國立政治大學法學院碩士在職專班

碩士論文

指導教授：陳起行博士

銀行國際傳輸客戶資料保護規範－以英國法為中心

研究生：林詩韻

中華民國一百零一年一月

致謝詞

本研究論文得以順利完成，首先感謝陳起行老師的細心指導。印象深刻的是在學生就讀法學院碩士在職專班二年級，修習陳起行教授開設之法理學課程時，老師採取開放式及以日常生活舉例之授課方式，開啟學生對於基礎法學的認識，並引發學生獨立思考及相互溝通對話之能力。在論文構思起草之初，感謝老師對於論文研究方向的提點及在論文撰寫過程中有困惑時，老師總能即時及適時給予學生指點及鼓勵，使得本研究論文在遵循教授的指導下，順利完成初稿。

口試過程中，特別感謝廖緯民教授及劉定基教授之提醒及提供詳細之指導意見，尤其是在對於我國銀行業國際傳輸個人資料保護規範之建議方面，提點學生可提出兼顧我國個人資料保護實務運作現況所能努力之改善建議方向，使得本研究論文之表達能更為完整，並能在理論與實務間取得平衡，由衷感謝老師們的耐心指正。

感謝在就讀法學院碩士在職專班二年半的過程中，家人的支持、體諒及陪伴，使得我在家庭、工作及學業間能夠兼顧無虞，也謝謝我貼心的同事及長官們在工作上的協助，使我成長許多。最後，謝謝政治大學法學院開設碩士在職專班課程，使非法律系的學生，亦能有機會學習法學相關知識，以及專班同學與助教們的熱心幫忙，學生將持續充實相關法律知識，並將所學應用於工作及生活上。

林詩韻　謹誌

2012 年 1 月

論文提要

隨著資訊技術之快速發展及受到金融交易全球化之影響，在營運模式及法令遵循之需求下，使得銀行業將客戶個人資料跨境傳輸至其他國家之公務或非公務機關所產生之資料保護或對資訊隱私權衝擊等議題漸增。為調和不同國家間對於個人資料保護文化及規範程度之差異，各國及各國際組織間均致力於如何在不影響商業交易需要、個人資料隱私安全及資訊自由流通之前提下，經由適當法律規範對於資料管理者國際傳輸個人資料之行為，予以適當控管。

隱私權之概念雖起源於美國，惟現行各國對於個人資料國際傳輸保護規範仍以歐盟委員會於 1995 年發布之個人資料隱私保護指令（Directive 95/46/EC）最為重要且影響層面較大。在歐盟指令仍須各會員國將其轉化為國內法，始得有效執行之前提下，本研究以金融服務產業發展較為領先之國家—英國，以英國銀行業適用之個人資料國際傳輸保護規範為研究主題，所涉法規包括：歐盟指令、英國 1998 年資料保護法（Data Protection Act, DPA）及英國金融服務業適用之相關規範等。

研究結果發現，英國 1998 年資料保護法在參照歐盟指令之相關規範下，對於資料管理者將個人資料國際傳輸已訂有相關限制規定及如何符合相關豁免規定之作業流程及評估程序，英國專責資料保護之監理機關（資訊自由及保護委員會），並已依據歐盟指令，發布規定授權英國企業得採用標準契約範本及經其個案核准採用共同約束條款，顯示英國對於國際傳輸之個人資料已有一定程度之保障。惟如同歐盟委員會之研究報告所述，英國相對於歐盟其他會員國，並未將國際傳輸規範明訂於資料保護法之本文，對於當事人資訊隱私權保護之法律位階，仍有待加強。

不同於我國係於銀行法明定銀行對客戶資料之保密義務，英國法院認為銀行對於客戶資料之保密責任，原始存在於銀行與客戶間之契約。惟英國與我國相同

於金融相關法令中僅針對銀行境外委外所涉之國際傳輸訂有相關監理規範(包括境外委外事先申請核准、申請程序及應檢附之文件)，以透過銀行與委外服務供應商之委外契約，確保金融監理機關能跨國有效行使其監理權限，保護當事人之權益，至於銀行因非委外事項，將客戶資料跨境傳輸至其他國家時，仍應回歸適用資料保護法有關國際傳輸之相關規定。

本研究最後就我國與英國對於個人資料國際傳輸相關保護規範之比較結果發現，我國個人資料保護法雖已於 99 年修正發布（新個資法），但對於國際傳輸之限制規定，修法後雖已明定國際傳輸之定義及加重非公務機關違反國際傳輸規定之罰則，惟未修正其實質規範內容，仍僅授權中央目的事業主管機關於非公務機關有第 21 條所列四項情形之一時，得限制其進行國際傳輸。在新個資法下，非公務機關對於個人資料之國際傳輸，已無須取得目的事業主管機關登記，並取得執照，雖有利於資料之國際流通，惟為保護當事人個人資料於傳輸後之安全，我國是否尚須其他配套措施，以落實個人資料於國際傳輸層面之保障，值得深思。

本研究對於我國銀行業國際傳輸個人資料保護規範之主要建議，包括（1）宜透過各中央目的事業主管機關對被監理機構之監理及其與相關公益團體間之合作，以強化各界對於個人資料保護之重視，（2）國際傳輸之限制規定應予細緻化，並透過產業自治逐步達成個人資料保護之目的，（3）金融監理機關宜配合個人資料保護法之修正，訂定銀行業國際傳輸之作業規範，（4）宜透過租稅合作協定，在不違反我國個人資料保護法及銀行法之原則下，協助我國金融機構解決美國「外國帳戶稅收遵從法」之實施，衍生對於個人財務資訊隱私權及跨境傳輸個人資料保護之問題。

目　　錄

第一章 緒論

第一節　研究動機與目的

第一項　研究動機

隱私權之概念，最早始於美國 Warren 和 Brandeis 於 1890 年在哈佛法學評論所發表之論文，其認為由於照相技術之發展及新聞業已侵入神聖之私人領域，使得「不受干擾之權利（the right to be let alone）」為時代所需，該項權力之基礎係基於人格之不可侵犯（an inviolate personality），而非基於私人財產應受到保障[1]。自此之後，個人隱私之保護，隨著資訊社會的快速發展更形重要，尤其當電腦、網路、傳播等各種科技，使得國家、企業甚或個人之各種資料，均能被迅速蒐集、儲存及傳送，並以不同組合之方式加以組成或呈現，進而作為一種資源或商品，加以利用[2]。

銀行業對於個人資料之蒐集、處理、利用及傳輸，相對於其他產業，更屬不可或缺。隨著金融交易的發展，銀行得以客戶臨櫃方式或直接透過網際網路提供客戶各種不同之金融服務，如辦理存款帳戶或薪資轉帳開戶、消費借貸、信用卡交易、金融商品投資或財富管理等金融服務，使得銀行業相對於其他一般企業而言，更易取得個人之相關資料（如身分證字號、個人相片、電話號碼、住址、電子郵件、投資偏好、財務狀況等），由於銀行每日須處理之客戶金融交易相關資料筆數龐大，使得銀行對於客戶個人資料之管理及處理機制（即對客戶財務資訊隱私權之保護[3]），更顯重要。

---

[1] Warren and Brandeis, The right to Privacy [The implicit made explicit], Harvard Law Review, Vol.4, 1890, 轉引自陳起行，資訊隱私權法理深討—以美國法為中心，政大法學評論，頁 299，2000 年 12 月。

[2] 王澤鑑，人格權保護的課題與展望（三）──人格權的具體化及保護範圍（6）──隱私權（上），臺灣本土法學雜誌，96 期，頁 21，2007 年 7 月。

[3]「財務隱私」（或金融隱私）係指個人或企業與金融機構進行金融交易之非公開資訊，包括個人

受到金融交易全球化的影響，銀行業為提升國際競爭力，近年來金融整併事件頻繁，除國際性大型銀行以合併國內金融機構之方式來台設立子行營運外[4]，在我國與大陸地區簽署「海峽兩岸銀行業監理合作備忘錄（MOU）」，建立兩岸金融監理合作機制後，隨著兩岸金融業務之開放，兩岸金融機構互設分子行營運之情形亦將逐漸普遍[5、6]。另美國財政部及稅務局（Internal Revenue Service, IRS）為落實「外國帳戶稅收遵從法」（Foreign Account Tax Compliance Act, FATCA）於 2010 年 9 月陸續發布 2010-60 通知函（Notice 2010-60）及 2011 年 4 月發布 2011-34 通知函（Notice 2010-34），要求外國金融機構自 2014 年起須每年向美國稅務局通報當年度美國納稅義務人（美國籍或持有綠卡）透過該機構帳戶所取得之利息、所得、資金流動、資本利得情形及帳戶年餘額等個人財務資訊[7]，亦產生國內銀行得否將其在台客戶之存款帳戶等相關個人財務資料跨境提供予美國稅務局等個人資料保護之問題。

在上開銀行業營運模式及法令遵循之需求下，使得我國銀行業（包括外國銀行在台子行及分行）因發展業務需要[8]、降低資料處理作業成

或企業之基本資料、帳務資料、信用資料、投資資料、保險資料等財務情況及其他相關資料。至於「財務隱私權」，則理論上係指個人或企業對於金融機構不法蒐集、處理、傳遞、利用及揭露之自主性權利，而金融機構有維護個人資料安全之義務、以防止客戶資料被竊取、竄改、毀損、滅失或洩漏；若受侵害，應得請求損害賠償。見王志誠，現代金融法，新學林出版股份有限公司，頁 257，2009 年 10 月。

[4] 如 2007 年英國渣打銀行合併新竹國際商銀、荷蘭銀行合併台東企銀（荷蘭銀行後於 2010 年 4 月與澳洲紐西蘭銀行合併）、匯豐台灣銀行合併中華銀行、花旗台灣銀行合併華僑銀行、2008 年新加坡星展銀行合併寶華銀行等，資料來源：金管會銀行局新聞稿。

[5] 截至 2011 年 11 月，本國銀行經金管會核准至大陸申設分行或子行者，計有 11 家，包括臺灣銀行上海分行、兆豐銀行蘇州分行、第一銀行上海分行及成都分行、土地銀行上海分行、合作金庫銀行蘇州分行、彰化銀行昆山分行、國泰世華上海分行、中國信託銀行上海分行、華南銀行深圳分行、上海商業儲蓄銀行子行設立上海分行、玉山銀行東莞分行、臺企銀上海分行，資料來源：金管會銀行局新聞稿。

[6] 截至 2011 年 11 月大陸地區計有中國建設銀行、招商銀行、中國銀行、交通銀行經金管會核准來台設立代表人辦事處，其中中國銀行及交通銀行已於 2011 年 10 月 27 日遞件申請升格為分行，資料來源：金管會銀行局新聞稿。

[7] 「個人資料保護法規對金融業影響之探討」研討會會議資料，金融總會，2011 年 5 月 17 日。

[8] 2009 年 12 月 28 日報載兩岸金融監理合作備忘錄(MOU)即將在 1 月 16 日生效，未來陸資銀行來台也成為台灣的聯徵中心會員，並查詢客戶資訊，也引發恐慌，擔心個人及企業徵信資料外洩，對此，金管會主委陳冲今(28)日在立法院財委會表示，徵信資料的查詢僅限於台灣使用，如果要

本，或因稅務處理、協助警察或司法單位進行金融犯罪調查等因素，而有需要將客戶個人資料國際傳輸（International Transfers 或 Transborder Data Flows[9]）至國外公務機關及非公務機關（如母行、分子行或委外服務供應商等），致使銀行將個人資料跨國傳輸至其他國家產生之資料保護或對隱私權衝擊等議題漸增。

國際傳輸個人資料應為適當限制之原因，在於各國對個人資料保護文化及規範程度不一，為避免個人資料自對資料保護已有相當法令規範之國家，輸出至資料保護規範不足之國家（如我國銀行因業務需要，將其在台客戶資料傳輸至其他國家等情形），產生資料一旦輸出後，未被妥善處理，甚而發生被不當使用之情形[10]。如何在不影響銀行業務發展及兼顧客戶個人資料隱私安全之前提下，經由相關法規機制對銀行國際傳輸予以適當控管，爰引發本研究之動機。

第二項　研究目的

我國現行對於銀行將客戶資料進行國際傳輸，並未訂定特殊規範，故應適用個人資料保護法（即現行「電腦處理個人資料保護法」[11]）、銀行法及相關金融法令等規定。在個人資料保護法方面，其涉及非公務機關將個人資料國際傳輸之相關條文，包括於第 21 條授權中央目的事業主

跨境查詢（將資料傳送至大陸地區之母行），須向金管會申請國際傳輸；聯合徵信中心董事長胡富雄也強調，若違法查詢，除可停權 90 天，情節嚴重者，將撤銷會員資格。原文網址: 陸銀登台可查詢徵信資料　陳冲：國際傳輸則要金管會同意 | 財經新聞 |NOWnews 今日新聞網。

[9] International Transfers（Transborder Data Flows or Cross-border data transfers）一詞於國內相關文獻有人將之譯為個人資料之跨境傳輸（遞）、跨國資料流通等，鑑於 2010 年 5 月 26 日修正發布之「個人資料保護法」第 2 條第 6 款已將該名稱修正為「國際傳輸」，並明定只要將個人資料作跨國（境）之傳輸，不論是屬處理或利用，皆屬該法所稱之「國際傳輸」，故本文中統一稱為「國際傳輸」。

[10] Lingjie Kong, Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law, Vol. 21 no. 2, 443（2010）.

[11] 我國於 2010 年 5 月 26 日發布修正「個人資料保護法」（原「電腦處理個人資料保護法」），新法主要參考 1995 年之歐盟個人資料隱私保護指令（Directive 95/46/EC）修訂，由於本次修正擴大適用範圍，除須進行相關宣導外，民間業者需相當時間調整與準備，相關法規亦需配合增修，故本次修正條文第 56 規定，本法施行日期，由行政院訂之（截至 2012 年 1 月止，行政院尚未明定施行日期）。

管機關[12]得於一定情況下，限制非公務機關之國際傳輸[13]、第 22 條中央目的事業主管機關為執行國際傳輸限制，得派員進行檢查、第 41 條及第 47 條違反國際傳輸規定之相關罰則等。至於金融相關法令，現行除銀行法第 48 條第 2 項訂有銀行之保密義務外，其餘相關金融法令僅於銀行將內部作業境外委外訂有國際傳輸之相關規範，至於非委外事項之國際傳輸，除個人資料保護法之上開規定外，未有特別規定，目前實務作法係由金融監理機關視個案情形監理，予以原則性之規範（如要求銀行於傳輸時，不得違反個人資料保護法、銀行法及相關金融法令等），在上開個人資料保護法及金融法令下，顯見我國現行對於國際傳輸仍欠缺具體明確之法令規範。

國際傳輸涉及多重管轄權及資料輸出國與接收國對於個人隱私權保護規範之程度不一，尤其當資料接收國欠缺隱私保護法制或保護標準遠低於輸出國時，可能引發更多問題[14]。現行各國對於限制個人資料國際傳輸之相關規範較為重要者，為歐盟委員會於 1995 年發布之個人資料隱私保護指令（Directive 95/46/EC[15]，以下簡稱歐盟指令），該指令於第 25 條及第 26 條針對歐盟會員國將個人資料傳輸至第三國家（third countries，即非歐洲經濟區內之國家），明訂有國際傳輸之原則及相關限

[12] 所稱「目的事業主管機關」，依個人資料保護法第 22 條立法說明，基於落實個人資料隱私權益之立法意旨，自宜設立專責機關為主管機關，但未設立專責機關之前，由於各行業均有其目的事業主管機關，有屬中央者，有屬地方者，而個人資料之蒐集、處理或利用，與該事業之經營關係密切，應屬該事業之附屬業務，自宜由原各該主管機關，一併監督管理與其業務相關之個人資料保護事項，較為妥適。依上開立法意旨，有關涉及銀行對於個人資料保護之監督，其主管機關應為我國金融監理之主管機關，即金管會。

[13] 依新版個人資料保護法第 21 條規定，非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之，包括涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護未有完善之法規，致有損當事人權益，以及以迂迴方法向第三國（地區）傳輸個人資料以規避本法之情形。

[14] Gehan Gunasekara, The “Final” Privacy Frontier？Regulating Trans-Border Data Flows, International Journal of Law and Information Technology, Vol. 17, No. 2, 378-832（2007）.

[15]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf（last visited November, 2011）.

制或豁免規定。考量歐盟指令仍須經由各會員國將其轉化為國內法，始得有效執行，而英國金融服務產業之發展始終處於世界領導地位，具國際競爭優勢，且英國早於 1998 年即以歐盟指令為基礎，修正其資料保護法（Data Protection Act, DPA），故本研究選擇以英國財務隱私權保護規範為基礎，蒐集英國資料保護法及金融服務業之相關規範予以分析比較，以期利用英國經驗，提供我國金融監理機關訂定銀行將客戶資料進行國際傳輸相關限制規定之建議，並供銀行於面臨類似問題時，可能處理方式之參考。

第二節　研究範圍與方法

有關國際傳輸之定義，有學者稱「廣義之國際傳輸」係指不論以交通工具實際將文件資料攜帶出境（實體傳送），或利用電腦傳輸資料（透過網際網路傳輸），均屬之[16]。我國修正後之「個人資料保護法」雖已明定國際傳輸之定義，係指將個人資料作跨國（境）之處理或利用，惟新法與舊法相同，並未明確定義何謂「傳輸」，例如企業為確保資料之安全，將異地備援之系統，設置於境外，並不定期將資料傳輸至該地，應屬企業營運之常態。在上開情況下，雖企業之實體備援系統係設置於其他國家，惟對於所儲存資料之控制仍在我國境內管理者之情況下，該項傳輸是否為跨國傳輸，仍待討論。在對於「傳輸」難以明確判斷之情況下，現行歐盟指令及英國資料保護法對於「國際傳輸」亦未給予明確之定義[17]。

個人資料國際傳輸依其傳輸之目的、型態、主體或客體之不同，可區分為以下之態樣：

一、 傳輸目的：可區分為三個層面，包括(一)成本效益考量，即境外委外

[16]黃莉雲，資料跨國流通法律問題之研究—相關理論與規範，國立臺灣大學法律學研究所碩士論文，頁 2，1994 年。

[17] 英國資料保護法於 1998 年修正時，曾對「傳輸」予以定義，傳輸常見之意思為如將資料由一個地方、一個人、一個所有者、一物體或一團體運送至另一地方、人、所有者、物體或團體，惟該定義最終並未納入資料保護法予以明定。見 Peter Carey, Data Protection—a Practical Guide to UK and EU Law, 105-106（2009）.

（offshore outsourcing）。如台灣之外商銀行為降低營運成本，將台北分行客戶申請信用卡之書面資料，委外由中國大陸廣州分行之員工進行輸入，轉為電腦檔案，再傳輸回台灣，或將客戶申貸資料委由外國公司處理等情形、(二)資訊技術考量—電子商務、資料銀行與資料探勘，如美國花旗集團（City Group）於全球 140 個國家設有 160 個營運據點對 2 億多個帳戶之客戶提供服務等、(三)罪犯調查之需要，如反恐怖攻擊行為或因應稅務機關之需求。如德國政府為查緝逃稅案件，收買列支敦斯登（Liechtenstein）所屬銀行離職員工，以取得銀行客戶個人資料之機密[18]。

二、 傳輸主體：可分各國公務機關間個人資料之國際傳輸、非公務機關間之國際傳輸，以及公務與非公務機關間之國際傳輸，其中非公務機關間之國際傳輸又分為跨國企業（集團）內部間（如跨國企業總公司與其在國外之子公司或分公司間）及公司與公司或其他非公司組織間之傳輸。

三、 傳輸客體：依資料性質區分為敏感性[19]及一般個人資料[20]。

由於公務機關間及非公務機關與公務機關間之個人資料國際傳輸，尚涉及取得公益與私益目的間之平衡、二國法權平等及互惠等面向之問題，與本文主要著重非公務機關如何落實個人資料保護制度之重點有所不同。故本研究仍以銀行業將客戶資料於非公務機關間（含企業因委外及非委外事項，將個人資料於集團間及集團外進行跨境傳輸）之國際傳輸所適用之個人資料保護規範為研究主題，在英國法方面將就 1998 年英國資料保護法（Data

[18]翁清坤，論個人資料保護標準之全球化，東吳法律學報，第 22 卷第 1 期，頁 5-11，2010 年 3 月。

[19]依修正後個人資料保護法第 6 條規定，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，除有所列情形者外，不得蒐集、處理或利用。上開五類個人資料即屬敏感性（特種）資料。

[20] 依修正後個人資料保護法第 2 條第 1 款規定，個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

Protection Act, DPA）及其資料保護監理機關「資訊自由及保護委員會」（Information Commissioner's Office,以下簡稱 ICO）所發布國際傳輸相關指引，暨英國金融服務與市場法（Financial Services and Market Act 2000）對於保密義務及金融業境外委外等涉及客戶個人資料國際傳輸之相關保護規範為英國法之研究範圍。

我國規範方面，將就個人資料保護法修正前後所涉國際傳輸之規定與銀行法第 48 條有關銀行保密義務等相關金融法令，暨聯徵中心發布有關會員機構辦理信用資料進行國際傳輸等相關規範為基礎予以整理，透過上開法律規範及相關文獻之閱讀，瞭解並分析比較英國及我國有關財務隱私權及國際傳輸客戶個人資料相關保護規範之現況，以期提出銀行將客戶資料進行國際傳輸時之可能模式及我國相關金融法規之可能改善建議。

國立政治大學
National Chengchi University

第二章 銀行國際傳輸客戶資料之探討

第一節　國際傳輸之態樣

隨著通信之全球化及網際網路的快速成長，個人資料進行國際傳輸變得非常容易，且存有潛在經濟價值。對跨國企業而言，將個人資料跨國傳輸以進行處理或利用，更為日常營運之重要部分，常見情形包括(一)設立於美國之跨國企業（母公司），透過內部網路定期將海外分支機構（如歐盟地區）之資料（含個人資料）傳輸至美國；(二)位於英國之企業將其公司內部之個人資料，傳輸並儲存設立於瑞士之資訊作業中心，或透過電子郵件（郵件內容含個人資料）將個人資料由英國傳輸至香港子公司，亦或(三)英國企業將人工資料傳輸至印度進行處理，並儲存於資料庫後，再傳回至英國之情形[21]。

國際傳輸個人資料之態樣，可依傳輸技術、傳輸主體與客體之不同予以區分，由於本研究主要探討銀行將客戶個人資料進行國際傳輸可能衍生之相關問題，故傳輸態樣中有關傳輸之媒介部分（即傳輸之技術），如實體運送、透過電子通訊或網際網路傳輸等，尚不在本文之討論範圍。以下分別就個人資料傳輸之主體及客體介紹如下。

第一項　傳輸主體

國際傳輸個人資料之主體，依傳輸目的之不同，分為以下三種類型：

一、 公務機關間（包括傳輸至其他國家之公務機關及國際組織）之國際傳輸

此種傳輸多基於為達成特定行政目的或為維持社會安全，兩國或國家與國際組織間，因相互合作進行個人資料之交換，最常見之情形為國際刑警組織會員國間有關犯罪資料之傳輸。又例如，我國為強化與各國政府間之聯繫，積極參與國際洗錢防制組織，並利用參與國際組織促進我國與各國從事洗錢情報之交換與犯罪偵查之

[21] Peter Carey, Data protection in the UK, London: Blackstone, 56（2000）.

合作，故於洗錢防制法第 16 條規定，為防制國際洗錢活動，政府依互惠原則，得與外國政府、機構或國際組織簽訂防制洗錢之合作條約或其他國際書面協定。對於外國政府、機構或國際組織請求我國協助之案件，除條約或協定另有規定者外，亦得基於互惠原則，提供受理申報或通報之資料及其調查結果(包括有關疑似洗錢交易報告、大額通貨交易報告或其他海關通報資料等可能涉及個人隱私資料之金融情報之國際交換）。

二、 非公務機關間之國際傳輸

非公務機關間之國際傳輸，可分為下列二種型態：

（一）跨國企業或集團內各公司間內部資料之國際傳輸(如跨國企業總公司與其在國外之子公司或分公司，或集團內設立於不同國家之關係企業間）：此種類型之國際傳輸最為常見，產生之爭議亦最多，上開二者間資料傳輸之內容可能包括人事、業務營運、市場銷售或研究發展等相關資料。

（二）企業與提供資料服務（處理）機構間之個人資料國際傳輸：此類型又可分為企業將資料提供予資料處理機構進行處理，如國際性銀行為降低客戶資料處理之作業成本，故將其分設於各國之分子行當地客戶之資料，跨國傳輸至特定國家（如印度）統一進行資料處理後，再傳回至各分子行之所在國；或從事蒐集、儲存與分析各種資料之機構，將其資料庫提供予客戶（企業）跨境查詢其所蒐集之資料，如信用報告機構將其蒐集之個人信用資料，跨境提供予會員機構進行查詢等情形。

三、 公務與非公務機關間之國際傳輸

此種類型與公務機關間之資料傳輸目的類似，多基於國家安全或特定行政目的（課稅目的）之考量，如美國於 2001 年遭受 911

恐怖攻擊後，於 2001 年「航空與運輸安全法」（The Aviation and Transportation Security Act of 2001, ATSA）規定，航空公司須於飛機起飛後 15 分鐘內，將旅客及機組員之姓名、出生日期、性別、國籍、護照號碼等美國政府機關認為，為確保飛行安全所必要之資訊，傳輸至關稅及邊界保護局，進而引發歐盟與美國間對於將歐盟公民之個人資料國際傳輸至美國之隱私保護爭議[22]，以及美國為遏阻美國公民透過海外帳戶進行逃漏稅之行為，要求國外金融機構自 2014 年起應向美國稅務局申報其客戶帳戶資產超過美金 5 萬元之美籍納稅義務人（含公民及具永久居留證者）之特定資訊，外國金融機構若未依規定申報，可處 1 萬美元之罰鍰，最高並可處 5 萬美元罰鍰[23]。美國國會通過之上開法令，係對美國公民財務隱私權所為之限制，提供稅務局適當之手段，驗證其課稅所得資料之正確性。惟對於部分國家（如香港、新加坡等）而言，銀行若將其美籍客戶之財務資料傳輸至美國，恐將違反當地隱私權保護之相關規範[24]，產生稅務資料之蒐集與個人隱私權保護間之衝突。

第二項　傳輸客體

國際傳輸之客體[25]，依資料性質可分為敏感性及一般性之個人資料：

一、 敏感性資料（Sensitive Personal Data）

敏感性資料係指於處理個人資料時，需較一般個人資料予以特殊處理之資料類型，可能包括人種、種族、政治傾向、宗教信仰、

---

[22] 歐盟與美國對於個人資料國際傳輸產生之個人資料保護爭議，直至歐盟與美國簽訂安全港協議後(即歐盟委員會認定美國對於個人資料之保護措施已符合歐盟個人資料隱私保護指令所設之標準)，始獲得一定程度之解決—翁清坤，同註 17，頁 10-11。

[23] Summary of Key FATCA Provisions, available at http://www.irs.gov/businesses/corporations/article/0,,id=236664,00.html（last visited November, 2011）

[24] US demands tax tolerance of foreign financial groups, Financial Times（2011）.

[25] 國際傳輸之客體亦有以資料種類進行區分者，例如生產及分配資訊、財務管理資訊、個人與薪資資訊、銀行與信用管制資訊、航空與旅行社訂位資訊、政府施政資訊、科學技術資訊及環境與氣象監督資訊—洪榮彬，資訊時代之資料處理與資料保護—以德國聯邦個人資料保護法為中心，輔仁大學法律學研究所碩士論文，頁 310，1993 年 6 月。

工會會員身分、生理及心理之健康狀況或條件、性生活及犯罪前科等[26]。一般人通常認為財務資料（financial information）及與年齡有關之資訊，同樣具敏感性，惟在資料保護法規中，該等資料並不被歸類為敏感性資料[27]。敏感性資料之蒐集、利用及處理應為特別規範之原因，係考量該等資料相對一般個人資料而言，若未被適當處理，將對當事人隱私權益之影響形成難以彌補之傷害，故當國際傳輸之個人資料為敏感性資料時，通常被認定為屬高度風險之傳輸，依英國資料保護法規定，若國際傳輸之客體為敏感性資料，企業於評估他國法令對個人資料保護是否符合適當程度時，應更為審慎處理且進行全面性之審查[28]。

二、一般個人資料

除敏感性資料外，其餘能透過直接或間接之方式辨識該自然人（living individual）之資料，均屬個人資料之範疇，依據英國資料保護法第 1 條(1)規定，個人資料尚包括任何對於該自然人（當事人）意見之表達（如公司主管於升遷時，對其員工工作表現之意見等人事資料），另依歐盟指令第 2 條(a)之規定，個人資料係指足以直接或間接辨識個人之資料，特別是能辨別當事人之身分證字號或當事人生理、心理、經濟、文化或社會特性之表徵[29]，其中個人之財務資料應屬對該個人經濟狀況之特徵。銀行傳輸客戶個人資料之可能類別如下[30、31]：

---

[26] 依我國修正後個人資料保護法第 6 條之立法說明，考量我國國情及民眾之認知，故未將人種、種族、政治傾向、宗教信仰、工會會員身分等資料視為敏感性資料。

[27] Richard Morgan and Ruth Boardman, Data Protection Strategy—Implementing Data Protection Compliance, London Sweet& Maxwell, 7（2003）.

[28] Data Protection Act 1998—The eighth data protection principle and international data transfers, 2.3.5, Information Commissioner’s Office, Version 4.0, 10（2010）.

[29] Peter Carey, *supra* note 21，at 11.

[30] Security of Personal Financial Information—Report on the Study Conduct Pursuant to Section 508 of the Gramm-Leach-Bliley Act of 1999, The Department of the Treasury, 14（2004）.

[31] 金融控股公司子公司間共同行銷管理辦法第 10 條。

（一）申請文件資料：包括基本資料（如姓名、出生年月日、身分證統一編號、電話及地址等資料)及基本財務狀況(如資產、收入、負債）。

（二）往來交易之歷史資料：包括帳戶號碼或類似功能之號碼、持卡期間、信用卡帳號、信用額度、存款帳號、帳戶餘額、交易帳戶號碼、存借款、支付紀錄、還款是否逾期、消費日期、金額及筆數、交易對手與客戶溝通資訊及其他往來交易與財務情況等資料。

（三）信用報告資訊：包括信用狀況及信用紀錄（退票紀錄、註銷紀錄、拒絕往來紀錄）等資料。

（四）外部資訊：包括工作證明、個人財產資料、信用狀況、其他連絡人及財產保險範圍等查證資訊。

（五）其他一般資料：未用於申請資格審查之統計資訊。

第二節　國際傳輸之需求

個人財務隱私受到侵害，例如因當事人之財務資料具有價值，即當他人取得當事人之個人財務資料時，他人將可能有從中獲利。財務隱私權通常代表個人之財務能力，故銀行對客戶（即當事人）之收入、支出、投資及財富等情況應保守秘密，上開個人資料對大部分人而言，通常不會在公開場合討論其薪水，或與朋友、同事討論其財產狀況，因該等財務情況之討論，或透過個人收入與支出之詳細資訊，即可瞭解個人所從事活動、消費、儲蓄習慣、職業、政治傾向及信仰等額外之個人資訊，使得他人得對當事人擁有之財富進行評估，進而要求當事人捐贈，甚或引來偷竊等行為。惟對當事人財務隱私之侵害，應不限於對於當事人財物損害已發生，只要未經當事人之同意，而將其個人財務資料向第三人揭露，對當事人隱私即已造成侵害，即對當事人財物之侵害，不限於財務損失結果已實際發生。

個人財務資料無法被絕對保密之原因在於金融機構（如銀行、信用卡公司及證券經紀商等）須透過財務資料之取得及傳輸，協助客戶進行金融交易[32]。銀行將客戶個人資料國際傳輸之需求，包括因應客戶金融交易之需要、遵循法令規定、降低客戶服務成本或獲取利潤等因素：

一、客戶金融交易之需要：隨著金融交易之全球化，銀行為履行與客戶間之合約義務，故須將客戶個人資料國際傳輸至其他國家，如臺灣銀行之客戶至國外渡假，並使用其信用卡作為旅館住宿費用之付款工具，則位於臺灣之發卡銀行可能需傳輸該信用持卡人之資料至國外當地旅館，以驗證該信用卡之真實性，或外國銀行在台分行於辦理在台客戶之授信業務，因授信戶申貸金額已超過在台分行之核准權限，故須將客戶授信等相關資料國際傳輸至國外總行，以進行審核。

二、法令遵循之需要：銀行為協助跨國偵查金融犯罪、防制洗錢、舞弊案件、遵循「注意義務」（due diligence）或「認識客戶」程序（know-your-customer）[33]，將客戶個人資料進行國際傳輸。

三、帳戶管理：為管理及服務客戶帳戶或將借款人授信資料歸戶分析與控管等需要，故將客戶個人資料傳輸至提供該等服務之公司，以委託他人協助進行某些帳戶之管理功能（如寄發對帳單等）[34]。

四、降低客戶服務成本：金融集團內由於可能會有銀行、證券及保險等子公司提供不同種類之服務，基於集團內組織架構及內部管理之需要，同一集團可能採功能別方式處理集團內不同公司相同事務之作業，以降低服務客戶之總成本。

---

[32] Cynthia Blum, Sharing Bank Deposit Information With Other Countries：Should Tax Compliance or Privacy Claims Prevail？, Florida Tax Review Vol. 6 no. 6, 603-608（2004）.

