous）之表示同意處理與其有關之個人資料。

為不具自主性。此外，「撤回同意」應與「給予同意」一樣容易。

為科學研究目的所為之資料處理，於資料蒐集當時，通常不可能完整指明該處理之目的。因此，當科學研究符合公認之道德標準時，允許資料主體僅就科學研究之特定範圍為同意之表示。資料主體應有機會僅就特定研究範圍或預期目的範圍內之部分研究計畫表示同意。

五、資料主體（當事人）之權利

（一）透明原則

個人資料之蒐集、利用、處理應向當事人公開，「透明原則」（principle of transparency）要求關於個人資料處理之任何資訊或聯繫，應方便取得、易於理解、且應以清晰易懂之語言為之。透明原則尤其關注於向資料主體公開控管者之身分、其處理資料之目的及其他進一步資訊，用以確保對當事人公正及透明之個人資料處理。當事人應獲告知有關個人資料處理之風險、規範、保護措施及相關權利，如何行使其權利，權利被侵害時之救濟及其方式。

（二）接近使用權

資料主體應有權接近使用（right of access）其被蒐集之個人資料，並得容易地、於合理之時間間隔行使接近使用權，以知悉並確認該處理之合法性。若有可能，控管者應提供得遠端使用之安全系統以提供資料主體直接之接近使用權。惟該權利不得對他人之權利或自由有不利之影響，包括營業秘密或智慧財產權，尤其是保護軟體之著作權。

為利於資料主體行使本規則之權利，應提供不同之免費管道，包括請求之機制及獲得之機制。於個人資料係以電子方式處理時，亦應提供電子化之請求方式。控管者有義務回應資料主體之請求，不得無故遲延且最遲應於一個月內為之。如因請求之複雜性及數量，必要時得再延長兩個月，控管者應於收到請求後一個月內通知資料主體該次展期，並說明遲延之原因。控管者不同意該請求時，應附具理由，並敘明向監管機關提出申訴及尋求司法救濟之可能性。

控管者應免費提供所處理個人資料之副本一份[5]，如資料主體要求更多副本，控管者得依行政成本收取合理費用。如資料主體係以電子方式提出請求，除資料主體有不同要求外，該資訊之提供亦應以電子方式為之[6]。

（三）更正權及刪除權（「被遺忘權」）

資料主體應有修改或刪除其個人資料之權利，以及當資料之保存違反本規則、歐

5 例如：我國唯一跨金融機構間信用資訊機構金融聯合徵信中心（以下簡稱聯徵中心），每年度免費提供社會大眾1份含加查其他信用資料之中文信用報告。

6 例如：為提升民眾便利之數位化金融服務，自104年11月1日起，我國年滿20歲民眾即可以內政部核發之自然人憑證在聯徵中心網頁線上查閱電子版本個人信用報告，自106年1月1日起，增加加查信用評分項目服務，並將推廣期間免費查閱服務延長至106年12月31日。

盟法或會員國法時，應有刪除權（right to erasure），或稱「被遺忘權」（right to be forgotten），於該個人資料就資料蒐集或處理之目的已無必要時；已拒絕其個人資料之處理時；或已撤回其同意時；或於其個人資料處理違反本規則時，資料主體應享有請求不再處理其個人資料之權利。另一方面，資料主體亦應有權完整化其有欠缺之個人資料，包括以提供補充說明之方式，即所謂「更正權（right to rectification）」。

為強化網路環境之被遺忘權，刪除權應擴張至「公開個人資訊」之控管者有義務通知「刻正進行個人資料處理」之控管者刪除任何該個人資料之連結、複製或仿製（links, copies or replications）。為確保個人資料未遭留存超過必要期間，控管者應設定個人資料銷毀之期限或定期確認，並採用各種措施更正或刪除不正確之個人資料。

惟本規則亦明定於以下情形不適用刪除權之規定，包括：為行使表意自由及資訊自由者；符合公共利益之職務執行或委託控管者行使公權力所必須者；基於公共衛生領域之公共利益且符合相關規定者；為實現公共利益、科學、歷史研究目的或統計目的且符合相關規定者；為建立、行使或防禦法律上之請求者。

（四）資料可攜權

為進一步強化資料主體對自己資料之掌控，當個人資料以自動化手段執行處理時，資料主體應有權以結構的（structured）、廣泛使用的（commonly used）、機器可讀的（machine-readable），以可共同操作的格式（interoperable format）接收其提供予控管者之資料，並有權將之傳送給其他控管者。資料控管者應被鼓勵發展使資料具可攜性（data portability）之可共同操作格式。當技術上可行時，資料主體應有權使該個人資料由一控管者直接移轉其個人資料予其他控管者。但資料可攜之權利不得優先於「刪除權」相關規定行使，並且，該權利不適用於符合公共利益而執行職務者，或委託資料控管者行使公權力而為必要處理之情形。

