資產管理人才培育與產業發展基金委託專題研究

個資保護規範下之大數據
現況運用與未來發展

財團法人中華民國
證券暨期貨市場發展基金會
SECURITIES & FUTURES INSTITUTE

2019 年 12 月


S-F-I

資產管理人才培育與產業發展基金委託專題研究

個資保護規範下之大數據現況運用與未來發展

計畫主持人　王儷玲

研 究 人 員　葉淑玲

陳恩儀

汪宛臻

財團法人中華民國
證券暨期貨市場發展基金會
SECURITIES & FUTURES INSTITUTE

2019 年 12 月


S-F-I

目　　錄

表目錄

圖目錄


S-F-I

第一章　緒 論

第一節　研究動機與目的

金融科技（FinTech）核心發展領域主要由人工智慧（Artificial Intelligence）、區塊鏈（Blockchain）、雲端運算（Cloud Computing）與大數據（Big Data）等 ABCD 四大支柱構成。其中 A（人工智慧）[1]與 D（大數據）[2]涉及大量個人資料的取得與利用。數位時代，資訊正成為一種生產資源，是繼土地、人力、資本後的新要素，無論政府、企業、個人等都深受其影響。

大數據（Big Data）又稱巨量或海量資料，本質上具有大量性（Volume）、即時性（Velocity）、多樣性（Variety）及真實性（Veracity）等 4V 特色。時下熱門的大數據技術，透過業者大量儲存使用者的使用紀錄，將資料以巨量分析及資料探勘等方式，萃取出有用或可供預測的資訊，除可幫助業者了解使用者行為，進而發展新服務，大數據技術也對科學與商業帶來極大利益，同時也影響國家政策方向。

在金融領域，大數據應用不僅為業者帶來嶄新服務商機，對客戶也帶來新的消費體驗，以「開放銀行」（Open Banking）為例，透過金融數據共享，消費者可用便宜快速方式串聯大數據分析等先進技術，獲得更多元的金融服務。另一方面，人工智慧與機器學習也顛覆傳統財富管理模式，許多資產管理業者運用自然語言處理、圖像識別及機器學習等技術分析大數據，以發掘投資機會，但在找尋適當資料提升

[1] 人工智慧的核心技術--機器學習，實際上是機器透過讀取大量的樣本數據，進行規律性分析，建構出自我的認知模型，僅單一的購物領域的智慧客服往往都需要數萬條問答樣本數據，才能實現一定的精準度。

[2] 大數據的核心並不在於數據的獲取，而在於數據的分析識別，只有透過分析才能獲取很多智慧的、深入的、有價值的資訊。而行動互聯網、物聯網、社交網絡、數位家庭、電子商務等是新一代資訊技術的應用形態，這些應用不斷產生大數據，而這些大數據的屬性，包括數量、速度、多樣性等等都是呈現了大數據不斷增長的複雜性。

投資報酬時，卻如同大海撈針，原因在於全球經濟與金融市場具有高度複雜性，蒐集到的資料通常零散雜亂，只有竭盡所能評估足夠多的資料量，才能有效判斷哪些訊息對投資過程最有用。此外，要提升預測品質，需藉由多個資料來源相互印證（如綜合消費資料，包括消費者網路搜尋紀錄、銀行信用卡交易紀錄等），然而，使用多來源資料時，需嚴守法遵制度以保障個人隱私。

美國總統科學技術顧問委員會（President's Council of Advisors on Science and Technology，PCAST）在「大數據與隱私報告」（Big Data and Privacy：A Technological Perspective）[3]中指出：以事前知情並同意作為個資保護，在大數據時代已不合時宜，因大數據時代對個人隱私權保護的最大挑戰，來自遠超過資料當事人所想像的巨量資料與高效率分析技術發展。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。

大數據應用本質上係追求資料開發的價值極大化，而個人資料（或隱私）保護目的則在保障個人對於個資的自主控制，兩者價值各異，實難置於同一天平上衡量輕重。目前許多企業或機構對個資蒐集，幾乎隨時隨處進行，且以隱性方式為之，令資料當事人根本難以察覺，日後用於各種延伸用途，更遠超過原始蒐集目的，個資不當使用將成最大隱憂。

[3]https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf

資產管理業者之核心業務是資產配置與投資管理，基金銷售過程中，大部分是透過銀行或證券商通路販售，此時並無接觸客戶資料，但也有部分是由投信業者直接銷售，則可能接觸客戶個資。另外，投信業者能接觸客戶個資的種類與數量，與銀行相比都少許多，故在個資保護方面是否採分級架構？以致於資產管理業者可負擔較輕的法令遵循成本。本基金會接受「資產管理人才培育與產業發展基金」委託，進行「個資保護規範下之大數據現況運用與未來發展」研究，最終希望探討在個人資料被保護的前提下，如何使資產管理業者能運用大數據分析技術拓展業務，以創造資料經濟的價值。