[33] Security of Personal Financial Information—Report on the Study Conduct Pursuant to Section 508 of the Gramm-Leach-Bliley Act of 1999, The Department of the Treasury, June 2004, 轉引自陳妍沂，美國財務資訊隱私權保護規定之研究，國立政治大學法學院在職專班碩士論文，頁 31-35，2008 年 5 月。

[34] 同前註，頁 31-35。

四、交互行銷，獲取利潤：金融集團基於法規因素及經營政策之考量，為提供消費者多樣化之金融商品與服務，同一金融控股公司之銀行、證券及保險等子公司得在符合相關金融法令之規定下，將客戶資料交互運用進行行銷，透過子公司間之資料分享，獲取利潤。

第三節　國際傳輸面臨之法律問題

個人資料國際傳輸所引發複雜之法律問題，在於國際傳輸之行為同時涉及跨國性、衝突性、脆弱性及經濟性等面向之考量，分述如下：

一、跨國性之法律規範

各國對於個人隱私權保護之文化與重視程度之落差，在兩國法律環境、司法管轄權不同之情況下，將造成各國對於個人資料保護規範程度之差異及國際傳輸之跨國性問題。各國訂定之個人資料保護規範，常受到當地政治或經濟環境之影響，目前各國國際傳輸之相關規定，以歐盟法律體系於 1995 年發布之歐盟指令對各國影響之範圍及程度最甚，該指令允許歐洲經濟區內（European Economic Area, EEA）之個人資料，得於各會員國間自由傳輸，惟對傳輸至歐洲經濟區以外之其他國家或地區（以下簡稱第三國家）時，卻設有相關嚴格之限制。

雖歐盟指令有關國際傳輸之規範目的，係為平衡各國資料保護規範程度不一之情形（消除資料傳輸之障礙）[35]，但由於在該規範下，已將歐洲經濟區與其他國家予以明確劃分，間接造成資訊自由流通之障礙。在歐盟指令國際傳輸之限制規定下，已迫使全球或區域性之組織致力於相互合作，調和各國間資料保護相關法律規範之一致性，以降低個人資料傳輸之阻礙。

二、全球資訊流通與個人資料保護規範之衝突

類似於貿易障礙，各國訂定之國際傳輸限制，相對於全球資訊之自

[35] Lingjie Kong, *supra* note 10, at 46.

由流通亦產生一定程度之限制。國家對於資訊自由流通之開放程度（含資訊之輸出與接收）受到國家主權、文化及經濟政策與環境之影響。當一國為擴張國家主權時，可能對資訊自由流通採取較為保守之政策（即禁止資料於各國間流通），並對個人資料訂定較為嚴格之國際傳輸限制，相反的，若一國對資訊流通採行較為開放之政策時，則該國有關國際傳輸個人資訊之法規限制，將相對降低或較為寬鬆。如何有效平衡資訊自由流通及個人隱私權保護間之衝突，取得適當平衡為各國訂定資訊自主權與個人隱私保護規範時之重要議題。

三、影響個人隱私權之特殊性

相對於個人財產權受到侵害時，其損害賠償請求權之範圍較為容易確定，隱私權因屬人格權，故其損害之有無及損失之範圍尚難認定。隱私權概念之不確定性，造成法律適用之不安定[36]。惟隨著網際網路及資訊技術之快速發展，個人資料一旦被不當進行傳輸後，當事人之個人資料可能已迅速散佈至不特定之國家，並已對當事人之隱私權產生侵害。在各國個人資料保護程度不一之情況下，當事人隱私造成損害後，因司法管轄權之不同，除不易獲得救濟外（可能涉及跨國訴訟，故即使可進行救濟，花費之成本及時間也甚難估計），若傳輸後資料散佈之範圍無法確定，將造成個人資料無法進行刪除、改正或塗銷；即使範圍可確定，後續補救之成效亦屬有限[37]。

四、營運需求與國際傳輸個人資料限制規範間之平衡

對企業來說，將個人資料進行國際傳輸之目的，不外乎為營運所需，以銀行業為例，一則為銀行營業自由、營運成本及經營風險之考量，二則是對於個人隱私之尊重，在國際洗錢、金融詐騙及恐怖攻擊相繼出現後，各國金融法制亦透過立法手段，調整財務隱私權之保護政策。藉由

[36] 王澤鑑，同註 2，頁 24。
[37] 洪榮彬，同註 25，頁 312-313。

客戶資料庫之建立、分享及傳輸，降低其授信、行銷或其他交易之風險及成本，但個人亦有不受侵犯之隱私領域，如何調和私益與公益間之衝突，並在個人資料保護與金融服務效率間取得平衡，為保護財務隱私權之核心課題[38]

第四節　小結

針對個人資料國際傳輸之限制，在非公務機關間，係為在保護個人資訊隱私、資訊自由流通與營運服務效率三者間取得平衡。若為公務與非公務機關間之國際傳輸，則應考量個人資訊隱私保護之基本權與公務機關自非公務機關取得該等個人資料所為維護之公共利益目的間之平衡，以避免違反比例原則。

銀行將客戶之個人資料（包括個人基本資料及其財產或財務資料），因金融交易、營運或法令遵循之需求，傳輸至國外之母行、分子行或提供金融服務之供應商時，如前所述，該等資料之自由流通為全球金融交易發展所需，對銀行日常營運及業務管理確有必要性，自不宜絕對禁止。惟客戶個人資料在傳輸後，若被資料接收者不當管理，進而被不當使用，對客戶個人隱私所造成侵害，亦難以補正，故在國際傳輸個人資料無法被絕對禁止之情況下，對於國際傳輸自應有合理之規範機制，予以適度限制。以金融監理之角度，對客戶個人資料之輸出限制，應重於資料之接收，銀行將當地國之個人資料輸出前，應瞭解資料接收國有關個人資料保護之相關法制及資料接收者對於個人資料是否有妥善之安全管理措施，避免資料遭受損害或濫用，資料傳輸後更應注意資料之處理及使用，是否符合原始傳輸之目的。

在當事人權益保護方面，個人資料傳輸後，若被不當使用，而對當事人之權益造成侵害，將涉及跨國法律問題，在資料輸出國之當事人，難以對國外之資料接收者主張其權益之情況下（若其損害可歸責於資料接收者之故意

[38] 王志誠，同註 3，頁 252。

或過失），對於國際傳輸自應有相關規範，以維護對當事人隱私權益之保護。

第三章　英國銀行國際傳輸保護規範

第一節　英國資料保護法

相對於美國採取分散式之立法形式，英國對於個人資料保護之立法與其他歐盟會員國相同，採全面適用式之資料保護法制，將對個人資料之保護統一訂定於單一法律，故英國銀行國際傳輸個人資料所應遵循之規範，以現行1998年資料保護法（Data Protection Act, DPA）為主要之法律依據。該法首次訂定公布於1984年，並於1995年因應歐盟委員會發布「個人資料隱私權保護指令」，故於1998年修正資料保護法（Data Protection Act 1998），將歐盟指令納入國內法律，修正後規定於2000年3月1日生效，取代1984年資料保護法。

資料保護法修正後，由於該次修正將個人資料之保護客體，由「電腦處理之個人資料」擴大為包含「人工資料」，英國政府為避免衝擊過大，故將1998年資料保護法分為兩個階段實施，分別於2001年10月24日及2007年10月24日逐步將人工資料納入適用[39]。本節將就1984年及1998年英國資料保護法之立法背景及該法中有關資料管理者將個人資料國際傳輸等相關規範進行探討。

第一項　立法背景

英國對於個人資料保護之立法需求，係因應1970年起電腦及資訊技術之快速發展，造成對個人隱私之威脅。英國政府鑑於當時現存之法律已不足以處理企業以電子型態持有及處理與個人資料相關資訊所衍生之問題，故開始資料保護法之訂定，立法歷程如下：

一、楊格報告書（The Younger Report）

[39]周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啟示，科技法律透析，頁55，2005年1月。

1970 年初英國楊格委員會（the Younger Committee on Privacy）針對電腦及資訊技術發展引發之個人隱私保護議題提出 10 項使用電腦處理個人資料保護之指導原則[40]。英國政府為回應楊格報告書所提議題，前後共計公布二份白皮書（White Papers），首份白皮書主要檢討公務部門對於個人資料之處理，續後發布之白皮書，英國政府開始思考是否須對個人隱私訂定更進一步之保護規範，以管理公務及非公務部門對於個人資料之處理[41]，並設立寧得普委員會（Lindop Committee）負責研究相關議題[42]。

二、寧得普報告書（Lindop Report）

寧得普委員會成立後於 1978 年發布報告指出由於「楊格報告書已就個人隱私之相關議題提出相關建議。本委員會之工作係針對個人資料保護之問題提出處理意見。事實上，該二領域相有重疊之處，重疊部分可稱為『資訊隱私』（information privacy），或『資料隱私』（data privacy）。本報告中使用『資料隱私』，以代表個人控制與其個人相關資料流通之權利。」該報告中同時建議英國政府應設立專責之資料保護機關（Data Protection Authority），針對不同產

[40] 楊格委員會對於隱私保護提出之 10 項指導原則，包括(1)因特定目的取得之資訊，未經適當授權不得為特定目的外之使用；(2)授權應能限制因特定目的所取得之資訊；(3)資訊之蒐集及持有必須是適當、相關且不超逾該特定目的之最低需求為限；(4)因統計目的，以電腦系統處理之資訊系統應有適當之設計及程式，以將處理中之資料與資料庫中之其他資料予以區分；(5)與當事人間應有適當之約定，持有與當事人相關之資訊時，應能告知當事人；(6)系統中應有一定程度之安全機制，並事先提供使用者明確詳細之說明，包括如何預防資料被故意的濫用或被錯誤的使用；(7)應提供監控系統以協助發現任何違反系統安全性之情形；(8)設計資訊系統之期間，不應將資料儲存於系統中；(9)持有資料之正確性，應有更正錯誤及資訊更新之機制；(10)編碼值判斷時，應採取適當之保護措施（care should be taken in coding value judgments），楊格報告書提出之立法建議，在當時最終未被英國政府所採用。See Peter Carey, *supra* note 21, at 1-8.

[41] Val Collins, Privacy in the United Kingdom：a Right conferred by Europe？, International Journal of Law and Information Technology, Vol. 1 No. 3, 293（1993）.

[42] 英國政府發布之白皮書中指出使用電腦處理個人資訊的時代已來臨，並提出電腦處理個人資料之 5 項特性，包括(1)有助於龐大資料之處理、記錄及保存於系統中；(2)可從各不同資訊點以簡便及快速之方式取得資料；(3)快速將資料由一個資訊系統傳輸至另一個資訊系統之可能性；(4)將資料予以合併處理之可能性增加；(5)可將資料儲存、處理及轉換為無法直接閱讀之型態。See Peter Carey, *supra* note 21, at 1-8.

業特性訂定資料保護之最佳實務守則，但寧得普報告所提建議，英國政府於當時並未採用[43]。

英國政府開始真正重視個人資料保護之原因，主要憂慮企業因商業活動，產生個人資料國際傳輸之需求時，若英國對於資料保護之立法與各國規範程度差異過大，將對英國資訊流通產生阻礙，進而影響其商業發展，故英國政府對於個人資料保護之立法政策，係基於商業交易需要，而非基於對個人隱私權之保護[44]。

第二項　1984 年資料保護法

一、立法過程

英國政府在上開立法背景下，雖已開始重視並逐漸推動資料保護之立法，惟直至 1981 年歐洲理事會發布個人資料自動化處理保護公約（the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data），為使英國資料保護之法律能與國際規範一致，避免英國因個人資料保護程度之不足，被其他國家視為非會員國，而限制其資料進行跨國傳輸（含資料之輸出及接收），英國上議院於 1982 年 12 月提出英國第一部之資料保護法案，但該法案因 1983 年之大選而終止，再次修正之法案於 1983 年 7 月提出，最終成為英國 1984 年資料保護法，該法計有 5 節 43 條條文及 4 個附錄，其中附錄一，並明定八項個人資料保護之基本原則[45]。

---

[43] Peter Carey, *supra* note 21, at 1-8.

[44] Val Collins, *supra* note 41, at 292.

[45] 英國 1984 年資料保護法於附錄一訂有八項資料保護原則：原則一，個人資料之取得及處理，應公平與合法；原則二，個人資料之持有，僅限於一項或多項特定且合法之目的；原則三，因任何目的持有之個人資料於使用及流通時，不得違反該特定目的；原則四，因一項或多項目的持有之個人資料，應適當、相關且不超逾該特定目的；原則五，個人資料應正確，必要時應保持更新；原則六，因任何目的所持有之個人資料，其持有期間不得超出該目的所需之期間；原則七，當事人有權請求(1)不得有不當之遲延或由當事人支付不當之費用，在合理之期間內，得要求資料者告知，其是否持有以該當事人為資料主體之個人資料及取得資料使用者所持有之相關資料、(2)在適當情形下，當事人有權請求資料予以更正或消除；原則八，個人資料應採取適當之措施，以防止個人資料被未經授權之取用、修改、揭露或毀損，或防止個人資料被意外喪失或毀損。見經社法規譯介叢書 028—英國資料保護法，頁 41-42，1988 年。

二、1984 年資料保護法國際傳輸之限制規定

1984 年資料保護法有關國際傳輸個人資料之規定，主要訂於第 4 條第 3 項 E 款、第 5 條第 2 項 E 款、第 12 條及第 39 條等條文，在該等條文規範下，英國資料保護監理機關透過事先登錄之機制，以控管企業將個人資料進行國際傳輸。

（一）事先登錄（第 5 條第 2 項 E 款）

依據 1984 年資料保護法第 3 條規定為達成該法訂定之目的，英國應設立資料保護登記處（Data Protection Registrar[46]），負責落實該法之執行。英國之資料使用者（Data Users）若擬將資料直接或間接傳輸至英國以外之國家或地區時，依同法第 4 條第 3 項 E 款規定，資料使用者應將該國家或地區之名稱及相關說明向登記處登錄。除已登錄者外，資料使用者不得直接或間接將其持有之個人資料傳輸至境外或未經登記處核准之國家或地區。

（二）禁止傳輸之通知（Transfer prohibition notices）（第 12 條）

1984 年資料保護法第 12 條規定，資料保護登記處若發現資料使用者或已向資料登記處登錄之人，將資料傳輸至非歐洲公約之會員國，且登記處認定該項傳輸可能違反或將導致違反該法所訂之資料保護原則，或資料雖係傳輸至歐洲公約之會員國，惟登記處認定該項傳輸可能將違反該法之資料保護原則，包括資料傳輸之人意圖將資料再傳輸至其他非歐洲公約之會員國，且再傳輸之行為可能違反或最終導致違反任一資料保護原則時，登記處得送達「禁止傳輸之通知」予資料使用者，明定於一定期間之內，完全禁止資料之傳輸（若登記處認為情況特殊，基於緊急之理由，禁止通知並可於送達時，立即生效）。

[46] 資料保護登記處為當時英國專責資料保護之主管機關。

登記處在決定是否發出禁止傳輸通知時，須考慮禁止通知能否防止對任何人之損害或侵害，並應考量英國與其他國家或地區間，對於資料自由傳輸之意願。個人資料傳輸若依據法律、法律相關授權規定或基於任何公約或其他文件，致使英國負有國際傳輸之義務時，則登記處不得發出禁止傳輸之通知。

（三）個人資料若原始在英國境外處理，並在境外使用，即使對該等資料之控制（即管理個人資料之資訊內容及使用）係來自英國境內之資料使用者，將不適用國際傳輸個人資料之限制規定。（第 39 條）

第三項　1998 年資料保護法

一、修法背景

為保護與處理個人資料當事人之隱私權，並調和各會員國間有關資料保護之法律規範，以期各國能在合法處理個人資料之情況下，保護當事人之權利及資料之品質，使各會員國之資料保護法制能維持在相當程度，以利資料於不同會員國間之傳送與接收，故歐盟委員會於 1995 年 10 月發布歐盟指令（Directive 95/46/EC），要求各會員國最遲應於 1998 年 10 月將歐盟指令納入國內法實施。

英國為因應歐盟指令之發布於 1998 年 7 月 16 日經立法通過，發布資料保護法，明定該法自 2000 年 3 月 1 日生效。1998 年資料保護法之修正雖為遵循歐盟指令，但該法之規範目的，主要仍為確保個人資訊能被適當使用（資訊隱私），而非為避免或保護對個人所處領域之隱私權之侵犯[47]。

英國上議院在 2003 年 Wainwright v Home Office 一案，指出英國普通法雖沒有就侵犯隱私權自由之行為提供任何程度之認定或保

[47] Richard Morgan and Ruth Boardman, *supra* note 27, at 235-238.

護。惟為補救對於隱私權保護之不足，英國法院對於侵犯隱私權之行為（如侵害秘密或公開誹謗等）承認以侵權行為作為訴訟之依據，並擴大其適用範圍[48]，例如在 Douglsa v. Hello 一案中，英國法院以違反信賴保護（Breach of Confidentiality），肯認隱私本身係屬於來自於個人之自主價值，應受法律之保護[49]。

為維護法律之安定與進步，英國法院採用漸增的方法，擴大對於隱私之保護，雖有學者批評此種方法，不足全面規範個人隱私之保護問題，另歐盟委員會司法部門所發布英國落實歐盟指令之研究報告，亦認為英國對於個人資料之保護，較欠缺憲法上之基礎。然於 1998 年英國已依據歐洲人權公約（Human Rights Convention）發布英國人權法（Human Rights Act 1998），對於個人隱私權之侵犯已予明文限制，肯定隱私為一種憲法上的權利與價值[50]。

二、規定內容

1998 年資料保護法，計有 75 條條文，分為六大部分，包括總則（第 1 條至第 6 條）、資料當事人之權利（第 7 條至第 15 條）、資料管理者之通知（第 16 條至第 26 條）、豁免條款（第 27 條至第 39 條）、執行（第 40 條至第 50 條）及附則（第 51 條至第 75 條），並訂有 16 個附錄（schedules）。

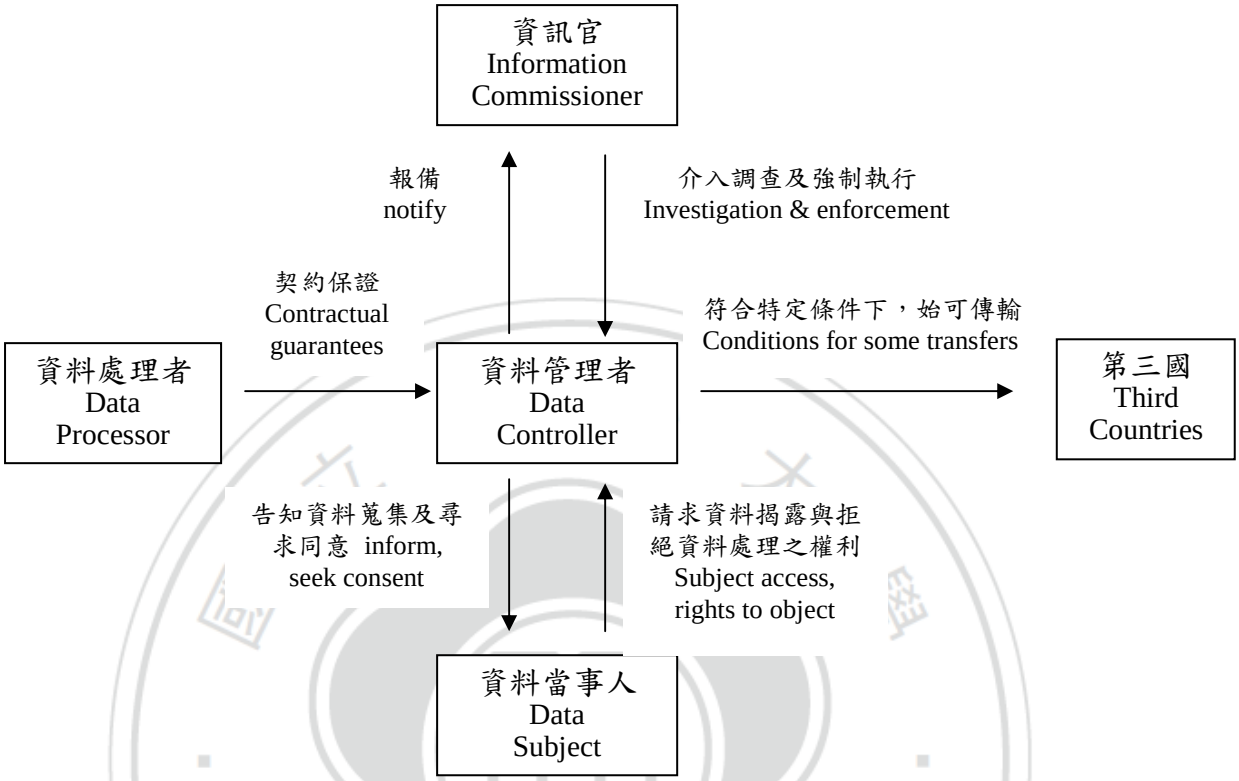
為確保資料保護之相關規範能具體落實，英國依據 1998 年資料保護法第 6 條之授權，設有資訊官之制度（Information Commissioner）（同 1984 年資料保護法第 3 條第(1)款(a)之規定），並設立專責之資

[48] Roger K. Baker, Offshore IT Outsourcing and the 8th Data Protection Principle—legal and regulatory requirements—with reference to financial service, International Journal of Law and Information Technology Vol. 14 No. 1, 3-5（2005）.

[49] 王澤鑑，同註 2，頁 35。

[50] 同前註，頁 36。

料保護法庭（Data Protection Tribunal）。在上開法律制度下，英國個人資料保護之基本架構如下[51]：



資訊官依據資料保護法之授權設有獨立之「資訊自由及保護委員會」（Information Commissioner's Office, ICO），以維護公眾之資訊權、推動公眾團體之資訊公開及個人資料之隱私權，並專責發布處理個人資料之最佳實務、提供各界有關資料保護之建議及相關指引（guidance）；維持各組織內資料管理者有關資訊處理程序之登記，以及協助解決與決定各組織內是否已適當遵循資料保護法，有關個人資料處理之相關規定[52]。

1998 年資料保護法第二章明定六項資料當事人（data subjects）之權利，包括個人資料近用權（Right of access to personal data）、損

[51]David Bainbridge, Data Protection Law 26, Figure 3.1，2005，轉引自李振瑋、江耀國，英國資料保護法中資料所有人權利之研究－－兼論我國個資法之相關規範及案例，中原財經法學，頁 39，2010 年 6 月。

[52] An overview of the Data Protection Act 1998, Information Commissioner Office, available at www.ico.gov.uk（last visited November, 2011）。

害防止請求權（Right to prevent processing likely to cause damage or distress）、直接行銷拒絕權（Right to prevent processing for purposes of direct marketing）、防止自動化之決定（Rights in relation to automated decision-taking）、損害賠償請求權（Compensation for failure to comply with certain requirements）、資料之更正、封鎖、刪除與銷毀（Rectification, blocking, erasure and destruction）。其中最重要者，為個人資料近用權，即賦予當事人經由書面申請（或電子方式傳輸），並支付適當費用後，得要求資料管理者提供其是否處理當事人個人資料之相關資訊，包括處理資料之內容、目的及揭露對象等[53]。

近期英國資料保護較具代表性之案例為 2003 年英國上訴法院對 Durant v. FSA 一案之判決[54]，原告 Durant 先生為巴克萊銀行（Barclays Bank）之客戶，雙方於 1993 年間因故涉訟，Durant 先生敗訴後，陸續於 2000 年至 2001 年間主張依據資料保護法第 7 條個人資料近用權之規定，向英國金融服務總署（Financial Services Authority, 以下簡稱 FSA[55]）請求其協助取得與上開訴訟案有關之個人資料。上訴法院判決結果認為，參酌歐盟指令修正之資料保護法，其規範目的在於保護個人之基本權，特別是與個人隱私權及保護當事人得以確認資料管理者處理資料之過程，是否有非法侵害其個人隱私，而非幫助當事人取得資料，並對第三人進行訴訟，亦非所有出現當事人名字之資料，皆屬資料保護法之個人資料範圍（須該筆資料之揭露將影響個人隱私或對當事人造成負面效果），本案原告請求之相關資料，不符合資料

[53] 周慧蓮，同註 39，頁 56。
[54] 針對該判決英國資訊自由及保護委員會（ICO）於 2006 年 2 月發表該判決對於 1998 年資料保護法之影響—The “Durant” Case and its impact on the interpretation of the Data Protection Act 1998。
[55] FSA 目前為英國金融服務產業之監理機關，網站：http://www.fsa.gov.uk。

保護法所稱「個人資料」，自不得主張依據資料保護法第 7 條之規定，取得相關資訊[56、57]。

三、英國資料保護法之修法重點[58]

英國 1998 年及 1984 年資料保護法修法前後之差異如下：

（一）保護客體納入人工處理之個人資料：1998 年資料保護法將部分人工處理之個人資料納入適用範圍。

（二）強化資料處理程序之合法性：增訂處理個人資料之最低門檻要求。

（三）增訂敏感性之資料類別（sensitive personal data）：新增敏感性資料之內涵，並明定除符合一定條件外，敏感性資料不得被任意蒐集或處理。

（四）修正國際傳輸之限制：除符合一定條件，否則英國應禁止個人資料傳輸至第三國家。

（五）強化當事人之權利：包括因非法處理個人資料造成對當事人之損害時，當事人損害賠償之請求權。

第二節　1998 年資料保護法之國際傳輸規定

1998 年資料保護法有關國際傳輸之限制規定，計有附錄一第一部分之資料保護原則八、第二部分解釋何謂原則八所稱符合個人資料保護之適當程度、附錄四有關原則八之豁免規定，以及 ICO 針對原則八發布之「資料保護

[56]周慧蓮，同註 39，頁 57-58。.

[57] 該判決同時指出，英國 FSA 依據 2000 年金融服務與市場法之授權為英國金融服務業之金融監理機關。直至 2001 年該法完全施行前，FSA 係依據 1987 年銀行法執行法定監理權限，在日常監理中，FSA 須自公司、企業及個人取得或收取許多資訊，FSA 依據 2000 年金融服務與市場法第 348 條規定，FSA 對於所取得之資料應負保密義務（1987 年銀行法第 28 條至 85 條亦訂有監理機關保密義務之相關規定，惟該等規定已被 2000 年金融服務與市場法所取代）。惟 FSA 之保密義務，已被 1998 年資料保護法第 27 條(5)之規定所取代。個人資料依同法第 7 條個人資料近用權之規定，要求所有資料管理者包括 FSA，應在金融服務與市場法之有效運作與對個人及第三人隱私權之保護間取得平衡。See Durant v. Financial Services Authority (Disclosure) [2003] EWCA Civ 1746, Court of Appeal (Civil Division), 2003-12-08 (Approx. 41 pages), 2-5（2003）.

[58] Peter Carey, *supra* note 21, at 6-7.

原則八及國際資料傳輸指引」（The eighth data protection principle and international data transfers，以下簡稱「國際傳輸指引」）。

第一項　原則八訂定背景及規定內容

一、歐盟指令

1998 年資料保護法有關國際傳輸之規範，主要參酌歐盟指令第 25 條及第 26 條規定訂定。依據該等條文規定個人資料於歐洲經濟區內（European Economic Area, EEA）得自由傳輸，惟若傳輸至第三國家，為衡平各國資料保護規範程度不一致之情形，應符合相關限制規定，歐盟指令並授權歐盟委員會得發布標準契約範本（Standard Contractual Clauses）及共同約束條款（Binding Corporate Rules, 以下簡稱 BCR），供各國員國使用，規範重點如下：

（一）國際傳輸原則[59]（第 25 條）

1、**會員國應於國內法訂定個人資料國際傳輸相關規範：**會員國將個人資料傳輸至第三國家時，不得違反歐盟指令，並應確保第三國家之個人資料保護法制能符合歐盟指令之資料保護標準。

2、**個人資料輸出之目的地國，須符合歐盟指令之資料保護標準：**第三國家是否符合歐盟之資料保護標準，資料輸出者應評估整體資料傳輸之作業環境，尤其應考量所傳輸資料之性質、目的、資料處理之所需作業期間、資料來源國及最終目的國、當地國之法律規範（含普通法及特別法）及其落實情形，暨與個人資料有關之安全維護措施等。

3、**第三國家之個人資料保護法制，不符合歐盟指令時之處理：**歐盟委員會或各國會員若認定特定第三國家不符資料保護之標準時，應相互通知，採行必要措施以防止會員國之個人資料向該

[59] 歐盟個人資料隱私保護指令第 25 條。見何金鍾編譯，金融與徵信叢書 No. 24「歐聯資料保護綱領」，財團法人金融聯合徵信中心，頁 69-71，1997 年 6 月。

特定第三國家進行傳輸。若資料已傳輸，歐盟委員會應採行相關救濟措施，必要時與該第三國家進行協商。對於歐盟委員會決定採行之措施，各會員國應配合辦理。

（二）**豁免規定**（第 26 條第 1 項）

當第三國家經認定對個人資料之保護程度不符合歐盟指令之標準時，會員國得將資料傳輸至該特定第三國家之情形如下[60]：

1、經當事人明示同意傳輸；

2、履行當事人與資料管理者間之契約約定之所需；

3、為履行當事人與第三人之契約，且該項傳輸有利於當事人；

4、為維護重大公共利益或為在法庭提出、行使或為維護當事人權利之需要；

5、為維護當事人重大利益所必要者；

6、登記處依法律或法令之規定，有將個人資料向社會大眾公開之義務，或提供給特定或不特定之人，公開查閱。

（三）**資料管理者因符合上開例外情形國際傳輸個人資料之處理**（第 26 條第 2 項至第 4 項[61]）

1、資料管理人應訂定適當安全措施，以保護當事人之隱私、個人自由及基本人權，安全維護措施得於適當之契約條款中訂定。

2、會員國因例外情形須將個人資料國際傳輸時，應通知歐盟委員會及其他員會國。歐盟委員會或其他會員國若認為該項傳輸有損害當事人隱私、自由及基本人權時，得依一定程序採行適當措施，委員會決定採行之措施，各會員國應配合辦理。

3、為確保國際傳輸能符合歐盟指令之規定，歐盟委員會得依一定程序統一訂定標準契約範本，提供會員國使用。

[60] 同前註，頁 71-73。
[61] 同前註，頁 71-73。

為確保歐盟各會員國居民個人資料及隱私之安全，歐盟指令鼓勵第三國家採用近似於歐盟指令之資料保護規定，以降低國際傳輸之障礙。

二、英國資料保護原則八及其豁免規定

（一）原則八—國際傳輸原則

1998 年英國資料保護法參照歐盟指令第 25 條規定，於附錄一之原則八明定國際傳輸之限制如下：

「個人資料，除該處理個人資料之國家或地區，對於當事人之個人自由與權利已有適當程度之保護（adequate level of protection）外，禁止傳輸至「歐洲經濟區」（European Economic Area, EEA）以外之國家或地區」。

相對於 1984 年資料保護法對於將個人資料自英國輸出，除要求傳輸者應告知登記處（register）其傳輸目的，並於必要時，得發出禁止傳輸通知外，其餘尚未訂定相關限制規定。1998 年資料保護法對於國際傳輸，明定個人資料若計畫輸出至第三國家，除輸出資料之資料管理者能確認該特定第三國家對當事人資訊隱私與自由已有適當程度之保護外，否則該項傳輸將被初步認定為不合法之傳輸行為[62]。

依原則八之規範國際傳輸時，資料管理者須考量的第一個要素為確認該項傳輸是否符合資料保護法「國際傳輸」(transfer)之定義，包括資料接收者位於第三國家及該個人資料之傳輸是否適用原則八之限制（如英國之 A 公司將員工個人資料，傳輸至位於德國之 B 公司，該等資料並經由瑞士（非歐洲經濟區之會員

[62] Peter Carey, *supra* note 21, at 56.