（五）拒絕權

資料主體得基於與其具體情況有關之理由，隨時拒絕關於其個人資料之處理，即所謂拒絕權（right to object）。控管者應不得再處理該個人資料，除非該控管者證明其處理有優先於資料主體權利及自由之法律依據、或為建立、行使或防禦法律上請求所為之者。個人資料之處理係為科學或歷史研究目的或統計目的所為者，資料主體應有權基於與具體情況有關之理由，拒絕與其有關之個人資料之處理，除非該處理係基於符合公共利益之職務執行之理由而有必要者。

（六）自動決策及建檔相關之權利

資料主體應有權不受自動化決策之拘束（not to be subject to a decision），該決策可能包括對其產生法律效果或類似之重大影響，並僅以自動化處理來評估其個人特徵之措

施。例如：網路貸款申請之自動拒絕，或不包括任何人為介入之電子化人力招募等。即使為締結或履行資料主體與控管者間之契約所必要，或資料主體已明確同意，資料控管者仍應執行適當措施，以保護資料主體之權利及自由及正當利益，至少應確保得以部分之人為參與（human intervention）、表達意見（to express his or her point of view）及獲得挑戰該決策（contest the decision）之機會等。

自動化處理包括以任何形式評估個人特徵之「建檔」（profiling）[7]，特別是為了分析或預測資料主體之工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、地點或動向等特徵，而對其產生法律效果或類似之重大影響。控管者應於建檔時使用適當之數學或統計程式、實施科技化且有組織的措施，以確保個人資料得以即時更正，並將錯誤風險最小化。

六、個人資料處理之安全性

關於個人資料處理之權利及自由之保護，須採取適當之科技化且有組織的措施，控管者應採取符合設計（by design）與預設（by default）資料保護原則之規則與措施。該等措施包括但不限於個人資料處理之最小化（minimising）、盡可能將個人資料予以假名化（pseudonymising）[8]、個人資料之處理與作用之透明化（transparency）、使資料主體得以監控該資料處理、並使控管者得以創造與提升安全功能等。開發、設計及選用處理個人資料之應用程式、服務與產品時，應將資料保護納入考量，以確保控管者和處理者得以完成其資料保護之義務。尤其在公開招標過程中，前揭「設計與預設資料保護原則」應納入考量。

考量現有技術、執行成本、處理之本質、範圍、脈絡及目的與對於當事人權利及自由風險之可能性與嚴重性，控管者及處理者應採取適當之科技化且有組織的措施，包括但不限於以下事項：

- 確保系統及服務持續之機密性、完整性、可用性及彈性；
- 在事故發生後及時回復個人資料可用性及可接近性；
- 定期測試、評估、衡量及確保安全措施之有效性。

七、個人資料保護影響評估

就個人資料之處理可能造成當事人之權利或自由有高度風險之情形，控管者應於處理前執行資料保護影響評估（data protection impact assessment），以衡量風險的來源、本質、特殊性與嚴重性，尤其應包括預計用以

7 依本規則第4條之定義，「建檔」（profiling）係指對個人資料任何形式之自動化處理，包括使用個人資料來評估與該當事人有關之個人特徵，特別是用來分析或預測有關當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵。

8 依本規則第4條之定義，「假名化」（pseudonymisation）係指處理個人資料，使其在不使用其他附加資訊時，無法識別出特定之資料主體，且該附加資料已被分開存放，並以技術及措施確保該個人資料無法識別當事人，故又稱「去識別化」。

降低風險、確保個人資料保護的措施與機制。為證明個人資料之處理符合本規則，在決定有關資料處理之適當措施時，前揭評估之結果應納入考量。

資料保護影響評估尤其應適用於處理地區性、國家或超國家層級可觀數量之個人資料，例如，大規模使用新技術之建檔資料，就相關當事人之個人特徵為體系性及密集性之評估、或透過特殊類型之個人資料、生物資料、或前科及犯罪資料或相關安全措施等之資料處理等。資料保護影響評估在大規模監控公共場合（monitoring publicly accessible areas on a large scale）亦有必要，特別是使用光學電子裝置或主管機關認為有可能對資料主體之權利與自由造成高風險之任何其他情形。

八、特種個資之處理

揭露種族或人種、政治意見、宗教或哲學信仰之個人資料、基因資料、用以識別自然人之生物特徵識別資料、涉及前科及犯罪之個人資料、與健康相關或性生活或性傾向等有關個人資料之處理，原則上應予禁止。但依本規則或會員國法律規定資料主體已明確同意或已公開、為履行義務及行使控管者特定權利之目的、為行使法律上之請求或司法機關執行司法權，或為保障資料主體之基本權及利益而有必要之處理等，不在此限[9]。

九、個人資料之國際傳輸

為了增進國際貿易與國際合作，個人資料之國際傳輸有其必要，但資料於國際流通之增加已然帶來了新的挑戰與有關個人資料保護之課題。在任何情況下，向第三國或國際組織之移轉僅得於完全遵循本規則之前提下執行，唯有當控管者或處理者已遵守本規則所定關於個人資料移轉至第三國或國際組織之規範，且受本規則所定其他條款之拘束時，個人資料之移轉始得為之。第三國應確保有效而獨立之資料保護監督機制（effective independent data protection supervision）、法治、對人權與自由之基本尊重，且應提供資料主體有效且可實現的權利及有效的行政與司法救濟。