第二節　研究流程

本研究進行之方法與步驟如下：

一、研究小組討論會議

不定期召開研究小組討論會議，由計畫主持人指導研究人員關於研究方向、報告架構與內容重點等，以利後續資料蒐集與研析。

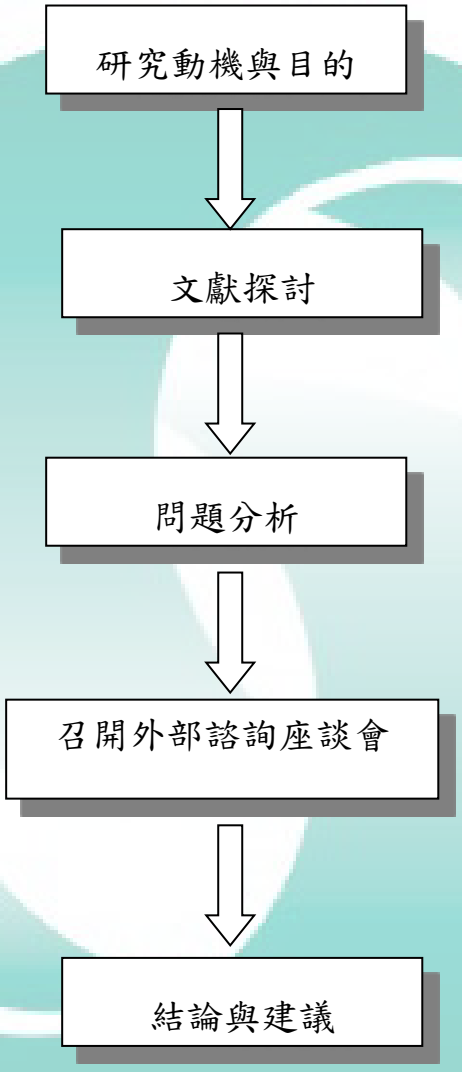
二、徵詢外部專家學者意見

為使本研究報告更臻完善，擬邀請政府機關、業界及學術界人士與會，藉由研究發現召開產官學座談會，提出分析意見，俾使本研究之建議方案更為切實可行。本研究已於今（108）年 10 月 30 日召開外部產官學諮詢會議，與會先進提出許多寶貴意見，會議實錄詳參附錄一。

三、撰寫文稿

由研究人員研讀文獻資料、整理國內外資料、召開產官學座談會，歸納分析各相關議題，依研究主題範圍撰寫報告文稿內容並提出建議。

本研究計畫之研究流程請參見下圖



第二章　巨量資料應用與個資保護

「資料經濟」（Data Economics）已成國際間熱烈討論的議題，資料儼然與能源並列為重要經濟資源，與其他經濟資源最大不同：資料不因使用而消耗，反而可不斷重組再利用。當大量多元資料與大數據統計分析應用技術結合時，可將技術用以尋求各種結構化、非結構化或半結構化資料間的關聯性，或將各式統計分析應用至科學研發、醫療保健、組織管理、趨勢預測等領域之產品或服務。

「大數據技術」即是透過大量儲存使用者的使用紀錄，例如在智慧手機的脈絡下，包括終端固有 IP、位置資訊、APP 使用紀錄等，將這些有系統的資料型態透過巨量分析與資料探勘（data mining）方式，萃取出有用或可供預測的資訊，大數據技術為資訊經濟開創新時代，也為科學及商業帶來極大利益，且影響國家政策制定方向。

然而，資訊洪流對個人隱私侵犯造成隱憂，各樣資訊如個人就診紀錄、位置資料、交易資料等，可輕易被複製並分享至全球各地，維護資訊安全與保護隱私愈來愈難。一般而言，去識別化（de-identification）被認為在利用資料分析技術時，可保護個人隱私，但有專家指出，即便已去除個人資料的識別性，仍可透過技術將去識別的資料「再識別」（re-identified）。因此，大數據時代下，資料大量產生後將會被有目的的蒐集與連結，因資料來源廣泛使可供比對的數量大幅增加，而資訊技術發展與資料識別能力快速攀升，資料愈來愈難以匿名方式保存，無疑對個人隱私造成極大衝擊。

全球主要市場中，近來歐盟在個人資料保護發展上相對積極，新通過施行之「一般個人資料保護規則」（General Data Protection Regulation, 縮寫 GDPR；歐盟法規編號：(EU)2016/679），已取代「個

人資料保護指令」（Data Protection Directive 95/46/EC）[4]。屬於歐盟法律中對所有歐盟個人關於數據保護和隱私的規範，GDPR 主要目的為取回公民及住民對個人資料的控制。

本章將探討大數據應用下的個資保護制度，並臚列主要國家（或組織）對隱私權與個資保護之重要原則；另外，介紹歐盟個資規則的主要改變及重要內容，最後，研析我國個資法與 GDPR 比較，了解大數據應用下個資保護的發展趨勢。

第一節　大數據應用與個資保護之兩難

大數據應用是追求資料開發的價值最大化，而個人資料保護的最終目的則在保障個人資料的自主控制，兩者價值各異；然若兩者價值產生衝突時，孰輕孰重仍應按法益衡量方式，調整既有框架尋求利益最大化之解（如大數據採用隱私保護設計概念，Privacy by Design, PbD[5]）。舉例言之：研究流行病學的國民健康保險資料涉及健康人權議題；六輕設廠後居民健康狀況變化的分析統計資料，攸關環境正義議題，皆有特殊公共利益，但若欠缺以大數據資料為基礎的實證分析，則無法形成健康產業政策的資訊基礎，現代法治國家負有「政府資訊

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

[5] 歐盟網路與資訊安全機構（European Union Agency for Network and Information Security, ENISA）2014 年 12 月公告一項「設計階段納入隱私與資料保護」報告指出，隱私保護的制度設計其實可以導入技術手段，並採納許多隱私設計策略與隱私保護技巧，包括：資料最小化、個資隱藏、個資分離、個資集結、通知、控制、執行與個資利用公告等八種隱私設計策略；以及包括驗證、資格 顯示、安全保密私人通訊、秘密通訊、資料庫隱私、統計揭露控制之隱私技術、保護隱私之資料探勘、私人資訊檢索、儲存隱私，以及維護隱私之運算等十種隱私技巧。葉志良，「大數據應用下個人資料定義的檢討：以我國法院判決為例」，資訊社會研究 31（2016），頁 26。