國）之電信網路進行傳輸。由於此項傳輸行為係發生於二個歐洲經濟區之會員國，自無須適用原則八）[63]。

若資料進行傳輸時，原始資料並非來自英國，如英國銀行之印度分行於當地蒐集之客戶資料，該等資料雖傳輸至英國進行處理，再傳回至印度，因該等原始資料即來自於印度，英國 ICO 認為該項傳輸行為無須適用英國資料保護法之規定，自不會對該等資料再傳輸至印度進行限制[64]。

（二）豁免規定

如同歐盟指令訂有若會員國認定第三國家之資料保護規範不符合歐盟指令之標準時，仍得將個人資料傳輸至特定第三國家之例外情形，英國 1998 年資料保護法於附錄四，亦訂有不適用原則八之豁免規定如下：

1、取得當事人之同意

當企業係直接自當事人蒐集個人資料時，較容易取得當事人之同意。但符合該款豁免規定，應注意當事人同意之有效性，須當事人主動及明示表示同意，且當事人為同意之表示時，應經由資料管理者之個別詢問，且無須支付額外成本，亦不得受任何拘束。

依據 ICO 發布國際傳輸指引，資料輸出者於詢問當事人是否同意其個人資料進行國際傳輸時，應告知當事人傳輸之理由及資料接收國等相關資訊。另資料管理者若已知悉資料傳輸過程中可能發生之風險（例如當接收資料之國家並無任何資料保護法令），亦應告知當事人[65]。資料管理者取得當事人「無效」及「有效」同意之情形，舉例如下：

---

[63] Peter Carey, *supra* note 21, at 57-58.
[64] Richard Morgan and Ruth Boardman, *supra* note 27, at 161.
[65] *Id.* at 163-164.

(1) **無效之同意**

若資料管理者以下述文字詢問當事人是否同意個人資料傳輸至第三國家時，由於該詢問方式，並未說明具體之傳輸原因，亦未提供有關資料接收國之相關資訊予當事人知悉，故將被認定係屬無效之同意：

「若您能同意本公司因業務需要，而傳輸任何本公司所持有關於您之個人資料至任何國家，請於下面之欄位簽名。」（by signing below you accept that we can transfer any of the information we keep about you to any country when a business need arises）

(2) **有效之同意**

資料管理者下述文字詢問當事人是否同意傳輸個人資料至第三國家時，因已明確說明傳輸目的、傳輸資料之範圍、資料接收國有關資料保護法制等相關資訊，此時當事人若同意資料之傳輸，將被視為有效之同意：

「若您同意本公司將有關您不動產申請書中之相關明細資料提供予位於新加坡之 XYZ 公司(該公司係本公司選擇用以處理不動產客戶資料之公司），請於下面之欄位簽名。請注意新加坡目前尚未訂有資料保護法令」（by signing below you accept that we may pass details of your mortgage application to XYZ Limited in Singapore whom we have chosen to arrange mortgages on our behalf. You should be aware that Singapore dose not have any data protection law）。

2、履行當事人與資料管理者間之契約義務或履行契約約定前或為締約目的所為之必要傳輸：例如，英國信用卡之發卡機構（資料管理者）為履行其與持卡人（當事人）間信用

卡服務契約，將持卡人申請發卡之個人資料傳輸至第三國家，以利持卡人於當地進行刷卡消費之情形。上開情形下，當發卡機構將持卡人資料進行國際傳輸將不適用原則八之限制。本項例外情形，特別適用於須經常處理個人海外事務或提供個人海外服務之機構或企業(如旅行社及金融業等)[66]。

3、為履行資料管理者與當事人以外之第三人間（包括該第三人將與當事人簽訂契約等）之契約或為締約目的所為必要之傳輸。

4、涉及重大公眾利益，包括預防或偵查犯罪、涉及國家安全及課稅資料之蒐集等情形。

5、為執行法律訴訟程序、取得法律諮詢意見或為行使或維護當事人之法定權利所必要者。例如第三國家之母公司因集團內之員工涉訟（該員工隸屬於集團中設立於歐盟之子公司），故要求歐盟之子公司傳輸與該訴訟員工有關之個人資料至母公司，以進行必要之答辯程序。

6、維護當事人重大利益所需：所稱重大利益必須攸關當事人之生命及人身安全（life and death，如需進行緊急醫療）[67]。

7、已公開登錄之個人資料（public registers）：部分情況下，已對外公開之個人資料可自由傳輸至第三國家。例如登記處依規定，故將個人資料向社會大眾公開揭露，並提供特定或不特定人之查閱。

8、經 ICO 之授權：本項例外規定係授權 ICO 得於特殊情況下，在確保當事人之自由及權利已有適當保護後，得將個人資

[66] Richard Morgan and Ruth Boardman, *supra* note 27, at 164.
[67] Data Protection Act 1998—The eighth data protection principle and international data transfers, *supra* note 28, at 26.

料進行國際傳輸（如 ICO 授權企業得採用歐盟委員會發布之標準契約範本）。

9、經 ICO 之個案核准：ICO 於確保企業對於個人資料已有適當程度之保護後，以個案方案核准個人資料之國際傳輸（如企業向 ICO 申請採用共同約束條款之情形）。

第二項　國際傳輸之限制

依據附錄一原則八之國際傳輸限制及附錄四之豁免規定，英國企業依據資料保護法，得將個人資料國際傳輸之方式如下：

一、經歐盟委員會認可之第三國家或地區

（一）第三國家經認可符合歐盟資料保護之規範

1、適用依據：依據英國資料保護法附錄一第二部分第 15 條規定，經歐盟委員會認可對於資料保護符合歐盟規範之第三國家，英國將同樣認可該第三國家。截至 2011 年 9 月底止，歐盟委員會依據歐盟指令第 26 條(6)規定，核准之第三國家名單計有 9 個國家或地區[68]（一般稱為 white list，白名單）。

2、評估重點

歐盟委員會評估第三國家之資料保護法制是否符合歐盟規範，係指評估第三國家對於個人資料傳輸作業程序之相關法律規範（含落實情形），包括資料之性質（是否為敏感性資料）、傳輸目的、資料處理之作業時間、資料輸出國及最終資料接收國之法律規範、細則、專業實務指引或安全措施等規定[69]。

---

[68] 截至 2011 年 10 月止，經歐盟認可之國家包括阿根廷、加拿大、格恩西島（Guernsey）、曼島（Isle of Man）、瑞士、英國澤西島（Jersey）、法羅島（Faroe Islands）、安道爾共和國（Andorra）及以色列—available at http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx（lasted visited November, 2011）。

[69] Lingjie Kong, *supra* note 10, at 444-446.

評估第三國家之資料保護法制，歐盟委員會之資料保護工作小組（Data Protection Working Party）已訂有相關評估規範。相對於第三國家，將資料保護規範明訂於法律為歐洲各國之立法趨勢，以使當事人權利受到侵害時，能得到適當保護。惟如何適當評估第三國家之資料保護法制仍有下列困難[70]：

(1)第三國家甚少制定有效之資料保護法，故目前僅少數第三國家能通過歐盟委員會之評估程序；

(2)美國、加拿大及澳洲等屬於聯邦法律系統之國家，由於各州之間之資料保護法制仍存有差異，評估上更為困難；

(3)評估第三國家資料保護法制之適當性，常涉及各國政治及經濟環境等因素之敏感性。

歐盟委員會在考量上開實務困難後，目前採取較為彈性之實務作法，即進行評估時，考量第三國家個人資料保護規範之正面因素多於負面效果。

（二）歐盟與美國簽訂之安全港協定（Safe Harbor Framework）

為解決歐洲與美國企業因商業交易，須將個人資料相互進行傳輸，歐盟與美國在 2000 年簽訂安全港協定，美國企業經申請加入安全港協定者，應遵循歐盟指令之資料保護相關規定，包括通知（notice）、選擇（choice）、個人資料之再轉出（onward transfer）、安全性（security）、資料正確性（data integrity）、資料取得（assess）及執行（enforcement）等 7 項資料保護原則及補充之常見問答等相關規範[71]。

[70] *Id.* at 444-446.

[71] 美國與歐盟於 2000 年簽訂安全港協定，該協定於 2000 年 11 月生效後，在安全港協定下，部分美國企業得以在不修改美國現行隱私權保護法令之情況下與歐盟國家進行貿易。見陳妍沂，同註 33，頁 26。

在安全港協定下，歐洲企業得將個人資料傳輸至已加入安全港協定之美國企業，惟美國企業須每年申請更新，並定期由內外部稽核查核企業內部相關之資料保護程序是否可持續符合安全港協定之規定。美國之企業目前僅有受美國聯邦貿易委員會（Federal Trade Commission, FTC）或交通部（the Department of Transportation, DOT）所管轄之企業，得加入安全港協定，故如通信業、肉品包裝批發商、銀行、保險公司、信用卡機構或非營利組織，若非為 FTC 之被監理機構，可能並未納入安全港協定之適用範圍[72]。故若美國銀行位於歐盟地區之分子行，如有將個人資料傳輸至美國境內母行之需求時，則可能仍需透過標準契約範本或共同約束條款之方式，方得進行個人資料之國際傳輸。

（三）加拿大之部分企業

加拿大於 1984 年採行 OECD 之資料保護規定，並於 2000 年 4 月立法發布「個人資料及電子文件保護法」(PIPEDA)，經歐盟委員會之評估，已將適用 PIPEDA 之加拿大企業，視為其資料保護已符合歐盟規範，惟個人資料傳輸至加拿大之資料管理者時，仍應注意 PIPEDA 法律架構之複雜性，且 PIPEDA 亦僅適用於少數企業[73]。

二、其他例外情形

第三國家未經歐盟委員會認可前，英國企業仍得將個人資料傳輸至第三國家之情形：

（一）企業自行評估第三國家之資料保護法制(self-assessment)

依據原則八個人資料進行傳輸前，除歐洲經濟區之國家或地區外，資料輸出者應確認資料接收國對於個人資料之保護是否符

[72] Peter Carey, *supra* note 17, at 119-110.
[73] Richard Morgan and Ruth Boardman, *supra* note 27, at 159.

合適當標準。當個人資料之傳輸超過一個以上之歐盟會員國時，企業應考量各會員國對於資料保護適當性評估之要求可能各有不同[74]，歐盟委員會及英國 ICO 提供企業評估第三國家之資料保護法制之基本原則如下：

1、歐盟委員會資料保護工作小組提供之基本評估原則[75]

(1)目的性限制原則：資料處理應符合特定目的，除法律另有規定者外，資料之使用亦僅限於該特定目的。

(2)資料品質及符合比例原則：應維持個人資料之正確性，必要時應持續更新。資料之傳輸或處理均不得逾越原始個人資料蒐集之目的。

(3)資訊透明度：除法律另有規定外（如歐盟指令第 11 條(2)規定之所訂情形[76]），資料輸出者應將資料傳輸之目的、第三國家之資料接收者及其他攸關之資訊，提供給當事人知悉。

(4)安全性原則：資料管理者應具備適當技術及安全機制，以降低資料於處理及傳輸過程中之風險。

(5)當事人對個人資料應有取得、更正及拒絕之權利：當事人應有取得其個人資料被處理等相關資訊之權利，若資料產生錯誤或有不正確之情形發生時，當事人將有權要求資料進行更正，除資料之處理涉及國家安全、國防或公共安全外，在特定情況下，當事人亦有拒絕個人資料被處理之權利。

[74] Data Protection Act 1998—The eighth data protection principle and international data transfers, *supra* note 28, at 14.

[75] Peter Carey, *supra* note 21, at 62-63.

[76] 依據歐盟指令第 11 條(2)規定，因統計、歷史或學術研究之目的，致使向當事人告知其資料蒐集相關資訊為不可行、須耗費不合理之成本或資料登錄及揭露為法律所明文規定者，則無須向資料當事人告知相關資訊，惟有以上情形時，會員國仍應訂有適當之安全維護措施。

(6)限制資料之再傳輸：個人資料之原始接收者（the recipient of the original data transfer）於取得資料後，若欲再傳輸至其他第三國家，第二資料接收國（second recipient）亦須符合資料保護之相關規範。

2、英國資料保護法提供之評估原則（附錄一第二部分第 13 條至第 15 條規定）

(1)資料管理者應逐案評估下列事項（一般性標準）

A.資料之性質：資料之國際傳輸可能損害當事人之權益，而損害之程度，受到個人資料性質之影響。例如，跨國企業將公司內部員工分機之電話表傳輸至海外子公司，該等傳輸一般不被視為有高度風險，因該類資料，若被未經授權之人取得，對當事人不致造成重大損害。相對地，若資料輸出者傳輸之資料為敏感性資料時(如當事人之健康檢查資訊)，因該等性質資料之遺失將對當事人隱私權益造成重大損害，故針對敏感性資料之國際傳輸保護規範，應較一般性質之個人資料為嚴格[77]。

B.資料原始來源國：當原始個人資料係來自對於資料保護程度較為不足之國家時，若資料係輸出至與其資料保護規範相當之國家時，應不致有相關限制。因當事人對於原始資料係取得自第三國家或取得自歐洲濟經區內之國家，對其個人資料之保護程度將有不同預期，故若資料原始係自第三國家取得時，自不適用英國資料保護法之規定[78]。

C.資料傳輸之目的地國家：當資料傳輸之目的地，並非初始接收資料傳輸之國家時，縱使最初資料接收國已有適當之

[77] Data Protection Act 1998—The eighth data protection principle and international data transfers, *supra* note 28, at 10-11.
[78] *Id.* at 11.

資料保護法制，資料輸出者仍應評估資料再傳輸至另一缺乏資料保護法律規範之第三國家之可能性[79]。

D.資料傳輸目的及期間：資料管理者應考量資料傳輸之目的及資料所需之處理時間，因時間愈長，個人資料暴露於風險之情形將提高[80]。

H.資料接收者對個人資料保護是否已採取適當安全措施（security measures）：輸出資料之管理者應能確保個人資料之安全性，不受到外部事件之干擾，如採行適當之資料加密技術或訂定適當之資料處理作業程序[81] (如資料接收者是否已取得 British Standard BS 7799 之國際認證[82])。

(2)評估資料接收國之資料保護法制

A.資料接收國是否已有資料保護法制

(A)收受資料之國家於國內法是否訂有資料保護法律及相關法令。

(B)資料接收國是否與歐盟委員會或其他國際組織簽訂相關之國際協定（義務）。

(C)資料接收國是否訂定適用於特定產業或區域之資料保護行為準則或有其他法令規定，並能有效落實。

B.評估資料接收國之法律制度時，資料輸出者尚應考量下列問題[83]：

(A)第三國家是否已採行 OECD 之隱私權保護及跨國傳

[79] *Id.* at 12.
[80] *Id.* at 11.
[81] *Id.* at 11.
[82] BS 7799（Code of Practice for Information Security）為英國標準協會（The British Standard Institution, BSI）針對資訊安全所制訂之國際標準，取得該國際認證之機構代表機構之資訊安全已符合國際標準。
[83] Data Protection Act 1998—The eighth data protection principle and international data transfers, *supra* note 28, at 13-14.

輸個人資料之指引及該國採行之措施為何？

(B)第三國家是否認可歐盟委員會發布之個人資料保護規範及是否已採行適當措施，遵循相關規範？

(C)第三國家之國內法若已訂有資料保護法令，該法令是否符合歐盟資料保護工作小組於 1998 年 7 月 24 日發布之工作文件[84]？

(D)第三國家是否有任何法律架構保護當事人之權利及個人資訊流通之自由？

(E)第三國家是否認可歐盟委員會發布之授權命令，特別是標準契約範本及 BCR？

(3)附錄四所列有關國際傳輸之豁免規定，除法令另有規定外，不適用原則八有關國際傳輸之限制。（第 14 條）

（二）資料管理者傳輸個人資料給資料處理者

當企業將個人資料傳輸至第三國家之資料處理者，若該資料處理者已符合資料保護原則七之規定，則該項資料傳輸原則上並不適用原則八之限制。例如，英國銀行以印度作為全球客戶服務中心之所在地，並將客戶帳戶明細等個人資料傳輸予一家位於印度之資料處理公司，若該英國銀行（即資料管理者）已依據資料保護法之規定，透過契約條款之制訂，要求資料處理者應遵循資料保護原則七之相關規定，將無須適用原則八之國際傳輸限制。

[84] European Commission—Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document—Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive（WP 12）（1998）, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

（三）使用歐盟委員會核准之標準契約範本（Model or Standard Contractual Clauses）

為確保接收資料之一方對個人資料保護符合一定標準，企業得與對方簽訂契約，透過契約條款約束第三國家之資料接收者應履行有關資料保護之契約義務。契約模式之採用，企業得選擇經歐盟委員會核准之標準契約範本或自行擬訂約束對方之契約條款內容，企業透過契約方式，將個人資料國際傳輸，將視為符合資料保護法附錄四之第 8 段或第 9 段之豁免規定。

（四）企業經 ICO 核准採用 BCR

除上開所列方式外，英國企業亦得選擇採用 BCR，惟該方式僅適用於跨國企業於集團內之國際傳輸(即跨國企業將資料傳輸至第三國家集團內之另一公司）。原則上，BCR 係訂於跨國集團之內部規章、協議或公司治理之相關內部規範。企業採行 BCR 後，個人資料雖得於集團內部自由傳輸，惟採用該方式須事先經各國資料保護監理機關之核准，並視為符合附錄四第 9 段之豁免規定。標準契約範本及 BCR 之詳細規範內容，將於第四章說明。

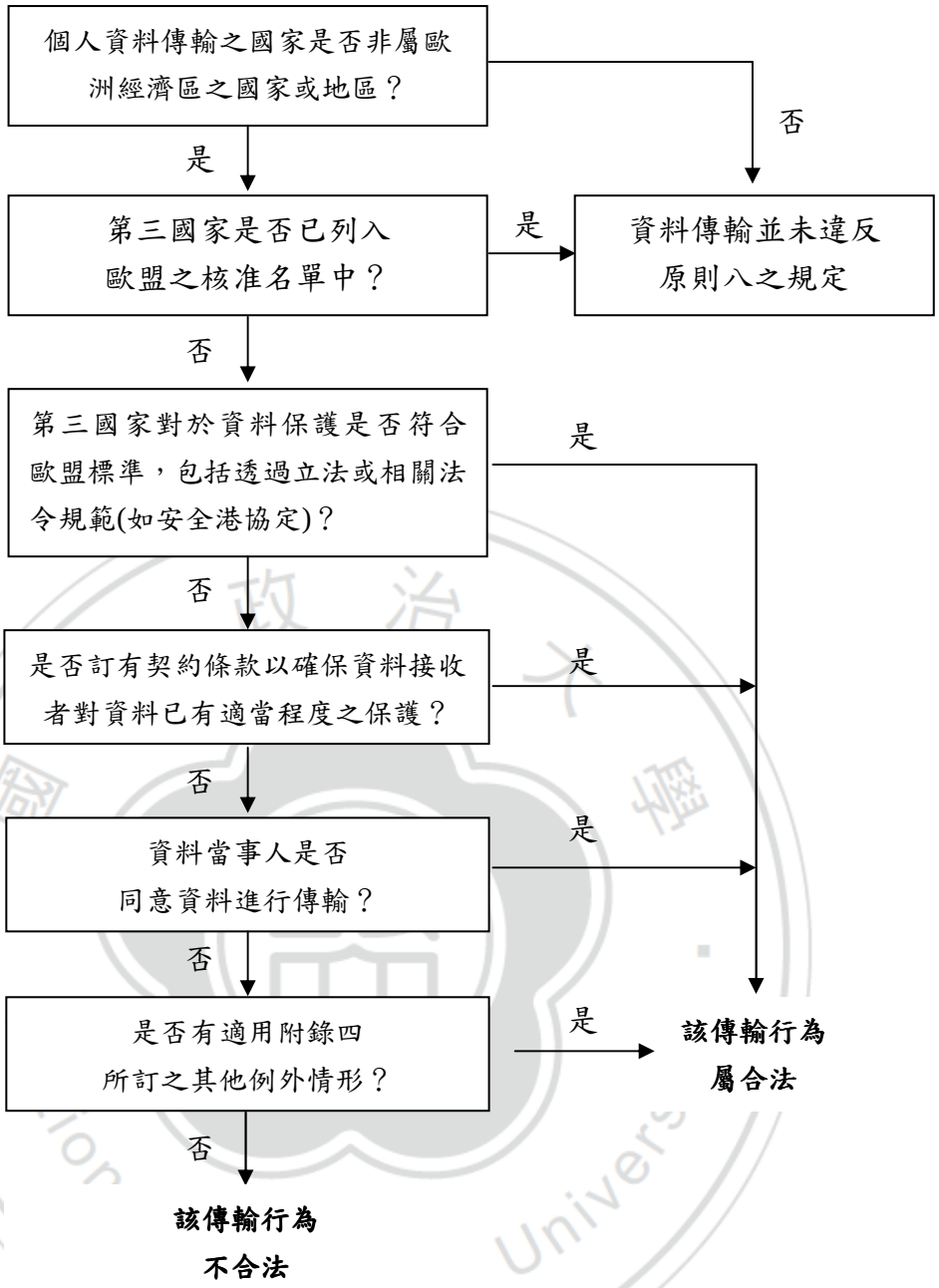
第三項　英國國際傳輸個人資料之架構

1984 年英國資料保護法有關非公務機關國際傳輸之控管，係採原則同意例外禁止之立法形式，透過事先登錄制度，規範資料使用者於國際傳輸前，應先向資料保護登記處登錄，登錄後（事後）若發現企業資料傳輸有違反資料保護原則之虞，則授權資料保護登記處發出禁止傳輸之通知。1998 年資料保護法修法後，依該法第 16 條至第 26 條規定，資料管理者雖仍須將其相關資料（包括資料管理者若有將有個人資料直接或間接傳輸至第三國家之需求時，該資料接收者之名稱等）向 ICO 登錄，始能進行個人資料之處理，惟修法後國際傳輸已改採原則禁止例外同意

之立法形式，從資料保護法訂定之例外情形觀之，英國對於國際傳輸似採取較為開放之立場，提供企業更多之選擇進行資料傳輸（包含自行評估、採用標準契約範本及 BCR 等），惟透過加重企業身為資料管理者之資料保護責任，強化對當事人權益之保護。

依據 ICO 發布之國際傳輸指引，個人資料傳輸至第三國家時，企業應先確認是否將傳輸資料至第三國家，再評估第三國家及其傳輸環境是否符合資料保護之標準，若第三國家對於資料保護尚未有適當法律環境，而企業仍擬將個人資料傳輸，接下來應考量資料接收者能否提供適當之安全措施，以確保個人資料接收後能對資料提供適當保護，若未符合上開規定，企業應再檢視傳輸是否有附錄四之其他例外情形。若企業在未符合上開情況下，仍將資料進行傳輸則將違反原則八之規定（違法傳輸行為）。英國個人資料國際傳輸之流程如下[85]：

[85] Peter Carey, *supra* note 21, at 69.



第三節　英國落實歐盟指令研究報告

歐盟委員會司法部門（European Commission—Justice）為瞭解各會員國落實歐盟指令之情形，並評估現行個人資料保護規範是否足以因應目前社會環境、資訊技術（如網路發展）、資訊全球化、個人資料蒐集及隨處存在之情形漸增、電腦及資料處理設備之功能及容量倍增、個人資料使用目的增加（尤其是涉及國家安全、防止犯罪及恐怖威脅等）等資訊社會之發展，故近年來針對各國不同法律體系（國家）之資料保護規範進行研究，以評估現行歐盟

指令對於個人資料是否仍能提供適當程度之保護或須進行修正。

該份報告研究之對象，包括歐盟委員會之會員國，如捷克、丹麥、法國、德國、希臘及英國等國家，以及歐盟會員國以外之國家，包括美國、澳洲、香港、印度及日本等[86]。該份報告中對於英國有關國際傳輸相關法律規範之評估結果如下（歐盟研究報告中，其研究團隊認為上開各國以德國聯邦資料保護法最為完善，且具有非常穩固之憲法基礎[87]）：

第一項　整體評估結果

英國因商業交易需要（更甚於提高對於基本人權之保護），經過十多年之協商及有關政府機關之研究，於 1984 年實施第一部之資料保護法（訂定當時，英國國內之法律體系對於個人資料之保護，尚未提供較上位之法律保障），並於 1998 年配合歐盟指令修正為現行之資料保護法後，英國於 2000 年 10 月再依據歐洲人權公約（Human Rights Convention）實施英國人權法（Human Rights Act 1998），將個人隱私生活之權利納入個人資料保護之基礎，賦予個人資料保護類似憲法上之地位。

但研究報告認為英國資料保護法仍有許多方面未完全遵循歐盟指令之要求，歐盟委員會經調查後認為歐盟指令之 34 條條文中，英國計有 7 條實際上並未完全落實（雖英國政府聲明該國已完全實施歐盟指令之規定），研究報告指出，雖然英國 ICO 已針對個人資料保護發布許多

---

86 European Commission—Justice, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments—Final Report Executive Summary（2010）, available at http:// ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

87 德國為世界上第一個制訂資料保護法制之國家（1970 年 10 月），並於 1977 年正式實施德國聯邦個人資料保護法，自 1983 年德國聯邦憲法法院作出「人口普查法案」之判決及提出「資訊自決權」（right to informational self-determination，係指當事人對於其個人資料之揭露及使用應有自主決定之權利）概念後，「資訊自決權」已成為德國資料保護法之憲法基礎。之後德國為因應歐盟指令亦於 2001 年修正其聯邦資料保護法，並於同年 5 月 23 日生效，聯邦資料保護法雖於 2009 年進行修正，惟德國對於個人資料之保護，仍以 2001 年聯邦資料保護法為主要規範。德國依據歐盟指令第 25 條及第 26 條之規定，於德國聯邦資料保護法第 4b 條及第 4c 條訂有個人資料傳輸至外國之相關規定，除明定資料傳輸至歐洲經濟區內及經濟區外之國家外，並訂有資料傳輸內容僅限於歐洲共同體法律所規範之業務範圍。See Douwe Korff, Comparative Studies on different approaches to new privacy challenges, in particular in the light of technological developments—country studies A.4—Germany, 2-3, 56-60（2010）.

實務指引及積極宣導，並於公私部門需要時，提供資料保護之看法或意見，惟相對於其他歐盟會員國，英國整體之資料保護法制仍有下列待改善之處[88]：

（一）英國對於個人資料之保護，較欠缺憲法上基礎。

（二）英國法院對個人資訊及隱私不願提供較為完善之保護（尤其是 Durant 一案之判決結果），資料保護法在英國法院判決之解釋下，未適當落實歐盟指令，例如對個人資料及個人資料檔案系統之定義採取較為寬鬆之解釋等。

（三）英國 ICO 受英國政府嚴格控管，已影響其獨立性。

（四）為達紛爭解決之目的（negotiated resolutions），英國資料保護法之訂定，採取相對柔軟，而非嚴格之立法政策。

（五）英國資料保護法在上開立法政策下，造成當事人個人資料遭受損害時，較難主張其權利，ICO 為達爭議解決之目的，可能僅提供有限之資源給當事人，故當事人若為取得補償僅能提起訴訟（惟訴訟成本昂貴，且耗費時間）。

第二項　英國國際傳輸規範之優缺點

該份研究報告認為英國國際傳輸規範之優點及待改善之處如下：[89]

一、優點

（一）為遵循歐盟指令第 25 條之規定，英國資料保護法於附錄一原則八已明定國際傳輸之限制，ICO 針對國際傳輸已發布相關指引，足以處理企業於國際傳輸可能面臨之相關議題。

（二）ICO 已於網站上發布經歐盟委員會認可之第三國家名單，並連結至歐盟網站，以隨時更新資訊。

---

[88] Douwe Korff, Comparative Studies on different approaches to new privacy challenges, in particular in the light of technological developments—country studies A.6—United Kingdom, 1-2, 72-73（2010）.

[89] *Id.* at 67-72.

（三）如何評估第三國家之資料保護法制是否符合歐盟規範，英國資料保護法已於附錄一之第二部分明定應考量之因素，提供給資料管理者自行評估（惟 ICO 並不自行評估）。

（四）第三國家無論係經歐盟委員會之認可或由資料管理者自行評估後認為第三國家已符合歐盟規範，企業將個人資料由英國傳輸至該第三國家均視為已符合原則八之規定，提供給企業較多自行判斷之空間。

（五）標準契約範本及 BCR 之使用，英國與歐盟指令係為一致性之規定，均授權企業得依歐盟指令辦理。

二、待改善之處

（一）依據歐盟指令第 1 條(2)規定，原則上，歐洲經濟區內之個人資料得於會員國間自由傳輸[90]。惟英國對於歐盟指令所訂個人資料之流通自由，並未明定於資料保護法之本文，僅於該法附錄中訂定國際傳輸之限制條件。

（二）依據英國原則八之規定，個人資料得自由自英國境內傳輸至歐洲經濟區內之任何國家，惟該法中並未明定傳輸是否僅限於歐洲共同體法律（Community Law）規範之業務範圍及傳輸與其他事項間之關係，未明定適用業務範圍之結果可能產生當資料傳輸至其他歐洲經濟區之國家，惟該國對於該等性質之資料並未納入國際傳輸資料保護之規範時，當事人若遭受損害，將無法對該國之資料接收者請求損害賠償。

[90] 依據歐盟指令第 1 條(2)規定，會員間不得以當事人基本人權與自由等保護規定為理由，限制或禁止會員國間個人資料之自由流通。

（三）ICO 發布之國際傳輸指引中，部分舉例之內容，可能違反歐盟指令之規定，如企業經評估國際傳輸係屬低風險，則無須評估第三國家之資料保護法制。

第四節　銀行保密義務及相關金融法令

第一項　英國銀行之保密義務

英國銀行之保密義務，始於 1924 年英國上訴法院對於 Tournier v. National Provincial and Union Bank of England 一案之判決[91]，該判決中確認銀行對客戶資料之保密義務，始於銀行與客戶間之契約，存在於銀行與客戶關係之間，並於銀行與客戶關係終止後持續存在[92]。

當時英國上訴法院認為銀行對客戶因默示責任，負有保密義務，故當銀行違反保密義務時，自應對客戶負損害賠償責任。英國法院進一步指出，銀行資料保密之範圍，不限於客戶帳戶本身，還包括銀行因與客戶間之關係，所獲取之任何資訊，且該保密義務並不因客戶將該帳戶結清或停止使用該帳戶而終止[93]。惟依上開判決內容，在某些例外情況下，銀行將客戶個人資料提供予第三者將視為合法之情形如下[94]：

一、依據法律規定（如法院之強制命令）。

二、涉及公共利益：銀行有義務向公眾揭露該等資訊，若不揭露或提供客戶交易資訊可能有害於公眾權益（如於戰爭時

[91] 在 Tournier v. National Provincial and Union Bank of England 一案中，銀行將其客戶跳票之資訊提供予該客戶所服務公司（亦為銀行之客戶），該信用不良記錄導致該客戶所服務之公司於雙方之雇用契約到期時，未再續聘該員工。請參考 Fayyad Alqudah, Banks' duty of confidentiality in the wake of computerized banking, Journal of International Banking Law, 2（1995）.

