個資保護規範下之大數據現況運用與未來發展

研究性質：「資產管理人才培育與產業發展基金」108 年度工作計畫
計畫主持人：王儷玲教授
研究期間：108 年 4 月～108 年 12 月
報告摘要：

回顧 2018 年全球發生許多數據洩漏大事，如新加坡知名保健集團的 150 份病歷資料外流；英國航空公司也有 38 萬名乘客信用卡支付資料被洩漏，最受全球注目的 Facebook 有 300 萬名歐洲用戶的數據流失。同年歐盟也施行了堪稱史上最為嚴格的「一般個人資料保護規則」（General Data Protection Regulation，GDPR），而 Google 成為違反 GDPR 遭 5 千萬歐元重罰的首例，可見大數據時代，個資保護已是當前最受重視的關鍵議題。

資產管理業者之核心業務是資產配置與投資管理，與其他金融機構比較，接觸到的客戶資料較少也相對單純，涉及個資部分，主要是直銷或網路下單的公司，個資種類僅限於聯絡資料、資產規模、風險胃納等。另一方面，資產管理業者無論在資本額或人員編制，皆不及銀行、保險等金融機構，若要符合國際個資管理規範（如 ISO27001）、設立獨立的資料保護長（DPO）、個資盤點、系統建置及修改資訊架構等以符合 GDPR 之精神及規定，對投信投顧業者可能產生龐大的法遵成本。

本研究建議希望落實於資產管理業者，使資產管理業者了解在目前個資保護的世界潮流下，該如何善盡業者義務；另方面，也考量資產管理業者資源有限，如何在有限資源前提下符合規範要求。為了解投信業者對保護客戶資料的相關作法，本研究撰擬相關問卷詢問投信業者。共計發放 37 份問卷，回收 14 份，原則上，回覆業者八成五到九成皆有做到個資保護程序（包括個資盤點、設置專責單位或人員、訂定個資洩漏通報程序及員工教育訓練），彙整結果如下表

單位：家數

	有	無	不清楚
1. 個資保護程序			
(1) 進行資料盤點，並刪除蒐集目的不存在資料	13	1	0
(2) 設置資料保護專責單位(人員)	12	2	0
(3) 訂定個資外洩時通報程序	14	0	0
(4) 舉辦個資保護員工教育訓練	14	0	0
2. 個資蒐集時，取得當事人同意有無困難？	13	1	0

3. 「個人資料保護法」相關規範對公司業務推展或實務執行上產生之困擾？

(1) 金管會為強化債券 ETF 投資人分散之管理措施，透過投信投顧公會通知各投信業，要求任一已掛牌 ETF 單一投資人持有比率應調降至 70%，新成立之 ETF 前六個月單一投資人持有比率不得超過 50%，六個月後應調降至 30%。惟因 ETF 於集中市場或證券櫃檯買賣中心掛牌交易，投信事業並無受益人明細，須向集保結算所申請基金受益人明細，以確認單一投資人之持有比率，而投信事業向集保結算所申請受益人資料時，集保結算所以個資法為由，將受益人資料進行遮蔽，遮蔽後資料難以判定真實受益人，致投信事業難以遵循主管機關之政策及要求。

(2) 開戶作業時，法人戶提供之文件如變更事項登記表、股東名冊等，除負責人以外之身分證字號會因個人資料保護法規範將 ID 遮蔽或不提供，造成困擾。

4. 建議開放條文

個人資料保護法第 19 條第 1 項及第 20 條規定，非公務機關對個人資料之蒐集或處理或利用，除第一條所規定資料外，應於特定目的內為之，並須符合法律明文規定，致集保結算所無法提供受益人明細，故建議上開條文有關法律明文部分，修正為法律或法令規定，俾利非公務機關業者得順利遵循主管機關要求。

為了落實產業發與個資法於資產管理業者之適用，本研究提出以下建議：

一、 法制面:

