美日兩國金融機構使用顧客資料相關法令之比較
－以銀行保險為例

The Comparison of Privacy Protection in the Bancassurance Field between Japan and USA

撰稿人：范姜真媺
Chiang Chen-Mei Fan

范 姜 肱
Chiang-Ku Fan

鄭 鎮 樑
Chen-Liang Cheng

美日兩國金融機構使用顧客資料相關法令之比較－以銀行保險為例

摘　要

個人資料保護是近日國際重視之議題，我國立法院已於 2010 年 4 月 27 日三讀通過個人資料保護法，新版個資法修法目的顯然是為進一步保護消費者權益，但對某些性質特殊行業，尤其是個人資料使用度相當高的保險相關產業，確實會帶來非常大的衝擊，包括核保、理賠、行銷、與經營成本。然現代化金融機構的經營，無庸置疑地，客戶的個人資料是其重要資產，金融機構可藉由客戶提供或自行蒐集的資訊來建立、調整經營策略；相對地，金融機構對客戶資訊的蒐集、使用、保存等程序也均須受到一定的規範並負一定的責任，以確保顧客之隱私權受有適當的保障。故如何合法使用顧客資料產生集團內綜效，金控公司應謹慎應對。美國與日本兩國均屬經濟高度發展的國家，亦有許多相關法令規範金融機構客戶資料的使用。本研究旨在對美、日兩國所設計之金融機構客戶資料保護的相關法令加以研究比較，並集中於研究銀行保險通路利用銀行客戶資料問題的分析。本研究採用比較分析的法學研究方法，以呈現兩國相關法令之異同特性。本論文之研究具有學術與實務之重要意義，其研究結果能提供銀行、保險業者與主管機關對於修改金融機構顧客資料使用限制相關法令之參考。

關鍵字：個人資料保護、金融控股、銀行保險、隱私權

范姜真嫩小姐：銘傳大學科技法律學系副教授
范姜肱先生：實踐大學風險管理與保險系副教授
鄭鎮樑先生：實踐大學風險管理與保險系副教授

壹、緒　論

現今電腦系統已可以在極短時間內處理分析大量顧客個人資料，將這些原先猶如烏合之眾的數據抽絲剝繭，並整理出顧客的消費行為。也就是利用電腦進行資料採礦(data mining)的速度，已讓人嘆為觀止。因此，拜科技因素所致，個人資訊隱私（The privacy of personally identifiable information）之被重視已進入前所未有的境界（Nordman & Krohm，2002）。無怪乎美國人會將「個人隱私」票選為 21 世紀他們所最關心的議題之一（Gustini，2002）。無獨有偶，個人資料遭濫用亦是新加坡人最關心的三大安全課題之一，甚至超越關切恐怖主義和戰爭的議題（康世人，民 96）。

在美國，金融機構顧客資料外洩或遭竊之情況相當嚴重。根據美國銀行（Bank of America）透露的訊息，在 2005 年 2 月間，有將近 120 萬筆的顧客資料遭人盜取。就連擁有全世界最多法律與商業資料之 LexisNexis 公司也難逃劫數，此公司在 2005 年 3 月時，他們所擁有的 31 萬筆顧客資料，包括姓名、地址、社會安全號碼與駕照號碼，已遭人盜賣。這些接踵而至的事件也意味著顧客在金融機構的個人資料，遭金融機構轉售或遭人盜賣之情事，已成為全美數以百萬計人民日常生活的一部分（Maffett，2005）。

在台灣個人資料遭人為因素盜賣或濫用的嚴重情況亦不惶多讓。2002 年與 2003 年就曾有兩家歷史悠久的銀行因行員疏失或不法盜賣，導致客戶資料外洩。雖然這兩家銀行已被主管機關去函要求改善並祭以行政處分，然客戶資料外露之情況似乎並無明顯的改善，反而有惡化趨勢。光在 2004 年，台灣就有三家知名金控旗下的銀行，因不當交叉使用資料並外洩客戶資料，遭到金管會之行政處罰（邱金蘭，民 93）。也難怪台灣有高達 75%的民眾擔心個人資料遭到不當濫用，

而原本給民眾最有信賴感的金融機構卻可能是資料外洩的大本營。依據警方查獲的個人資料發現，詐騙集團最青睞的就是金融業所擁有的客戶資料。據了解，這是因為詐騙集團認為金融業擁有客戶最重要的身分證字號及財務狀況等個人隱私資料（蔡靜紋，民 95）。

個人資料外洩之禍首並不在於電腦，反倒是有約 50%~80%資料外洩的原因是肇因於人為因素，尤其是金融機構員工缺乏顧客資料安全意識，或顧客資料保護之專業素養訓練不足，或者是因為金融機構未建立健全的顧客資料保護程序。綜合來看，這些人為因素當中，至少有 20%到 40%是屬於金融機構員工缺乏保護顧客個人資訊之訊息所致（Maffett，2005）。

我國銀行法雖無明文規定銀行業得直接經營保險中介業務，但若根據保險代理人、經紀人、公證人管理規則第 20 條之規定，銀行業是被允許經營與其業務相關之保險中介業務，且實際上我國銀行業直接擔任保險中介人，早已行之有年。

近幾年來，受到銀行存款利率大幅下降、經濟成長率逐年下降、非銀行業進入銀行領域發展等因素影響，銀行面臨競爭的壓力與生存的困難。立法院為了維持金融體系的發展健全，在 2000 與 2001 年間相繼通過了「金融機構合併法」與「金融控股公司法」。經過多年來的整合，國內愈來愈多的金融機構已積極的拓展其經營規模，希望透過多元化經營，競爭力能逐漸提昇。截至 2007 年已有 14 家金融控股公司成立。為何短短幾年間，有如此多之金融控股公司成立，其原因不外乎是著眼於經營上之綜效。因為金融控股公司最大效用即在於資本效率、交叉行銷、降低成本之 3C，其中資訊共用是左右金控是否可以產生 3C 效用之最大因素。金控公司旗下業務可能包括銀行業務、保險業務、創投業務、證券業務等，若允許客戶資料的互相流用，則金融控股公司集團就可以擁有龐大數量的個人資料（吳尚昆，民 96）。

如前所言，金融控股公司成立之初，利用旗下公司個人資料進行交叉行銷被視為最大利基之一，但也因此引發社會大眾對於個人資料可能遭受往來金融機構濫用的疑慮。另一方面，個人資料保護之議題也是近日國際重視之議題。所以現代化金融機構的經營，無庸置疑地，客戶的個人資料是其重要資產，金融機構可藉由客戶提供或自行蒐集的資訊來建立、調整經營策略；相對地，金融機構對客戶資訊的蒐集、使用、保存等程序也均須受到一定的規範並負一定的責任，以確保顧客之隱私權受有適當的保障。故如何規範並合法使用個人資料產生綜效，政府主管機構與金控公司均應謹慎應對。