[92] 該判決同時指出，銀行對於客戶資料保密義務之擴張性及存續性等二項特性，前者不以客戶帳戶為限，範圍擴張自從客戶所得知之任何訊息，後者則指不因客戶終止使用帳戶，而免除銀行之義務。見李福隆，金融隱私權與銀行監理之間--從全球金融海嘯看我國金融危機事件下銀行保密原則之修正，2010 年世界人權高峰會收錄文章。

[93] 林育廷，金融隱私權保障與財富管理發展之衝突與協調—兼評美國與台灣之規範政策，科技法學評論第 4 卷第 2 期，頁 156，2007 年 8 月。

[94] Roger K. Baker, *supra* note 48, at 4.

期或因利益衝突、客戶涉嫌與敵方進行交易、發現舞弊或洗錢案件等）。

三、銀行於特定情況下，因自身利益提供客戶資訊，惟銀行若未經客戶事前同意（opt-in agreement），仍不得因行銷目的將客戶資料提供予集團內之公司。

四、經客戶明示或暗示之同意。

英國銀行與客戶間因契約產生之保密責任，不限於銀行是以人工紙本或電腦處理之個人資料，或於英國境內或境外處理客戶之個人資料。在英國資料保護法下，銀行身為資料管理者（data controller）對於所持有個人資料之相關處理程序（包括境外處理客戶資料），自應負最終責任[95]。

第二項　相關規定

所謂「銀行秘密」係指金融業之職業秘密及業務秘密，銀行與客戶間之來往，係以財產關係為中心，客戶對銀行之信賴為銀行經營之基石，從而銀行對於因與客戶往來所知悉之財務及非財務資料，自應負保密義務。惟該等義務在某些特殊情況下，因法益衡平之考量（如權衡客戶隱私與該等資訊公開之公眾利益），而以立法例外要求銀行或監理機關應對外揭露銀行某些客戶之個人財務資料。

英國於「金融服務與市場法」制訂前，對於「保密義務」主要規範於 1979 年銀行法第 19 條及第 20 條有關英格蘭銀行(當時之金融監理機關)因監理需要自銀行取得各種資料之保密義務與 1984 年銀行法第五章有關資料揭露限制（Restriction on disclosure of information, 第 82 條至第 87 條）之相關規定。2000 年金融服務與市場法發布後，有關「保密義務」係訂於該法第 23 部分「資料公開、資訊揭露及合作」（Part XXIII, Public Record, Disclosure of Information and Co-operation）

[95] Roger K. Baker, *supra* note 48, at 4-5.

第 348 條至第 353 條中，惟上開規定主要規範銀行如何在守密之餘，因應金融監理機關及其他因職務而需知悉銀行客戶資料之人之需求[96]，故將銀行與客戶往來間之資料提供予政府機關（即政府機關因職務需要取得銀行客戶資料之保密義務[97]）。

在金融服務與市場法及資料保護法之規範架構下，英國銀行對於客戶資料之保密義務，係屬契約責任，故未明定於相關法令中，銀行除依金融服務與市場法規定，將客戶資料提供予政府機關外，對於個人資料之保護仍應適用資料保護法之規定。考量本研究主要探討銀行國際傳輸客戶個人資料之相關規範，故有關英國銀行在資料保護法下，因身為資料管理者應遵循之個人資料保護規定如下：

一、 資料管理者（Data Controller）

資料管理者係指決定個人資料蒐集目的（資料蒐集應符合特定目的）及資料處理方式之人，其於開始個人資料之蒐集及處理前，應將個人資料之性質、處理之目的、是否有將個人資料直接或間接傳輸至第三國家之需求等相關資料，向 ICO 登記（第 1 條(1)及第 16 條至第 19 條）。

二、 資料管理者蒐集、處理及利用個人資料，應遵循之資料保護原則（第 4 條及附錄一）

（一）除第 27 條之豁免規定外，資料管理者對於個人資料之蒐集、處理及利用，應遵循以下之資料保護原則：

---

[96] 包括英國 FSA、為執行法定職權之其他政府機關、國務大臣、自上開人員知悉資料之人、FSA 因監理需要將相關資訊提供予專業人士之人等。見 Financial Services and Market Act 2000，Section 348.

[97] 在德、奧通說上認為，銀行保密義務係基於銀行與客戶間之業務關係所生之信賴責任，此項責任係基於無主要給付義務之法定債之關係所生之責任。因此，銀行之保密義務，應依誠實信用原則，在締結契約之磋商接觸期間即已存在，如有違反應負締約上過失責任，如已締結契約，則成為契約關係之附隨義務，此項義務毋待明文約定，即使銀行與客戶間之業務關係已結束，銀行之保密義務仍應繼續存在，即為一般所謂事後之契約義務。見蕭長瑞，銀行法令實務(一)，增修訂 6 版，財團法人台灣金融研訓院，頁 161，1998 年 4 月。

1、原則一：個人資料應經公平及合法之處理，一般及敏感性個人資料，除符合附錄二及附錄三訂定之個人資料處理目的之條件之一者外，不得任意處理。

2、原則二：個人資料之取得應符合特定及法律認可之目的，且不得為特定目的外之使用。

3、原則三：個人資料之處理，應適當、相當，且不得逾越原始資料蒐集之目的或額外增加之目的。

4、原則四：應保持個人資料之正確性，於必要時，持續更新。

5、原則五：個人資料之持有時間，不得長於原資料蒐集目的或額外增加目的之所需時間。

6、原則六：個人資料之處理不得違反資料保護法有關當事人權利之規定。

7、原則七：資料管理者應採行適當之技術及管理制度，以避免個人資料未經授權被不當或不法處理，或因過失致個人資料遭受損失、破壞或傷害。

8、原則八：個人資料除該處理個人資料之國家或地區，對於資料當事人之個人自由與權利已有適當程度之保護外，禁止傳輸至「歐洲經濟區」以外之國家或地區。

（二）豁免規定：因國家安全、犯罪調查及稅務、個人健康、教育及社會工作、執行法定職權、新聞、學術及人文研究等目的所為個人資料之揭露規定，應優先適用於任何法律、法律授權之法令或預先授權所定有關資料揭露之禁止或限制規定。（第 27 條）

第三項　境外委外規定

英國 FSA 對於銀行將客戶個人資料進行國際傳輸，雖未有訂有特殊規範，惟在銀行將內部作業委外時，FSA 除訂有一般委外原則之要求

外，銀行若擬將內部作業境外委外至第三國家時，FSA 於「進階管理安排、系統及控制」（Senior Management Arrangements, Systems and Controls, SYSC）審慎監理手冊（FSA Handbook）之第 8 章「委外」明定相關限制規定。

一、一般委外要求（Outsourcing）

銀行將具重要性之作業或服務委外時，不因作業委外而影響銀行本身應負之責任，且應遵循下列條件[98]：

（一）委外服務供應者應具備專業能力及可信賴性，並經相關法律核准得執行所提供之委外功能、服務或作業。

（二）委外服務供應者應有效完成委外服務作業，銀行應建立適當程序，評估服務供應者提供之服務是否符合委外要求。

（三）服務供應者應自行檢視是否已確實執行受託之業務，並適當管理相關風險。

（四）當銀行發現服務供應者未能有效執行委外作業或遵循相關法令要求時，應採取適當措施，以為因應。

（五）銀行應保有必要之專業，以有效管理委外風險。

（六）委外服務供應者應向銀行揭露任何對委外作業能力或法令遵循有重要影響之發展。

（七）必要時，銀行應在不損及客戶權益之情況下，終止委外安排。

（八）委外服務供應者對於提供之委外作業應與 FSA 及其他相關之監理機關密切合作。

（九）必要時，銀行及其稽核人員、FSA 或其他相關監理機關應能取得與委外作業相關之資料。

[98] FSA Handbook—Senior Management Arrangements, Chapter 8 Outsourcing, 8.1.8, available at http://www.fsa.gov.uk/pages/handbook （last visited November, 2011）。

（十）委外服務供應者應保護攸關銀行及銀行客戶之任何機密資訊。

（十一）銀行及委外服務供應者因應委外之功能、服務或作業，應建置、落實及維持災難回復之緊急應變計畫，並定期測試委外相關之備援設備。

二、申請境外委外之規範

依據 FSA 審慎監理手冊第 8.2 章規定,銀行將客戶個人資料因境外委外傳輸至第三國家時，應額外遵循之規定如下[99]：

（一）銀行將內部作業境外委外至第三國家之服務供應者時，應符合下列規定：

1、委外服務供應者於母國經核准登記設立，並經適當監理。

2、FSA 與第三國家之監理機關已簽訂相關之合作協議。

（二）為遵循歐盟金融市場指令（MiFID），銀行於辦理境外委外時，應事先向 FSA 申報，FSA 在一定期間內未表示意見時，銀行始得辦理境外委外作業。

（三）所稱「一定期間」係指 FSA 收到銀行之申請文件後一個月內，惟 FSA 得視實際需要，延長審查期限（如須進一步之資訊，以決定該境外委外之妥適性等）。

（四）若銀行在一個月內未收到 FSA 之反對意見或要求其補件，則銀行得開始辦理該項委外作業。

（五）銀行僅在對該服務供應者已提供適當監督，並符合第 8.3 章規定之情況下，始得向 FSA 申請該項境外委外作業。依第 8.3 章規定，銀行向 FSA 申請境外委外前，應自行評估是否符合相關規定。

（六）銀行向 FSA 申請境外委外時，應檢附文件如下：

[99] *Id.* at 8.2.1- 8.2.9.

1、說明委外服務供應者是否有不符合委外相關標準之情形。

2、委外服務供應者若經當地監理機關核准，並應符合相關法令規定時，應提供相關資訊包括該委外服務供應者當地監理機關之聯絡方式等。

3、銀行承諾在繼續經營之基礎下，對於境外委外產生之損失，應負損害賠償責任。

4、銀行將內部作業委外給服務供應者之理由。

5、銀行與委外服務供應者，預擬之委外服務契約內容。

6、內部作業正式委外之日期。

7、銀行自行檢視是否符合第 8.3 章規定之自行評估結果，若不符合，並應說明原因為何。

（七）額外要求：當 FSA 對於銀行申請之境外委外作業未表示反對意見時，銀行應依據 FSA 發布監理規範（SUP 15）之規定，若發現有任何事項將影響銀行提供客戶服務之能力、有嚴重損害客戶權益或相關資訊已有重大變動時，應立即通知 FSA。

三、境外委外之作業指引

依據 FSA 審慎監理手冊第 8.3 章規定，銀行將客戶個人資料境外委外傳輸至第三國家時，應依下列事項辦理[100]：

（一）銀行無論係直接或間接透過第三人辦理委外作業，均適用本指引中有關直接委外之規定。

（二）當銀行已依本指引規定，經評估後認為委外服務供應商能持續符合委外作業規定，並能對消費者提供適當保護措施時，FSA 原則上對於銀行境外委外，並不會表達反對意見。

[100] *Id.* at 8.3.1-8.3.7.

（三）若委外契約允許委外服務供應商進行複委外時，該複委外之行為並不影響原服務供應者應負之責任。

（四）委外契約應明定當委外服務供應者所有權或控制權有改變，或受破產宣告、進行清算或被接管、或有持續重大違反契約條款之情形時，銀行應有終止委外契約之權利。

（五）當委外服務供應商未經母國監理機關之核准或登記，或未經適當監理時（如當地國對於服務供應商並無特殊之監理規範）：

1、銀行應有權對於服務供應商就受託服務範圍內進行檢查。

2、銀行應向FSA說明委外服務供應商有能力及有足夠之資源提供服務，以履行委外契約。

3、服務供應者應揭露任何重大影響其提供委外服務能力之事項，包括母國發布對於服務供應者提供委外服務有負面影響之法律或命令，或服務供應商已辨識出之其他潛在風險。

4、銀行應確保委外服務供應商之財務狀況良好。

5、銀行應要求服務供應者提供其依據當地法令規定編製之年度財務報告等相關資料，並說明其財務報告之編製是否符合或相當於國際會計準則及是否經會計師查核簽證。

6、若服務供應者預期或已知悉會計師將對其當期財務報告出具保留意見或修正式無保留意見時，委外服務供應商應立即通知銀行。

7、銀行應訂定適當程序以確保服委外服務供應者對於因受託服務取得之機密資訊已有適當保護。

8、服務供應者應保護攸關銀行與客戶權益之任何機密資訊，當供應者有違反保密義務情形時，應立即通知銀行。

9、委外契約應於契約明定適用歐盟會員國之管轄法律。

（六）委外服務供應商之監理機關未與 FSA 簽訂合作協議時，委外服務契約應能確保下列事項：

1、委外契約應確保銀行能提供任何與委外作業相關之資訊予 FSA，使 FSA 能進行有效監理。銀行應評估服務供應商遵循當地法律規範之情形及是否有任何限制銀行取得委外作業相關資訊之法令，如有任何法令限制，銀行應立即通知 FSA。

2、委外契約應要求服務供應商提供其設立於英國之分支機構之相關資訊。FSA 在契約條款下，於必要時，應得要求服務供應者直接提供相關委外作業資訊。

第五節　小結

第一項　銀行傳輸個人資料之型態

相對於歐盟指令及德國聯邦個人資料保護法之立法目的係為保護個人之資訊隱私權，英國資料保護法之訂定，係因應商業交易之需求，故英國之資料保護規範較著重於資料管理者應有適當之程序，以管理個人資料，並合法使用。

在上開立法政策及英國法院對於 Durant v. FSA 案之判決結果下，使得英國資料保護法之落實及英國法院對於資料保護法律適用之限縮解釋，受到歐盟委員會之關切（歐盟研究報告之結論認為英國並未完全落實歐盟指令），另部分學者亦批評英國將商業交易需要置於個人隱私不受侵犯之權利之前，對於個人資訊隱私權之保護仍有不足。

金融服務業相對於其他產業，因提供金融交易服務之需要，更易取得消費者之個人資料，其對於個人資料之保護除應遵循資料保護法外，並應同時依據 FSA 發布之相關規定辦理。銀行除為履行與客戶間之金

融交易服務或依法律規定者外，因內部作業需要，故須將客戶個人資料傳輸至境外之情形如下：

一、集團內之傳輸

（一）相同法律主體：總行與分行間之客戶資料傳輸，包括外國銀行之英國分行將英國當地之客戶資料傳輸至國外總行，或英國銀行要求設立於全球各地之分行，將分行當地之客戶資料傳輸至英國總行。

（二）不同法律主體

1、母子公司間：總行與子行間之客戶資料傳輸，包括外國銀行之英國子行將英國當地之客戶資料傳輸至國外總行，或英國銀行要求設立於全球各地之子行，將子行當地之客戶資料傳輸至英國總行。

2、關係企業間：銀行將客戶資料統一傳輸至集團內專責客戶資料處理作業之關係企業。

二、客戶個人資料傳輸至委外服務供應者

（一）銀行將客戶之個人資料傳輸至歐洲經濟區內之委外供應商，尚無須適用英國資料保護原則八之規定，惟仍應遵循FSA 發布之一般委外作業規定。

（二）銀行將客戶之個人資料傳輸至第三國家之委外供應者時，該項傳輸行為應同時遵循資料保護法及 FSA 發布之委外作業規定。

三、綜上，英國銀行將客戶之個人資料國際傳輸（含資料之輸出與接收），可能適用之規範如下：

資料輸出者	資料接收者	適用英國資料保護法原則八相關規範	適用 FSA 發布之相關規範	
			一般委外要求	傳輸至第三國家之境外委外要求
外國銀行於英國之分子行[101]	歐洲經濟區內之總行/委外服務應供商	X	○	X
	第三國家之總行/委外服務供應商	○	○	○
英國銀行設於各國之分子行	英國總行	X	X	X
	英國之委外服務供應商	X	X	X

資料來源：本研究整理

第二項　遵循原則八之實務困難

依據英國資料保護法之規定，企業雖得自行評估接收資料國家對於資料保護法制之適當性，惟除企業定期傳輸大量個人資料至特定之第三國家外，大部分企業並沒有意願、資源甚或該等專業得以對第三國家之資料保護法制進行評估，且自行評估對企業而言，相當花費時間，且耗費成本。當企業依據自行評估結果將個人資料國際傳輸至第三國家，亦無法確保英國 ICO 是否同意企業自行評估之結果或看法[102]。

原則八雖為英國資料保護法所列原則之一，但企業通常認為遵循該項原則有其實務困難[103、104]：

一、 如何認定第三國家之資料保護法制符合歐盟規範

（一）縱使經歐盟委員會認定之國家，個人資料進行國際傳輸前，仍須經資料管理者之確認，且須評估資料接收者是否需對個人資料提供額外之保護措施，並應考量特定產業是否有特殊之要求（如金融服務產業）。

[101] 英國銀行（總行）將客戶資料傳輸至歐盟經濟區內及第三國家時所適用之規範，亦同。
[102] Richard Morgan and Ruth Boardman, *supra* note 27, at 160-161.
[103] *Id.* at 170.
[104] Roger K. Baker, *supra* note 48, at 9.

（二）ICO 所發布之國際傳輸指引，雖可適用於一般情況，但並非適用於所有殊特情況。

（三）特定情況下，有關資料保護規範之妥適性難以認定，例如國際性企業或集團於內部訂定之政策、作業規章或採用 BCR，是否具有法律上之拘束力。

二、企業自行評估之成本效益：對許多資料管理者而言（特別是規模較小之公司），評估第三國家是否訂定適當之資料保護規範，可能不符合比例原則、困難、耗費時間及成本。

三、歐盟各會員國對於國際傳輸認可程序之不一致：許多歐盟國家之資料保護監理機關對於資料輸出至第三國家採事先核准制，如法國、奧地利等，惟亦有採事後備查者。但英國資料保護法未如其他會員國訂有事先核准或事後備查機制。

四、個人資料經當事人同意傳輸及傳輸之必要性：英國資料保護法附錄一所稱「同意」，並未明定係指當事人明示、暗示、或經書面之同意（除敏感性資料外），另資料傳輸之必要性為何，該法中亦未有明確定義。

第三項　監理重點

為尋求第三國家較低之資料處理作業成本，金融產業因將客戶資料境外委外處理，所衍生資料傳輸等相關議題逐漸普遍，且有增加之趨勢。英國 Lloyds TSB 集團工會曾對 Lloyds TSB 提起訴訟，主張該銀行將內部作業委外至印度之決定，將違反歐盟指令，因印度對於個人資料之保護程度，未能達到英國所要求之標準，將使消費者之資訊隱私權受到侵害[105]。

[105] Justin Kent Holcombe, Solutions for Regulating Offshore Outsourcing in the Service Sector：Using the Law, Market, International Mechanisms, and Collective Organization as Building Blocks, 7 u. Pa. J. Lab. & Emp. L. 539, 540-542 (2005), 轉引自翁清坤，同註 18，頁 5-7。

英國銀行對於客戶資料之保密義務，並不限於人工紙本或電腦處理之個人資料，或於英國境內或境外處理之客戶資料。對金融監理而言，銀行將個人資料傳輸予第三人時，監理重點在於該項傳輸行為之合法性及如何防止客戶資料被不當使用，故英國銀行若因內部作業委外將個人資料傳輸予委外服務供應者時，無論該服務供應者係於英國境內、境外，或是否位為歐洲經濟區之國家甚或第三國家，均應遵循審慎監理手冊有關委外作業之規範。

由於英國金融監理機關得行使監理權限之範圍，僅限於金融服務與市場法明定之受監理機構（即英國之金融服務產業），故 FSA 所發布境外委外作業指引之規範重點，除明定銀行對其委外作業負最終責任外，並要求銀行對於委外服務供應商作適當之評估，以確保客戶資料於境外委外處理作業時之安全性。另英國 FSA 為能於必要時，直接自委外服務供應商取得與委外作業相關之資訊，以為適當監理，故要求銀行應於委外服務契約條款中，明定委外服務供應者應遵循之相關規定，以利其行使監理權限。

英國資料保護法對於國際傳輸雖已於原則八訂定相關限制及相關豁免規定，惟部分學者批評，資料保護法附錄四（Schedule 4）之豁免規定，已使得英國未完全遵循歐盟指令之規定，且對於國際傳輸，該法僅規定資料管理者應向 ICO 登錄有國際傳輸之需求，惟未有企業於傳輸前須經 ICO 事先核准或事後備查之機制。

但上開批評並不適用於英國之金融服務產業，基於對金融服務業之高度監理，且由於國際性銀行之營業據點（如辦事處、分行或子行）通常分佈於全球各地，使其對於個人資料流通之需求更為重大，故英國 FSA 針對金融服務業所有重要資料之輸出行為（所有重要之境外委外作業）均規定銀行應事先向 FSA 申請核准，並將相關資料適當文件化（申請文件包括資料輸出及相關控制措施、資料之處理程序、安全措施、系

統及控制等）。在上開規範下，已使 FSA 對於英國銀行國際傳輸行為之監理，較資料保護法對於國際傳輸之規定更為嚴格，亦間接使得 FSA 已執行 ICO 之職權[106]。

[106] Roger K. Baker, *supra* note 48, at 9-10.

第四章　標準契約範本與共同約束條款（Binding Corporate Rules, BCR[107]）之規範

第一節　標準契約範本之制訂背景及適用依據

許多企業例行性地傳輸個人資料至位於境外集團內之另一公司，如傳輸至集團內負責提供或執行人力資源或薪資管理之服務中心或企業等，或將資料定期傳輸至國外之母公司。但個人資料之傳輸亦可能是基於特定目的（如將員工個人資料與其僱傭契約透過電子郵件進行傳輸[108]）。個人資料之國際傳輸常涉及各國間經濟環境及政治利益等因素之影響，故歐盟指令發布前，許多國家及跨國公司（集團）已使用契約方式處理國際傳輸可能產生之法律問題。歐盟委員會參考現存之實務處理方式，將契約模式納入歐盟指令有關國際傳輸之法律架構。依據歐盟指令第 26 條規定，資料管理者得透過契約條款，約定雙方對於當事人權利已提供適當保護，並允許資料輸出者及接收者得透過契約自行約定或選擇使用歐盟委員會發布之標準契約範本（Standard Contractual Clauses, SCC[109]）。採用契約模式雖符合歐盟指令有關國際傳輸之規定，惟契約模式並無法確保資料接收國對於個人資料保護規範已有適當之法律制度[110]。

第一項　歐盟指令規定

依據歐盟指令第 26 條第 4 點規定，為確保個人資料傳輸之資料接收者能符合歐盟委員會之資料保護標準（包括必要之安全維護措施），委員會得依一定程序發布標準契約範本，供會員國使用。會員國應採行必要措施，配合委員會所作之決定。目前經歐盟委員會核准使用之標準契約範本計有三種：

---

[107] 共同約束條款第 1 次於本文出現，見第 28 頁。
[108] Richard Morgan and Ruth Boardman, *supra* note 27, at 164.
[109] 標準契約範本第 1 次於本文出現，見第 28 頁。
[110] Lingjie Kong, *supra* note 10, at 453-454.

一、歐盟委員會於 2001 年 6 月 15 日發布之 2001/497/EC 15「管理者傳輸予管理者」：個人資料自歐洲經濟區內之資料管理者，傳輸至第三國家之資料管理者適用。（SET 1，範本一）

二、歐盟委員會於 2004 年 12 月 27 日發布之 2004/915/EC 17「管理者傳輸予管理者」：同樣為個人資料自歐洲經濟區內之資料管理者，傳輸至第三國家之資料管理者適用。（SET 2，範本二）

三、歐盟委員會於 2010 年 12 月 27 日發布之 2010/87/EC「管理者傳輸予處理者」：個人資料自歐洲經濟區之資料管理者，傳輸至第三國家之資料處理者適用[111]。（範本三）

第二項　英國資料保護法規定

依據英國資料保護法第 54 條(6)有關國際合作（international co-operation）之規定，英國應遵循歐盟委員會依據歐盟指令第 26 條(3)或(4)[112]，依一定程序所為之決定（即採用標準契約範本）。為符合歐盟指令英國 ICO 已分別於 2001 年、2003 年及 2010 年發布規定[113]，授權英國企業得採用歐盟委員會發布之標準契約範本。企業一旦採用標準契約範本，除商業條款（如賠償條款、爭議解決條款及額外之契約終止權等）於不抵觸標準契約所訂條款之情況下，得自行於契約條款中增訂外，企業原則上不得自行修改契約條款內容（包括自行刪減或增加可能影響原契約條款效力或約定目的之其他約款）[114]。

為確保資料之傳輸能符合契約條款之要求（包括當損害發生時，當事人能依據契約條款向資料輸出者或接收者主張其權利），標準契約範本賦予資料輸出者及接收者一定之契約義務。如契約條款內容之變更係

[111] 2010 年發布之標準契約範本已取代 2001 年 12 月 27 日 2002/16/EC 之標準契約範本。

[112] 即歐盟委員會為對個人資料傳輸提供必要之安全維護措施，依第 31 條第 2 款規定程序訂定之標準契約範本，會員國亦應遵循歐盟委員會採取之措施。

[113] Data Protection Act 1998（Section 54(6) and Schedule 4, Paragraph 9）Authorisation, ICO, 2003 and 2010.

[114] Data Protection Act 1998—The eighth data protection principle and international data transfers, *supra* note 28, at 16-18.

因資料之傳輸涉及二個以上之契約當事人時，則標準契約範本所訂之契約義務應同時適用所有之契約當事人，並具有法律拘束力。

第二節　標準契約範本內容

第一項　規範目的及適用範圍

標準契約範本係介於合約雙方及法律規範之特殊契約，由於各國法令對個人資料保護程度各有不同，透過標準契約範本得補充資料接收國有關資料保護法律規範之不足，簡化國際傳輸之程序及降低傳輸成本，惟採用標準契約範本畢竟僅能拘束契約雙方，尚無法取代各國資料保護之立法，採用標準契約範本之目的如下[115]：

一、解決各國因資料保護規範之差異產生國際傳輸複雜之法律問題。

二、在尊重個人隱私權之前提下，協助個人資料之自由流通。

三、承認國際貿易因資料傳輸獲取之利益。

四、推動各國對個人資料保護規範之重視。

在全球對於個人資料保護缺乏一致性之規範下，由於採用標準契約範本能對當事人權益提供額外之保障，故為企業國際傳輸個人資料時所常見採行之方法。標準契約範本由於係以契約模式約束雙方應履行之契約義務，故僅適用於個人資料於二個獨立之經濟個體間之傳輸、集團內不同公司間（不同法律主體間）之資料傳輸，以及資料管理者與提供資料處理服務公司間之資料傳輸。

相對於資料之接收，歐盟委員會更為重視自歐盟輸出個人資料之管理（含資料輸出前及輸出後），故在整體資料保護法律架構下，係賦予資料輸出者較大之監督義務。當標準契約範本之一方違反契約條款時，自應由資料輸出者負主要責任（或與資料接收者負連帶責任），故當資

[115] Lingjie Kong, *supra* note 10, at 449.

料接收者違反契約條款時，當事人除得依據契約條款直接向輸出者請求損害賠償外，並要求資料輸出者採行適當措施[116]。

第二項　條款內容

目前經歐盟委員會核准採用之標準契約範本計有三種，二種為資料管理者輸出資料至第三國家之資料管理者適用，另一種則適用於資料管理者輸出資料至第三國家之資料處理者，三種類型之標準契約範本依條款內容得分為一般條款及其他條款內容：

一、一般條款內容（general clauses）

（一）名詞定義：明定標準契約範本所稱「個人資料」、「資料之分類」、「資料處理」、「管理者」、「處理者」、「個人資料之當事人」及「監理機關」等名詞之定義與歐盟指令之規範相同，資料輸出者係指負責傳輸資料之資料管理者、資料接收者係指因資料處理需求，而自資料輸出者接收資料之資料處理者。另於範本三明定複委託者（sub-processor）係指接受第三國家之資料接收者之委託，再進行資料處理之處理者。

（二）國際傳輸之資料內容：標準契約條款明定資料輸出者應依據附件格式填列所欲傳輸個人資料之內容、性質及傳輸目的等詳細資訊，並將該附件列為標準契約範本之一部分，另因傳輸資料之內容可能涉及商業機密，故除依據法律、監理機關、其他政府機關或當事人之要求外，該等資訊內容不得揭露予第三人知悉。

（三）契約管轄法律：標準契約條款應明定契約應適用資料輸出者當地國之資料保護法律。

[116] Lingjie Kong, *supra* note 10, at 450-451.