公開」與「個人資料保護」之義務，政府機關可否以個人資料保護為由拒絕提供學術研究機構相關資料，如何求取平衡成為關鍵議題。

一、 大數據已成新戰略資源

數位時代，資訊正成為一種生產資源，是繼土地、人力、資本後的新要素，無論政府、企業、個人等都深受其影響。大數據（Big Data）又稱巨量資料，就是過去廣泛用於企業內部的資料分析、商業智慧（Business Intelligence）和統計應用。但大數據已不只是資料處理工具，更是企業思維和商業模式，因資料量急速成長、儲存設備成本下降、軟體技術進化及雲端環境成熟等客觀條件具備，使資料分析從過去洞悉歷史進化到預測未來，開創前所未見的商業模式。

一般而言，大數據的定義是 Volume（容量）、Velocity（速度）和 Variety（多樣性），但也有人另外加上 Veracity（真實性）和 Value（價值）兩個 V（參圖 2-1）。但不論是幾 V，大數據資料特質和傳統資料最大的不同是：資料來源多元、種類繁多，大多是非結構化資料，且更新速度快，導致資料量大增。而要用大數據創造價值，不得不注意數據的真實性。

圖 2-1 大數據定義

資料來源：一次搞懂大數據(上)
https://www.bnext.com.tw/article/35807/bn-2015-03-31-151014-36

事實上，數據貫穿每個人各個生命階段，從懷孕生子、工作到理財，大數據將全面影響每個人與企業。例如有一款名為 Ovia Fertility 的 App，藉由分析 30 萬名會員的數據，開發演算法，精準計算排卵期，提高懷孕機率，該款 App 已成功幫助 5 萬名會員懷孕。又如 Workday 推出一套軟體，預測員工的薪水漲幅與可能跳槽時間，幫助企業決定每名員工的加薪幅度、時間點和轉職時機。理財也逃不過大數據的掌控，騰訊於 2015 年初推出第一家用大數據決定借貸與否的銀行，微眾銀行結合人臉辨識和公安部門資料，決定借貸者的信用等級。

現今社會所產生、使用和擁有的資料量是空前龐大，然而，IDC（國際數據資訊，International Data Corporation）預測全球資料領域將在未來幾年持續增長，現今的資料量根本微不足道。IDC 估計，2025 年全球將創造和複製高達 163zettabytes 的資料量[6]，（達 1 萬億 gigabytes），是 2016 年產生資料量的 10 倍之多。運算和資料儲存密度及其可用性突飛猛進，創造數位科技和服務的全新應用。隨之企業工作和生活模式所衍生的需求，驅動蒐集、管理、處理和傳送資料技術的進一步發展，如此循環的結果，導致全球資料領域呈爆炸性成長（參圖 2-2）。

[6]將 163ZB 經過轉化，相當於把 Netflix 網站上所有影片播放 4 億 8,900 萬次，或把內容燒成 40 兆片 DVD，而 DVD 疊起可以來回地球和月球 1 億次。

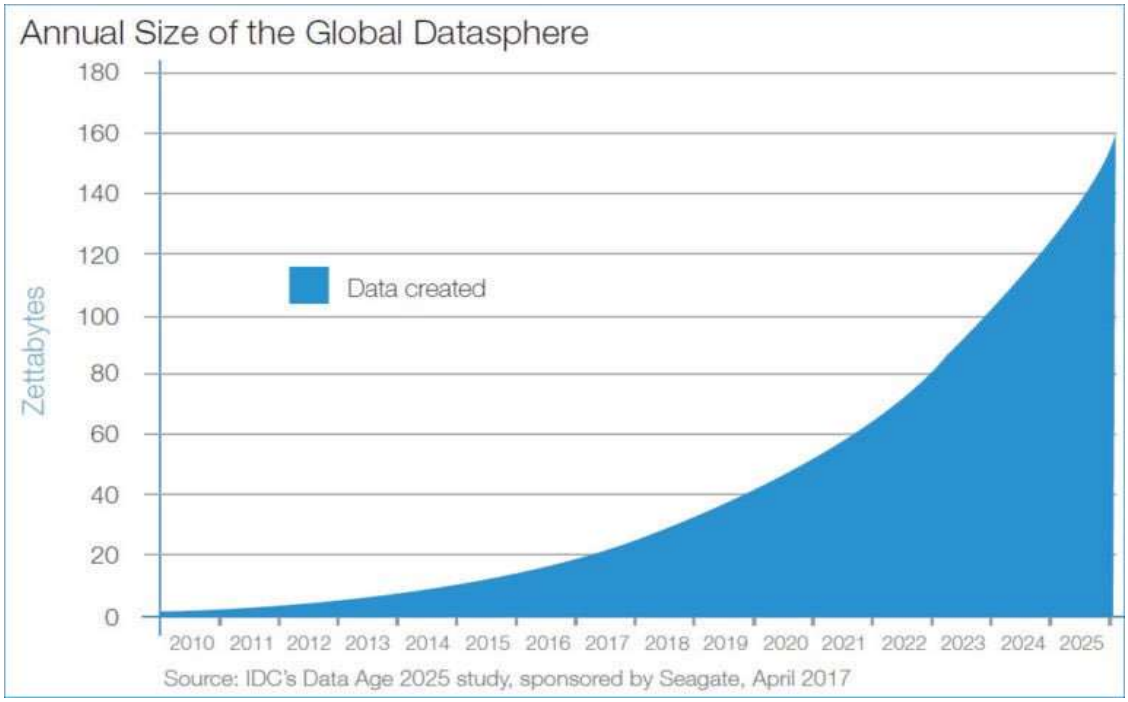


圖 2-2 全球每年資料領域總量

僅僅 10 年，我們就見證從類比到數位的轉變，而下一個 10 年，資料力量帶來的改變將無可限量。試想，虛擬個人助理在早上將您喚醒，依據氣象預測和您的行事曆建議適合的穿著，接著自動駕駛汽車便會載您前往目的地。或者根本無須通勤到辦公室，因為透過互動介面，科技會像變魔術般讓辦公室浮現在空中，而全息式（holographic）電話會議將成為與同事虛擬溝通的常態。週末可透過擴增實境 app 瀏覽新家具，看看沙發在客廳擺放的樣子再下單。週六夜，您賴在沙發上叫的外送 pizza 將會是由機器人製作、並透過無人機送達。我們正快速地邁向嶄新的數據時代。從自動駕駛汽車到人形機器人，從智慧個人助理到智慧家庭裝置，我們周遭的世界正經歷根本上變化，改變著我們的生活、工作和娛樂方式。