未來即將實施新版「個人資料保護法」嚴格保護個資，需要顧客名單進行銷售的金融保險業首當其衝。所以金融保險業者莫不憂心忡忡。民營銀行主管指出，雖然施行細則的規範還不清楚，但如果未來銀行向客戶蒐集個人資料時，必須明確告知蒐集目的、類別、個人資料利用期間、地區、對象和方式等，將造成銀行作業成本大增。另外，對於旗下擁有金控公司的金融機構衝擊更大，因為原先可發揮銀行存款、購買基金、賣保險、股票下單等「交叉行銷」的綜效，未來可能不能如此「自由」運用客戶資料，效益恐大幅縮水。如此，是否就代表我國對金控公司顧客個人資料的管制，比先進的國家嚴格，各界似乎也有不同之見解。

本研究採比較分析之法學研究方法，歸納、分析、比較美國與日本現行金融機構顧客資料保護的相關法令。研究之結果除了能提供社會消費大眾與金融機構更為清楚的瞭解先進國家對顧客個人資料保護之實際作法，亦可供政府作為將來修法時之參考，以達到保障顧客個人資料與經營綜效雙贏的局面。

貳、相關法規與文獻探討

一、OECD 個人資料的國際流通及隱私保護準則

(一) OECD 準則決議背景

隱私權之概念為美國於 19 世紀末,因對抗新聞媒體濫行報導個人私生活而被主張之基本人權，其最初之概念為「一人獨處之權」(To be let alone) (Warren and Brandeis，1890) ，之後再發展為私生活不被濫行侵入、公開之以侵權行為法保護之權利 (Prosser，1960)；而至近年個人對自己資訊制權,「資訊隱私權」則被主張為隱私權之重要內容(佐藤幸治，1997)，至 1970 年代開始，因電腦及通訊技術之發達，經濟規模世界化，政府機關為執行有效率之行政管理，企業為迅速掌握市場，提供顧客完善服務，均以電腦大量收集、儲存、傳送個人資訊，個人資訊隱私權被侵害之風險急速升高，而各國對個人資訊保護之法律與標準不一致，更對個人資訊之保護形成威脅，也阻礙國際間個人資訊之傳遞與利用；因此經濟合作與開發組織 (Organization for Economic Co-operation and Development，OECD)之理事會於 1980 年 9 月 23 日通過決議，確立各加盟國處理、傳遞個人資訊時應遵守之八大原則 (Recommendation of the Council Concerning Guideline Governing the Protection of Privacy and Transborder Flows of Personal Data)，於保障個人權利利益不受侵害之前提下，讓個人資訊得以安全流通，加以合理利用。而此八大原則成為日後各國個人資訊保護法立法或修正之準據；而為 OECD 加盟國之日本、美國與非會員國之我國於立法時亦均將此八大原則具體化為條文成為個人資訊保護法之主要內容[1] 。

[1] 日文部分請參閱堀部政男，個人情報保護法制化の背景と課題，法律のひろば，7 頁，2002 年 2 月。而我國部份，請參閱許文義，『個人資料保護法編』，180 頁以下，三民書局，2001 年 1 月

(二) 八大原則之內容：

OECD 八大原則主要內容如下：

1.收集限制原則 (Collection Limitation Principle)：個人資訊之收集應依適當、公平之手段、且應在適當之場合於資訊本人知悉或得到同意後收集之。

2.資訊內容原則 (Data Quality Principle)：個人資訊應符合利用目的、且於其所集目的範圍內保持其正確性、完整性與最新性。

3.目的明確化原則 (Purpose Specification Principle)：收集個人資訊之目的應於不遲於收集時之時點予以明確化；此其後之資訊利用，被限制於為該當收集目的之達成或與該當收集目的不互相矛盾之範圍內，或為與每次已明確作變更之他目的之達成。

4.利用限制原則 (Use Limitation Principle)：個人資訊不得為明確化目的以外之利用或供其它之用，但有以下之情者不在此限：①資訊本人同意、②依法律規定者。

5.安全保護原則 (Security Safeguard Principle)：個人資訊應以合理之安全保障措施保護其不被遺失、不當接觸、破壞、使用、篡改、公開等。

6.公開原則 (Openness Principle)：有關個人資訊之開發、運用與政策，應採一般性公開原則。個人資訊之存在、性質與其主要利用目的，與資訊管理人之識別，住所等應以容易利用之方式明示之。

7.個人參與原則 (Individual Participation Principle)：資訊本人有權①自資料管理人或他人確認資訊管理人是否保有有關自己之資訊②於合理期間內，如有必要時，負擔適當之費用依合適之

方法以容易理解之方式知悉資料之內容。又上 2 項要求被拒絕時，應告知理由並得申訴。再者，關於自己資料得要求消去、修正、補充。

8.責任原則 (Accountability Principle)：資訊管理人有責任遵守實現上述 7 項原則之措施。

之後 1995 年歐盟 (EU)又通過「有關個人資訊處理之個人保護與該當資訊自由傳送之 1995 年 10 月 2 日歐洲議會與理事會 95/4.6/EC 指令 (以下簡稱 EU 指令)」[2] ，該指令內容亦承受上述八大原則，並於第 31 條規定在指令通過後 3 年內，各加盟國應依指令內容訂立或修正有關個人資訊保護法，使指令實際轉化為有拘束力之歐盟各國國內法；而影響個人資訊保護法，成為國際上重視且國際標準化者，則為其第 25 條 1 項規定，各加盟國如欲將個人資訊移轉至第三國時，必須該當第三國對個人資訊之保護已達足夠之水準者，使得為之。因此於高度資訊化社會與經濟市場地球村化之今日，即使非 EU 之加盟國，而只要與 EU 有貿易、金融關係或涉多國籍企業之人事管理之其他各國，均須與 EU 談判，並同時檢討或調整本國之個人資訊保護法制以避免將來面臨資訊傳遞與利用發生困難。為此美國亦於 1998 年 7 月開始與 EU 進行著名之「安全港 (Safe harbor)」交涉，至 2000 年 5 月達成 7 項「安全港原則」協定，以確保個人資訊之國際流通 (劉靜怡，民 91)。

綜上可知吾人在討論銀行金融業者有關個人資訊之收集、利用等問題時，不問法制面或實務面，均須回溯至 OECD 八大原則始能了解個人資訊保護之基本原則。

---

[2] Directine95/4.6/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, 375Lo046, Offical Journal L 281, 23/11/1995 p. 0031- 0050

自 1990 年代後期各國以 OECD 八大原則為基準具體立法保護個人資訊，以蔚為不可避免之趨勢；然因各國國情不同，所採之立法方式亦有不同，大致可分為 3 種：(1)總合方式 (Omnibus)，即對政府機關與民間企業團體等之處理個人資訊，以同一法律規範之。(2)分離方式 (Segment)，對政府機關與民間企業團體分別以不同之法律規範。(3)共同原則下分離領域方式 (Sectary)，即先以法律位階訂出保護個人資訊之共同基本原則；然後各個不同領域之業界再委由其相關團體或組織以下位階之法令，針對其業務上需要與特色，制定保護個人資訊之規範或協議。歐洲各國各採(1)之立法方式，而美國、加拿大採(2)之以尊重民間企業自律為主之立法方式；日本則採折衷(1)與(2)之立法方式 (宇賀克也，2005)。