（四）契約條款之變動：明定契約雙方不得以任何理由，變動或調整標準契約範本所訂之條款內容（除通知監理機關變更傳輸資料之內容外）。

二、其他條款內容

（一）2001 年發布之範本一（管理者傳輸予管理者適用）[117]

1、第三人利益條款：當事人應能向資料輸出者及接收者主張本契約條款訂定之第三人利益條款，契約雙方並不得拒絕當事人行使其權利。（第 3 條）

2、資料輸出者之義務（第 4 條）

(1)處理個人資料應持續遵循契約條款內容，且不得違反資料保護法律之相關規定。

(2)傳輸之資料若包含敏感性資料，輸出者應於傳輸前，應通知當事人個人資料可能被傳輸至尚未有適當資料保護法律規範之第三國家。

(3)輸出者應依據當事人之申請，提供與其個人資料傳輸之相關資訊。

(4)輸出者應於合理時間內回復監理機關詢問有關個人資料由資料處理者進行處理之相關問題。

3、資料接收者之義務（第 5 條）

(1)資料接收者不得以任何理由，阻礙輸出者對其所為之監督行為，若因資料保護法令變動造成資料接收者可能違反契約義務，致對當事人權益產生重大負面之效果時，接收

[117] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_181/l_18120010704en00190031.pdf（last visited November, 2011）

者應立即通知資料輸出者，輸出者並有權停止資料之傳輸或終止契約。

(2)接收者對個人資料之處理應分別依下列情況適用標準契約範本附錄二或附錄三訂定之資料保護原則：

A.情況一：資料接收者之國內法律對於自然人基本權利與自由之保護，尤其是涉及處理個人資料之隱私權部分，並未符合資料輸出者所在國之資料保護法律[118]。

B.情況二：第三國家或該國之特定產業經歐盟委員會認可對於資料保護已符合歐盟規範[119]。

---

[118] 標準契約範本第 5 條(b)第 1 段規定，資料接收者應遵循之資料保護原則，計有 9 項，對於該等原則應與歐盟指令為一致之解釋：

1、 目的性限制：個人資料之處理及續後之使用或更進一步之傳輸，僅限於原始訂於附錄 1 所述之目的。資料持有之期間不得超過其傳輸目的所需之時間。

2、 資料品質及比例原則：資料應正確、必要時持續更新至最新資料，個人資料之傳輸及進一步之處理，應適當、攸關且不超逾原個人資料傳輸之目的。

3、 透明性：須提供必要之資訊予資料當事人，並確保資料傳輸過程之正當性（例如個人資料處理、傳輸之目的及位於第三國家之資料管理者）。

4、 安全及保密：資料管理者應採取適當技術及安全措施，以避免個人資料於處理傳輸或處理過程中，被意外、不法破壞、修改或未經授權之揭露、存取之情況發生。在未經資料管理者之授權下，任何人（包括資料處理者）均不得進行個人資料之處理。

5、 取得、更正、刪除及凍結資料之權利：依據歐盟指令第 12 條之規定，資料當事人應有權取得與處理其個人資料相關之資訊，以及當個人資料未依本附錄所述之原則進行處理時，有權將資料予以更正、刪除或凍結，特別是當資料有不完整或錯誤之情形。在特殊情況下，當事人應能拒絕其個人資料被處理。

6、 資料再傳輸之限制：資料接收者僅在下列情形之下，得將資料再傳輸予另一位於第三國家之資料管理者時（該第三國家尚未經歐盟認可對於個人資料保護符合歐盟標準之國家）。

   (1) 當事人明確同意將其資料進行再傳輸或已提供予當事人拒絕資料再傳輸之機會，提供予當事人之資訊應以當事人可瞭解之語言予以表達，並至少包括資料再傳輸之目的、位於歐盟經濟區內之資料輸出者、資料之收受者、資料傳輸之最終目的地國、資料再傳輸之目的地國對於個人隱私之保護尚符合歐盟指令之標準等資訊。

   (2) 資料輸出者及資料收受者同意將嚴格遵守標準契約範本所訂之條款內容，資料再傳輸之另一資料管理者亦應成為本契約條款之一方，並遵循與資料收受者相同之義務。

7、 特殊分類之資料：當個人資料涉及種族、血源、政治立場、宗教或哲學信仰或所屬商業同業公會、健康、性生活、犯罪紀錄、被判刑有罪等資料時，資料收受者應採行額外適當之安全措施，例如加強資料之加密以進行傳遞或任何敏感性資料之存取記錄。

8、 直接行銷：若資料之處理目的係為進行直接行銷，應有一有效之程序以允許資料當事人在任何時間，均有權「選擇退出」(opt-out)。

9、 自動化之個別處理（Automated individual decisions）：除符合歐盟指令第 15 條(2)之情形外，若個人資料處理之產生將對資料當事人產生法律效果或重大影響當事人之權利時，例如經由個人資料自動化之處理以評估當事人之工作績效、信用狀況、信賴程度、管理能力等，不得採行任何之自動化之處理。

(3)接收者應於合理時間內適當處理輸出者或當事人提出之詢問，並遵循監理機關對於個人資料傳輸提出之建議。

(4)輸出者得依據監理機關之規定，自行或委託外部獨立之人員對接收者處理個人資料程序是否符合契約約定進行查核。

(7)資料接收者應依據當事人之申請，提供其處理個人資料之契約內容（但得移除涉及商業機密之條款）。

4、契約雙方之責任（第 6 條）

(1)當事人因契約雙方違反標準契約範本第 3 條規定，造成當事人權益之損害時，除契約雙方能證明未違反契約條款外，對當事人應負損害賠償之責。

(2)資料輸出者及接收者對於因違反契約義務，致對當事人權益造成損害，應負連帶賠償之責。

(3)契約雙方同意，當一方違反契約條款，致另一方須先對當事人負損害賠償之責時，另一方於支付當事人相關賠償後，得向違反契約條款之一方請求賠償。

5、爭議處理機制與司法管轄權（第 7 條）

(1)契約雙方同意，若當事人與契約之一方產生爭議，並依據第三人利益條款主張其權利時，應同意當事人所作之下列決定：

A.要求將爭議案件交付監理機關進行調解。

B.要求將爭議案件於資料輸出者之管轄法院提起訴訟。

[119]標準契約範本第 5 條(b)第 2 段規定，資料接收者應遵循有關(1)目的性限制、(2)取得、更正、刪除及凍結資料之權利，以及(3)資料再傳輸限制等 3 項資料保護原則。

(2)契約雙方同意，當事人與契約之一方產生爭議時，若該方國家已納入國際仲裁紐約公約（New York convention）之會員國時，得依該公約規定進行仲裁。

(3)契約雙方應同意當事人所作之選擇，並不得以遵循當地法律或因其他契約條款之限制，損害當事人之訴訟權。

6、與監理機關之合作：契約雙方同意將契約內容之影本，依據資料保護法律之規定提供給有關之監理機關（第 8 條）。

7、契約之終止：契約雙方同意契約條款得於任何時點、任何情況下終止（第 9 條）。

（二）2004 年發布之範本二（管理者傳輸予管理者適用）[120]

為強化標準契約範本對當事人權益之保護，歐盟委員會於 2004 年發布範本二，並修訂範本一之條款內容，包括賦予資料輸出者得查核接收者對於所接收個人資料之保護、要求資料接收者提供其財務能力之證明，以確保當事人個人資料遭受損害時，接收者有損害賠償之能力、加強當事人行使第三人利益條款之權利，例如當接受者違反契約條款，但輸出者仍繼續輸出個人資料時，當事人得採行之措施、當事人有權要求於輸出者所在國提起訴訟、授權監理機關得於接收者拒絕合作時，終止或暫緩個人資料之傳輸等，範本二之條款內容如下：

1、資料輸出者之義務

(1)個人資料之蒐集、處理及傳輸應遵循資料輸出者所在國適用之資料保護法律等相關規定。

[120] Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF（last visited November, 2011）。.

(2)輸出者應採行適當評估程序以決定接收者是否能履行契約之法定義務。

(3)資料輸出者應提供其所在國之資料保護法令等相關規定予資料接收者。

(4)若資料接收者不願或無法回復當事人及監理機關提出之之相關問題，輸出者應協助答復其知悉之相關資訊。

(5)資料輸出者應依據當事人之要求提供契約影本。

2、資料接收者之義務

(1)資料接收者應有適當技術及安全措施以保護個人資料不被意外或非法之破壞或損失、或未經授權之揭露或存取。

(2)接收者應訂定經授權之第三人（含資料處理者）能存取個人資料之適當作業程序。接收者應重視及維持個人資料之機密性及安全性，任何經接收者授權之人，對於個人資料僅能依據接收者之指示進行處理。惟本條款不適用於依法律或命令經授權或要求存取個人資料之人（如監理機關）。

(3)當資料接收者當地國之法律，對於契約條款產生重大負面效果時，資料接收者應立即通知輸出者。

(4)個人資料之處理應僅限於原始之特定目的。

(5)資料接收者對於輸出者、當事人及監理機關詢問有關個人資料處理程序之相關問題，應於合理期間內答復。

(6)資料接收者應依據輸出者之要求提供相關財力證明，以確保接收者有能力履行其損害賠償之義務(含投保情形)。

(7)資料接收者應依據輸出者之要求，提供個人資料處理設備、資料檔案及文件化等相關資訊，供資料輸出者檢視、

查核或驗證。輸出者於提出上開要求時，應依據法令或經接收者當地監理機關之同意或核准。

(8)資料接收者對於個人資料之處理，應選擇其所適用之資料保護原則：

A.資料輸出者所在國之資料保護法律規範。

B.歐盟委員會發布歐盟指令第 25 條(6)之相關規定。

C.範本二附錄 A 訂定之資料處理原則[121]。

(9)資料接收者除經輸出者同意或符合下列情形之一者外，不得揭露或再傳輸個人資料：

A.將個人資料傳輸給經歐盟委員會認可之第三國家之第三方資料管理者。

---

[121] 歐盟委員會於 2004 年發布之標準契約範本於附錄 A 訂有資料處理之八項原則如下：

1、 目的性限制：個人資料之處理及續後之使用或進一步之傳輸，除經資料當事人之授權外，僅限於原始訂於附錄 B 所述之目的。

2、 資料品質及比例原則：個人資料應正確，必要時，應持續更新。個人資料之傳輸及進一步之處理，應適當、攸關且不超逾原所蒐集個人資料之目的。

3、 透明性：須提供必要之資訊予資料當事人，以確保資料傳輸過程之正當性（例如個人資料處理及傳輸之目的）。

4、 安全及保密：資料管理者應採取適當技術及安全措施，以避免個人資料於處理傳輸或處理過程中，被意外、不法破壞、修改或未經授權之揭露、存取之情況發生。在未經資料管理者之授權下，任何人（包括資料處理者）不得處理個人資料。

5、 取得、更正、刪除及拒絕之權利：如同歐盟指令第 12 條之規定，除資料之輸出係法律所明定規定者外，組織應告知當事人其所持有該當事人個人資料之情形。資料輸出者除經監理機關之事先核准外，不得進行資料之存取，以避免個人資料之傳輸可能嚴重損害資料接收者或其他組織之利益，但該等利益並不影響當事人之基本權利與自由。當個人資料發生錯誤時，當事人應有權對其個人資料進行更正、修改、刪除。當對個人資料之合法性產生疑義時，於個人資料進行更正、修改或刪除前，企業應要求進一步之解釋。在特定情況下，當事人應有權拒絕與其個人資料相關之處理。

6、 敏感性資料：若傳輸之個人資料為敏感性資料，資料接收者應採行額外之安全措施。

7、 因行銷目的使用資料：當個人資料處理之目的係為市場行銷時，當事人於任何時點均有「選擇退出」（opt-out）之權利。

8、 自動化之處理(Automated decisions)：指資料輸出者及資料接收者所作決定若對資料當事人產生法律效果或重大影響當事人之權利時，經由個人資料自動化之處理以評估當事人之工作績效、信用狀況、信賴程度、管理能力等。除下列情況外，資料接收者，不得採行任何之自動化之處理：

(1)(i)該等處理係資料接收者為履行與資料當事人契約所必須。

(ii)資料當事人有機會與另一方討論自動化處理之結果。

(2)依據資料輸出者所在國法律之規定。

B.第三方資料管理者已簽署標準契約範本或其他於歐盟境內核准之資料傳輸協定。

C.將再傳輸之相關資訊提供予當事人，使其有拒絕資料傳輸之權利（包括資料傳輸之目的、再輸出之資料接收國及該國對於個人資料之保護程度可能與資料輸出國不同等相關資訊）。

D.若再傳輸之資料為敏感性資料時，已取得當事人明確同意進行再傳輸。

3、共同責任與第三人利益條款

(1)契約雙方因一方違反契約條款，對另一方造成損害時，應負損害賠償之責，惟損害賠償義務僅限於填補實際損害，不包括懲罰性賠償。契約雙方因一方違反契約條款對當事人造成之損害，應負損害賠償之責，但該賠償責任，並不因此降低輸出者依據資料保護法所應負之責任。

(2)契約雙方同意當事人有權依據契約條款之規定主張第三人利益條款，對抗資料輸出者及接收者。當違反契約條款之一方為資料接收者時，當事人應要求輸出者採取適當行動，以保護當事人之權益。若輸出者未於合理期間（正常情形下，該期間通常為一個月）採取任何措施，當事人得直接向資料接收者主張其權利。

4、契約雙方與當事人或監理機關間產生爭議之處理

(1)若當事人或監理機關對契約一方有關個人資料之處理程序產生疑義時，該方應通知另一方，並相互合作在合理期間內回復當事人或監理機關之詢問。

(2)契約雙方同意任何由當事人或監理機關選擇之調解程序。在訴訟程序中，若因距離過於遙遠，契約雙方得選擇使用電話或其他電子設備。

(3)契約之一方應遵守資料輸出者所在國之管轄法院作出之最終判決結果。

5、契約之終止

(1)若資料接收者違反契約義務時，輸出者得暫時停止資料之傳輸至資料接收者改善其缺失或至契約終止時。

(2)在下列情況下，資料輸出者有權終止契約，並應於適當情況下通知監理機關（反之，若有下列 A、B、E 之情況發生時，資料接收者亦同樣終止契約之權利）：

A.在上開(1)之情況下，資料輸出者已暫緩個人資料之傳輸達一個月以上。

B.資料接收者遵循契約條款，可能違反當地法律或法令規定。

C.資料接收者重大或持續違反契約條款。

D.資料輸出者或接收者因違反契約條款，資料輸出者所在國之管轄法院或監理機關已作出最終之判決。

E.資料接收者之管理階層被起訴或結束營業(如接收者被破產管理人接收、資產被受託管理人管理或有其他類似情況發生）。

(3)歐盟委員會依據歐盟指令第 25 條(6)規定，發布與資料接收者當地國之相關規範或替代規定，或該第三國家已實施歐盟指令時，契約之任一方得終止契約。

(4)契約雙方同意於任何時點或情況下終止契約時(除發生(3)之情況外)，不得免除雙方依據契約條款所應負之個人資料傳輸義務。

（三）2010 年發布之範本三（管理者傳輸予處理者適用）[122]

1、適用情形

(1)各員會國之資料保護監理機關在契約機制下，應確保個人資料於傳輸後能被適當保護。若資料輸出者拒絕或無法適當管理資料接收者，致當事人權益遭受損害時，監理機關於資料傳輸之範圍內，應能依據標準契約範本查核資料接收者及其負責資料處理之部門，並有權禁止或暫緩資料之傳輸至接收者對於當事人之個人資料已能提供適當之保護。

(2)為避免個人資料因故意或過失遭到破壞或有未經授權揭露或被他人取得個人資料之情形發生，標準契約範本有關個人資料之保護，應確保資料處理者具備適當技術及安全措施，包括當地國適用之資料保護法令及保護資料所使用之最新技術及成本等。

(3)未經資料輸出者事先之書面同意，資料接收者不得將個人資料複委託予另外之資料處理者（sub-processing）。

(4)當事人與資料接收者產生爭議時，接收者應提供當事人調解或提起訴訟之權利。調解時，當事人得要求由資料輸出者所在國之監理機關擔任調解人。

---

[122] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/45/EC of the European Parliament and of the Council, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF（last visited November, 2011）。

2、條款內容

(1)第三人利益條款：當事人應對資料輸出者及接收者主張契約訂定之第三人利益條款，契約雙方不得拒絕當事人權利之行使。（第 3 條）

(2)資料輸出者之義務（第 4 條）

A.處理個人資料應持續遵循契約條款內容，且不得違反資料保護法律之相關規定。

B.資料輸出者於資料處理期間應持續監督資料處理者是否符合資料保護法律之相關規定。

C.資料接收者應具備適當技術及安全措施，並應將其所採行之技術及相關措施納入契約附件，作為契約之一部分。

D.資料接收者訂定之安全措施應能適當保護個人資料，避免被不法或因過失受到破壞、損害或被修改、未經合法授權之揭露或取得，尤其當資料處理係以網際網路傳輸時。

E.資料接收者應確保訂定之安全措施能被有效執行。

F.傳輸資料若含敏感性資料，傳輸前應通知當事人或於傳輸後儘快通知當事人。

G.資料輸出者於收到接收者依據第 5 條(b)（因法令變動對契約義務之履行產生重大負面效果）或複委託之資料處理者依據第 8 條(3)之規定（因當地法令規定，致資料輸出者之監理機關無法對資料處理者進行必要之查核時）所為之任何通知時，若仍將繼續傳輸個人資料或解除暫緩傳輸之限制時，資料輸出者應立即通知監理機關。

H.除契約附件所列之安全措施涉及商業資訊外，當事人得要求取得其個人資料進行傳輸之相關資訊。

I.個人資料若再傳輸予複委託者，其對於資料之處理應適用標準契約範本第 11 條有關複委託之相關規定。

(3)資料接收者之義務（第 5 條）

A.資料接收者應依據輸出者之要求處理個人資料，若資料處理者因任何理由無法履行與輸出者之契約義務時，輸出者有權停止資料之傳輸或終止契約。

B.資料接收者不得以任何理由，阻礙輸出者對其所為之監督行為，若因資料保護法令變動造成資料接收者可能違反契約義務，致對當事人權益產生重大負面之效果時，接收者應立即通知資料輸出者，輸出者並有權停止資料之傳輸或終止契約。

C.處理個人資料前，資料接收者應確保相關安全措施已適當執行。

D.有下列情形者，資料處理者應立即通知資料輸出者：

(a)當地執法機關因犯罪調查需求，要求資料處理者提供所處理個人資料之相關資訊。

(b)個人資料因過失或未經授權被存取。

(c)資料處理者收到當事人之要求。

E.資料處理者應立即及適當處理資料輸出者提出之要求，並遵循監理機關對於資料保護之所提建議。

F. 輸出者得依據監理機關之規定，自行或委託外部獨立之人員對接收者處理個人資料程序是否符合契約約定進行查核。

G.資料接收者應依據當事人之申請，提供其處理個人資料之契約內容（但得移除涉及商業機密之條款）。

H.資料處理者若擬將資料再傳輸給另外之資料處理者時（複委託，Sub-processing），應事先通知資料輸出者，並取得書面同意。

I.負責資料之再處理者（複委託者），應適用標準契約範本第 11 條之規定。

(4)共同責任（第 6 條）

A.當事人因契約雙方違反標準契約範本第 3 條（第三人利益條款）及第 11 條規定（複委託處理個人資料之規定），致當事人權益受到損害時，資料輸出者應對當事人負損害賠償之責。

B.當事人若無法依據前款規定對輸出者主張其權利（因輸出者已不存在或已破產），得向資料接收者請求損害賠償。

C.當事人若無法依前二款規定對資料輸出者或接收者主張其權利，若個人資料之處理，有複委託者時，當事人得向該複委託者請求損害賠償，惟其損害賠償之範圍，僅限於其所負責處理個人資料之作業部分。

(5)調解程序與司法管轄權（第 7 條）

A.當事人依據第三人利益條款主張其權利時，資料接收者應同意當事人所作之下列決定：

(a)要求將爭議案件交付監理機關調解。

(b)將爭議案件於資料輸出者之管轄法院提起訴訟。

B.契約雙方應同意當事人所作之上開選擇，不得以遵循當地法律或因其他契約條款之限制，損害當事人之訴訟權。

(6)與監理機關之合作（第 8 條）

A.資料輸出者同意將雙方之契約內容影本，依據所在國資料保護法律之規定提供予有關之監理機關。

B.契約雙方同意監理機關有權對資料接收者進行查核。

C.資料接收者若受限於當地法律規定，致無法遵循前款規定，應立即通知資料輸出者。

(7) 資料處理之複委託（Sub-processing）（第 11 條）

A.資料接收者未經輸出者之事先書面同意前，不得將資料處理作業，再另訂契約轉委託他人處理。當資料接收者依據契約規定，將個人資料複委託予他人處理時，複委託處理者應與接收者負相同之契約義務。若複委託者違反資料保護之義務時，接收者應完全承擔其所應負之責任。

B.資料接收者與複委託者訂定之契約，應依據標準契約範本第 3 條規定，明定當事人之第三人利益條款。

C.複委託者應遵循資料輸出者所在國之資料保護法令。

D.資料接收者將資料處理複委託予另一資料處理者，資料輸出者應留存資料接收者與複委託者間之契約條款等相關資料，並應至少每年更新一次。另資料輸出者之監理機關亦得取得相關資訊。

(8)個人資料處理服務終止後之義務（第 12 條）

A.契約雙方同意於資料處理服務終止時，除依法律另有規定者外（資料接收者應保證對於已取得之個人資料

負保密義務，且不再進一步處理或傳輸），資料接收者及複委託者，應返還或銷毀於資料處理期間所接收之個人資料。

B.資料接收者及複委託者，依上開規定未將所接收之個人資料銷毀時，應同意資料輸出者及其監理機關對其儲存資料之相關設備進行查核。

三、標準契約範本之規範內容如下：

範本類型	資料輸出者（exporter）	資料接收者（importer）	規範內容
範本一（2001/497/EC）	資料管理者	資料管理者	名詞定義、傳輸資料之內容、第三人利益條款、資料輸出者之義務、資料接收者之義務、共同責任、爭議處理及司法管轄權、與監理機關之合作、契約終止、契約雙方不得任何變動條款內容、契約管轄法律。
範本二（2004/915/EC）	資料管理者	資料管理者	名詞定義、資料輸出者之義務、資料接收者之義務、共同責任及第三人利益條款、契約管轄法律、與當事人或監理機關間之爭議處理、契約終止、契約雙方不得任何變動條款內容、傳輸資料之內容。
範本三（2010/87/EC）	資料管理者	資料處理者	名詞定義、傳輸資料之內容、第三人利益條款、資料輸出者之義務、資料接收者之義務、共同責任、爭議處理及司法管轄權、與監理機關之合作、契約管轄法律、契約雙方不得任何變動條款內容、複委託處理（sub-processing）、個人資料處理服務終止後之義務。

資料來源：本研究整理

第三項　條款特色

由於標準契約範本之規範目的係為保護個人資訊之隱私，故標準契約範本訂定之部分條款內容，並不常見於一般商業契約（條款內容亦通常不被商業行為所接受），特別是有關第三人利益條款及與監理機關合作之相關條款。標準契約範本條款之特色如下：

一、契約條款不得任意調整（non-negotiable）

標準契約範本之條款內容係為使輸出資料之管理者能確保資料接收者已遵循資料輸出國對於個人資料之保護規範及契約雙方能於當事人提出詢問或申訴時予以適當處理，故契約範本明定資料接收者應遵循歐盟指令之資料保護原則及相關限制之義務。

另為確保資料接收者當地國之法律不致阻礙或影響標準契約範本條款之效力[123]，故歐盟指令明定標準契約範本之條款內容，契約雙方不得任意變動，雖得另訂補充條款，但補充條款內容亦不得影響或降低標準契約範本之訂定目的。

二、傳輸敏感性資料之限制

依據標準契約範本之規定，若資料管理者輸出之資料係屬敏感性資料時，該等資料於傳輸前，資料輸出者應與各資料當事人聯繫，通知其敏感性資料之輸出情形。惟若當事人之人數眾多時，將造成該項條款之落實有其實務困難。

三、任何情況下，資料輸出者均須對資料處理者之行為負責。

四、當企業在歐洲經濟區內使用標準契約範本時，各會員國須承認契約之有效性[124]。

五、第三人利益條款（The third-party beneficiary clauses）

標準契約範本之條款內容賦予當事人於損害發生時，得向契約雙方主張第三人利益之權利，該等條款可協助當事人在各國不同資料保護法下，能依據雙方契約之約定，主張其權利[125]。另標準契約範本中亦明定當契約之一方對當事人造成損害時，需互負連帶損害賠償之責（如資料接收者有侵害當事人資訊隱私之情形時，當事人得同時對資料輸出者或接收者提起訴訟）。

123 Richard Morgan and Ruth Boardman, *supra* note 27, at 165.
124 *Id.* at 165-166.
125 Lingjie Kong, *supra* note 10, at 451-452.

六、個人資料保護機制之落實

為確保契約雙方能履行契約之法定義務，標準契約範本中明定監理機關得採行相關監理及補救措施之條款，包括資料輸出者所在國之監理機制得限制或終止資料之傳輸、資料接收者之當地國修改與個人資料保護之相關規定，致標準契約範本之契約效力產生重大負面影響時，資料接收者應即通知輸出者所在國之監理機關、資料接收者拒絕與監理機關合作或有違反標準契約條款之規定時，資料輸出者應採行之措施、明定當事人無法依據第三人利益條款解決其與契約雙方之爭議時之處理機制，包括得向獨立之第三人請求調解（如監理機關）、向資料輸出者所在國之法院提起訴訟或向仲裁機構提出仲裁。

歐盟委員會制訂標準契約範本之目的，係為歐盟地區居民之個人資訊隱私建立一道防火牆，惟事實上各會員國資料保護之監理機關對於如何有效監理企業國際傳輸個人資料之行為，仍有實務困難[126]。

第四項　不同標準契約範本條款內容之差異

目前歐盟委員會發布之三種標準契約範本，相對於範本一，為加強當事人權益之保護，範本二及範本三訂定之契約條款內容較為明確且詳細，契約雙方所應負之契約義務亦較多，三種標準契約範本之主要差異如下：

一、當事人之損害賠償請求權：在範本一，資料輸出者及接收者因違反契約條款內容，致對當事人資訊隱私造成損害時，須共同對當事人負損害賠償之責。惟範本二，僅規定當事人得對違反契約之一方請求賠償。

[126] Lingjie Kong, *supra* note 10, at 453.

二、資料接收者之義務：相對於範本一，範本二賦予資料接收者較多之契約義務，包括接收者應有適當程序（含相關資料之文件化），以確保個人資料之安全、為確保資料接收者能於當事人權益受到損害時，有履行損害賠償責任之能力，接收者應提供相關財力證明，以及資料接收者除經輸出者同意外，不得將所接收之個人資料揭露或再傳輸。

三、契約之終止：範本一對於契約之終止，僅規定雙方同意即得於任何時點、任何情況下終止契約，惟未明定契約終止之事由。範本二及範本三則分別針對資料輸出者及接收者明定雙方有權終止契約之各項事由。範本三另訂定契約終止後資料接收者對於所接收個人資料有銷毀或返還之義務。

四、範本二與範本三之契約條款內容較為相近，惟該二範本最大之差異在於範本三訂有複委託之條款內容，包括資料處理者辦理複委託時，應遵循適當程序及複委託者應履行之契約義務。另範本三並訂定契約終止後資料接收者對於所接收個人資料有銷毀或返還之義務。

第三節　BCR 之制訂背景及適用依據

相對於採用標準契約範本，許多大型之跨國企業選擇將國際傳輸之控管訂定於集團政策及內部規章中。尤其當企業之國外營運模式係設立分支機構（即分公司），而非子公司之型態（因分公司與總公司仍為同一法律個體，二者間無法區分各自之法律責任，自無法採用標準契約範本）[127]。

另外，對於組織架構較為複雜之跨國企業而言，由於其關係企業或分支機構可能遍及全球，個人資料於集團內各企業間傳輸之需求龐大，若採用標

[127] Richard Morgan and Ruth Boardman, *supra* note 27, at 166.

準契約範本，各公司間除須逐一簽訂契約外，隨著集團組織架構之變動，契約亦需持續更新，使得採用標準契約範本之程序過於複雜，且耗費時間。

BCR 為跨國企業之內部行為準則，目的係為使個人資料傳輸至第三國家時，能確保個人資料及資訊流通之安全。企業採用 BCR 後，個人資料雖得於集團內部自由傳輸，惟採用前，需先取得歐盟會員國之資料保護監理機關之事先核准，首次採用時之程序將較為複雜及費時。

第一項　歐盟指令規定

使用 BCR 之目的，係為建立一套適當之安全機制，以允許跨國企業在第三國家無法符合歐盟指令第 25 條第 2 點之情形下，仍能將資料自歐洲經濟區傳輸至設立於第三國家之關係企業。

第二項　英國資料保護法規定

一、適用依據：英國 ICO 於 2011 年 3 月發布授權企業得向 ICO 申請採行 BCR。企業向 ICO 申請採行 BCR 時，應先自行確認企業訂定國際傳輸之內部規章是否符合歐盟委員會發布有關 BCR 之最低要求，包括歐盟資料保護工作小組發布之相關工作文件（working document），如第 74 號採用 BCR 將個人資料國際傳輸應符合之最低標準、第 108 號企業申請核准 BCR 之標準檢查表（Model Checklist）及第 153 號監理機關核准企業採用 BCR 之審查要素及原則等相關規定[128]。

二、BCR 之申請程序

跨國企業向歐盟各員會國之資料保護監理機關申請採行 BCR 時[129]，由於跨國企業除於第三國家設有分支機構外，其於歐盟各國

[128] 2005 年至 2011 年經核准採用 BCR 之企業包括通用奇異公司（General Electric Company，經核准之 BCR 為員工資料保護標準）、菲利浦電子（Koninklijke Philips Electronics NV, 經核准之 BCR 為菲利浦隱私規章及隱私條款）、摩根大通公司（JPMorgan Chase & Co, 經核准之 BCR 為 JPMC 集團內協議及 JPMC 全球隱私標準）等 10 家公司。請參考 ICO 於 2011 年 3 月 31 日發布之 Binging Corporate Rules Authorissation。

[129] 依據歐盟資料保護工作小組於 2007 年 1 月 10 日發布之第 133 號工作文件（WP 133），跨國

亦可能設有不同之據點，為節省企業向不同歐盟會員國之監理機關申請採用 BCR 之時間及成本，歐盟部分國家已採取共同合作程序（co-operation procedure），故歐洲經濟區內之企業得自行選定會員國之一國之資料保護監理機關作為該跨國企業之主要監理機關（lead authority[130]），向其申請採用 BCR。當主要監理機關已核准該跨國企業採行 BCR 後，其他合作之監理機關亦須認可主要監理機關發出之核准函（mutual recognition[131]），主要監理機關並應依據該企業之需求，將核准函提供給該企業國際傳輸所涉及相關國家之資料保護監理機關。

企業之內部規章一旦經監理機關核准符合 BCR 之要求後[132]，企業即有義務持續監控內部採用 BCR 之情形，包括定期之稽核及相關之教育訓練。由於 BCR 為組織內部對於個人資料及隱私權保護之內部規範，故企業於申請時，應考量企業內部預訂傳輸個人資

企業向監理機關申請採行 BCR 時，應備文件計有二大部分：

1、 第一部分為基本資料：包括(1)申請者及集團企業之基本資料（含總公司之所在地及聯絡方式等）、(2)簡要說明所需國際傳輸個人資料之性質及範圍、(3)決定主要之資料保護監理機關（lead PDA）；

2、 第二部分為背景資料文件：包括(1)BCR 之約束力（含 BCR 之對內及內外之法律效果、當有訴訟案件發生時，集團內之負責訴訟案件之單位、特定產業（特別是金融服務業）之監理機關以法令禁止集團內位於某一國家之單一企業，對於集團內位於另一國家之另一企業負損害賠償責任，若申請者有該等情形時，應將相關詳細資料提供予資料保護監理機關，並解釋企業集團內是否有其他機制，以確保當事人權益受到侵害時，能獲得適當之賠償）、(2)有效性，企業應說明其所制訂之 BCR 如何有效落實於集團之各關係企業或分支機構，另由於並非所有當地資料保護法令均允許資料保護監理機關進行查核，申請者需自行聲明負責核准該集團企業之 PDA，於必要時，得進行相關之查核、(3)與 PDA 之合作，申請者應說明企業如何與 PDAs 之合作機制、(4)申請者應完整說明個人資料於集團內之傳輸情形、(5)報告及 BCR 修訂之機制、(6)詳細說明企業 BCR 中之資料保護機制。

3、 另申請者應將企業制訂之 BCR 影本作為申請案之附件資料。

[130] 企業選擇主要監理機關時，應考量因素包括：(1)歐盟集團企業總公司之所在地；(2)集團中負責遵循資料保護相關規範部門之所在地；(3)集團中負責申請及執行 BCR 部門或公司之所在地；(4)資料處理過程中決策制訂之所在地；(5)最常將個人資料傳輸至 EEA 以外國家之集團內公司之所在地。

[131] 截至 2011 年 4 月底歐盟已有 19 個國家採行共同合作程序，包括奧地利、比利時、保加利亞、塞普勒斯、捷克、法國、冰島、愛爾蘭、意大利、拉脫維亞、列支敦斯登、德國、馬爾他、芬蘭、挪威、斯洛維尼亞、西班牙及英國等。

[132] 在監理機關共同合作程序下，英國 ICO 認為一企業自申請採用 BCR 至取得監理機關核准，約需一年之時間（視跨國企業組織及個人資料傳輸之複雜程度）。

料之性質及種類、如何使員工瞭解並有效遵循相關規範及第三國家之員工如何進行資料之處理等，訂定 BCR 時應將各種可能發生之情形納入考量，避免當傳輸情況改變時（如因企業政策或資料傳輸之型態已超逾原經監理機關核准 BCR 之範圍時），須再重新申請核准。

第四節　BCR 規定內容

第一項　適用情形

如同標準契約範本，BCR（或稱「公司法律模式」、「集團政策」）亦為歐盟委員會保護國際傳輸個人資料之另一工具。如前所述，BCR 之適用範圍僅限於跨國企業或同一集團內部間之國際傳輸，且僅適用於公司內特定部門之資料處理者，故 BCR 中並未訂有資料輸出者與接收者損害賠償責任分攤及有關資料保護之義務[133]（屬共同義務），BCR 之性質係屬單方面之條款，對資料輸出者及接收者並不直接產生權利或義務。

任何集團政策在法律上應能被有效執行，使 BCR 具有法律效果，並於當事人個人權益受到損害時，能依據 BCR 行使其權利，另監理機關於必要時，亦能依據 BCR 進行適當之干預。採用 BCR 對於消除或解決大型跨國企業將個人資料於全球各地傳輸之問題，具有效益。但對於中小型企業，歐盟委員會訂定之 BCR 可能過於嚴格，且不具成本效益。

第二項　BCR 訂定之最低要求

依據歐盟委員會於 2003 年 6 月 3 日發布之第 74 號工作文件（WP 74[134]），企業申請採行 BCR，將資料傳輸至第三國家之適用標準如下：

---

[133] Lingjie Kong, *supra* note 10, at 453-454.