十、關於兒童之特別保護

鑑於兒童未能完全知悉其個人資料處理之風險、後果、相關保護措施及權利，兒童就其個人資料值得受特別之保護，尤其在為行銷或建立使用者檔案之目的。任何提供予兒童之資訊及溝通，應採用兒童易於理解且清晰簡易之語言。

如兒童年滿16歲，兒童之個人資料處理應屬合法；如該兒童未滿16歲，僅限於父母或監護人授權或同意之範圍內，該等

9 詳細之排除要件規定，請詳本規則第9條「特殊類型之個人資料處理（Processing of special categories of personal data）」第2項各款規定。

處理始為合法[10]。惟直接向兒童提供預防性（preventive）或諮詢性（counselling）之服務時，無須得其父母或監護人之同意。資料主體於兒童時期所為之同意，應推定為未能完整理解該處理所存在之風險，其後希望移除其個人資料（特別是網路上資料）時，得依本規則行使「刪除權」及「被遺忘權」。

十一、資料保護官（員）

由公務機關或機構執行個人資料處理處理時；或控管者或處理者需要定期且系統性地大規模監控（regular and systematic monitoring）資料主體時；或大規模處理特殊類型個人資料或與前科及犯罪相關之個人資料時，應指定具資料保護法律與實踐之專業知識之資料保護官/資料保護員（data protection officer）。

資料保護官直接向處理或管理者之最高管理階層報告，並應確保其免於任何有關執行職務之指令，且不得因執行職務被解任或處罰。控管者及處理者應確保資料保護官適當且及時的，涉入所有有關個人資料保護之業務。

十二、歐盟個人資料保護委員會

為促進本規則之適用，設立有法人格地位之獨立委員會（Board），取代歐盟指令95/46/EC所設立之個人資料處理保護小組（Working Party）。其組成應包括各會員國監管機關及歐盟資料保護監管機關之首長或相對應之代表。歐盟執行委員會應參與委員會之活動，但無表決權，歐盟資料保護監管機關應有特別表決權（specific voting right）。

十三、資料保護認證及資料保護標章（誌）

為提升本規則之透明度與對本規則之遵循，鼓勵認證機制（certification mechanisms）與資料保護標章及標誌（data protection seals and marks）之建立，以證明控管者及處理者之處理活動遵守本規則，並使資料主體得以快速評估相關產品及服務之資料保護程度。相關認證及標章（誌）均須定期接受評估及更新。

十四、個人資料侵害之通報及損害賠償

一旦控管者發現個人資料侵害已然發生，應即向監管機關通報，不得無故遲延。若可能，應於發現後72小時內通報，控管者如證明依歸責原則，該個人資料之侵害不可能造成當事人權利與自由的風險者，不在此限。當該通知無法於72小時內到達時，遲延之原因應與通知一併提交，並且不得更進一步遲延。

10 本規則第8條「涉及資訊社會服務適用兒童同意之條件（Conditions applicable to child's consent in relation to information society services）」另規定，歐盟各會員國得以國內法另定較低之年齡，但不得低於13歲。另，關於兒童個人資料處理之合法性，不影響一般契約法（例如與兒童有關之契約）之成立或有效性。

因違反本規則而遭受物質上或非物質上之損害時，任何人應有權自控管者或處理者就其損害獲得賠償。惟如控管者或處理者可證明其對於損害之造成不可歸責時，得免除賠償責任。

十五、行政罰鍰之裁處

違反本規則有關控管者及處理者之義務、認證機構之義務或監管機構之義務者，最高處以一千萬歐元之行政罰鍰，如為企業，最高處以前一會計年度全球年營業額之百分之二，並以較高者為準。

違反有關資料處理之基本原則、個人資料國際傳輸之規定、侵害本規則所定資料主體之權利、或違反依照本規則通過之會員國法律所定之任何義務者，最高處以二千萬歐元之行政罰鍰，如為企業，最高處以前一會計年度全球年營業額之百分之四，並以較高者為準。鉅額之法定裁罰額度及有效之計算基準（跨國企業之全球年營業額），對違法者嚇阻力十足。

肆、結語

歐洲共同市場的運作除促進社會與經濟之融合，亦增加個人資料之跨境流通。個人資料在機關與私人間，包含跨歐盟各國間之個人、組織及企業間之資訊交換規模大幅增加，特別是在涉及網路活動時。科技的快速及全球化發展，對個人資料保護也帶來新的挑戰，蒐集、處理及共享個人資料之規模並顯著提升，並更加公開化與國際化。為確保個人資料之全面保護，應賦予當事人對其個人資料更高度且更全面的保護與控制權。本文謹就本次歐盟「個人資料保護規則」之大幅擴充之規範內容（包括長達173點之法規前言及共11章、99條之法條本文）作初步導讀及綱要性介紹，期能拋磚引玉，並將此一劃時代的重要法典中譯並引介給我國政府相關部門、產業及學術研究等各界卓參。