二、美國有關金融機構顧客個人資訊保護之法規

(一) 美國 GLBA 立法背景與立法目的

Gramm-Leach-Bliley Act (GLBA)又稱之為金融服務現代化法案(Financial Modernization Act of 1999)，是美國國會立法通過，並經美國前任總統柯林頓(Clinton)於 1999 年 11 月 12 日所簽署生效的一項法案。在 GLBA 法案通過前，受限於 Glass-Steagall ACT(1993)之規定，美國的銀行禁止兼營證券業務。另外所謂的銀行控股法(Bank Holding Company, 1940 年)亦只允許銀行控股公司得在人口小於 5000 人的小城鎮同時從事信用、人壽與年金等三項金融商品的代理業務。如此反而造成美國一些規模較大且知名的金融機構(例如：Citibank; American Express; Travelers Group)只能以技術違法方式兼營各種不同之金融服務，當然也迫使美國國會不得不正視此問題而制訂 GLBA。至此也開啟銀行、保險、證券三者間之異業競爭關係。如前所言，金融業者通常都擁有大量的客戶個人資料，在允許其合併提供各種不同類型金融服務之同時，異業之間客戶資料的相互流用就格外引人注意。美國金

融監理機關自然在開放金融整合服務時會有保護顧客個人資料之配套措施。所以綜觀美國 GLBA 之內容與學者的意見，顯然此法案存在有兩項主要的立法目的，其一為允許大型金融機構同時提供各式各樣的金融服務；其二為保護金融機構顧客個人資訊(Giglio，2002)。所以不同之金融業都可以整合，而成為所謂的「金融服務業」(Financial Service Indusery)。然 GLBA 並未將 1940 年之 Bank Holding Company ACT 有關「銀行控股公司不得所有非金融機構」之限制去除。也就是說在 GLBA 下，在 Bank Holding Company 之組織架構下，是不能有非金融單位存在的。

(二) 美國 GLBA 保護金融機構顧客個人資料之重要原則及其涵蓋範圍

GLBA 是美國聯邦政府所提出之法案，並責成相關之聯邦機構遵循執行之。所以 GLBA 並非用以取代或凌駕美國各州之相關法令。且截至 2002 年秋季為止，在美國共有 49 州外加哥倫比亞特區，其個人資料保護相關法令的嚴格程度至少同等甚至超越了 GLBA 的規定(Nordman and Krohm，2002)。故 GLBA 可說是美國境內保護顧客個人資料之最低基本要求。GLBA 包括了四項金融機構顧客個人資料保護措施的原則，分別為：

1.至少每年一次，清楚且明顯地對其顧客揭示公司蒐集與分享顧客個人公開資訊之政策。

2.在有限例外之情況下，提供公司顧客有權利拒絕其個人非公開資訊公開或分享予非公司掌控之第三人。

3.禁止向市場上之第三者公開可取得顧客資料的途徑。

4.遵守新的法律規範以保護公司顧客非公開個人資訊，以確保其安全性與機密性。

舉例來說，如金融機構得將個人非公開資訊 (Personally

Identifiable Information，PII)公開或分享予同金融機構所掌控(Own or Control)之公司，且這些公司是代表金融機構行使金融行銷服務者。例如：代表金融機構處理郵購之公司；代表金融機構處理顧客抱怨或訂購之公司；或協助金融機構處理行銷事務之公司。諸如此類之 PII 公開或分享，顧客是無從拒絕的。金融機構若將個人非公開資訊公開或分享予所掌控(Own or Control)之公司，而這些公司並非是代理金融機構行使金融行銷服務者，例如非金融公司與保險公司，則顧客有權利拒絕此類之個人資訊公開(Xoom Privacy Policy, 2007)。

綜觀 GLBA 共涵蓋了三項主要內容。首先是金融隱私規定(Financial Privacy Rule)，涉及的範圍為收集與公開個人金融資訊，包括有如何寄送隱私權通知(Privacy Notice)，拒絕公開權利(Opt Out)條款，與非公開個人資訊（Non-public personal information）之使用。其次是安全保護規定(Safeguards Rule)其內容主要是要求金融機構提出有管理性、技術性與具體性的安全保護措施，以確保個人金融資訊之隱私與機密。第三是防範詐取資料規定(Pretexting Protection Rule)，其中包括禁止使用不當或詐騙手段以獲取個人資訊或個人非公關資訊(Schneck，2005)。以下是此三項主要內容之說明。

1.金融隱私規定

在此規定之下，GLBA 要求金融機構提供給予每一位顧客隱私權通知(Privacy Notice)，此隱私通知在顧客與金融機構建立關係當時即必須告知，而後每一年，金融機構都要定期發送此隱私通知予其顧客。隱私通知之內容必須說明：收集顧客之資料為何；這些顧客資料將分享在什麼地方；這些顧客資料將如何被使用；這些顧客資料將如何被保護。此外，此隱私通知亦要確認顧客可選擇拒絕其個人資料分享予非屬金融機構可掌控第三者之權利。

2.安全保護規定

在此規定下，金融機構必須發展出一套資訊安全計劃。在此計劃當中，要詳述金融機構現在與未來如何持續保護其顧客的個人非公開資訊，而且此計劃亦適用於過去曾是（現在已不是）金融機構顧客者身上。

GLBA 亦規範金融機構的資訊安全計劃內容必須包括：

(1)至少指派一名員工管理資訊安全保護事宜。

(2)金融機構每一單位均要有處理顧客非公開資訊的風險管理措施。

(3)發展、監控、測試此資訊安全計劃的執行步驟，以確保顧客個人資料之安全。

(4)當顧客資料收集、貯存、使用的方式不同時，此資訊安全計劃的內容在必要之情況下亦要有所改變。

綜合而言，安全保護規定，將使金融機構更加詳細檢視其現階段顧客隱私管理與資料保護危險分析之狀況是否有缺失。

3.防範詐取資料

所謂詐取資料(pretexting)是指某人在未被授權之狀況下企圖收集或取得個人非公開資訊。在 GLBA 之下，亦要求金融機構採取所有必要之預防措施，以保護或防護其顧客的非公開個人資料遭到他人非法盜用。

(三) 美國 GLBA 對金融機構顧客個人資料保護之具體要求

從上述美國 GLBA 保護金融機構顧客個人資料之重要原則及其涵蓋範圍內容可知，此法案基本上有四項個人金融資訊保護之要求

(Byme，1999)：

1.GLBA 要求相關之聯邦或州的監理單位，採取行動監督其所管轄之金融機構，並要求金融機構建立具有管理性、技術性與具體性之安全保護準則，以保障其顧客個人資料之安全與機密。

2.GLBA 進一步允許金融機構的顧客可拒絕將他們之非公開個人金融資料分享給非金融機構可掌控的第三者。

3.GLBA 禁止金融機構，包含各類銀行、證券商與保險公司將其顧客之帳戶資料公開予非金融機構可掌控之第三者作為電話行銷或其他直效行銷目的之用。

4.GLBA 最重要的一項要求即是，所有的金融機構在與其客戶建立交易關係當時與其後的每一年，並須將其顧客個人資料保護政策與如何保護顧客非公開資訊的步驟作為，清楚具體地向其所有顧客揭示。