我國當事人個資保護適用「個人資料保護法」，該法主管機關為法務部，但涉及不同領域時則由各該目的事業主管機關發布相關函令解釋。因此，「個人資料保護法」屬普通法性質，以金融業來說，因金融服務所生的個資疑義，應由金管會解釋。前述業者所提供建議：包括 ETF 之真實受益人明細、法人開戶作業時，除負責人外的其他自然人 ID，皆因個資法要求而進行遮蔽，造成業者業務執行上的困難，這部分建議主管機關可以行政函令方式加以解釋，應可排除個資法適用。

二、 個資保護要求宜採分級架構

投信業者規模差異不大，訂定一致規範適用於所有投信業者應可行，但仍與銀行、保險之規模與業務複雜度相差甚遠，應有差異化規定。另投顧業者業務型態差別更大（全委投顧，媒體投顧，僅提供建議投顧），除與投信相較規模也小，業務相對單純外，更應有不同標準。或可參考資安分級管理（依規模、營運模式）之精神，訂定適用於資產管理業之個資規範。

三、 透過金融科技降低資產管理業者個資保護法遵成本

投信投顧業以資本額或員工人數而言，算小型金融機構。從經濟效益方面分析，法律遵循往往改變作業流程，大幅墊高作業成本，而投信投顧業者難以獨自負擔。因此，若要完全遵守個資/ GDPR 要求，業者可能會為了減輕法遵壓力有兩極反應：一是透過金控母公司之協

助導入 GDPR 之精神及規定；另一則是減少直接銷售業務（將不接觸客戶個資），專心從事資產管理部分。

參考世界發展趨勢，目前已有分級管理與資料中心（Data Center）概念，由資安等級較安全的資料中心處理資料後供業者使用，能減少業者蒐集、處理及運用的硬體架構成本，也降低業者違反個資保護規範機率。另外，也有一種標準化平台，該平台上提供合乎法規之標準化規範及資安環境，業者於該平台上處理資料則能降低違反個資保護的風險。如此可使資產管理業者減少個資保護的法遵成本。

四、 因應個資保護應檢視組織架構與提升資安技術

資產管理業者可參酌本身組織架構、業務性質，或許考量設置專責單位(或人員)，統籌管理資訊安全相關事宜，另為提升全員資安概念，台北 101 的測驗機制與情境演練也是很好的範例。本研究回覆問卷 14 家業者，其中 12 家皆有設置個人資料保護專責單位（或人員），僅 2 家未設專責單位。未來各公司應積極檢視目前公司在資安與個資保護程序是否達到實際效益？是否還有資安漏洞之虞？

五、 借鏡 GDPR 納入隱私保護預設機制

「當事人明確同意」將會是未來個資保護的重點，目前常發生在不自覺的情況就「同意」對方使用個資，因此 GDPR 規範「同意」須以聲明或清楚、積極的行為為要件，單純沉默不構成當事人同意。但此要件在網路金融服務比率不斷攀升的情況下，隨著個資當事人「資料可攜權」、「被遺忘權」之主體意識高漲，未來若客戶主張其權益受損時，該如何證明客戶曾經同意的軌跡？或許是業者應認真思考的議題。因此，研究建議可借鏡 GDPR，未來應納入隱私保護預設機

制，以協助避免在預設選項設計上違反個資保護相關規定。

六、 依循業務特性以個資生命週期方式徹底個資盤點

本次研究調查回覆問卷 14 家業者中，有 13 家均有進行個資盤查作業，並會刪除蒐集目的已不存在的資料，僅 1 家未進行相關盤點。由此可見，個資盤點已在組織之中受到重視，了解組織中有那些部門接觸個資？擁有那些個資項目？個資如何被利用？個資使用目的是否與當初告知客戶目的相同？個資流向如何維護等是企業維護個資非常重要的機制。但是以目前全球資安發展與個資保護趨勢而言，本研究建議未來資產管理業者應進一步依循其業務特性，以個資生命週期方式進行個資盤點，才能更嚴謹有效率地掌握個資動向，確實做好個資保護。