IDC 於"Data Age 2025"中針對資料如何深化對世界的影響，提出五大趨勢[7]，其中一項提到「安全是關鍵的基礎」。2015 年企業產生的

7 https://www.seagate.com/www-content/our-story/trends/files/data-age-2025-white-paper-traditional-chinese.pdf

資料不到全球總資料量的 30%，但到 2025 年，預估數字將增加至近 60%。以用戶在社群媒體產生內容為例，雖然每人分別上傳自己的影片、照片並撰寫貼文，但終究社群媒體平台必須在其基礎設施中儲存和管理這些資料。企業有權限存取和管理這些不斷增加的個人資料，因此對隱私權和安全風險也必須承擔更大的責任。

此外，隨著嵌入式感測器數量的增加，交易資料在不知不覺中被擷取，個資外洩情形增加，使得資料的安全防護需求更加迫切。儘管絕大部分的資料都需要受到某種形式的保護，但真正受到保護的資料量卻遠低於此(參圖 2-3)。如此大的差距代表產業對安全和隱私技術、系統和處理流程的需求將明顯增加。因此，如何在資料分析的過程中仍保護個人隱私，已成為大數據時代極重要的議題。

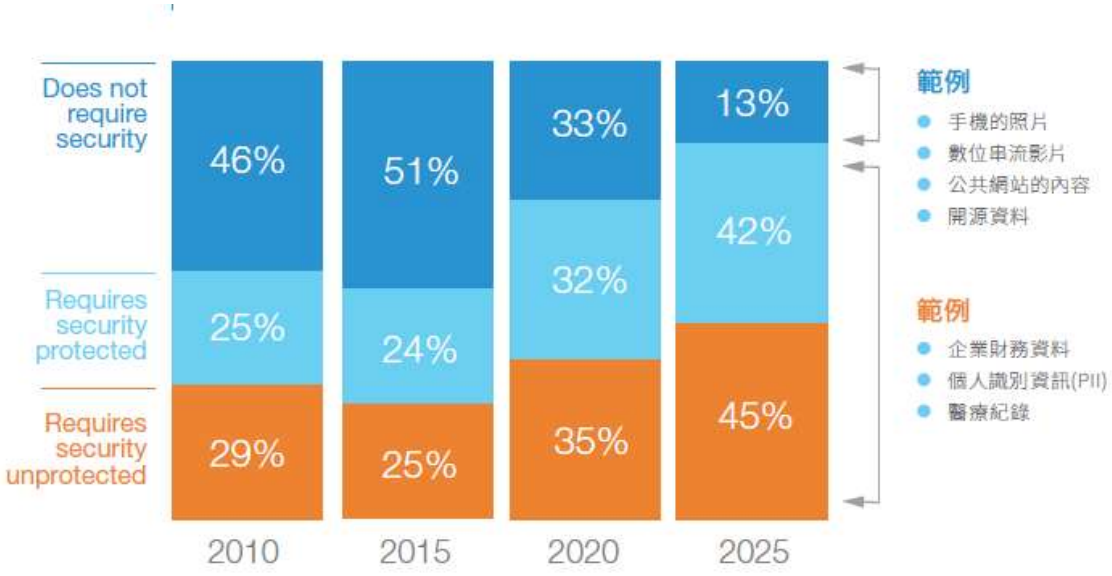


圖 2-3 資料防護真實情況

資料來源：

https://www.seagate.com/www-content/our-story/trends/files/data-age-2025-white-paper-traditional-chinese.pdf

二、 世界主要國家個人資料保護制度概述

歐盟的基本人權憲章（The Charter of Fundamental Rights of the European Union）明確指出隱私權與個人資料保護的重要性，該憲章第 7 條規定，任何人皆須尊重他人私人生活、家庭活動與個人通訊（Everyone has the right to respect for his or her private and family life, home and communications.）；第 8 條規定，任何人皆享有個人資料受法律保護之權利（Everyone has the right to the protection of personal data concerning him or her.）。

隱私權保護觀念的演進，與科技技術發展密切相關；其定義也隨社會環境改變而演化，由原先「不受干擾的權利」逐步演變為「選擇對何人提供何種個人資訊的權利」[8]。但這種隱私權並非絕對，仍應受公共利益及本人同意之限制。

1930 年代通訊隱私權(Communication Privacy)保護的概念興起，到 1960、70 年代個人資訊隱私（Information Privacy）保護漸成為重要趨勢，美國 1974 年制定聯邦隱私權法（US Privacy Act of 1974），提出影響個資保護立法極為深遠的「公平資訊實務準則」(Fair Information Practice Principles, FIPPs)，但當時美國隱私權立法並未落實這些原則，反而是國際經濟暨合作組織（OECD）根據 FIPPs 精神訂定 OECD 個資隱私保護準則。1995 年歐盟制訂「個人資料保護指令」(1995 Data Protection Directive 95/46/EC)，保障個人資料被處理及自由移動權利，該指令主張「明示同意」為使用與處理個人資料的基本前提。