銀行一旦選擇在某一天寄發隱私權通知，之後每年都必須在大約相同之日期，再寄發隱私權通知，除非環境或者情況改變，每年所寄發之通知內容可能一樣，而所謂的選擇拒絕(Opt Out)的權利，除非有所改變，否則亦是沿襲前一年之選擇。GLBA 要求金融機構寄發顧客隱私通知給其所有的往來客戶，並告知顧客所有公開其個人資料的可能情況，並提供顧客方法以拒絕金融機構公開其個人資訊。若未遵守 GLBA 之規定，將處以每次最多美金 1 萬元的民事罰款(Daily Record Staff，2005)。相對的，為了遵從 GLBA 之規範，在美國一般規模較小之銀行必須花費在每一個顧客身上之成本為美金 2.37 元，而規模較大之銀行則可能有較少之成本花費(Gustini，2002)。

(四) 美國 GLBA 有關顧客隱私通知之內容要求

在 GLBA 下，隱私通知(Privacy Notice)之內容中必須向其顧客告

知並解釋顧客有機會享有選擇拒絕其資料分享予金融機構掌控公司之權利。唯下列三種狀況顧客不能拒絕其個人資料的分享：

1.資料分享的對象是那些提供金融機構更優先服務的機構。

2.資料分享的對象為金融機構行銷其產品或服務的機構。

3.資料的分享確實是法律上所要求的。

(五) GLBA 通過後美國金融機構保護顧客個人資料之概況

根據(Brown，2001)的說法，GLBA 法案中所謂金融機構所掌控之聯屬公司(Affiliated Company)，必須符合充份管理與充份私有化(well capitalized)之條件。而一般所謂金融控股公司(financial holding company)體系下之子公司均能符合此條件，故在 GLBA 法案下，金融控股公司體系下各子公司間顧客資料的公開分享是有條件被允許的。其他所謂一般的銀行控股公司(Bank Holding Company)則未必符合 GLBA 法案中所謂金融機構所掌控之公司(Affiliated Company)之要求。也就是說銀行控股體系下子公司間顧客資料之公開與分享基本上是屬於非金融機構所能掌控之第三者(Nonaffiliated Third Party)，故在顧客資料公開使用上將受到較多的限制。

相當具有歷史意義的加州金融隱私法(Financial privacy law)，已在 2003 年 7 月 1 日生效，但非所有的金融業者都贊同此案。根據一美國的全國性報紙所載，銀行業紛紛尋求翻案的可能，以確保他們分享顧客個人資訊之利益與方便性。根據最新的加州金融隱私法，金融機構必須取得顧客同意之後才能將顧客個人資訊，包括銀行帳戶內容與消費習性等資料，提供予非屬金融機構所掌控之公司(Non-affiliated company)。另外金融機構顧客亦有權選擇拒絕將他們的個人資料分享予或售予與金融機構簽訂有聯合行銷合約的公司，例如銀行的顧客就可以拒絕他的銀行將其個人資料公開予與銀行合作之信用卡公司。再

者，金融機構顧客亦可有權選擇拒絕其金融機構將其個人資料轉售予在同一集團下可掌控的另一家不同性質的金融機構。例如銀行顧客可拒絕銀行將其個人資料轉售給同一金融控股公司旗下的保險公司。這些不利於金融機構的規定已迫使加州許多金融機構向地方法院提出訴訟，希望扳回一城，但卻遭地院駁回，法院並解釋州法本來就可以比 GLBA 更嚴峻(The Information Management Journal，2004)。

一般金融機構普遍認為現行法律足以保護顧客之個人非公開資訊，相反地各州政及消費團體卻認為可以努力的空間還很大。而對於 GLBA 之最主要爭議之處乃在於此法案內的”選擇拒絕”(Opt Out)權利條款與金融機構顧客無法實際控制其個人資訊分享予金融機構所掌控(own and control)之其他機構(Affiliated companies)

根據一研究之實際訪察發現，所有之金融機構確實允許其顧客可以選擇不公開其個人資訊予其他公司之權利，但是顧客必須向其金融機構清楚且明白的表示其意念(Giglio，2002)。

另外值得注意的是有關隱私權通知的設計，GLBA 給予各金融機構有彈性調整的空間以適應各金融機構所處市場環境不同之不同需求，此法立意良好，但實際上自 GLBA 執行以來，多數顧客均未仔細閱讀這些隱私權通知，尤其是當這些隱私權通知每年均會寄發一次時，情況更是嚴重。已有些許的州或聯邦之監理單位決定一起合作以找出一個更為簡易之方法以符合 GLBA 下隱私權通知之要求，目前正在進行之工作有兩項(ABA Trust Letter，2006)：

1.發展一能讓人更易閱讀．更容易讓人明白使用的隱私權通知。

2.執行密集的消費者研究，期許建立一有效能之隱私權通知範本或設計參考。

三、日本有關金融機構顧客個人資訊保護之法規

(一) 日本金融機構顧客個人資訊保護法之相關法源背景

日本原於 1988 年即針對行政機關規範其蒐集利用個人資訊而制定「行政機關電子計算機處理個人資訊保護法」，後為因應世界之潮流與日本推動高度資訊通信社會政策下，及商務電子交易普及化之需要，於 2003 年 5 月 23 日完成「個人資訊保護法 (以下簡稱個資法)」之立法，並於 2005 年開始施行。此法被定位為日本個人資訊保護法制之「基本法」，其第 1 章至第 2 章主要明定個人資訊保護之國家政策與基本原則，不分行政機關或民間私人企業等處理個人資訊時，均須以其為基準；而其第 4 章則針對民間業者等處理個人資訊時應遵守之一般原則與法律義務，予以明確列出。並於第 6 章規定民間業務處理個人資訊之最低標準 (minimum standard)，而各領域之業者，則希望業界團體自己在針對其所處理個人資訊之特色與其業務上之所需，定出更周密有關保護所處理個人資訊之方針與措施，並要求其成員遵守之(藤田義治，2004)。

事實上日本於個資法制訂施行前，金融業界已組成「金融資訊系統中心」 (FISC, 2004)，對個人資訊之保護進行調查、研究並訂出基本方針；故個資法之施行對金融業者，基本上並未造成太大之衝擊。

個資法立法後，基於同法第 7 條 2 項 6 款、7 款規定：政府必須對個人資訊處理業者 (下稱業者)應採取之保護個人資訊措施有關基本事項，及個人資訊處理有關申訴之處理事項，訂出基本方針；日本內閣會議於 2004 年 4 月公佈「個人資訊保護基本方針」，確立以下五個重要原則：(1)業者應制定並公佈其「隱私權政策」(Privacy Policy)，至少包含：甲. 個人資訊不利用於目的外，乙. 適當申訴處理機制之建立。(2)個人資訊外漏時之對外公佈：以防止二次傷害、迴避類似案件之再度發生。(3)責任制度之建立：甲. 防止外來不正當接觸 (access)

資訊之策略；乙. 管理人之設置；丙. 內部人員接觸之管理；丁. 攜出防止方法等，內部安全管理體制之建立、與委託外部處理個人資訊時有效率之監督制度；(4)從業人員之教育訓練；(5)申訴處理制度之建立；具體規劃出處理個人資訊業者有關保護個人資訊之基本骨幹。