[134] Data Protection Working Party, Working Document：Transfers of personal data to third countries：Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers（2003）, available at www.europa.eu.int/comm/privacy（lasted visited November, 2011）。

一、基本規範

（一）歐盟資料保護工作小組重申集團企業設於第三國家之分支機構，由於當地國可能並無資料保護之立法或未有資料保護政策之情形時，歐盟企業於發展 BCR 時，應更為詳細且易於瞭解，並能符合第三國家分支機構對於個人資料之處理程序。

（二）細則及規章之更新

集團企業之 BCR 應針對不同國家或地區訂定相關作業細則，以因應不同國家或地區之法令或實務需要。集團企業之內部組織可能隨時會有變動，惟符合下列情況下，企業修改經監理機關核准之 BCR 時，得無須再向監理機關再次申請核准：

1、集團企業內新設之分支機構尚未有國際傳輸之需求。

2、集團企業內有專責人員或部門，負責記錄並追蹤 BCR 之修正及集團內企業名單變動之情形，並適時提供必要資訊給當事人或監理機關。

3、修正後之 BCR 或集團內企業名單之變動，應每年向監理機關申報，並說明變動原因。

集團企業之 BCR 若有重大修正，且修正內容已涉及資料保護原則、傳輸目的及傳輸資料之類型時，則 BCR 之修正，仍應經監理機關之事前核准。

二、BCR 之落實

（一）制度之建立：集團企業內部應建立適當制度，以使集團內各企業或分支機構（無論分支機構或關係企業係於歐盟境內及境外）均確實執行 BCR 之規定。申請採用 BCR 之集團企業應證明已透過適當訓練及相關資訊之分享（如透過內部網路），使得集團內部之員工均知悉、瞭解且能有效落實集團

內部訂定之隱私政策。集團企業應取得高階主管之支持，指定適當人員，專責 BCR（如隱私政策）之監督與遵循。

（二）稽核功能

BCR 應明定由內部或外部稽核定期進行查核之規定，稽核報告應直接呈報至母（總）公司之董事會及監理機關。當企業經核准使用之 BCR 有變動時，稽核單位亦應隨時通報監理機關。另 BCR 亦應明定與監理機關之合作義務，包括同意監理機關自行或委託獨立之稽核人員進行查核（尤其當監理機關無法自企業取得相關稽核報告或無法瞭解企業遵循 BCR 之情形時）。

（三）申訴案件之處理：BCR 應明定企業內部負責處理個人資料申訴案件之部門，負責處理該等申訴案件之人員於企業中應具有適當之獨立性。在當地法律或相關法令之規範下，企業亦得選擇將監理機關納入爭議處理機制。

（四）企業與其他資料保護監理機關之合作義務

集團企業應遵循及落實資料保護監理機關發布與 BCR 有關之解釋函令或適用規定，包括企業處理當事人或監理機關提出申訴案件之處理結果。當集團企業設立於各國之分支機構，因當地資料保護法令之規定，致無法遵循母（總）公司資料保護監理機關之相關規定時，監理機關得暫緩、中止或取消對特定第三國家資料傳輸之許可。若有上開情形發生，監理機關應通知歐盟委員會及其他國家之資料保護監理機關。

（五）企業責任

BCR 對當事人各項權利之保護，應與歐盟指令第 22 條及第 23 條之規定一致，惟上開規定僅適用於原始自歐盟地

區輸出之個人資料。集團企業之總公司或該公司位於歐盟員會國負責資料保護事宜之代表人，應接受並同意當集團企業第三國家之分支機構有違反 BCR 之情形，致造成當事人之損害時，應採取相關之因應措施，並負損害賠償之責。

集團企業於歐盟境內之總公司或其代表人，於歐盟境內應有充足之資產（包括相關保險等），以有損害賠償之能力，並應同意在下列情況下，以歐盟之會員國作為訴訟管轄法院，為適當之損害賠償：

1、因集團企業違反 BCR，致當事人發生損害。

2、當事人雖未提起訴訟，但集團企業對於其申訴案件之處理，無法與當事人達成共識。

（六）管轄法院

集團企業應同意當事人之訴求及選擇以當事人資料原始輸出國或集團企業於歐盟境內總公司之所在地或其代表人之所在地，作為訴訟管轄法院。

（七）資訊之透明

集團企業應將經資料保護監理機關核准之 BCR、個人資料保護採行之安全措施，以及個人資料傳輸至第三國家等相關資訊提供予當事人知悉（上開說明義務，得僅限於與當事人權益攸關之資訊）。

第三項　BCR 之有效性

由於 BCR 仍為企業內部之政策、規章及細則，故各國監理機關在核准集團企業採用 BCR 時，應考量下列因素對 BCR 法律效果之影響：

一、BCR 面臨之法律問題

（一）BCR 與其他依歐盟指令規定（如各會員國依歐盟指令第 27 條規定，發布之標準契約範本及因應各產業需要訂定之自律規範等）之差異，在於 BCR 係訂於集團企業之內部規章，該內部規章無法取代各會員國及第三國家於國內法訂定有關資料保護之規定，且 BCR 能否發揮其功能，有賴於企業能確實落實。

（二）跨國企業之資料保護政策（或隱私政策）通常受到當地法律、社會文化及企業願景之影響，第三國家若無健全的資料保護法制或商業慣例，公司雖得直接將歐盟指令之資料保護相關原則納入內部規章，惟 BCR 能否落實，仍須考量個人資料接收國之當地法律及社會環境對 BCR 之影響，避免 BCR 之內容有違反當地法令致無效之情形[135]。

二、 為確保跨國企業於歐盟境內及境外之分支機構或子公司，已確實有效遵循 BCR 之規定，企業應透過相關訓練課程使員工或集團成員瞭解相關規定， 並應能證明 BCR 已於集團內有效落實[136]。

三、 雖歐盟部分之會員國對企業申請採用 BCR 已建立共同合作審查模式，惟跨國企業之分支機構若分布於不同國家，若該等國家之監理機關尚未簽訂共同合作模式，則企業之 BCR 仍需經其他監理機關之核准，惟各國監理機關之審查標準可能不同，提出之審查意見亦可能有不一致之情形。

第五節　小結

無論是採用標準契約範本或 BCR，歐盟委員會均係期望企業能透過產業自治之方式，使企業因商業交易及作業需要，將個人資料國際傳輸之另一國

[135] Lingjie Kong, *supra* note 10, at 454-455.
[136] Richard Morgan and Ruth Boardman, *supra* note 27, at 167-168.

家時，能確保資料於傳輸過程之安全、資料接收者對於資料能有適當之資料保護機制、當資料傳輸對當事人權益造成損害時，確保當事人行使損害賠償請求權時無任何阻礙，以及資料輸出國之監理機關如何在不同司法管轄權下，仍能有效監理資料管理者之國際傳輸行為。使用標準契約條款及 BCR 之差異如下：

一、適用對象

標準契約範本因係透過簽訂契約之方式，故適用於二個獨立之法人（經濟個體），包括集團內不同公司間之資料傳輸，惟 BCR 僅適用於跨國集團內之資料傳輸（含集團內之關係企業、子公司或分公司間），故當資料之輸出或接收之一方為跨國企業之分公司時，因二者仍屬同一法律個體，自無法以標準契約範本之模式約束契約雙方之權利義務。

標準契約範本相對於 BCR 已分別明定資料輸出者及接收者之契約義務及對當事人之損害賠償責任，故標準契約範本較適用於資料傳輸模式及關係較為單純（如企業因資料處理需要，將資料傳輸至專責處理個人資料作業之公司，再將處理完成後之資料傳輸回原來輸出資料之企業），且為二家獨立（即非為關係企業）之企業。

二、申請程序

歐盟委員會雖已針對 BCR 訂定最低要求，惟 BCR 之具體內容仍係由各企業自行訂定，故企業採行 BCR 時，須事先經監理機關之審查，以確保企業 BCR 之訂定符合一定要求且能有效落實，至於標準契約範本，因範本條款內容固定，且不得任意變更，故企業自得自行使用。

三、法律效果

標準契約範本為性質特殊之商業契約，雙方於契約簽訂後，即受契約之法律拘束力。至於 BCR，因其性質為企業之內部規章，故原則上僅發生對內部之效力（僅能拘束內部之員工），對外之法律效力則將受到各國不同法令之影響。

四、條款內容之差異

BCR 規範重點在於 BCR 之訂定應能於企業內部有效落實，以確保集團內部個人資料傳輸之安全、當事人申訴案件能被適當處理，並定期透過內部稽核之查核，瞭解資料保護安全措施及爭議處理機制之落實情形，BCR 之內容並不涉及資料輸出者或接收者各自應負之資料保護責任、當事人損害賠償之責任分攤或資料傳輸終止後資料接收者之義務。標準契約範本及 BCR 之差異彙整如下：

項目	標準契約範本	BCR
適用對象	二個獨立之 法律個體	跨國企業之分支機構（含分公司、子公司）及關係企業
適用範圍	契約雙方	申請時，納入 BCR 之集團內企業名單
是否須經監理機關事先核准	否	是
法律效力	拘束契約雙方 （外部法律效力）	拘束集團內部成員
條款內容	資料傳輸者及 接收者之契約義務	未明確區分
	契約雙方對當事人損害賠償義務之區分	未訂
	雙方終止契約之條件	未訂
	資料處理服務終止後 之義務	未訂

資料來源：本研究整理

第五章　我國銀行國際傳輸保護規範

我國憲法雖未將隱私權明文列舉為基本權，惟在憲政實務上，司法院大法官解釋再三肯認「隱私權」為一種受憲法保障之基本權利[137]。依據釋字第 603 號解釋，維護人性尊嚴與尊重人格自由發展，乃民主憲政秩序之核心價值，基於人性尊嚴與個人自主體之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 23 條所保障（釋字第 585 號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障，並非絕對，國家得於符合憲法第 23 條規定意旨之範圍內，以法律明確規定對之予以適當之限制。

隱私權係屬人格權[138]之一種，係攸關個人一己，得拒絕他人知悉所有訊息之總稱。沒有法理上之依據，他人不得刺探，或加以宣揚。隱私權之內涵包括個人出身、健康資料、基因資訊、財務狀況、學經歷、黨籍、思想傾向、宗教信仰、一般私生活、日記之記載等，甚至包括電話號碼及地址等[139]。銀行取得客戶個人資料之性質，除因交易需要取得之個人基本資料外，尚包括與客戶往來過程中之財務交易資料，惟我國有關財務隱私權之保護，並未訂有特殊規範，仍以個人資料保護法（普通法）及銀行法涉及客戶資料保護義務等相關金融法令（特別法）為銀行主要應遵循之規定[140]。

---

137 大法官釋字第 293 號、第 585 號及第 605 號解釋。

138 一般所謂「人格權」，係指以保護個人發展其自我的「個人人格權」。人格發展自由指在保護個人私有之領域免於國家不當侵害。我國民法第 18 條規定，人格權受損害時，得請求損害賠償。依民法第 195 條，人格權包括身體、健康、名譽、自由外，更包括「信用、隱私、貞操、基於父、母、子、女或配偶關係之身分法益或其他人格法益。見李惠宗，憲法要義，5 版第 1 刷，頁 368，2009 年 9 月。

139 同前註，頁 374。

140 2010 年 5 月 26 日公布修正之個人資料保護法，刪除現行第 2 條條文，依其修正說明個人資料保護法之性質應為普通法，其他特別法有關個人資料蒐集或利用之規定，不論較該法規定更為嚴格或寬鬆，依特別法優於普通法之法理，自應優先適用各該特別規定，惟上開立法說明恐將架空個人資料保護法之規定，且不利於我國個人資料保護之推動與落實。

第一節　個人資料保護法

第一項　制訂背景及修正緣由

我國現行個人資料保護之基本規範以 84 年 8 月 11 日公布訂定之「電腦處理個人資料保護法」為主，該法主要規範公務及非公務機關以電腦處理個人資料之行為，包括個人資料之蒐集、處理及利用，惟在該法下之保護客體僅限於經電腦處理之個人資料，並訂有行業別適用之限制規定。

隨著資訊科技及網際網路之快速發展，個人資料被蒐集、處理及利用之情形大幅增加，對個人隱私造成影響，為因應社會發展及迎接個人資料保護全球化時代之來臨，立法院於 99 年 4 月 27 日三讀通過「電腦處理個人資料保護法」修正案，並更名為「個人資料保護法」（以下簡稱新法），新法主要參考 1995 年歐盟指令、德國聯邦個人資料保護法、奧地利聯邦個人資料保護法、日本個人資訊保護法等國之立法例，強化個人資料之揭露、查詢及更正等自主控制，並將「亞太經濟合作論壇（APEC）隱私保護綱領」揭示之預防損害、告知、蒐集限制等原則納入規範，同時令各目的事業主管機關應積極履行其法定監督職責，以確實防止個人資料之外洩[141]。

新法修正重點包括(一)將個人資料之保護客體擴大至所有個人資料（含電腦處理及人工紙本之個人資料），將適用主體擴大至所有法人、團體及個人，並刪除行業別適用之限制規定；(二)為兼顧「個人隱私」與「新聞自由」之平衡，對於大眾傳播業者因於新聞報導之公益目的而蒐集之個人資料，免得告知當事人；(三)臉書、部落格等張貼有他人合影之照片行為，屬於社交活動或家庭生活之目的範圍內，得排除適用個

[141] 依據「個人資料保護法」第 56 條修正說明，由於本次修正涉及擴大適用範圍、民間業者需相當時間調整與準備及相關法規亦需配合增修，包括個人資料保護法施行細則之訂定等，故本次修正後規定之施行日期，將由行政院另定。請參考 2010 年 4 月 27 日法務部新聞稿及「電腦處理個人資料保護法」修正條文對照表。

人資料保護法，回歸民法；(四)提高違反個人資料保護法之民、刑事及行政責任；(五)明定對於醫療、基因、罪犯前科等個人資料（即特種資料或敏感性資料）須在符合法律明文規定之嚴格條件下，始得蒐集、處理及利用；(六)利用個人資料於商品行銷者，應於首次行銷時，提供當事人表示拒絕接受行銷之權利。

第二項　國際傳輸相關規範

由於修正後之個人資料保護法目前尚未正式施行，故以下將分別說明現行適用之「電腦處理個人資料保護法」（舊個資法）及修正後「個人資料保護法」（新個資法）有關國際傳輸個人資料之相關規定。

一、電腦處理個人資料保護法

現行法計分為六章，第一章為總則、第二章為公務機關之資料處理、第三章為非公務機關之資料處理、第四章為損害賠償及其他救濟、第五章為罰則及第六章為附則，其中涉及國際傳遞之規定如下：

（一）公務機關將個人資料之國際傳遞及利用，應依相關法令為之（第 9 條）。

（二）非公務機關未經目的事業主管機關依法登記並發給執照者，不得為個人資料之蒐集、電腦處理或國際傳遞及利用（第 19 條第 1 項）。

（三）非公務機關為國際傳遞及利用個人資料，有下列情形者，目的事業主管機關得為限制之規定，包括涉及國家重大利益者、國際條約或協定有特別規定者、接受國對於個人資料之保護未有完善之法令，致有損當事人權益之虞者，及以迂迴方法向第三國傳遞及利用個人資料規避本法者（第 24 條

[142]）。該條規定主要參考歐洲議會發布之保護個人資料自動化處理公約第三章第 12 條[143]及英國法第 4 條及第 12 條[144]之立法例，考量資訊跨界流通，如有危害公益或私益之情形時，為避免損益當事人之權益，故授權主管機關得酌情限制之[145]。

（四）違反國際傳輸規定之刑罰及行政罰

1、意圖營利違反第 19 條第 1 項或目的事業主管機關依第 24 條所發布之限制命令者，致生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 4 萬元以下罰金(第 33 條)。

2、非公務機關違反第 19 條第 1 項及違反中央目的事業主管機關依第 24 條所發布之限制命令者，得處負責人新臺幣 2 萬元以上，10 萬元以下罰鍰，並令限期改正，逾期未改正者，按次處罰之，情節重大者，並得撤銷依本法所為之許可或登記（第 38 條第 1 項第 2 款、第 4 款及第 2 項）。

---

[142] 電腦處理個人資料保護法第 24 條所謂國家利益，指關於國家安全、外交、國防、重大經濟利益等，惟實際運用時，則依具體情形來認定；接受國對於個人資料的保護未有完善法令，致有損當事人權益之虞者，如 A 國不尊重人權，其對個人資料的保護無完善的法令，故對 A 國為國際傳遞及利用個人資料，我國政府自得予以限制；另以迂迴方法向第三國傳遞及利用個人資料規避本法之規定，如我國非公務機關欲傳遞個人資料至 A 國，但因該國家對個人資料之保護尚無完善之法律，致有損當事人權益之虞，恐遭禁止，非公務機關乃先傳遞至 B 國，再由 B 國傳遞至 A 國等情形。見法務部出版「電腦處理個人資料保護法問答手冊」(上)，第 36 頁。

[143] 依據歐洲議會於 1981 年通過之保護個人資料自動化處理公約第三章「跨國資料傳輸」第 12 條「個人資料跨國傳輸及國內法」規定，當自動化處理或蒐集後以自動化處理之個人資料進行跨國傳輸時，原則上監理機關不得以個人隱私權保護之單一目的，禁止或限制一方將個人資料跨國傳輸至另外一方，除非接受國對於個人資料之保護未有完善之法令或資料傳輸之一方意圖以迂迴方法向第三國（地區）傳輸個人資料以規避上開規定。請參考 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108, Chapter III—Transborder data flow, Article 12, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm（last visited November 16, 2011）。

[144] 依英國 1984 年個人資料保護法第 4 條第 3 項第 E 款規定，若擬將個人資料傳輸至英國以外之國家或地區時，應將該國家或地區之名稱及相關說明向登記處登錄。見經社法規譯介叢書 028「資料保護法」，行政院經濟建設委員會健全社法規工作小組，頁 5-6，1988 年 9 月。

[145] 立法院公報第 84 卷第 46 期院會記錄，1995 年 7 月。

（五）相關解釋函令

電腦處理個人資料保護法發布迄今，法務部針對該法中涉及國際傳輸相關規定發布之解釋函令甚少，僅以下二則：

1、個人資料傳輸至大陸地區是否為國際傳輸

依法務部 94 年 8 月 26 日法律字第 0940029553 號函規定，按非公務機關對個人資料之國際傳遞，依電腦處理個人資料保護法第 19 條第 1 項規定，非經目的事業主管機關登記並發給執照者，不得為之；國際傳遞規定之立法目的係為落實個人資料之保障，避免跨境個人資料流通失控，故就我國政府法律權限未及地域之跨境傳遞予以規範管理。因此，公務或非公務機關將個人資料傳輸至我國法權未及之地域，即屬該法所稱之「國際傳遞」，從而向大陸地區傳輸個人資料，自為該法所定之「國際傳遞」。

2、外國在台分公司將其持有之客戶個人資料傳遞至外國本公司，是否違反電腦處理個人資料保護法

依法務部 90 年 4 月 27 日法律決字第 014746 號函，電腦處理個人資料保護法第 23 條規定：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用：(一)為增進公共利益者。(二)為免除當事人之生命、身體、自由或財產上之急迫危險者。(三)為防止他人權益之重大危害而有必要者。(四)經當事人書面同意者。」又該法第 3 條第 5 款就「利用」乙詞已明文規定，係指公務機關或非公務機關將其保有之個人資料檔案為內部使用或提供當事人以外之第三人。依上開意旨，保險公司將其保有之保戶保險資料提供外國人之本公司（總公司），符合上開第 23 條規定自得為之。

至於非公務機關為個人資料之國際傳遞，依該法第 19 條第 1 項規定，非經目的事業主管機關登記並發給執照者，不得為之，故該公司既已向目的事業主管機關登記並取得執照，依上開規定自得為國際傳遞。

二、個人資料保護法

新法計分為六章，第一章為總則、第二章為公務機關對個人資料之蒐集、處理、及利用、第三章為非公務機關對個人資料之蒐集、處理及利用、第四章為損害賠償及團體訴訟、第五章為罰則及第六章為附則，其中涉及國際傳輸之規定如下：

（一）明定國際傳輸之定義：指將個人資料作跨國（境）之處理或利用。依該款立法說明，國際傳輸之範圍包括機關內部之資料傳送（屬資料處理），如總公司將資料傳送給分公司、公務機關將資料傳送給國外辦處事處，或將資料提供予當事人以外之第三人（屬資料利用），如母公司將資料提供予子公司或他公司、公務機關將資料傳送給他公務機關等情形，均屬之。（第 2 條第 6 款）

（二）非公務機關為國際傳遞及利用個人資料，有下列情形者，中央目的事業主管機關得為限制，包括涉及國家重大利益者、國際條約或協定有特別規定者、接受國對於個人資料之保護未有完善之法令，致有損當事人損益之虞者、以迂迴方法向第三國（地區）傳輸個人資料，以規避該法規定者等四種情形（第 21 條）。

（三）中央目的事業主管機關或直轄市、縣（市）政府為執行國際傳輸限制或其他例行性業務檢查而認有必要或有違反該法規定之虞者，得派員攜帶執行職務證明文件，進入檢查。並

得命相關人員為必要之說明、配合措施或提供相關證明資料（第 22 條第 1 項）。

（四）違反國際傳輸規定之刑罰及行政罰：

1、非公務機關違反中央目的事業主管機關依第 21 條規定，所發布限制國際傳輸之命令或處分，足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。意圖營利犯前項之罪者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金（第 41 條）。

2、非公務機關違反中央目的事業主管機關依第 21 條規定限制國際傳輸之命令或處分者，中央目的事業主管機關得處新臺幣 5 萬元以上，50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之（第 47 條）。

三、新舊法有關國際傳輸規範之差異

無論修法前或修法後我國有關國際傳輸之規定，除增訂國際傳輸之定義（依上開法務部 90 年 4 月 27 日之解釋函令，分公司與母公司間個人資料之傳輸，似尚無國際傳輸規定之適用，惟依新個資法有關「國際傳輸」之定義，已包含機關內部將個人資料作跨境之處理或利用，故在新法下，似已擴大國際傳輸之適用範圍）及加重違反國際傳輸規定之罰則外，並無重大修正。對於非公務機關將個人資料進行國際傳輸，均採原則同意例外限制之立法形式，依修法前之規定及法務部 90 年發布之解釋函令，非公務機關國際傳輸個人資料，於經目的事業主管機關依法登記並發給執照，且傳輸符合特定目的，即可進行傳輸，至於如何確保個人資料傳輸後之安全性，則未有相關規範，對於個人資訊隱私權之保護，似未周全。

另由於新個資法已取消非公務機關行業別之適用限制，修正後規定將適用任何自然人、法人、機構或其他團體，故新個資法已將

現行第 19 條第 1 項有關非公務機關應經目的事業主管機關依該法登記並發給執照，始得為個人資料之蒐集、電腦處理或國際傳輸及利用等規定已予以刪除。在新法下，因非公務機關國際傳輸個人資料已無須再向目的事業主管機關核准，應宜有相關配套措施，以保護當事人個人資料之安全。

第二節　亞太經濟合作會議（APEC）隱私保護綱領

一、共同發展跨國隱私規章

為加強亞太經濟合作會議（Asia-Pacific Economic Cooperation, APEC）之各會員體對於個人資料保護之措施，APEC 於 2004 年 10 月通過「APEC 隱私保護綱領」（APEC Privacy Framework），為落實隱私保護綱領中有關促進各會員體間跨國資料之傳遞，APEC 並於 2007 年起推動「資訊隱私開路者倡議計畫」（APEC Data Privacy Pathfinder Projects），以期經由企業內部建構處理隱私之相關程序及對消費者如何處理其個人資料之承諾，透過產業自治之方式，協助建置可資信賴之跨國資料流通制度[146]。

依據 APEC 隱私保護綱領第四章「執行」第 46 條至第 48 條有關共同發展跨國隱私規章（Cooperative Development of Cross-border Privacy Rules）之規定，各會員經濟體將盡力確保相互承認或接受跨國隱私規章之架構或機制（各會員國應確保核發之隱私規章已遵循 APEC 隱私原則），使其具有法律效力，透過該制度之建立，在對個人隱私有效保護之前提下，促進各會員體間跨國資料之傳遞，避免造成對跨國資訊流通不必要之障礙[147]。

為建立跨國隱私規章，APEC 於 2007 年開始推動「資訊隱私開路

[146] 戴言同，歐盟資訊與通訊科技政策與規範之研究—檢視我國雲端政策之問題，國立雲林科技大學科技法律研究所碩士論文，頁 102-103，2011 年 6 月。
[147] APEC 隱私保護綱領（中英文對照），法務部編印，頁 47-50，2006 年 12 月。

者倡議計畫」,在該計畫下共計分為9項子計畫,由於各員體落實APEC隱私保護綱領之程度不一,目前計有13個會員體[148]選擇加入該推動計畫，其中我國係參與第 2 項及第 9 項子計畫（我國係於 1991 年成為 APEC 之會員體)，該 9 項子計畫可區分如下[149]：

（一）自我評量階段（self-assessment)：計畫 1—建立企業之自我評量準則。

（二）遵循程度之檢視（compliance review)：計畫 2—建立可信賴之標章組織參與跨境隱私保護規章、計畫 3—檢視各組織遵循跨境隱私規章之情況。

（三）認可/接受（recognition/acceptance)：計畫 4—跨境交易爭議解決之組織名單。

（四）爭議解決及執行（dispute resolution and enforcement)：計畫 5—建立各經濟體間負責資料保護之監理機關及其單位負責人之聯絡方式、計畫 6—建立跨境組織間合作之契約或備忘錄之範本、計畫 7—建立處理跨境交易隱私爭議之表單範本、計畫 8—建立各經濟體間有關跨境隱私規章之準則及程序。

（五）最後，計畫 9 為發展跨境隱私保護規章之前導個案（Pilot Project)，以完整落實整個計畫。

二、臺灣個人資料保護與管理制度（TPIPAS）

由於我國亦為 APEC 之會員體之一，為保障民眾個人隱私，並推動跨國隱私保護規章之建立，經濟部商業司於 98 年委託資策會辦理「電子商務個人資料管理制度計畫」,規劃建立「臺灣個人資料保護與

[148] 包括澳洲、加拿大、智利、香港、日本、韓國、墨西哥、紐西蘭、秘魯、台灣、泰國、美國及越南計 13 個國家,自行選擇參與各子計畫之推動。請參考 APEC Data Privacy Pathfinder Projects Implementation Work Plan，頁 4，2008 年 2 月 24 日。

[149] 同前註，頁 3-13。

管理制度」(Taiwan Personal Information Protection and Administration Systems, TPIPAS),藉由協助並輔導企業建構個人資料保護管理制度,並經驗證通過後,由經濟部核發「個人隱私資料保護標章」,並透過推動跨國相互認證,將有助於跨國資料之流通[150]。

TPIPAS 計畫之目標係透過分析國內法制以及電子商務個人資料保護需要,建立完善之電子商務個人資料管理制度,協助產業有效管理個人資料,遵循法規並降低可能之責任風險。該計畫全程自 99 年至 104 年,包括基礎建立階段、深耕擴大階段及全面擴散階段,其中基礎建立階段係自 99 年 9 月至 101 年 6 月,主要工作重點如下:

(一)99 年 9 月至 100 年 6 月:建立個人資料管理制度主體規範、必要文件與推動組織架構、建立隱私標章發放、管考機制及驗證機構資格、管考機制、驗證規則、流程等必要規範、遴選儲備驗證機構、建立專業人才資料、管考等相關資訊,並培訓儲備專業人才與種子人才、個人資料觀念宣導、認知調查與管理制度宣導說明。

(二) 100 年 7 月至 101 年 6 月:進行實際試行推廣,就試行結果進行制度調整與完備、推行組織運作及制度細部規範研議及加強驗證機構、導入企業輔導與人才訓練,鞏固全面推行基礎。

依上開推動計畫,101 年為試辦階段,初期原則上將以經濟部商業司主管之電子商務業者為試辦對象,至於金融業及醫療業,因各有其目的事業主管機關,礙於產業差異性之緣故,故暫不列入範圍[151]。

第三節　銀行法及相關金融法規

相對於英國設有獨立之「資訊自由及保護委員會」(ICO),作為推動個

[150] 我國推動 TPIPAS 之計畫,請參考網址:www.tpipas.org.tw 網頁相關資訊。
[151] 廖珮君,資安人科技網,2011 年 4 月 11 日,網址:www.isecutech.com.tw。

人資料保護之專責機關，我國個人資料保護之主管機關，依個人資料保護法第 22 條立法說明，基於落實個人資料隱私權益，自宜設立專責機關為主管機關，但未設立專責機關前，由於各行業均有目的事業主管機關，有屬中央者，有屬地方者，而個人資料之蒐集、處理或利用，與該事業之經營關係密切，應屬該事業之附屬業務，自宜由原各該主管機關，一併監督管理與其業務相關之個人資料保護事項，較為妥適。

依據上開立法意旨，有關銀行對個人資料保護之監督，在我國未有個人資料保護之專責機關前，應以金管會為銀行個人資料保護之主管機關。現行金融相關法令中，有關個人資料之蒐集、保密及利用已訂有相關規定，就其規範內容，似呈現金融監理機關二種政策思維之對立[152]，一則是金融機構營業自由、營運成本及經營風險之考量，二則是對於個人隱私之尊重，如何調和私益與公益之衝突，並在個人資料服務與金融服務效率間取得平衡，為財務隱私權保護之核心課題[153]。另鑒於國際洗錢、金融詐騙及恐怖主義保護攻擊之出現，各國金融法制亦透過立法手段，調整財務隱私權之保護政策。

為保護客戶之個人資料及交易往來之相關資料，我國銀行法及金融控股公司法參酌國外立法例，分別訂有從業人員之保密義務，其保密對象包括為客戶利益應保密之事實 (如商業機密) 及帳戶之金錢往來資料(如帳目、帳冊)等。另為維護社會公益，並兼顧個人隱私權之保護，現行金融法令並設有相關義務免除之規定如下：

一、 銀行法第 48 條第 2 項規定，銀行對於客戶之存款、放款或匯款等有關資料，除法律或主管機關另有規定、一定金額以上之大額轉銷呆帳客戶資料及經檢察官提起之公訴案件外，應保守秘密。

[152]為降低金融業者之遵循成本，金管會建議法務部在「個人資料保護法施行細則」草案中訂定，在個資法通過之前業者已經取得的舊有客戶資料，可利用網際網路、新聞媒體「公告」方式，告知個人，以取代一一告知本人且經同意的方式。對此作法，消基會董事長蘇錦霞表示，這種規定如果成真，將違反母法，讓上千萬消費者的權益受損。見 2011 年 3 月 17 日工商時報第 17 版報導。

[153] 王志誠，同註 3，頁 252。

二、 金融控股公司法第 42 條第 1 項規定，金融控股公司及其子公司對於客戶個人資料、往來交易資料及其他相關資料，除其他法律或主管機關另有規定者外，應保守秘密。

三、 政府機關向金融機構要求提供客戶資料，對於司法、軍法、稅務、監察、審計及其他依法律規定具有調查權之機關，若為行使調查權或因辦理業務或偵辦案件之需要，得依規定之一定程序，正式備文，向相關銀行查詢客戶存、放款、保管箱等有關資料為銀行法第 48 條第 2 項有關銀行保密義務排除之規定。

第一項　銀行保密義務

參照大法官釋字第 293 號解釋「銀行法第 48 條第 2 項規定『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權」。可認為銀行保密義務係屬於我國憲法第 22 條所定之基本權利，並應受憲法第 23 條法律保留原則之限制。在法律保留原則下，國家立法干預銀行秘密，原則上應受憲法禁止過當之限制，並應維持對公益為合乎事理及理性之公平衡量[154]。

銀行對於客戶資料之保密義務，最早訂於 78 年 7 月 17 日修正公布之銀行法第 48 條第 2 項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守祕密」，該規定係參考當時如德國、新加坡及香港等外國立法例，其保密對象包括為客戶利益應保密之事實（如商業機密），帳戶之金錢往來資料（如帳目、帳冊）。至於銀行保密義務之豁免規定，因涉及人民之隱私權，長期而言，不宜僅以行政命令訂定，故銀行法於 97 年 12 月 30 日修正時，將當時已發布客戶資料不在銀行保密義務範圍之例外規