以下整理主要國家/組織關於隱私權與個資保護之重要原則：

[8] 彭金隆、陳俞沛、孫群，「巨量資料應用在台灣個資法架構下的法律風險」，載於臺大管理論叢第 27 卷第 2S 期，2017 年 5 月，頁 94。

表 2-1　主要國家/組織對隱私權與個資保護之重要原則

國家/機構	個資保護立法例	重要原則
美國	2012 年 2 月商務部提供關於「公平資訊實務準則」(FIPPs)原則的報告	1. 無針對非公務機關個資保護之聯邦統一立法，僅對特定行業、特定群體予以特殊保護(如「1986 電子通信隱私法」(Electronic Communications Privacy Act, ECPA)。 2. 隱私權與個資保護體系原則 (1) 個人管控 (2) 透明性 (3) 尊重情境脈絡(respect for context) (4) 安全性 (5) 接觸與正確性 (6) 重點蒐集 (7) 課責性
歐盟(註)	**「個人資料保護指令」**（1995 Data Protection Directive 95/46/EC）	1. 個人對其個資的控制權視為消費者基本人權，僅消費者積極主動表示願為個資之揭露，對方才可使用該個資。 2. 取代以隱私權保護為基礎的個資保護，而以個資控制權為核心，包含： (1) 知情權 (2) 更正權 (3) 資訊蒐集拒絕權
德國	**「德國聯邦個人資料保護法」**(1977)	1. 個資為人格權的一種(資訊自決權)，將個資與隱私分開，視個資為人格尊嚴的組成部分，採人格權保護模式保障個資。 2. 個資保護原則 (1) 直接原則 (2) 更正原則 (3) 目的明確原則 (4) 安全保護原則 (5) 公開原則 (6) 限制原則
日本	**「個人資訊保護法」、「行政機關個人資訊保**	個資保護原則： (1)目的明確化原則

國家/機構	個資保護立法例	重要原則
	護法」、「行政機關個人資訊保護法等施行準備法」	(2)利用限制原則 (3)蒐集限制原則 (4)資料內容完整正確原則 (5)安全保護原則 (6)公開原則 (7)責任原則 (8)個人參加原則
OECD	**「隱私權保護與個人資料跨境傳輸指導原則」**（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）	1. 確立各國個資立法最低標準，以自由流通與合法限制為原則，對個資跨國流通加以規範。 2. 個資保護原則如下： (1) 開放原則 (2) 個人參與原則 (3) 責任原則 (4) 使用限制原則 (5) 資料品質原則 (6) 蒐集限制原則 (7) 特殊目的與安全原則

(註)：2018 年施行之「一般個人資料保護規則」(GDPR)將於第二節中介紹

資料來源：彭金隆、陳俞沛、孫群，「巨量資料應用在台灣個資法架構下的法律風險」；本研究整理。

三、 個人資料定義與識別性

個人資料保護法的立法目的，在於保障個人資料免受公務或非公務機關侵害，保護前提必須是，資料可連結到資料當事人才有保護必要。倘從資料本身無從或難以識別資料擁有者；或縱依客觀方式推測，仍無法確認是何人資料，則不屬個人資料範疇。對該等資料的蒐集、處理或利用，則不會侵害特定個人，自然不須個資法保護。反之，若就資料本身觀察，足以辨識、特定具體個人，此時就涉及個人資料的保障，而有個人資料保護法的適用。

國際間對個人資料定義與判斷標準未予統一，各國皆有不同定義，某些屬於較抽象之判斷標準，解釋上有很大彈性空間，以應未來技術發展所面臨情形（如歐盟），有些則採列舉方式規定個資定義（如我國）。以下表列主要國家對個人資料之定義：

表 2-2　主要國家對個人資料定義

國家	個人資料定義
美國	能區別(distinguish)特定個人身分；或連結(link)到特定個人之資料。
歐盟(註)	1. 用以識別(identify)特定自然人或具備辨識可能性的任何資料。 2. 所謂**可識別之個人(identifiable person)**是指某一個透過身分證號碼或一項以上之專屬於其人身分之因素，包括其個人之身體、精神、心理、經濟、文化或社會地位，可直接或間接被他人所識別。
德國	任何有關該個人之資訊或已識別或可識別之個人的實質情形。
日本	藉由姓名、出生年月日或其他可描述該個人之資料。若經揭露仍足以識別為某一定特人，且該資料易與其他資料為對照、組合，藉以識別出特定個人者。
臺灣	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。（個人資料保護法第 2 條第 1 項）

(註)：此為 1995 年歐盟個人資料保護指令之定義。

資料來源：葉志良，「大數據應用下個人資料定義的檢討：以我國法院判決為例」，載於資訊社會研究，2016 年 8 月；本研究整理。

個資法保護的個資須具有特定個人的「識別性」，原則上須盡一切方法以該資料為依據以識別出、連結到或確認該個人之所在。但資料與特定個人間，是否具有足以連結的相關性，各國實務上均有其見解，我國法院認為，重點須置於「直接識別性」與「識別重要性」二基礎上。

「直接識別性」指資料須直接與個人連結，姓名、國民身分證統一編號、護照號碼、指紋等資料具有直接特定個人之識別性；至於我國個人資料保護法第 2 條第 1 款規定的其他例示性資料(如：婚姻、家庭、教育、職業、病歷、醫療等)，單獨提出無法特定個人，一定要與前述姓名等資料結合，或有複數資料一起呈現，始能識別特定個人。

「識別重要性」指資料本身能否「間接」識別出資料擁有者的程度。如該資料經比對、連結、勾稽，可達到直接識別資料的擁有者，此份資料就具有個人資料保護的價值。若資料欠缺「關鍵」或「重要性」的價值，無法特定出某一個人，就屬於無用的個人資料，不受保護。