再依此基本方針，主管各業種之中央政府省廳，對其主管領域之個人資訊處理業者，針對該領域處理之個人資訊之性質 (特別是醫療、金融、信用、通信領域)與利用方法尚需注意之特性，在訂出更具體之準則 (Guide Line)，以貫徹個資法之確實施行。因此日本金融廳於 2004 年 12 月公告「金融領域個人資訊保護準則」(下稱金融 GL)，其內容有與個資法所規定業者之義務相同內容者，有針對個資法規定作解釋性說明者；此外更重要的是對金融業者處理個人資訊上特別被要求之較嚴格規範。之後同廳又於 2005 年 1 月對個人資訊安全管理措施，另訂出「安全管理實務指針」。

以上為政府主管機關為落實個資法之施行所制定出之規範，但如前述日本個資法立法時，已保留各個業界團體針對自己所須訂立自律公約之空間，希望民間處理個人資訊業者以半自律方式，遵守保護個人資訊之法令，而政府立於監督之地位即可。因此個資法第 4 條第 2 項規定，各業者團體得於得到主管大臣之許可後成立「個人資訊保護法人」[3]，以處理其團體成員處理個人資訊時發生之申訴事件；提供其團體成員適當處理個人資訊之資訊；與其他確保其團體成員合法適當處理個人資訊，個人資訊保護法人應致力於依個資法立法宗旨，對有關利用目的之特定、安全管理措施、因應資訊本人請求之程序等事項、作成並公表「個人資訊保護指針」；並對其團體成員未遵守前述指針作必要指導、勸告與措施，讓其得為「Privacy Mark」制度[4]之認定機關，

[3] 日本原文爲「認定個人情報保護團體」。詳細條文得參酌其各子法第 37 條、第 41 條、第 43 條等規定。

[4] 爲實現民間處理個人資訊業者之自律規範，由日本之通商產業省外圍機構「財團法人日本情報處理開發協會 (JIPDEC)」，導入之有關個人資訊保護民間評鑑制度，即對在個人資訊之處理上

以增加其對團體成員之約束力。

日本銀行業界，於 2005 年 4 月以銀行 (包括外國銀行之分行)、長期信用銀行、銀行控股公司、全國各地銀行協會與全國銀行協會為成員組成「全國銀行個人資訊保護協議會」[5] ，並依個資法規定得到主管大臣之許可，成為「個人資訊保護法人」，制定公佈銀行業界之「個人資訊保護指針」 (下稱為協議會保護指針)，此指針為協議會會員所必須遵守之規範，其內容基本上多與個資法、金融 GL、安全管理實務指針相同，但仍為較具體、嚴格之規定。

綜上可知日本對有關金融機關 (特別是銀行業界)，處理個人資訊、顧客資訊之法規命令上自中央法律，下至業者自律規章，可分為 4 層：①. 個資法； ②. 個人資訊保護基本方針； ③. 金融 GL、安全管理實務指針； ④. 全國銀行個人資訊保護協議會（以下簡稱協議會）保護指針。以下即就各階層法令規範有關銀行業界處理個人資訊，有關本文主題之應遵守重要義務與原則介紹說明如下。

(二) 日本銀行業界保護個人資訊義務與原則

1.個人資訊取得之限制

此乃對應 OECD 八大原則中之「收集限制原則」而設置之規定。所謂適當取得：依個資法第 17 條、金融 GL 第 7 條與協議會保護指針 II 4 之規定：銀行協議會會員應於業務上必要範圍內，依適當且合法之手段取得個人資訊。如係由第三人取得個人資訊時，亦不得不當侵害本人之利益；亦即銀行業者不得以詐欺、偽造名義或虛偽之目的取得個人資訊，亦不得接受第三人以違法、不正當手段所取得之個人資訊之第三人所提供之資訊。

具備有完善保護措施之民間業者，授與「Privacy Mark」，容許其於事業活動中使用該標識。

[5] 至 2006 年 4 月為止，其會員數共有 247 位。

2.利用目的之通知與公表

此為 OECD 八大原則中「公開原則」與「個人參加原則」之實現。依個資法第 18 條、金融 GL 第 8 條與保護協會指針 II 2：銀行業者取得個人資料時：甲. 除已預先公表其利用目的者外，原則上應對本人通知或公表其利用目的；乙. 如以直接記載於書面方式自本人取得資訊時，原則上應預先對本人明示；丙. 授信業務之利用目的，原則上應得到本人之同意。但如對本人通知利用目的：①對第三人生命、身體、財產其他權利利益造成損害之虞時；②有損害協議會會員之正當權利、利益時；③將對有必要協助國家機關、地方自治團體遂行之法定事務，造成障礙之虞時；④自取得之狀況觀之，其利用目的被認為已非常明確時，則得例外無須取得本人同意。例如協助檢警機關犯罪搜查，而提供嫌犯之個人資訊者，為③適例；而對收購股票並於股東大會鬧事之職業股東資料之收集則為①之適例。而取得同意之方法原則上由本人於記載有同意文字之書面上署名為之；亦可以口頭方式、或以電子郵件方式取得同意；但不問任何方式，均應留下紀錄。另有關利用目的明示方法，可記載於書面，可以廣告方式張貼，可以發送手冊或傳單方式，同樣不問任何方式均應留下曾明示之紀錄。

3.利用目的之特定

此為對應 OECD 八大原則中之「目的明確化原則」所為之規範，原金融 GL 第 3 條承襲個資法第 15 條規定：金融領域之處理個人資料業者，其所取得之個人資訊為供如何之事業使用？依如何之目的利用？應儘可能以本人能合理預測方式予以特定。亦即不能抽象的「以供本公司所需目的使用」表明利用目的 (淺井弘章，2006)。銀行業界則考量其個人資訊：利用之特

殊性與銀行法之規定，保護協會保護指針 II 1 規定：「會員只得以法令所認可，執行業務之目的下為個人資訊之處理」；而在此指針下，再詳列一表特別將所謂特定利用目的之具體記載方式供業者參考；例如：「本行儲金業務、金融商品或服務之申請受理」、「本人之確認、利用金融商品或服務之資格確認」、「融資之申請或繼續利用之判斷」、「市場調查、依資料分析或問卷調查以開發或研究金融商品之用」、「發送 DM (direct mail)廣告等，以為有關金融商品或服務之推展介紹」、「業務合作公司之商品服務之推展介紹」、「授信事業，對個人信用資訊機關提供個人資訊」等，要求銀行業界應儘量將其個人資訊利用之內涵與外延，以顧客易於理解之方式為具體明確之記載。

4、利用目的之限制

此為對應 OECD 八大原則之「目的明確化原則」與「利用限制原則」而衍生之規定，亦即依個資法第 16 條、金融 GL 第 4 條與協議會保護指針 II 6-2 規定：協議會銀行會員除法令有規定或本人事先同意外，不得超越達成特定利用目的所必要之範圍，而為個人資訊之處理、利用。而上述本人之同意，原則上應以書面由本人簽章為之。