[154] 蕭長瑞，同註 97，頁 160。

定，明定於銀行法第 48 條第 2 項之各款，現行銀行對於客戶之存款、放款或匯款等有關資料，得排除適用保密義務之情形如下：

一、法律另有規定。

二、對同一客戶逾期債權已轉銷呆帳者，累計轉銷呆帳金額超過新臺幣五千萬元，或貸放後半年內發生逾期累計轉銷呆帳金額達新臺幣三千萬元以上，其轉銷呆帳資料。

三、依銀行法第 125 條之 2、第 125 條之 3 或第 127 條之 1 規定，經檢察官提起公訴之案件，與其有關之逾期放款或催收款資料。

四、其他經主管機關規定之情形。

上開第 2 款及第 3 款之訂定，係考量銀行資金來自於存款大眾，呆帳之產生，或可能涉及人謀不臧，有害於公眾利益，為維護社會公益，並兼顧個人隱私權之保護，對於大額、短期發生逾期之轉銷呆帳資料，及涉及詐害銀行債權或違法放款情事者，經檢察官提起公訴案件之逾期放款及催收款資料，因與公眾利益相關，故明定上開客戶資料不在銀行保密義務之範圍。

至於銀行違反銀行法第 48 條第 2 項銀行保密義務時之罰則，依銀行法第 129 條規定，違反該法第 48 條規定者，處新臺幣二百萬元以上，一千萬元以下罰鍰。

第二項　委外或非委外事項之國際傳輸

銀行將客戶資料國際傳輸之需求，可分為委外及非委外事項，其中銀行為節省內部作業成本，故將資料委外處理或集中存儲於提供資料處理服務之供應商（即作業委外），至於非委外事項，則係國際性銀行為彙整及統一授信額度與風險管理之需要，故要求設立於全球各地之分子行，將客戶資料統一傳輸至母行或集團中負責彙整資料之單位等。惟無論客戶資料係委外或非委外事項之國際傳輸，若傳輸之資料為個人資

料，應即屬國際傳輸之範疇。

一、委外事項

銀行將作業委外，初期係為節省成本，故將列印及資料儲存等作業予以委外，其後隨著資訊技術之發展，有關資訊服務之委外愈趨普遍。近期更有將內部作業境外委外（off-shoring，即跨越國境之作業委外）之趨勢，許多大型企業集團透過在境外進行交易之處理（資料處理中心）及設立客服中心（call centers），以創造全球化之效率。境外委外相對於一般委外作業，其主要風險在於須注意委外契約之效力將可能受到委外機構所在國政府政策及該國政治、社會及經濟環境與法律制度之影響[155]。

（一）立法背景

我國銀行得否將完成業務交易具重要性之作業流程予以委外，在我國銀行法尚未明文規定前，金管會已依職權訂有「銀行作業委外之應注意事項」作為金融監理規範，94 年 5 月 18 日銀行法修正後，增訂銀行法第 45 條之 1 第 3 項規定「銀行作業委託他人處理者，其對於委託事項範圍、客戶權益保障、風險管理及內部控制原則，應訂定內部作業制度及程序；其辦法，由主管機關定之。」

依據銀行法之授權，金管會於 95 年 9 月 18 日參酌國外立法例、邇來外界關切重點、消保團體建議及目前金融機構實務運作，制定發布「金融機構作業委託他人處理內部作業制度及程序辦法」（下稱金融機構委外作業辦法）。為強化對金融機構作業跨境委外之規範，並配合民法等法令之修正，金管會於 100 年 12 月 8 日公告金融機構委外作業辦法修正草案，其中針對境外委外部分之修正重點包括增訂金融機構申請作業跨境委外應檢附之

[155] 同前註，頁 123-124。

書件內容[156]、訂定將作業項目委託至境外時，應遵守之規定[157]、明定本國銀行不得將消費金融相關資訊系統之資料登錄、處理、輸出等事項委託至境外處理、增訂本國銀行於該辦法修正施行前，不符修正規定者，應自該辦法修正施行後 4 年內調整至符合規定。金融機構委外作業辦法修正草案預告期間已結束，但尚未正式對外發布施行[158]，故以下仍就現行規定予以說明。

（二）規範重點

依據金融機構委外作業辦法第 3 條及第 4 條規定，銀行得將內部作業委外之事項計有 20 項，其中除信用卡發卡業務及車輛貸款以外之消費性貸款之行銷作業、應收債權催收作業等之委外，應事先報經主管機關核准辦理外，其餘委外事項銀行應在不影響健全經營、客戶權益及相關法令之原則下，依董事會核准之委外內部作業規範辦理。依金融機構委外作業辦法，銀行將作業委外應遵循之規定如下：

1、一般規定：

(1)銀行針對委外事項，應訂有內部委外作業規範，內容包括

[156] 依據金融機構委外作業辦法修正草案第 18 條規定，金融機構應檢具下列書件向主管機關申請核准後，始得將作業項目委託至境外處理，包括受託地金融主管機關書面確認文件、委外內部作業規範、董事會決議錄、委外對營運之必要性及適法性分析、客戶資訊保護措施、外國銀行在台分行應取得總行出具有關資料取用、安全控管及配合我國監理要求之承諾書，至於金融機構若無法取得受託地金融主管機關之書面確認文件時，則受委託機構應出具同意金融機構及我國監理機關指定之人對受託事項進行查核之同意函、受委託機構之內部控制制度及相關作業程序之審查情形、律師出具受託地對客戶資訊之保護相當於我國之意見書、受委託機構最近期經會計師查核簽證之財務報告、受委託機構出具近 3 年未發生人員舞弊及資通安全事件之聲明書等。

[157] 依據金融機構委外作業辦法修正草案第 19 條規定，金融機構將作業項目委託至境外處理者，應依下列規定辦理：一、金融機構應充分瞭解及掌握受委託機構對客戶資訊之使用、處理及控管情形；二、金融機構提供予受委託機構之客戶資訊僅限與受託事項直接相關之必要資訊；三、金融機構應要求受委託機構確實遵守以下事項：(一)金融機構之客戶資訊僅限由受委託機構之獲授權人員於受託事項範圍內使用及處理；(二)金融機構之客戶資訊應與受委託機構及其處理他機構之資料有明確區隔；(三)受託機構處理之客戶資訊應能及時提供予主管機關及金融機構；四、金融機構應定期及不定期就受委託機構對客戶資訊之使用、處理及控管情形進行查核及監督。

[158] 為強化對金融機構作業跨境委外之規範，並配合民法等法令之修正，金管會於 101 年 1 月 19 日第 390 次委員會議決議通過修正「金融機構作業委託他人處理內部作業制度及程序辦法」，將於近日發布實施。資料來源：金管會銀行局 101 年 1 月 19 日新聞稿。

指定專責單位及其職權規範、委外事項範圍、客戶權益保障之內部作業及程序、風險管理原則及作業程序、內部控制原則及作業程序、其他委外作業事項及程序。(第 4 條)

(2)有關客戶權益保障之內部作業及程序，應包括：(第 7 條)

A.作業委外涉及客戶資訊者，應於契約簽訂時訂定告知客戶之條款；其未訂有告知條款者，銀行應書面通知客戶委外事項，並明定客戶於接獲銀行通知未於一定合理期間以書面表示反對者，視為同意。

B.客戶資訊提供之條件範圍及其移轉之程序方法。

C.對受委託機構使用、處理、控管客戶資訊之監督方法。

D.銀行作業委外應訂定客戶糾紛處理程序及時限，並設置協調處理單位，受理客戶之申訴。

E.其他客戶權益保障之必要措施。

F.另銀行將作業委外時，若因受委託機構或其受僱人員之故意或過失致客戶權益受損，仍應對客戶依法負同一責任。

(3) 銀行作業委外契約應載明之事項：(第 10 條)

A.委外事項範圍及受委託機構之權責。

B.銀行應要求受委託機構配合遵守第 19 條規定[159]。

C.消費者權益保障，包括客戶資料保密及安全措施。

D.受委託機構應依銀行訂定之標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度。

E.消費者爭端解決機制，包括解決時程、程序及補救措施。

[159] 依金融機構委外作業辦法第 19 條規定，金融機構作業委外不得違反法令強制或禁止規定、公共秩序及善良風俗，對經營、管理及客戶權益，不得有不利之影響，並應確保遵循銀行法、洗錢防制法、電腦處理個人資料保護法、消費者保護法及其他法令之規定。金融機構辦理作業委外應確實遵守相關法令及中華民國銀行商業同業公會全國聯合會訂定之相關業務規章或自律公約及中華民國信用合作社聯合社發布之相關規定。

F.受委託機構聘僱人員之管理，包括人員晉用、考核及處分等情事。

G.與受委託機構終止委外契約之重大事由，包括主管機關通知依契約終止或解約之條款。

H.受委託機構就受託事項範圍，同意主管機關及中央銀行得取得相關資料或報告，及進行金融檢查，或得命令其於限期內提供相關資料或報告。

I.受委託機構對外不得以銀行名義辦理受託處理事項，亦不得進行不實廣告或於辦理貸款行銷作業時向客戶收取任何費用。

J.其他約定事項。

銀行應於契約中要求受委託機構非經銀行書面同意，不得將作業複委託。委外契約中應針對複委託情形，訂明複委託之範圍、限制或條件。複委託契約應準用第 10 條規定訂定之。

(4)銀行將作業委外，主管機關及中央銀行得取得相關資料或報告，並進行金融檢查。（第 20 條）

2、境外委外

金融機構委外作業辦法於 95 年制訂時，鑒於目前金融機構實務上確有將部分作業委託其海外總機構、分支機構或其他海外機構辦理之情形，基於金融監理及確保客戶權益之考量，並參酌以往金管會核准銀行作業委託至海外申請案核准函之加註條件，另考量我國尚未正式與其他國家簽署合作備忘錄（MOU），就外交關係及金融合作監理，確有其實務執行上之困難[160]。為確

[160] 見 1996 年 9 月 18 日訂定公布「金融機構作業委託他人處理內部作業制度及程序辦法」第 18 條立法意旨。

立我國監理權限並兼具考量銀行業務發展之需要，金融機構委外作業辦法第 18 條訂有銀行境外委外之相關規定如下：

(1)銀行之境外委外，應事先確認下列事項並報經主管機關核准辦理：

A.銀行應取得國外主管機關同意監理合作之同意函，其內容應包括該主管機關知悉並同意受委託機構執行受託事項、允許我國主管機關及委託之銀行得對受託事項進行必要之查核，以及該主管機關如有必要對受託事項進行查核時，應事先通知我國主管機關。

B.銀行應說明客戶資料保護措施及是否已取得客戶同意，以確保委外服務品質及客戶權益。

(2)銀行如無法取得前項國外主管機關之同意函者，應事先確認取得受委託機構出具之同意函，同意必要時得由銀行指定之人（例如會計師、律師等），對受託事項進行查核。上開指定之人亦得由我國主管機關指派之，其費用由銀行負擔。

（三）罰則

依據銀行法第 129 條第 1 項第 7 款之規定，銀行未依銀行法第 45 條之 1 規定辦理或未確實執行者（即金融機構委外作業辦法之授權依據），處新臺幣二百萬元以上一千萬元以下罰鍰。

三、非委外事項

（一）銀行因非委外事項，將客戶資料國際傳輸予母行之情形，包括為遵循母國之法律規定（如母國為課稅需要）、因客戶之授信額度已超逾國外分子行之授信權限，故需將客戶授信等相關資料傳輸至母行，以取得授信額度、以及母行為進行客戶授信管理及風險控管需要，故需將客戶資料統一集中彙整及

分析。

（二）信用資料之國際傳輸

1、背景

財團法人金融聯合徵信中心（下稱聯徵中心）為我國信用報告之查詢機構，該中心目前僅有金融相關事業[161]始得加入成為會員機構，參與信用資料之交換及利用，其營運特徵係兼具歐陸公共信用登記制度及日本會員制性質之封閉式信用資訊機構[162、163]。我國於 98 年 11 月與大陸地區簽署「海峽兩岸銀行業監理合作備忘錄（MOU）」後，陸續引發陸資銀行來台後成為聯徵中心會員，得否將其查詢臺灣客戶之資料跨境傳輸至大陸地區等疑義。

為防止會員機構將自聯徵中心查得之信用資訊作違法或不當之國際傳輸，聯徵中心於 99 年 6 月 4 日依據金管會 99 年 4 月 21 日之來函，發布信用資料進行國際傳輸之作業機制及控管措施等相關規範。

2、規範重點

（1）會員機構依據電腦處理個人資料保護法第 20 條第 1 項第

[161] 截至 2011 年 7 月 9 日止，聯徵中心之會員機構計有 424 家，包括 38 家本國銀行、19 家外銀在台分行、8 家票券金融公司、2 家證券金融公司、25 家信用合作社、25 家漁會信用部、277 家農會信用部、18 家人壽保險公司、2 家產物保險公司及其他金融機構計 10 家（包括信用卡公司、中華郵政、中小企業信用保證基金等），資料來源：聯徵中心網站資料。

[162] 賴敏慈，信用資訊與隱私權保護--由信用資訊之揭露與隱私權之衝突檢討個人信用資料保護法制，中原大學財經法律研究所碩士論文，頁 94，2005 年。

[163]英國信用報告機構（Credit Reference Agency, CRA）成立歷史約 30 年，其營運係以商業徵信公司為基礎之信用資訊管理模式（即民營模式），獨立於政府及金融機構之外，其資訊來源廣泛，且得為市場中所有主體提供信用調查服務債權人對於信用報告機構所提供信用資料之使用，則係自 15 年前開始。在信用報告機構成立之前，消費者若向金融機構借款，則須自行向債權人證明其信用狀況及還款能力。英國目前主要有 3 家信用報告機構（CRA），包括 Callcredit、Equifax 及 Experian，這些機構持有大部分成年人之特定資訊，稱為信用報告檔案或信用報告。信用報告機構有關個人信用資料之來源主要來自於債權人、選舉人名冊（透過選舉人名冊以確定或證明該信用資料之所有人是否仍存在）及其他來源—Credit explained leaflet，available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/credit_explained_leaflet_2005.pdf，（last visited November, 2011）。

9 款規定，經目的事業主管機關核准登記許可國際傳輸資料者，如傳遞資料範圍或資料蒐集方法包括經由聯徵中心查詢或蒐集之資料時，會員機構在合於授信管理目的之必要範圍及經當事人書面同意，並於內部「信用資料查詢作業控管要點」相關規範，增訂國際傳輸客戶資料相關作業之控管機制，並報經該中心同意備查後，始得進行國際傳輸客戶資料之相關作業。

（2）會員機構內部之控管要點應訂有下列事項：

A.因授信管理目的，需將客戶資料傳輸至國外總行之必要情形（如母國總機構規範其海外分行授信業務審核權限達一定金額，或對於發生授信異常、呆帳或舞弊等案件時，應通報總行或母國監理機關之內部控制或授信審查程序）。

B.傳送時，需經單位主管核定後始得為之。

C.應設簿登記所傳輸之傳送對象、傳送時間、傳遞項目（傳送內容）、傳遞目的、傳輸方式（所使用之傳輸設備）及傳送地點（目的地）等傳送記錄；相關資訊及當事人同意為國際傳輸資料之同意書，相關傳輸記錄自傳送日起保留 5 年，且於該中心要求時提供之。

（3）上開所稱「傳遞項目」以自該中心查得之資料中引述之部分內容（如授信總餘額等）為限，不得將該中心原始資料全部傳遞，另執行國際傳遞單位，應依該中心規定及內部之控管要點，定期查核內部相關作業之執行情形。

第三項　金融監理實務

無論銀行因內部作業委外或因非委外事項而有必要將客戶資料傳輸至境外之委外服務供應商或國外之母行或分子行，若客戶資料涉及個人資料，則銀行將該等資料國際傳輸時，應同時遵循銀行法及電腦處理

個人資料保護法之相關規定。依電腦處理個人資料保護法第 19 條規定，非公務機關未經目的事業主管機關依該法登記並發給執照者，不得為個人資料之國際傳輸，故以往銀行若有將個人資料進行國際傳輸之需求時，均依該法規定向目的事業主管機關（即金管會）申請登記並發給執照，若國際傳輸同時涉及內部作業之委外時，並應依金融機構作業委外之相關規定辦理。

銀行依電腦處理個人資料保護法相關規定向金管會申請登記國際傳輸個人資料之直接收受者時，除應說明其國際傳輸是否為委外作業外，並應提供資料收受者之名稱及地址、國際傳輸之目的、傳輸資料之內容、傳輸是否符合電腦處理個人資料保護法下之特定目的、當事人是否同意及國際傳輸作業原則等相關資料，包括作業流程控管、保密措施（如銀行是否與資料收受者簽訂跨國之資料保護契約及服務契約、資料收受者對於預防資料遭毀損、洩漏、變造等管理措施等）、員工訓練與資訊運用之控管，暨相關法律責任之管轄權歸屬等書面資料。金管會於審核銀行申請國際傳輸時，係就銀行國際傳輸之合理性及必要性、資料收受者之基本背景（係集團內之公司，如母行、其他分子行或集團內負責處理個人資料之作業服務中心，亦或為非集團內之企業等），暨銀行相關控管作業等事項進行瞭解，以評估銀行將個人資料國際傳輸相關作業之妥適性。

金管會對於銀行國際傳遞個人資料申請案之核准函，除加註銀行與國際傳遞個人資料之直接收受者應共同遵循銀行法、電腦處理個人資料保護法及金融機構作業委託他人處理內部作業制度及程序辦法等相關規定，且應維護主管機關對資料之查核權限外，銀行並應落實內部控制及內部稽核作業，以確保資料保管須有嚴密之控管程序，非經授權人員不得隨意存取、使用資料外。委外及非委外事項之個人資料國際傳遞，原則均須事先取得客戶之同意，對於委外事項之國際傳遞，亦僅限於資

料處理，不得有資料運用情事[164]。

第四節　我國規定與英國規定之比較

在分別檢視我國及英國有關國際傳輸個人資料之保護規範後，以下分別就兩國有關個人資料保護之立法形式、國際傳輸之保護規範及銀行業跨國傳輸客戶個人資料之規定，比較說明如下：

一、法律位階及立法形式

英國及我國有關個人資料保護之立法形式，採統一訂定之資料保護法律（英國為 1998 年資料保護法；我國為個人資料保護法）。此種立法形式之優點在於可涵蓋所有關於個人資料之保護規範，缺點則為可能無法詳細規範處理特殊領域所面臨之資料保護議題[165]。雖我國新個資法於立法說明，將個人資料保護法之性質定位為普通法，即若其他法律對個人資料之蒐集或利用，有特殊規定者，無論較個人資料保護法為寬鬆或嚴格，依特別法優於普通法之法理，均優先適用其他法律之規定，惟法務部之上開立法說明恐有架構我國個人資料保護法之情形，且不利於我國對於個人資料保護之推動及落實。至於英國資料保護法，由於該法係屬個人資料保護之專責法律，當其他法律訂有涉及個人資料隱私權議題之相關規定時，若有違反資料保護法之規定，則將被視為牴觸資料保護法，而無效（英國資料保護法非屬普通法之法律位階）。因此，英國之

[164] 依據金管會銀行局於網站公告近期經核准國際傳遞個人資料之銀行，包括 1998 年 9 月 12 日核准花旗銀行新增「國際傳遞個人資料」之直接收受者，包括 Citibank N.A. Singapore、Citigroup Transactions Services（Malaysia）Sdn Bhd CTSM、ASPAC Capital Markets Regional Processing Centre, Citibank Pty Limited、Citibank N.A. Regional Operating Headquarter, Philippine、Citibank N.A. New York、Global eXchange Services Inc.、Citicorp Global Services Ltd、CheetahMail, Inc、Asia Pacific Regional Product Control Group, Citibank Pty Limited 等位於新加坡、馬來西亞、菲律賓、美國紐約等國家之 9 家公司、渣打銀行於 2008 年 9 月 8 日經核准於金融業電腦處理個人資料新增「國際傳遞個人資料之直接收受者」，包括 Electronic Data System Corporation, Plano, Texas, U.S.A.總公司及其全球子公司、分公司（包括但不限於 Electronic Data System Int'l Ltd.英國分公司、Electronic Data System Int'l Ltd.美國分公司、EDS International（S）Pte Ltd.新加坡分公司）、海外匯款往來銀行、國際商業機器股份有限公司（IBM Corporation）美國總公司及其全球子公司、分公司（包括但不限於，台灣國際商業機器股份有限公司）、財團法人金融聯合徵信中心及其他類似徵信機構及其他金融機構依法收受者、美國運通銀行總行及其他分行。

[165] 陳妍沂，同註 33，頁 185-186。

金融監理機關僅得在不牴觸資料保護法之原則下，針對金融服務業訂定額外之資料保護規範。

由於我國個人資料保護法並未針對特定產業考量其行業特性，訂定相關特殊規範，故其他各業別之目的事業主管機關仍應針對主管業別之行業特性在兼顧受監理機構營運需求與個人資訊隱私權保護下，另訂更進一步之資料保護規範。

英國在上開立法架構下（歐盟各國亦同），對於個人資料之保護設有專責機關（ICO）負責資料保護法令之推動、落實及解釋，即使有關金融服務業之個人資訊隱私等相關法令，若涉及資料保護，在英國仍應以 ICO 之見解為主要依據。至於我國個人資料保護法之主管機關雖為法務部，惟法務部主要為溝通聯繫之機關，並非資料保護之專責機關，故有關各行業別之個人資料保護事項，在未設立專責機關之前，仍應回歸各行業之目的事業主管機關，由各該機關一併監理管理與其業務相關之個人資料保護事宜[166]。

二、國際傳輸之保護規範

（一）我國已將國際傳輸規範納入個人資料保護法予以明文規定

英國資料保護法係於附錄一訂定國際傳輸之相關規定，雖該法第 4 條已明定資料管理者對於個人資料之蒐集、處理及利用，均不得違反該法附錄一之資料保護原則。另英國專責資料保護之監理機關（ICO）亦已針對附錄一原則八之國際傳輸原則發布相關之國際傳輸指引，供企業使用，故英國個人資料之國際傳輸在配合歐盟指令之規範下，對於維護個人資料之安全，已有一定程度之規範及保障。惟歐盟委員會之研究報告仍批評，英國未將國際傳輸個人資料訂於資料保護法之本文，應為改善。

我國現行國際傳輸之規範係參考 1981 年歐洲議會之保護個

[166] 參閱 99 年 5 月 26 日修正公布「個人資料保護法」第 22 條立法說明。

人資料自動化處理公約及英國 1984 年資料保護法之相關規定，訂定於電腦處理個人資料保護法之本文。惟現行條文僅規範在所列四項情況下，目的事業主管機關得對非公務機關發出國際傳輸之限制，故我國對於非公務機關國際傳輸之監理，仍須透過目的事業主管機關之事前審查，以保障當事人之資訊隱私權及其個人資料國際傳輸之安全。

（二）我國有關國際傳輸規範之立法形式，課予非公務機關國際傳輸之責任較為不足

電腦處理個人資料保護法於修法後，配合該法已刪除行業別適用之限制，故在新個資法下，亦已刪除非公務機關須經目的事業主管機關登記並發給執照，始得進行個人資料之蒐集、處理及利用（含國際傳輸）之規定。修法後，由於企業進行國際傳輸已無需再向其目的事業主管機關提出申請，故各目的事業主管機關除另有規定外，未來似難以知悉並評估企業是否有將個人資料進行國際傳輸及其傳輸行為是否有限制傳輸之必要。為保護當事人之權利，新法在刪除上開規定後，宜有相關配套措施，以監理非公務機關國際傳輸之行為。

依據英國資料保護原則八之規定，個人資料除該處理個人資料之國家或地區，對於當事人之個人自由與權利已有適當程度之保護外，禁止傳輸至「歐洲經濟區」以外之國家或地區。故英國國際傳輸之規範係採原則禁止例外情形同意之立法形式，僅在第三國家之個人資料保護法制符合適當程度或有附錄四之例外情形時，始得傳輸。相對我國個人資料保護法第 21 條規定，中央目的事業主管機關僅在非公務機關有所列四項情形時，始得限制其國際傳輸，故我國有關國際傳輸之規範係採原則同意例外禁止之立法形式（原則不禁止傳輸）。在英國之立法形式下，由於非公務機

關應自行檢視確定其國際傳輸已符合所訂例外情形之時，始得傳輸，可提高非公務機關對於國際傳輸之法定責任，為強化非公務機關對於國際傳輸之重視，我國個人資料保護法有關國際傳輸之規定，建議可參考英國或歐盟之立法形式，以加強國際傳輸對當事人資訊隱私權之保護。

（三）對於國際傳輸英國已提供較詳細明確之規範，供企業遵循

就當事人權益之保護及資料管理者之資料保護義務而言，英國資料保護原則八之規定較我國規定更為嚴謹，英國企業除符合附錄四之豁免規定外，得將個人資料傳輸至第三國家，僅限該特定第三國家（資料接收國）已有適當之資料保護法制，故企業於國際傳輸前，至少應查詢該第三國家是否已取得歐盟委員會之認可，或自行評估該第三國家是否已有適當之資料保護法制。相對於我國個人資料保護法，則並未實質課予企業應評估資料接收國是否有完善之資料保護法制。

（四）英國對於如何評估其他國家資料保護法制已提供相關指引，供企業使用

英國資料保護法及我國個人資料保護法雖同樣訂有資料接收國對於個人資料之保護是否有完善法規之規定，惟英國資料保護法已於附錄一第二部分針對第三國家之資料保護法制是否符合適當程度訂定基本評估原則，至於我國則未對如何評估接收國之資料保護法制訂定相關規定，故各中央目的事業主管機關應如何評估其他國家之資料保護法制及如何依據該款規定限制非公務機關進行國際傳輸，似有其實務困難，且在未有一致評估原則之情況下，亦可能產生非公務機關與各目的事業主管機關評估標準不一，甚或未進行評估之情形。

（四）歐盟對於企業採用契約模式或自訂內部規章將個人資料國際

傳輸已訂定明確之規定

英國參照歐盟指令規定，針對國際傳輸若企業無法自行評估第三國家之資料保護法制或第三國家未有適當之資料保護法制時，為避免企業因營運所需，仍有將個人資料進行國際傳輸之必要，故發布企業得選擇採用標準契約範本或 BCR 之相關規定，賦予資料輸出者及接收者對於所傳輸個人資料之相關責任及義務，俾於資料傳輸之同時，亦能確保個人資料之安全，並透過條款之訂定，以維護當事人之權益。至於我國個人資料保護法，則未有相關規定。

三、銀行業跨國傳輸客戶個人資料之規範

（一）銀行對於客戶資料因契約關係負有保密義務

在財務資訊隱私權之保護規範方面，英國銀行對客戶資料之保密義務係基於契約關係，故英國相關金融法令包括金融服務與市場法，並未訂定銀行對客戶資料之保密責任，僅訂有金融監理機關因職務所需取得銀行或其客戶個人資料之保密義務。至於我國則相反，係於銀行法明定銀行對客戶資料之保密義務，至於金融監理機關因監理需要取得銀行客戶之個人資料時之保密義務，則未予以規範。

至於銀行國際傳輸個人資料方面，英國與我國相同，在相關金融法令並未針對銀行國際傳輸另訂特殊規範，而僅於銀行辦理內部作業之境外委外時，訂定額外應遵循之規定。

（二）英國 FSA 對於境外委外之規範較為完整

英國 FSA 針對銀行將內部作業委外（含境外委外），已於審慎監理手冊訂定「委外」之相關規範與限制，其中對於境外委外並訂定應額外遵循之規範，以使英國 FSA 對委外服務供應商在銀行委外之服務範圍內能進行有效監理。至於我國有關銀行作業委

外之相關規定亦同，分別訂有一般委外及境外委外應遵循之規定。有關一般內部作業事項之委外（不含債權催收及信用卡發卡業務等），銀行僅須依據一定程序即得自行委外辦理，惟若涉及境外委外，則無論委外作業之性質為何，由於境外委外事涉跨國監理權限等問題，故英國 FSA 與我國金融監理機關均要求銀行須事先經監理機關之核准。

我國金融機構委外作業辦法，對於金融機構境外委外，除規定須經監理機關事先之核准外，僅要求金融機構事先取得委外當地國主管機關同意監理合作之同意函，若無法取得同意函，則需取得受委託機構同意必要時銀行或我國主管機關得指定一定之人，至當地對受託事項進行查核之同意函，另銀行應說明客戶資料之保護措施及是否已取得客戶同意之相關資訊。現行規定為確立本國監理機關之監理權限，故已就境外委外訂定相關規定，惟尚未就銀行境外委外可能產生之特殊問題（如需考量當地國法律規範對委外作業之影響等），訂定相關規定。

英國 FSA 於銀行境外委外之規範（英國銀行之境外委外規範與資料法保護法有關國際傳輸之適用對象相同，僅適用於銀行將內部作業委外至非歐洲經濟區之第三國家），係分別就該委外服務供應商於當地國有無受適當機關之監理及 FSA 與當地監理機關有無簽訂監理合作協議訂定不同之規定，並已明訂銀行申請境外委外時之標準程序及應檢附之文件。

當該委外服務供應商於當地國並未受特定機關之監理時，FSA 要求銀行應能於委託範圍內對委外服務供應商進行檢查、銀行應向 FSA 說明受委託者有能力履行委外契約之要求（包括對於因受託服務所取得資訊之保護及保密措施等）、其財務狀況是否良好（應定期取得受委託者經會計師查核簽證之財務報告）、當

地國之相關法律規定是否會重大影響該委外作業之執行及有無複委託之情形等。若 FSA 與當地監理機關並未簽訂監理合作之協議時，FSA 要求銀行應確保經由委外契約，提供使 FSA 能進行有效監理之委外相關資訊（包括該受委託者於英國境內設有分支機構時之相關資訊）及在委外契約下，FSA 得直接要求該受委託者提供相關資訊之權利，故銀行向 FSA 申請境外委外時，尚須檢附預擬之委外契約內容。英國及我國銀行境外委外規範差異如下：

項目	英國規定	我國規定
取得監理機關之同意	是	是
是否針對境外委外訂定申請程序及應檢附文件	是，包括銀行自行說明委外供應商是否符合委外之相關標準（含是否符合審慎監理手冊第 8.3 章之規定）、當地監理機關之聯絡方式、銀行承諾對於境外委外產生之損失，應負損害賠償之責、預擬契約內容等。	否
與委外服務供應商當地國之監理機關簽訂監理合作協議	由 FSA 與當地國之監理機關簽訂。	由銀行取得國外主管機關同意監理合作之同意函。
委外服務供應商於當地未有監理機關之處理	1、銀行對該受託機構於受託事項範圍內得進行查核。 2、銀行應向 FSA 說明受委託機構有能力及適當資源履行委外契約。 3、受委託機構應說明當地法令對其提供委外服務或委外契約之可能影響。 4、銀行應確保受委託機構財務狀況良好，並取得經會計師簽證之財務報告。 5、銀行具適當程序確保受委託機構對提供委外服務取得之資訊有適當保護。 6、受委託機構應保護銀行與客戶權益攸關之機密資訊。 7、委外契約應適用歐盟之管轄法律。 8、當地國法律規範若有影響委外契約效力之情形時，銀行應立即通知 FSA。 9、受委託機構於英國境內是否設有分支機構等資訊。	銀行請受委託機構出具同意函，同意於必要時我國主管機關或銀行指定必要之人，對受託事項進行查核。

資料來源：本研究整理。

（三）銀行因非委外事項之國際傳輸，金融法令未有特殊規定，應回歸適用資料保護法之規定。

銀行因非委外事項，將個人資料國際傳輸之情形，包括遵循母國法律規定或母行與分子行間因授信管理需要進行之資料傳輸（如大額授信案件之審批、授信資產品質及限額之管理等），該等情形之資料傳輸性質相對較為單純。英國及我國金融法令對於銀行該等情形之國際傳輸，並未訂有相關規定，該項傳輸行為若符合英國資料保護法及我國個人資料保護法有關「國際傳輸」之定義時，應適用資料保護法之相關規定辦理。

第五節　小結

我國於個人資料保護法訂定之國際傳輸規定，係參考英國 1984 年之資料保護法訂定，惟英國資料保護法已因應 1995 年歐盟指令之發布而修正。我國銀行將客戶個人資料進行國際傳輸時，為維護資料之安全及當事人之權益，現行我國金融監理機關分別依據銀行法授權訂定之金融機構委外作業辦法及現行「電腦處理個人資料保護法」相關規定，以個案審查方式核准銀行將個人資料進行國際傳輸。參考 1998 年英國資料保護法及銀行因業務發展使得個人資料國際傳輸需求漸增之情形下，提出我國銀行國際傳輸之資料保護規範之可能改善建議如下：