關於「識別性」，較有爭議的是「可間接識別的個人資料」，我國個人資料保護法施行細則第 3 條規定，所謂「得以間接方式識別」係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。另歐洲理事會 No. R(90)19 之建議案認為[9]：倘若必須以不合理的時間、成本或人力始能識別該個人，該個人不得被認為是「可識別」(identifiable)。

[9] 轉引自葉志良，「大數據應用下個人資料定義的檢討：以我國法院判決為例」，載於資訊社會研究，2016 年 8 月，頁 9。

四、 大數據應用與隱私保護之權衡—隱私工程與去識別化

資訊科技不斷進步，各種資訊設備與網路連結，使每個人隨時隨地可產生、傳遞、分享並處理訊息，個人隱私問題也格外受重視。隱私是讓人們決定何時、以什麼方式、將多少個資料向他人傳達的權利，而隱私保護的相關規範是建立在個人對資料管控的需求上，例如「最小蒐集原則」及「目的限制原則」等。但這二原則在大數據時代中，資料蒐集最小化可能不再是保護隱私的一種方式，而當隱私與其他社會價值（包括公共衛生、國家安全、法律執行、環境保護以及經濟效率等）相互權衡時，就必須確保資料處理的合法性。政府部門認為，去識別化的大數據只能做到合乎個資法的基本要求，要做到合法且安心使用大數據，除了去識別化技術，也應該完成隱私衝擊評估，意即事先評估：若應用這些資料時，可能侵犯個人隱私或違反個資法的風險有多大，此外，更應做到告知當事人，並提供允許當事人退出的機制。

歐盟實施「一般個人資料保護規則」（下稱「個資規則」，GDPR）後，愈來愈多企業意識到須調整公司對個資的使用方式。事實上許多行業皆受該法影響：不只在歐盟設點的企業需面臨法遵要求，單純提供歐盟民眾服務、與歐盟有生意往來的企業也受規範。企業對 GDPR 的討論，單純從條文內容和如何遵循的作法等，進一步開始討論從 IT 技術上，克服企業進行法遵時面臨的困難。

GDPR 本質就是保護隱私，而在資料保護之餘，促進資料的合理使用也是 GDPR 關心重點。實務界已從「隱私工程」著手尋求解方，隱私工程就是使用數學或計量方式，甚至是加密、解密方式，將資料處理成不具識別性。如此在「隱私保護需求」與「資訊自由運用」間取得平衡，此即隱私工程的效益與目的（參圖 2-4）。

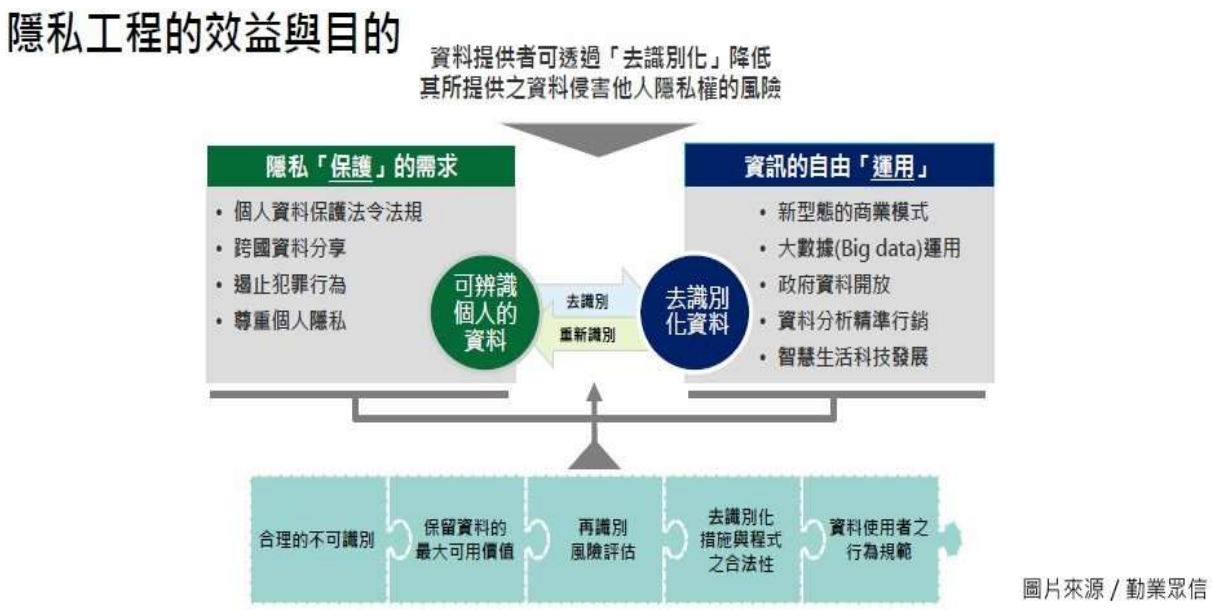


圖 2-4　隱私工程效益與目的

資料來源：https://www.ithome.com.tw/news/127226

由上圖可看出，「可識別個人的資料」經由去識別化技術轉換為「去識別化資料」，即可降低資料侵害隱私權的風險，使「隱私保護需求」與「資訊自由運用」取得權衡。國際間逐漸在個資保護框架下，建構「去識別化」方法，例如英國 2012 年提出「匿名化應用準則」、2014 年歐盟公布「匿名化技巧意見書」；日本 2018 年 9 月修訂「個人情報保護法」也將去識別化納入法律規範。由各國採行的作法看出：隱私工程中的「去識別化」（de-identification）是重要發展方向，針對個資中各種可識別的資訊，予以移除或模糊化，降低個人不想揭露資訊的風險[10]。

「去識別化」常見技術包括「假名化」（pseudonymization）和「匿名化」（anonymuzation），二者差異在處理後的資料是否可逆（reversible）？假名化的資料是可逆轉的，資料經假名化後，仍得藉資料控制人掌握之 key 值回溯辨識當事人。德國聯邦個人資料保護法