在此較特別者為個資法上未規定，而協議會保護指針 II 3 特別規定之事項：資訊本人請求直效行銷 (direct marketing)利用之中止；亦即協議會之銀行會員於有資訊本人要求其中止直效行銷目的下之個人資訊利用時，應即中止其利用或提供。此時即使協議會會員銀行事前已得到資訊本人同意直效行銷之利用目的，事後本人仍得請求中止或提供利用。

5.第三人提供之限制

自保護資訊本人利益觀點，處理個人資訊業者如事前未得

到資訊本人同意，原則上被禁止將該當資訊提供給第三人，因如此將使資訊本人無法掌握其被收集資訊如何被利用？傳送至何處？致有遭受不測之損害之虞。此一限制同樣為 OECD 八大原則中之目的明確化原則與利用限制原則所衍生而來者，由個資法第 23 條、金融 GL 第 13 條與協議會保護指針 V 予以明文規範。而此一限制事實上亦為最有爭議性之限制，因此處所謂「第三人」究竟範圍為何？應採如何之限制機制？顧客個人利益之保護、與銀行業者有效利用資訊以為經營間，能取得平衡，是重要之課題 (澤重信，2002)。尤以現今金融控股公司之成立，銀行業兼營保險業務或以子公司、企業集團方式販賣金融商品兼營理財、投顧等事業者眾多；另外亦有將不良債權委外催收者、或將顧客資訊委託給外部第三人整理、建檔者；而為銀行透過個人信用資訊機關 (如聯合徵信中心)進行業界間顧客資訊之交換，以確保授信之適當性與防止多重債務者問題發生等事，均行之有年或多有存在之個人資訊之現狀。

6.正確性、安全管理規則

(1)個人資訊正確性確保原則

基於保障資訊本人權益之觀點，因錯誤或老舊資訊被繼續利用或提供等，常會造成其損害，故 OECD 八大原則一明訂有資料內容原則，對應於此個資法第 19 條、金融 GL 第 9 條與協議會保護指針 III 均明定：處理個人資訊業者，於達成其利用目的之必要範圍內，應致力保持正確且最新內容之個人資訊。故而儲蓄存款客戶之個人資訊，其保存期間除法令有規定外，應依其利用目的，於契約終了後一定期間內予以消除。而此外要求之最新內容僅針對其個人資料之最新性，

如為過去破產紀錄等某特定時點之事實記錄，即無更新之必要。

(2)安全管理措施

依 OECD 八大原則中之安全性保護原則，個資法第 20 條、金融 GL 第 10 條與協議會保護指針 IV，對防止個人資訊之洩漏、滅失或毀損與其它安全管理，均明定業者有採取必要且適當措施之義務，要求其在組織上、人事上、物理與技術面之具體管理方法。① 組織上之安全管理措施：包括明定個人資訊管理責任人之責任與權限；制定安全管理規則、並對於其運作進行檢查、監督；具備得以確認個人資訊處理狀態之手段等，業者對安全管理體制之建立與施行措施。② 人事上之安全管理措施：與員工訂立個人資訊保密契約；進行員工有關安全管理措施之教育訓練；明確員工之職務與責任等；自人事上對員工自人事上監督個人資訊之安全管理事務。③ 技術上之安全管理措施：建立個人資訊利用人之認識與識別手段；個人資訊區分管理之限定與接觸之限制機制；防止個人資訊洩漏、毀損之方法；處理個人資訊之資訊系統監督與紀錄分析等，有關業者在技術面上之安全管理措施。

日本除了上述以法制面要求業者於保護個人資訊安全之前提下，為個人資訊之合理運用；更以「隱私權標章 (Privacy Mark)」之認證制度，加強業者重視保護個人資訊之意願與健全安全之管理體制。日本之「財團法人日本情報[6]處理開發協會 (JIPDEC)」，於 1999 年導入有關個人資訊保護日本工業規格「個人情報保護遵法 (Compliance)計畫要求事項」

[6] 日本之「情報」用詞爲取自英文「Information」一字，故於本文使用日本機關、團體原始名稱時，即選用日本之原文。

(JISQ15001)[7]，此規格中要求業者有關個人資訊保護應訂立遵法計畫與其施行、運用之細則，與個人資訊收集、利用與提供等措施、履行其適當管理個人資訊之義務，以資訊本人為權利主體對自己個人資訊有公開、訂正與消除之請求權、拒絕利用、提供之權利等，並對符合上述要求事項之業者由該協會發給 Privacy Mark；而取得認證之業者在其公司治理上是否滿足「風險管理」要項之認定時，為重要之判斷指標。如此制度之建立，讓業者自律性的遵守法令、健全制度以保護個人資訊，讓日本個人資訊保護，自法律面、實務面相互結合而更完整、周延。

[7] 詳細內容可自 http://www.jsa.or.jp/讀取。

參、美日兩國銀行保險通路利用銀行客戶資料法律依據的分析

一、美國銀行保險通路利用銀行客戶資料之相關規定分析

如前所言，GLBA 雖是美國聯邦法案，但非用之以取代或凌駕美國各州之相關法令。在美國共有 49 州外加哥倫比亞特區，其個人資料保護相關法令的嚴格程度至少同等甚至超越了 GLBA 的規定。故 GLBA 對銀行保險使用銀行客戶資料的規定，可說是美國境內之最低基本要求，本研究即以 GLBA 檢視之。以下分為兩種情況說明：

(一) 若銀行保險通路屬銀行所能掌控(own or control) 之聯屬公司(Affiliated company)，則銀行將其客戶資料公開或分享予銀行保險通路機構是被允許的。唯仍必須遵循 GLBA 有關金融隱私規定、安全保護規定、與防範詐取資料規定。

(二) 若銀行保險通路屬銀行所不能掌控之第三者，則銀行顧客可依拒絕公開權力(Opt Out)條款，選擇其個人資料不予公開。且在銀行每年寄發給顧客的隱私權通知書中，必須清楚揭露顧客可享有權拒絕其個人資料分享予非屬銀行所掌控第三者之權利。若銀行顧客未行使拒絕公開權利，銀行亦不得將其顧客資料公開予非屬銀行所掌控之第三者，作為電話行銷或其他直效行銷目的之用。換句話說，銀行若提供客戶資料給非屬銀行所掌控之銀行保險機構作為其推銷保險目的之用(如電話行銷保險或其他直效行銷保險)，是不被允許的。

值得特別注意的是，美國加州對於金融機構使用顧客個人資料的相關規定，已更趨嚴格。其中較為特別的是，金融機構顧客有權選擇拒絕將其個人資料公開予金融機構所能掌控之聯屬公司，也就是說，

銀行顧客有權選擇拒絕將其個人資料公開予銀行所能掌控之銀行保險機構。此修法內容將嚴重影響銀行保險分享顧客個人資訊之利益與方便性，故仍在爭訟中。

二、日本銀行保險通路利用銀行客戶資料之相關規定

日本銀行法第16條之二第5項規定銀行得以子公司方式經營保險業。再依同法第2條第8項規定：所謂子公司為銀行之母公司保有股東大會表決權50%以上之公司。依上述規定可知，日本銀行得設立子公司經營保險業務，母公司之銀行對子公司之保險公司握有絕對之掌控權。