一、個人資料保護法

個人資料保護法第 21 條雖已明定當國際傳輸之資料接收國對於個人資料之保護未有完善法規，致有損當事人權益之虞時，中央目的事業主管機關得限制非公務機關進行國際傳輸，惟如何評估其他國家對個人資料保護是否具完善之法規，建議個人資料保護法之主管機關，應訂定相關授權規定或解釋函令，明定評估其他國家資料保護法制之最低要求，協助非公務機關及中央目的事業主管機關於必要時進行評估，以有

效落實國際傳輸之規定。

我國個人資料保護法有關國際傳輸之規範，係採原則同意例外禁止之立法形式，建議可參考歐盟及英國之規定，改採原則禁止例外同意之方式，並透過產業自治之方式，規範企業在符合一定條件或在例外情形下，始得進行國際傳輸，以加重非公務機關於傳輸前，自我評估之責任。

二、銀行業之國際傳輸規範

配合「電腦處理個人資料保護法」已刪除非公務機關須經目的事業主管機關登記並發給執照，始得進行國際傳輸之規定。為加強銀行業對客戶資料國際傳輸之監理及保護當事人之權利，建議金融監理機關宜針對銀行將個人資料進行國際傳輸（無論為委外或非委外事項），參考歷次銀行向主管機關申請核准個人資料國際傳輸之直接收受者之個案情形，訂定銀行業國際傳輸之一般性規範（包括申請文件及申請應具備之資格條件等），以有效監理銀行業國際傳輸之行為。

三、銀行內部作業之境外委外

銀行委外事項國際傳輸之資料接收者，包括集團內專責資料處理及人事管理之作業中心及集團外專業之電子資料處理及儲存之公司，我國現行金融機構委外作業辦法，對於境外委外已訂有須事先報經主管機關核准辦理及應取得國外主管機關同意監理合作之同意函（若無法取得，應取得受委託機關同意查核之同意函），並應說明對客戶資料之保護措施及是否已取客戶同意等規定，惟由於境外委外涉及跨國性之法律規範及當客戶個人資料於當地遭受損害時之司法管轄權等問題，故對於境外委外事項，除應遵循金融機構委外作業辦法有關境內委外事項之一般性規定外（包括銀行應訂定客戶權益保護、風險管理及內部控制程序等作業規範），建議主管機關可參考英國境外委外之規定，針對銀行境外委外之特性及可能面臨之問題，訂定額外應遵循之事項或較詳細之規範。

第六章　結論與建議

第一節　結論

以下分別就英國及我國有關銀行國際傳輸客戶個人資料相關保護規範之情形，說明研究結論如下：

一、 英國資料保護法

英國政府為商業交易需要於 1984 年制定發布資料保護法，後參照歐盟指令之規定於 1998 年修正發布資料保護法，其中為遵循歐盟指令第 25 條及第 26 條有關國際傳輸之規定，故於資料保護法附錄一及附錄四，訂定個人資料禁止傳輸至第三國家之限制及豁免情形等相關規定。英國國際傳輸個人資料之規範在上開附錄規定及其專責資料保護之監理機關（ICO）發布之國際傳輸指引及依據歐盟指令規定，發布授權規定，允許英國企業得採用標準契約範本及使用 BCR 下，英國對於國際傳輸個人資料之保護已有一定程度之要求及應如何適用之作業流程及評估程序。

在上開規範下，英國企業（即資料管理者及資料輸出者）若擬將個人資料傳輸至第三國家時，依據資料保護法附錄一原則八之規定，資料輸出者應先確定該第三國家是否已經歐盟委員會認可得進行資料傳輸之國家，若該第三國家尚未經歐盟委員會認可，則輸出者應考量是否自行評估該第三國家之資料保護法制，若該第三國家未有資料保護法制或輸出者選擇不自行評估時，接下來輸出者應考慮該等個人資料之傳輸是否有符合資料保護法附錄四之豁免規定，包括取得當事人明示之同意、採用標準契約範本或輸出者業經歐盟各國資料保護監理機關核准使用 BCR 等情形，若資料輸出者在未符合上開任一情況，仍逕行將資料傳輸至第三國家，則將被視為違法之國際傳輸行為。

惟如同歐盟委員會司法部門之委外研究報告所述，英國相對於歐盟之其他會員國係將國際傳輸規範明訂於資料保護法之本文（如德國），英國僅於資料保護法之附錄訂定國際傳輸之限制，對於國際傳輸時，當事人資訊隱私權保護之法律位階仍有不足。英國應參考其他歐盟之會員國將國際傳輸規範納入資料保護法之本文，以提高對當事人資訊隱私權之保護。

英國於 1998 年資料保護法修正後，雖仍要求資料使用者將其對於個人資料之蒐集、利用及處理情形等基本資訊（包括是否有國際傳輸之需求等）於資料處理前向資料保護監理機關登錄，惟一旦登錄後，若實際將資料傳輸至英國境外之國家或地區時，則無須再取得資料保護監理機關之事先核准。惟目前部分歐盟之會員國，為控管資料管理者將個人資料輸出之情形，仍訂有資料輸出者於將個人資料傳輸至第三國家前，應事先向監理機關登記或核准之規定，對當事人資訊隱私權之保護，較為周延。

英國 ICO 雖已發布國際傳輸指引，供資料管理者使用，惟該國際傳輸指引僅就一般共通性事項予以規範，考量各產業持有個人資料之性質或有不同，應就因業務或交易需要，可能持有龐大個人資料之特定產業（如金融服務業、醫療業等），發展符合不同產業特性之資料保護實務指引，以強化各產業對於個人資料之保障。

二、 英國銀行境外委外之規定

不同於我國係於銀行法明定銀行對客戶資料之保密義務，英國銀行之保密義務始於 1924 年英國上訴法院對 Tournier v. National Provincial and Union Bank of England 一案之判決。在該判決下，銀行對於客戶資料保密之責任，原始存在於銀行與客戶間之契約，故英國金融服務與市場法主要僅規範金融監理機關因職務需要，知悉或取得銀行客戶資料之保密義務。

英國與我國相同於金融法令中僅針對境外委外所涉及之國際傳輸訂定相關規範（其性質類似為資料保護法之補充規定），至於銀行因非委外事項，將客戶資料傳輸至其他國家時，金融法令則並無相關規範，惟仍應適用英國資料保護法之相關規定。英國 FSA 對於銀行將內部作業委外於審慎監理手冊第 8 章「委外」，明定委外作業應遵循之事項（含境內及境外之委外），其中境外委外規定之適用範圍與資料保護法之規定一致，僅適用於將內部作業委外至第三國家時，始應依據其所訂規定辦理（即第 8.2 章及第 8.3 章之境外委外作業程序）。

英國銀行將作業委外至第三國家時，在第三國家可能未有資料保護法制之情形下，英國 FSA 針對境外委外之監理重點，除加強銀行對於該委外服務供應商就其受託事項範圍內之監督責任外，為保護客戶之權益，銀行應確保委外服務供應商能對個人資料提供適當之安全措施及於發生損害客戶權益之狀況時，若歐盟未與該第三國家簽訂合作監理機制之情況下，如何透過銀行與該委外服務供應商之委外契約條款，使 FSA 能進行有效監理，以保護當事人之權益。

英國資料保護法，除資料管理者擬採行 BCR，故須經 ICO 之事先核准外，資料管理者若擬依其他豁免規定將個人資料傳輸至第三國家，現行資料保護法並未要求需事先經 ICO 核准。惟英國銀行業在 FSA 監理規範之要求下，針對境外委外仍應事先經監理機關之同意，FSA 於審慎監理手冊並訂有銀行申請境外委外之作業程序及申請時應檢附之相關文件包含預擬之契約條款內容，經由事先審查，確認銀行與委外服務供應商簽訂之契約能符合 FSA 境外委外之規定，以確保其能有效行使監理權限。

三、 我國個人資料保護法

我國個人資料保護法於 99 年修正後，雖尚未正式施行，惟其中有關國際傳輸之規範，修正後規定已明定國際傳輸之定義（國際傳輸之

定義包含機關內部將個人資料作跨境之處理或利用，故在新法下，似已擴大國際傳輸之適用範圍)，並加重非公務機關違反中央目的事業主管機關發布限制國際傳輸命令或處分，足生損害於他人時之罰則（含刑罰及行政罰)。惟有關國際傳輸之相關限制規定，修法前後僅係作文字調整，而未修正其實質規範內容，對於非公務機關之國際傳輸，僅規定非公務機關有第 21 條所列四項情形之一時，中央目的事業主管機關得限制非公務機關進行國際傳輸。

在個人資料保護法第 21 條所訂之四項情形中，除國際條約或協定有特別規定者之判斷較為明確外，其他如涉及國家重大利益、接受國對於個人資料之保護未有完善之法令及非公務機關以迂迴方法向第三國傳輸個人資料，以規避個人資料保護法等情形，於實務運作上似較難以判斷（例如，如何判斷對國家有重大利益，其重大利益之基準為何)。另個人資料保護法修法後，已刪除非公務機關進行國際傳輸需經目的事業主管機關依法登記並發給執照，修法後之規定實質上已放寬原適用電腦處理個人資料保護法之特定行業之國際傳輸，將使得該等特定行業別之中央目的事業主管更難以落實該法第 21 條有關國際傳輸之限制規定[167]。

四、 我國銀行境外委外之規定

我國銀行對於客戶資料之保密義務係明定於銀行法第 48 條第 2 項，另為兼顧維護社會公益及個人隱私權之保護，現行銀行法並訂有客戶資料保密義務之例外規定。惟銀行法第 48 條第 2 項各款所訂例外規定之使用，由於將影響人民資訊隱私權受保障之範圍，自應受憲法

[167] 在歐盟指令架構下，對於個人資料國際傳輸之法律適用，有非常細緻的處理。相較於同樣對於個人資料國際傳輸有所規範的我國，在新的個人資料保護法通過後，為個人資料國際傳輸，不再須取得事業主管機關登記，並取得執照，似較為寬鬆，而有利於資料之國際流通。然後，本法此規範之意旨，是在防免個人資料跨境失控之疑慮，此疑慮不會因新舊法的更迭而消失，在此情況下，我國是否尚需要其他配套措施來落實個人資料於國際傳輸層面之保障，值得深思。見財團法人資訊工業策進會科技法律研究所編著，給科技研發與創新服務提供者的個資運用藍圖，資策會科技法律研究所，頁 237-238，2011 年 10 月。

法律保留原則之限制，以在公益與私益間取得平衡。金管會以往亦均審慎處理此項規範之職權（例如，要求銀行應揭露大額轉銷呆帳客戶資料），在不同法益面臨衝突之情況下，例外規定是否宜由行政機關以行政函令規範，仍存有爭議[168]。

我國銀行存有境外委外之需求者多為外國銀行之在台分子行，由於該等銀行之母行為國際性銀行為使全球各分支機構之客戶資料能作一致性之處理及因授信管理需要，故要求其在台分子行將客戶資料定期傳輸至總行或其設立於第三國家之資料處理作業中心（若為本國銀行，則涉及其國外分子行如何依當地國資料保護法之相關規範，將當地國客戶資料傳輸至國內之問題）。我國金融監理機關為因應銀行之上開需求及能行使其監理權限，現行金融機構委外作業辦法針對境外委外已規範銀行應取於國外主管機關同意監理合作之同意函或取得受託機構同意於必要時，我國金融監理機關得就受託事項對受委託機構進行查核之規範，並限制委外事項之傳輸目的僅限於資料處理，不得有資料運用之情事。

第二節　建議

本研究經將英國資料保護法及 FSA 境外委外之監理規定與我國個人資料保護法及銀行業境外委外中有關國際傳輸限制規定加以瞭解及比較後，謹就我國個人資料保護法及銀行業之個人資料國際傳輸保護規範，提出相關改善建議如下：

一、在我國個人資料保護尚未設立專責機關前，宜透過各中央目的事業主管機關對被監理機構之監理及其與相關公益團體間之合作，以強化各界對於個人資料保護之重視

現行歐盟各國如德國及英國等，對於個人資料之保護已設立獨立

[168] 陳妍沂，同註 33，頁 211。

專責之監理機關負責監理公務及非公務機關對於資料保護法之執行（如德國之資料保護聯邦專員及英國之資訊自由及保護委員會）、受理及處理人民與公務或非公務機關間有關資料保護之申訴案件及發布有關個人資料保護之作業規範，並定期向政府及民意機關提出報告及近期有關資料保護之重要發展等。

我國個人資料保護法雖已參考歐盟指令及德國聯邦個人資料保護法等相關規範修正，惟對於非公務機關個人資料保護之監理架構，仍維持現行方式，由各中央目的事業主管機關自行監理。為健全個人資訊隱私權之保護，長期而言，我國雖宜參考各國立法趨勢，設立資料保護之專責獨立機關，惟一機關之設立，除須法律授權外，尚涉及政府組織編制及預算等相關因素，故在我國尚未設立專責之資料保護監理機關前，仍應於各公務及非公務機關設置機關內負責推動及處理個人資料保護相關議題之專責人員，以確實保護人民之權益及有效落實個人資料保護法之規定。

我國制訂及推動個人資料保護法之主管機關雖為法務部，惟對於非公務機構是否落實個人資料保護法之監理，則回歸至各行業別所屬之中央目的事業主管機關。在上開立法架構下，人民與非公務機構間，因個人資料處理產生之爭議及相關申訴案件，須視其申訴對象反映至該特定對象之目的事業主管機關（如民眾與金融機構間之個人資料保護爭議，應向金管會銀行局申訴），惟各目的事業主管機關之監理人員係專責該事業機構之日常監理，在監理人員非熟知資料保護相關規範之情況下，未必能有效執行個人資料保護之相關規定或能適當處理該等類型之申訴案件。

為健全我國對於個人資料之保護，尤其在新個資法修正後，短期而言，仍應由各中央目的事業主管機關透過相關監理法規，針對所轄行業別之產業特性，訂定被監理機構有關個人資料保護之相關規範，

以對其落實個人資料保護法之情形予以適當監理。另為強化社會大眾對於個人資料保護之觀念，我國已於 97 年 8 月成立「財團法人台灣個人資料保護協會」，各目的事業主管機關、各產業公會與台灣個人資料保護協會間，宜建立相互溝通之管道，定期就個人資料保護發展之相關活動進行意見交流，應有助於政府機關有關個人資料保護相關政策或法規之推廣及相關申訴案件之處理。

二、個人資料國際傳輸之限制規定應予細緻化，並透過產業自治達成個人資料保護之目的

現行我國個人資料保護法之國際傳輸規定係參考 1981 年歐洲議會之個人資料自動化處理公約及英國 1984 年資料保護法，惟隨著資訊全球化及網際網路之快速發展，暨企業營運模式之改變，歐盟委員會已於 1995 年發布歐盟指令，其各會員國包括英國亦於 1998 年參照歐盟指令修正其國內法之相關規定（即 1998 年資料保護法）。歐盟指令及英國資料保護法有關國際傳輸，除已明定相關應遵循之事項外，對於如何落實國際傳輸對於個人資料之保護規範，並已陸續發布國際傳輸指引及如何透過企業內部個人資料保護制度之建立，以符合相關豁免規定之方式，包括如何評估第三國家是否具適當之資料保護法制、發布標準契約範本之適用範圍及條款內容、訂定向資料保護監理機關申請採行 BCR 之適用範圍、申請程序及有關條款內容之最低要求等。

我國個人資料保護法之國際傳輸規範，僅明定符合所訂四種情況之一者，中央目的事業主管機關得予限制傳輸，惟上開立法形式對於人民資訊隱私權之保障明顯不足，建議應參考歐盟指令之規定，改採原則禁止例外同意之立法形式，針對非公務機關將資料跨境傳輸之類型及國際傳輸產生爭議時所可能發生之問題，明確課以資料管理者（輸出者）一定作為之義務，包括非公務機關將國內個人資料傳輸至境外時，資料輸出者對於資料接收國之資料保護法制至少應有一定程度之

瞭解、當產生跨國資料保護爭議時，資料輸出者應協助當事人或監理機關取得當地國之相關資訊，並於必要時，允許當事人得直接向資料輸出者請求損害賠償，以強化當事人權益之保護。

針對如何評估其他國家資料保護法制之妥適性，為使評估符合一定程序及評估結果具一致性，建議應統一由個人資料保護法之主管機關（即法務部）針對我國非公務機關有大量傳輸個人資料需求之國家進行研究，參考歐盟模式公布我國認可之國家名單或該國家之資料保護法制係與我國規範程度相當之國家，以使非公務機關將資料傳輸至安全名單以外之國家時，能自行注意將資料傳輸至該等國家可能產生之風險，亦有助於各中央目的事業主管機關進行適當監理。

歐盟委員會針對國際傳輸已訂定較為細緻之作業規範，其目的係為調和各國間保護程度不一之資料保護法制，而我國經濟部商業司為落實 APEC 隱私保護綱領有關建立跨國隱私規章之規定，已委託資策會規劃建立「臺灣個人資料保護與管理制度」，協助企業內部建構個人資料保護制度，取得「個人隱私資料保護標章」，以期透過產業自治之方式，達到個人資料保護之目的。以銀行業為例，建議金管會可參考歐盟國際傳輸之監理方式，由銀行公會邀集相關單位，考量銀行業之行業特性後，訂定銀行業於國際傳輸個人資料時所適用之標準契約範本（即定型化契約）或類似共同約束條款之自律規範，以確保銀行業在個人資料國際傳輸之需求下，亦能對當事人之資訊隱私權予以適當之保護。

三、金管會宜配合個人資料保護法之修正，訂定銀行業國際傳輸之作業規範（含委外或非委外事項）

銀行業受到高度監理及相對於其他產業，更易取得客戶個人資料之特性，為確實保障當事人之權益，金融監理機關針對銀行業將個人資料進行國際傳輸，在參考歐盟標準契約範本及 BCR 之相關規定後，

建議應訂定相關監理規範如下：

（一） 銀行對於個人資料之蒐集、處理及利用，應向金管會登錄

修正後之個人資料保護法，雖已刪除非公務機關應向目的事業主管機關登記並發給執照後，始得進行個人資料之蒐集、電腦處理或國際傳輸及利用之規定，惟為瞭解銀行業內部個人資料保護制度之執行情形，以保護存款人及消費者之權益，建議金管會相對於其他產業，仍應採取較為嚴格之監理，至少要求銀行於蒐集、處理及利用個人資料前，應先向金管會登錄，俾於必要時，能對銀行個人資料之處理，進行適當之控管。

（二） 銀行國際傳輸個人資料前，應事先取得主管機關之核准

我國個人資料保護法修正後，非公務機關國際傳輸之直接收受者已無須再經目的事業主管機關依法登記並發給執照，為確保銀行業對於跨境傳輸個人資料已有適當之內部作業程序予以控管，以保護當事人之權益，建議應於相關金融法令明定銀行於將個人資料進行國際傳輸前，無論係委外或非委外事項，應向主管機關申請核准（變更或新增國際傳輸之資料收受者，亦同）。

（三） 銀行業將個人資料國際傳輸應遵守下列規定（所列規定應明定於委外契約條款或銀行內部之相關作業規範）

1、資料之傳輸僅限於特定目的，不得為特定目的外之使用。

2、當事人權益受損害時，除得直接向資料輸出者（即銀行）主張其權利外，並得選擇以資料原始輸出國作為訴訟管轄法院（即當發生有損當事人權益之民事、行政責任時，應以我國法令規定辦理）。

3、銀行內部應指定專責單位或人員控管國際傳輸之相關事宜（包括當事人與銀行間之申訴案件），並於必要時，能提供資料接收者之相關資訊予當事人或我國金融監理機關。

4、內外部稽核應定期對銀行之國際傳輸作業進行查核，並將查核報告定期報送至金融監理機關。

5、資料接收者若擬將資料處理作業複委託時，應事先經原始資料輸出者（即銀行）之書面同意。

8、資料接收者及複委託者於處理個人資料過程中，應遵守我國個人資料保護法、銀行法及金融法令等相關規定（銀行應評估資料接收者能否履行契約及我國個人資料保護法令與相關金融法令之法定義務）。

9、通知義務：

(1)資料接收者當地執法機關因犯罪調查等需要，要求資料接收者提供其所處理個人資料之相關內容時，應立即通知銀行（資料輸出者）。

(2)資料接收者若發生違反我國個人資料保護法之行為（包括個人資料因過失或未經授權被存取等），致有損當事人之權益者，資料接收者應立即通知銀行，銀行於收到相關資訊時，應通知我國金融監理機關。

（四） 明定銀行向金融監理機關申請國際傳輸應檢附之文件

1、傳輸個人資料之內容、性質、目的及傳輸過程（如是否有透過第三國家再進行傳輸之情形），若申請變更資料接收者，應說明變更之原因。

2、最終資料接收者之基本資料（包括名稱、地址、聯絡方式、與銀行之關係、所辦理業務之性質、資料接收者於資料接收當地國是否受相關監理機關之監理、如何控管所接收個人資料之安全、過去 3 年是否曾發生個人資料處理不當，致有損當事人權益之情事等）。

3、個人資料傳輸是否符合我國個人資料保護法之特定目的。

4、是否經當事人之同意。

5、當事人權益受損時，資料輸出者（即銀行）及資料接收者損害賠償責任之劃分、相關法律責任之管轄權。

6、資料接收者於當地國應遵守之資料保護法令及其法令是否有未符合我國個人資料保護法或相關金融法令之情形。

7、若資料接收者於當地國受監理機關之監理時，銀行應取得之合作監理之同意函；若無，應取得資料接收者同意我國金融監理機關於必要時，得由指定之人於國際傳輸範圍內（或委外事項範圍內）進行查核之同意函，並得暫緩或禁止個人資料之傳輸。

8、銀行對於國際傳輸之資料保護機制及相關作業流程之內部控管程序（含資料接收者對個人資料保護採行之控管及保密措施）。

9、內部稽核對銀行國際傳輸相關內部管理機制之查核結果。

（五） 銀行因內部作業委外（即境外委外）將個人資料國際傳輸，另應額外檢附下列文件

1、委外契約之預擬內容。

2、若有複委託之情形，應檢附複委託之預擬契約內容。

3、資料接收者最近期經會計師查核簽證之財務報告。

4、個人資料處理服務終止後，資料接收者及複委託者對於所接收個人資料之續後處理機制。

四、宜透過租稅合作協定，以在不違反我國個人資料保護法及銀行法之原則下，協助我國金融機構解決美國稅務局要求外國金融機構應自 2014 年起向其申報當年度美籍客戶個人財務資訊之問題

美國法令要求我國金融機構（非公務機關）定期將美籍客戶之財務資料國際傳輸至美國稅務局（外國公務機關），衍生之國際傳輸個人資料之爭議，與前述非公務機關間個人資料傳輸之規範重點在於資料接收者對所接收之個人資料是否已有適當程度之保護不同，非公務機

關與公務機關間之個人資料國際傳輸（通常是非公務機關向公務機關申報），主要問題不在於對當事人個人資料之保護是否妥適（設想美國稅務局對於個人資料應已有適當程度之保護），而係涉及對個人財務資料隱私權之侵害及各國法權是否對等之問題，為協助我國金融機構處理上開問題，本文初步建議似仍宜由我國稅務主管機關（即財政部賦稅署）透過與美國稅務局簽訂租稅合作協定之方式，以解決上開爭議。

參考資料

一、 中文資料（依作者姓氏筆劃排序）

（一）專書

1、王志誠，現代金融法，1 版，新學林出版股份有限公司，2009 年 10 月。
2、李惠宗，憲法要義，5 版，元照出版有限公司，2009 年 9 月。
3、財政部金融司儲委會金融研究小組，各國銀行法之比較(上篇)，1991 年 5 月。
4、財團法人金融聯合徵信中心譯，德國聯邦個人資料保護法，2008 年 10 月。
5、財團法人金融聯合徵信中心譯，歐聯資料保護綱領，1997 年 6 月。
6、財團法人資訊工業策進會科技法律研究所編著，給科技研發與創新服務提供者的個資運用藍圖，資策會科技法律研究所，2011 年 10 月。
7、陳冲，比較銀行法，財團法人金融人員研究訓練中心，1992 年 11 月。
8、許美滿、高美雲譯，1987 年英國銀行法，中華民國加強儲蓄推行委員會金融研究小組編印，1992 年 8 月。
9、經社法規譯介叢書，英國資料保護法，行政院經濟建設委員會健全經社法規工作小組，1988 年 9 月。
10、 蕭長瑞，銀行法令實務，6 版，財團法人台灣金融研訓院，1998 年 4 月。
11、 APEC 隱私保護綱領（APEC PRIVACY FRAMEWORK）（中英文對照），法務部編印，1996 年 12 月。

（二）期刊文章

1、王澤鑑，人格權保護的課題與展望（三）──人格權的具體化及保護範圍（6）──隱私權（上）（中）（下），臺灣本土法學雜誌，2007 年 8 月。
2、李振瑋、江耀國，英國資料保護法中資料所有人權利之研究－－兼論我國個資法之相關規範及案例，中原財經法學，2010 年 6 月。
3、李福隆，金融隱私權與銀行監理之間--從全球金融海嘯看我國金融危機事件下銀行保密原則之修正，2010 年世界人權高峰會收錄文章。
4、周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啟示，科技法律透析，2005 年 1 月。
5、周慧蓮，資訊隱私保護爭議之國際化，月旦法學雜誌第 104 期，2004 年 1 月。
6、林育廷，金融隱私權保障與財富管理發展之衝突與協調—兼評美國與台灣之規範政策，科技法學評論第 4 卷第 2 期，2007 年 8 月。
7、洪榮彬，論資訊時代跨越國際之資料處理與資料保護，法學叢刊，法學叢刊雜誌社，159 期（40 卷 3 期），頁 80-103，1995 年 7 月。
8、翁清坤，論個人資料保護標準之全球化，東吳法律學報第 22 卷第 1 期，

2010 年 3 月 26 日。

9、 陳起行，資訊隱私權法理深討—以美國法為中心，政大法學評論第 64 期，2000 年 12 月。

10、 陳超雄，歐洲「資訊保護與隱私權法」立法研究，東海大學法學研究，1989 年 11 月。

11、 陳榮傳，由法律觀點論資料跨國流通，經社法制論叢，第 5 期，1990 年 1 月。

12、 楊秀惠，會員辦理國際傳輸作業外銀首長座談會紀要，金融聯合徵信雙月刊，第 15 期，2010 年 10 月。

（三）論文

1、王俊傑，銀行作業與服務委外的管理與監理，國立政治大學行政管理碩士學程碩士論文，2007 年。

2、洪榮彬，資訊時代之資料處理與資料保護—以德國聯邦個人資料保護法為中心，輔仁大學法律學研究所碩士論文，1993 年 6 月。

3、陳妍沂，美國財務資訊隱私權保護規定之研究，國立政治大學法學院在職專班碩士論文，2008 年 5 月。

4、黃莉雲，資料跨國流通法律問題之研究—相關理論與規範，國立臺灣大學法律學研究所碩士論文，1994 年。

5、賴敏慈，信用資訊與隱私權保護--由信用資訊之揭露與隱私權之衝突檢討個人信用資料保護法制，中原大學財經法律研究所碩士論文，2005 年。

6、戴言同，歐盟資訊與通訊科技政策與規範之研究—檢視我國雲端政策之問題，國立雲林科技大學科技法律研究所碩士論文，2011 年 6 月。

二、 英文資料

（一）專書

1、Carey, Peter, Data protection in the UK, London: Blackstone Press Limited（2000）.

2、Carey, Peter, Data Protection—A Practical Guide to UK and EU Law, Oxford University Press（3rd ed. 2009）.

3、Richard Morgan and Ruth Boardman, Data Protection Strategy—Implementing Data Protection Compliance, London Sweet& Maxwell（2003）.

（二）期刊及研究報告

1、Cynthia Blum, Sharing Bank Deposit Information With Other Countries：Should Tax Compliance or Privacy Claims Prevail？, Florida Tax Review Vol. 6 no. 6（2004）.

2、Fayyad Alqudah, Banks' duty of confidentiality in the wake of computerized banking, Journal of International Banking Law（1995）.
3、Gehan Gunasekara, The "Final" Privacy Frontier？Regulating Trans-Border Data Flows, International Journal of Law and Information Technology, Vol. 17, No. 2（2007）.
4、J.C. Sharman, Privacy as Roguery：Personal Financial Information in an Age of Transparency, Public Administration Vol. 87, NO. 4（2009）.
5、Lee A. Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, Vol. 6 No, 3（1998）.
6、Lingjie Kong, Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law Vol. 21 no. 2（2010）.
7、M. Stallworthy, Data Protection：Regulation in a Deregulatory State, 11 Statute L. Rev. 130（1990）.
8、Roger K. Baker, Offshore IT Outsourcing and the 8th Data Protection Principle—legal and regulatory requirements—with reference to financial service, International Journal of Law and Information Technology, Vol. 14 No. 1（2005）.
9、Roy M. Goode, The banker's duty of confidentiality, Journal of Business Law（1989）.
10、Shalini Agarwal, Sakate Khaitan, Satyendra Shrivastava and Matthew Banks, Destination India：offshore outsourcing and its implications, Computer and Telecommunications Law Review, 11(8)（2005）.
11、Steve R. Salbu, The European Union Data Privacy Directive and International Relations, William Davidson Working Paper No. 418（2001）.
12、Val Collins, Privacy in the United Kingdom：a Right conferred by Europe？, International Journal of Law and Information Technology, Vol. 1 No. 3（1993）.
13、The Department of the Treasury, Security of Personal Financial Information, Report on the Study Conduct Pursuant to Section 508 of the Gramm-Leach-Bliley Act of 1999（2004）.

（三）判決

Durant v. Financial Services Authority (Disclosure) [2003] EWCA Civ 1746, Court of Appeal (Civil Division), 2003-12-08 (Approx. 41 pages).

（四）網路資料（有作者部分依姓氏字母順序排列，其他依文件開頭字母順序排列）

1、APEC Data Privacy Pathfinder Protects Implementation Work Plan, 17th Electronic Commerce Steering Group Meeting, Lima, Peru（2008）, available at http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group（last visited January, 2012）.

2、Binding Corporate Rules, available at http://www.ico.gov.uk/youth/sitecore/content/Home/for_organisations/data_protection/overseas/binding_corporate_rules.aspx（last visited November, 2011）.

3、 Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries（2004 controller to controller）, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF（last visited November, 2011）.

4、 Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC（2001 controller to controller）,available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_181/l_18120010704en00190031.pdf （last visited November, 2011）.

5、 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/45/EC of the European Parliament and of the Council（2010 controller to processor）, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF（last visited November, 2011）.

6、Douwe Korff, Comparative Studies on different approaches to new privacy challenges, in particular in the light of technological developments—country studies A.6—United Kingdom （2010）, available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm（last visited November, 2011）.

7、Douwe Korff, Comparative Studies on different approaches to new privacy challenges, in particular in the light of technological developments—country studies A.4—Germany （2010）, available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm（last visited November, 2011）.

8、Data Protection Act 1998—The eighth data protection principle and international data transfers, Information Commissioner’s Office, Version 4

（2010）, available at http://www.fsa.gov.uk（last visited November, 2011）.
9、Data Protection Act 1998 Legal Guidance, Version 1, available at http://www.ico.gov.uk（last visited November, 2011）.
10、 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf（last visited November, 2011）.
11、 Data Protection Act 1998, available at http://www.legislation.gov.uk/ukpga/1998/29/contents（last visited November, 2011）.
12、 Financial Services and Market Act 2000, available at http://www.legislation.gov.uk/ukpga/2000/8/contents（last visited November, 2011）.
13、 FSA Handbook—Senior Management Arrangements, Chapter 3 Systems and Controls, available at http://www.fsa.gov.uk/pages/handbook （last visited November, 2011）.
14、 FSA Handbook—Senior Management Arrangements, Chapter 8 Outsourcing, available at http://www.fsa.gov.uk/pages/handbook （last visited November, 2011）.
15、 The “Durant” Case and its impact on the interpretation of the Data Protection Act 1998（web version 4）, Information Commissioner’s Office, 27 February 2006, available at http://www.ico.gov.uk（last visited November, 2011）.