[10]【GDPR 施行後的法遵議題】深度剖析隱私工程 https://www.ithome.com.tw/news/127226

規定「假名/化名」指為使資料當事人不可能被辨識或難以辨識，而改以另一識別符號取代姓名或其他得以辨別之特徵，日後若有需要，可檢索key值將數據連結回個人，因此，假名化後的資料是可逆轉的。而匿名後的資料是不可逆的，即特定個人之資料在匿名化後將無法透過所有、可能、合理的方式被辨識出來。因此，匿名化被視為處理個人資料之一項技術，依目前技術水準，形成如同刪除般的永久效果。

至於去識別化的實作技術，可從是否需更改原始資料加以區別[11]。若需更改原始資料內容，降低資料洩漏可能的風險和隱私侵犯，可交叉使用下列四種技術實作方式：重排（permuntation）、概括化（generalization）、遮蔽（masking out）以及亂數（random）。倘無須更改原始資料內容，則可透過：資料欄位移除（removing）、資料加密（encoding），及資料筆數變異（add false information）等方式，降低資料洩漏風險。

整體來說，去識別化是個過程，當機敏資料加上去識別化方法和技術，可降低個資遭到濫用的風險。而決定資料是否要去識別化之前，企業須經過「盤點」、「分類或分級」、「去識別化」及「管理」等四步驟持續予以檢視（詳圖 2-5），詳細拆解整個過程：

（一） 資料盤點：盤點資料內容欄位，確認包含哪些機敏資料，以及是否要進行去識別化或完全不開放；

（二） 分類或分級：確認欄位屬性，針對不同特定領域資料，依機敏程度和風險水準進行資料分類或分級；

（三） 去識別化：依據資料等級，選擇不同安全性的去識別化技術和演算法；

（四） 管理：依據分類後資料欄位屬性，選定驗證方法。

[11] 同前註。

圖 2-5　資料去識別化前之四步驟

第二節　歐盟「一般個人資料保護規則」（General Data Protection Regulation；GDPR）

1995 年歐盟頒布「個人資料保護指令」（1995 Data Protection Directive 95/46/EC，下稱個資指令），調和歐盟地區各國對個人資料保護相關法令，並提供共通的法律框架與指導原則。然該指令已頒布超過 20 年，資訊科技發展千變萬化，個人資料保護議題日趨複雜，該指令無法完全因應變化；此外，其法律位階為指令（directive），尚須透過各會員國立法轉換程序，使目前各會員國對個人資料保護之程度及保護具體規範仍存有極大差異。

鑑於此，歐盟欲訂定對各會員國直接具有規範效力的「規則」（regulation），統合各會員國間對個人資料保護之法規範標準，2010 年 11 月初，歐盟對外公開修正內容，歐盟執委會於 2012 年 1 月提出草案，因草案規範嚴苛，爭議頗大，直至 2013 年底，歐洲議會公民自由、司法與內政委員會（European Parliament Committee on Civil Liberties, Justice and Home Affairs）才通過對執委會版草案之修正意見；其後歐盟執委會、議會與理事會（European Council）持續進行三方協商討論，2015 年末終獲共識，提出歐盟個資規則之三方協議版草案，直到 2016 年 4 月 27 日歐洲議會才通過，同年 5 月 4 日公布，然因考量該新法規影響層面深遠，各國公務機關及非公務機關等（尤其是跨國企業）需相當時間因應，特將該法生效日期延後兩年，於 2018 年 5 月 25 日生效並於歐盟境內實施，正式取代 1995 年個資指令，法案演變進程參圖 2-6。

圖 2-6　歐盟個人資料保護法案演進過程

資料來源：從歐盟 GDPR 看全球隱私與安全保護發展趨勢，勤業眾信聯合會計師事務所，2018/8

一、 歐盟個資規則主要改變[12]

現今以數據驅動的世界中，GDPR 目標是保護所有歐盟公民免受隱私和數據洩露。相較於 1995 年頒布的「個資指令」(95/46/EC)，「個資規則」的內容有以下重大改變。

（一）適用範圍擴大

「個資指令」僅在資料處理者在歐洲經濟區（European Economic Area, EEA）內有住居所或機構，或利用境內的設備蒐集、處理或利用個人資料時始適用。相較之下，「個資規則」的適用範圍明顯擴大，即符合下列情形之一，則有該規則適用：

1. 凡設立於歐盟境內之資料管理者及資料處理者所為之所有個人資料處理活動，不論個人資料處理活動是否發生於歐盟境內。
2. 非設立於歐盟境內之資料管理者或資料處理者，對歐盟境內的資料當事人為下列行為而蒐集、處理或利用個人資料之情形：

[12] https://eugdpr.org/the-regulation/

（1）提供商品或服務，無論是否需要付費；

（2）在歐盟境內的行為進行監控。

綜上所述，一旦私人企業著手處理歐盟公民的資料，即便處理過程非發生於歐盟，在「個資規則」的管轄範圍內，此等公司也得派駐代表於歐盟。

（二）明確資料當事人同意

「個資指令」未規定資料當事人之同意，係明示或默示，「個資規定」則新增「以聲明或清楚、積極的行為」要件，便於釐清指令時「單純不作為(沉默)」是否符合同意之爭議[13]，新舊法比較詳表 2-3：

表 2-3 「個資規則」與「個資指令」當事人同意內涵比較

個資規則	個資指令
資料當事人同意為了**一項或數項特定目的**，蒐集、處理其個人資料。	資料當事人**明確地**（毫不含混地 unambiguously）同意。
同意是資料當事人經告知後，任何出於自由意願，**以聲明或清楚、積極的行為**，允許其個人資料被蒐集、處理或利用的具體、明確表示。	同意是資料當事人經告知後，任何出於自由意願，允許其個人資料被蒐集、處理或利用的具體表示。