依前述日本個人資料保護相關法令之分析可知銀行業者在使用其顧客資料時所受到之規範可簡要說明如下：

(一) 原則上採事先取得同意以(Opt In)機制使用顧客資料。即銀行業者應事先得到顧客本人之同意，始得將其個人資訊提供給第三者；而法令另有規定、或為保障時、對國家、地方自治團體或受其委託人所執行法令上規定事務有協助之必要、第三人之生命身體財產因得到本人同意將對該當事業遂行發生阻礙時，則不在此限。所謂「事前同意」，即為以 Opt In 機制保護顧客本人(田島正廣，2005)；在使用顧客資料時，應先得到同意，一旦得到本人同意而提供給第三人者，事後即使本人要求停止提供，銀行業者可不予回應。在此所謂之第三者應解為：非處理個人資訊之業者與顧客之本人者，均屬「第三者」。但下列三者非此所謂「第三者」:

1. 業者為達成利用目的所必要之範圍內，將個人資訊委託處理時。銀行業者常見之例子為委託外部公司為資料之輸入儲存、廢棄等。但此時銀行業者對受託人仍應進行必要且適當之監督。

2.因合併或其它事由繼受事業而受個人資訊之提供者。例如銀行業者因合併、分割而對新業者提供顧客資訊；此時受提供業者之個人資訊利用，仍不得超越原提供前該當個人資訊之利用目的範圍，以免個人顧客遭受不測之損害。

3.集團之共同利用者。事業集團之公司行號間互相共同利用顧客資訊之事，亦為常見之事例。銀行業者應事先以書面將共同利用之事情、被共同利用之項目、共同利用者之範圍、利用者之利用目的與該當資訊之管理責任人姓名或名稱等，通知顧客本人，獲致於本人容易得知之狀態 (例如於業者網路上揭載)，否則仍屬違法。此外上述通知之「共同利用者之範圍」，應採個別列舉方式記載，即使以外延方式記載者，亦希望採顧客本人容易之方式具體特定其共同利用人，例如：「本公司與有價證券報告書上記載之子公司、持股公司、合作事業等，....」為其適例[8] 而銀行以子公司，或為銀行事業集團中之適用多數持股之關聯公司，必然屬共同利用者，而非第三人，但仍應事先通知顧客本人。

(二) 銀行業者得採選擇拒絕公開(Opt Out)機制使用顧客資料。亦即業者不採 Opt In 機制在事先先取得資訊本人之同意其提供第三者利用，而是採在一定要件下，即使業者未事先得到資訊本人同意，亦容許其將該資訊提供給第三者之機制。詳言之，銀行業者對第三者提供個人資訊時，如於「事先」將①已對第三人提供為其利用目的，②提供給第三人之個人資訊之項目，③提供之手段或方法，④得應顧客本人請求停止將該當資訊對第三者提供，等事項以書面通知顧客本人或置於顧客容易得知之狀態時，得無需事先得到顧客本人同意而將該當資訊提供給第三者；有人亦稱本

[8] 請參閱 MIZUHO 金融集團共同利用規則通知，http://www.mizuhobank.co.jp/policy/kyodo-riyo.html。

項規定為 Opt In 機制之例外。申言之，如顧客本人要求停止公開其個人資訊時，銀行業者不問理由為何，應即停止其對第三人之提供行為，此為相應於前項 Opt In 機制對業者不利之處。而此項所謂「事先」之意義，因其非以取得個人資訊時之同意為要件，而係作為對第三者提供之要件而要求之通知，故應解為以對第三者開始提供之時點為基準，在此之前應通知顧客本人。在此所謂第三者為非處理個人資訊之業者與顧客之本人均屬之。

綜上所述，可知日本銀行業者個人資訊提供給屬於前述(3)之共同利用人，即金融集團之子公司，持股公司時，及不屬於對第三人提供個人資訊，故其共同利用個人資訊之行為，無須得到顧客(即資訊本人)之同意；但業者仍須在事先告知資訊本人：共同利用人之範圍、被利用個人資訊之項目、利用目的、該當資訊管理責任人等，始得合法為共同利用之行為。顯然本質上仍具有 Opt-In 之精神在，資訊本人對自己個人資訊之流向、用途，在事先仍有知悉之機會。

但如銀行業者將顧客個人資訊提供給非事業集團內(非共同利用人)之其他第三人時，原則上採 Opt-In 機制，再提供給第三人之事先必須取得資訊本人之同意；但亦可選擇 Opt-Out 機制，此時則必須將提供第三人之事、個人資訊之內容，提供方法與應本人要求停止提供等事項，在提供給第三人前，預先通知資訊本人。

一般而言 Opt-Out 制，對業者有利，因為只要資訊本人(顧客)未表示不同意，其即得與其他業者共有顧客資訊；僅於事後當資訊本人要求停止提供時，不問其任何理由，業者均應立即停止提供及利用。

三、美國與日本銀行保險通路利用銀行客戶資料規範之比較

觀察美日兩國對於銀行保險通路使用銀行客戶資料之規範，在分享顧客資料予可掌控或集團下之銀行保險通路時，兩國之規定差異不大。若是分享顧客資料予不可掌控或非集團下之銀行保險通路時，兩

國之規定則有較大之差異。請參閱表一。

表一、 美國與日本銀行保險通路利用銀行客戶資料規範比較表

		銀行顧客資訊分享予可掌控或集團下之銀行保險通路	銀行顧客資訊分享予不可掌控或非集團下之銀行保險通路
美國銀行業者	是否被允許	無須事先徵得顧客之同意即可將顧客資料分享予銀行保險通路，銀行顧客無從拒絕。（但少數幾州例外）	若顧客選擇其個人資料不予公開，則銀行業者不得分享其顧客資料予銀行保險通路（Opt Out 機制）。
	是否有使用條件	多數仍遵循GLBA之金融隱私規定、安全保護規定、與防範詐取資料規定。	若顧客未選擇其個人資料不可公開，銀行業者仍不得分享其顧客資料予銀行保險通路作為電話行銷或直效行銷之用
日本銀行業者	是否被允許	係為共同利用，銀行業者無須徵得顧客之同意即可將顧客資料分享予可掌控或集團下之銀行保險通路，銀行顧客無從拒絕。	原則上採 Opt In 機制，須事先以書面徵得顧客之同意始得將顧客資料分享予非屬集團下之銀行保險通路。 例外採 Opt Out 機制，若銀行顧客選擇拒絕公開其個人資料，銀行業者不得將顧客資料分享予非可掌控或非集團下之銀行保險通路。
	是否有使用條件	銀行業者事先須以書面將共同利用之情事、項目、共同利用人之具體範圍、目的與管理資料人之姓名或名稱通知顧客。	在 Opt In 機制下，顧客書面同意銀行業者使用其個人資料後，基本上不得反悔。 在 Opt Out 機制下，銀行業者必須清楚向其顧客揭示有關「可選擇拒絕公開個人資料」之訊息。
	例外	有關直效行銷之中止，不問為集團內之關係企業共同利用或為經同意提供給第三人使用，亦不問是否採 Opt In 或 Opt Out 機制，只要資訊本人要求停止提供資訊供直效行銷使用時，均應為停止提供、利用行為。	

資料來源：本研究整理

四、我國新版個資法與金融控股公司法之相關規定：

過去保險業雖列在舊有電腦處理個人資料保護法的「八大行業」，只要保險公司向目的事業主管機關申請執照（保險業電腦處理個人資料執照）就可依規定使用；但新個資法全面上路後，執照便告失效，必須改依新法行事。新法施行後，凡使用個資都必須經當事人同意，新法對保險業有許多顯著的衝擊，一是將重挫電話、網路行銷等新型態通路，主管機關若未規劃配套，幾乎是對電銷為主的公司宣告死刑；二是「特種資料」的規定，恐使健康險的核保、理賠作業窒礙難行，除業界可能不敢再賣健康險，舊保單保戶權益也將因理賠時的病歷查證有問題而受損。以上種種衍生問題均將對保險業之正常經營產生重大衝擊

再查我國金融控股公司法（下稱金控法）第 42 條之規定：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。主管機關得令金融控股公司及其子公司就前項應保守秘密之資料訂定相關之書面保密措施，並以公告、網際網路或主管機關指定之方式，揭露保密措施之重要事項。及其第 43 條規定：金融控股公司與其子公司及各子公司間業務或交易行為、共同業務推廣行為、資訊交互運用或共用營業設備或營業場所之方式，不得有損害其客戶權益之行為。前項業務或交易行為、共同業務推廣行為、資訊交互運用或共用營業設備或營業場所之方式，應由各相關同業公會共同訂定自律規範，報經主管機關核定後實施。前項自律規範，不得有限制競爭或不公平競爭之情事。

依上述金控法之規定，於金控集團下各關聯企業應解為可以共同利用客戶個人資訊；而對此個人資訊之共同利用，僅概括以「法律」、「主管機關規定」、「應保守秘密」等規範，在立法上實已過於簡陋、模糊，易滋生適用上之困擾；且對於「保密措施」亦僅規定主管機關

「得」令金融控股公司等訂定「相關書面保密措施」，並以公告等方式「揭露」，此處規定為「得」，顯然主管機關並無法律上義務命金融控股公司訂定保密措施及揭露之，讓應立於最後一線保障人民權益之政府機關有卸責之辭，是否妥當？仍有商榷之餘地。再者，所謂「揭露」，依字面上觀之，似乎未包括對顧客本人之「通知」，對客戶個人權利之保障，亦嫌不足。

肆、結　語

行政院金管會保險局面對新版個資法對保險業所帶來之重大衝擊，傾向於利用新版個資法第 6、8、9、19、20 等條文中所賦予主管機關另立法排除個資法之適用，另修保險法 177 條內容因應之。綜觀上述美、日之有關銀行保險使用銀行顧客資料之規範，至少吾人可以得到以下之結論，可作為主關機關修訂保險法 177 條內容實之參考：

一、法令位階規範建立之必要性：

不問美國或日本均以政府機關居於主導之地位，以立法或行政命令評定方式，建構金融機關使用顧客個人資訊之基本準則，讓以營利為目的之金融業者有一最低限度應共同遵守之規範，此對於相對弱勢之顧客而言，至少能因此得到一定程度之權利保障。

二、金控集團下各關連公司共同顧客資訊原則之建立：

美、日兩國均允許同意金控集團中之企業共用顧客之客人資訊，當然對金融業者而言，可以節省經營之成本，方便行銷；但對顧客而言，卻增加個人資訊被外洩、濫用之風險，且如此之共同利用，資訊本人幾乎無置喙之餘地，實際上有違 OECD 八大原則中之個人參與原則，因此即使為同一金控集團下之個人資訊之流通，如何讓資訊本人更確實掌握其個人資訊之利用狀況，有更多自主之權利，應是一個應思考之方向。

三、Opt In 制與 Opt Out 制之選擇或併用：

承上所述，為讓顧客之自我資訊控制權更能落實，對金控集團間共同利用其個人資訊上，至少應建立 Opt In 機制、或 Opt Out 機制，讓顧客自己能有機會預見自己個人資訊在共同利用過程中可能負擔之

風險與被利用之範圍。美、日兩國或採 Opt Out 制、或併用兩制，其目的應即在於此。

參考文獻

中文部分

1.邱金蘭(民 93)。客戶資料外洩三銀行挨罰，10 月 19 日，經濟日報，A1 版。

2.康世人(民 96)。http://www.epochtimes.com/b5/7/5/2/n1697563.htm

3.吳尚昆(民 96)。金控客戶資料保護的法律問題，5 月 13 日，經濟日報，C7 版。

4.劉靜怡(民 91)。隱私權保護的國際化爭議，月旦法學，86 期，195 頁。

5.蔡靜紋(民 95)。保密任務壽險業啟動毀滅裝置，9 月 5 日，經濟日報，B2 版。

英文部分

1.ABA Trust Letter. (2006). The quest for friendlier privacy notices. ABA Trust Letter, Washington. 486, 1-2.

2.Brown, W. N. (2001). Financial Services Modernization Act 1990-US, Regulation of financial institutions, Right of privacy. International Financial Law Review, London.

3.Byme, J. (1999). What is-and what could have been. ABA Banking Journal, 91(12), 17-18.

4.Daily Record Staff (2005). Attorneys held exempt from privacy provisions of Gramm-Leach-Bliley Act. Daily Record, NY, Dec 8, 1.

5.Giglio, V. (2002). Privacy in the world of cyberbanking: emerging legal issues and how you are protected. The Secured Lender. 58(2), 48-55.

6.Gustini, R. J. (2002). Privacy law's annual review, Community Banker. 11(5), 44-45.

7.Maffett, N. (2005). Six steps to better protection of benefits information, Employee Benefit News, Dec 1. 1.

8.Nordman, E. & Krohm, G..(2002). A view of the growing saliency of privacy as insurance regulatory issue. Journal of Insurance regulation. 21(1), 79-85.

9.Schneck P. (2005). GLBA puts bank e-mail firmly on the hot seat. Bank Technology News. 18(7), 44.

10.The Information Management Journal (2004). California passes online privacy Bill. The Information Management Journal, September/October, 11.

11.Warren , S. D. and Brandeis L. D.(1890). The Right to Privacy, HARV. L. Rev, 4, 193.

12.Prosser,W. L. (1960). Privacy, CALIF L. Rev. 48, 383- 389.

13.Xoom Privacy Policy (2007). Privacy Policy, https://www.xoom.com/privacy.

日文部分

1.FISC (2004). 財團法人『金融資訊系統中心』 (The Center for Financial Industry Information Systems)簡稱

FISChttp://www.fisc.or.jp/ippan.htm。

2.田島正廣，2005。個人情報保護法と金融機關，經濟法令研究會，7月，192頁。

3.宇賀克也，2005。個人情報保護法の逐條解說 (第2版)，22頁。

4.佐藤幸治，1997。憲法，青林書院，428頁。

5.淺井弘章，2006。個人情報保護法と金融實務，金融財政事情研究會(第3版)，71頁。

6.澤重信，2002。銀行による生命保險の窓販にフいて(中)，銀行法務NO. 611，11月號，60頁。

7.藤田義治，2004。個人情報保護法と金融實務，銀行法務NO. 633，1頁。