資料來源：本研究整理

有關當事人同意，「個資規則」臚列四項要件說明與分析：

1. **以同意作為合法使用個人資料的事由時，當事人是否同意，應由資料管理者證明**。藉由要求資料管理者證明當事人同意的存在，緩和欠缺書面證明文件對資料當事人造成的不利益。
2. **若當事人同意是以書面聲明為之，而該書面同時包含其他事項，則當事人同意的部分，須與其他事項清楚分離，並且以清晰可**

[13] 有關同意的形式，仍不以書面為限，依據立法理由說明，任何積極的行為，例如書面聲明（包括以電子方式為之）、口頭聲明均屬之；實際操作上，瀏覽網頁時勾選同意欄位、選擇技術上設定，或其他聲明或行動，只要能清楚表現資料當事人允許的意思，均符合規則要求。相反地，沉默、已預先勾選同意欄位或不作為，都與規則同意的要件不符。

理解、易於接近、清楚並淺白的文字呈現。立法目的在於使當事人對同意事項有清楚認知，避免資料管理者以夾帶方式，將個人資料使用的同意隱藏在其他事項之中，使當事人在不注意的情形下予以同意。

3. **當事人有權隨時撤回同意**。當事人同意前應告知可隨時撤回，且撤回同意與給予同意一樣容易，此乃確保當事人自主權。
4. **評估同意是否出於自願時，取決於資料當事人是否有真正的選擇機會**。因此，業者履行契約或提供服務時，要求當事人提供與契約履行或服務提供無關之個人資料作為交換條件，則可被視為剝奪當事人選擇機會，非出於自由意願，影響同意效力。

（三）新增被遺忘權、資料可攜權

「個資指令」對資料當事人權利之規範類別及內涵較為簡略，「個資規定」與時俱進，不僅豐富資料當事人權利內涵，且新增被遺忘權（right to be forgotten）及資料可攜權（right to data portability），分述如下：

1. **被遺忘權（刪除權）**

被遺忘權（刪除權）是個人資料保護法制中，當事人自主控制權利的具體展現。依據「個資規則」第 17 條第 1 項規定，有下列情況之一時，當事人有權要求資料管理者立即刪除其個人資料：

（1）蒐集或處理個人資料之目的已不復存在。

（2）當事人撤回同意且欠缺其他資料處理的法律依據。

（3）資料當事人反對資料處理。

（4）個人資料被非法處理。

（5）為符合法律義務，個人資料應被移除。

但當事人對資料刪除權非毫無限制，歐盟個資規則第 17 條第 3 項規定，資料處理係為以下情形所必要時，資料當事人不得主張該資料刪除權：

（1）基於行使表達自由及資訊權利。

（2）為遵循法定義務；或資料管理者受託履行基於公共利益相關或行使公權力所需之任務。

（3）基於公共健康領域內之公益理由。

（4）基於公益存檔之目的、科學或歷史研究或統計目的。因刪除權的行使可能會對前述目的實現造成嚴重妨礙或無法達成，故與公益目的衡量之下，某程度限縮當事人的資料刪除權。

（5）為法律上權利之主張、行使或抗辯。

主張被遺忘權（刪除權）時，須於個案中與其他利益進行權衡，包括公益及可能涉及之第三人利益，例如：言論自由、資訊自由、新聞自由或學術自由等，判斷面向包括涉及資料之類型、對當事人私生活之影響程度、公眾知的權利等，此法益權衡往往是被遺忘權（刪除權）在實務操作上遇到的最大挑戰[14]。

2. 資料可攜權

所謂「資料可攜權」即當事人移轉個人資料的權利。例如：將資料從一個資料管理系統移動到另一系統，而不受資料管理者阻擋。歐盟個資規則第 20 條規定，當事人有權要求已獲取其資料之資料管理者，以結構的、常用的及機器可讀形式之格式，提供個人資料

[14] 法務部「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告，中華民國 105 年 12 月 30 日，頁 31。

之複本，且有權透過該資料管理者，無障礙地將該個資傳輸予其他資料管理者。

（四）隱私保護設計（Privacy by Design，PbD）

無論是隱私保護設計（Privacy by Design）或隱私保護預設（Privacy by Default），皆為近年歐盟談論個資或隱私保護的重要觀點。因此，在歐盟個資規定中也正式納入相關規範制度[15]，要求企業或組織從設計系統開始就應包含隱私資料保護的應用，而不再是事後追溯的補充性應用。換言之，將隱私保護構想嵌入 IT 系統和業務流程設計中，設計重點例如：用戶同意（user consent），企業或機構因提供產品/服務而蒐集用戶資訊時，須使用戶明確表達願將個人資訊提交使用，即**不能**使用任何先行勾選方式**預設用戶同意**，系統或流程設計上，使用者須明確的勾選確認同意；又如「用戶隱私管理及刪除」之機制亦屬之。

企業建置隱私保護設計制度，主要有七個原則須掌握[16]：

---

[15] 參歐盟個資規則第 25 條第 1 項(Data protection by design and by default）：考量到現有技術、執行成本以及處理之性質、範圍、內容及目的以及處理對當事人之權利及自由所生諸多可能且嚴重之風險，不問係在決定處理方式時或係在處理中，控管者均應實施適當之科技化且有組織的措施，例如假名化，且該等措施旨在實現資料保護原則，如資 料最少蒐集原則，並採取有效方式且將必要保護措施納入處理程序， 以符合本規則之要求並保護資料主體之權利。（Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of 54 the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.）

[16] 因應歐盟 GDPR 掌握隱私保護設計制度七原則，https://www.pwc.tw/zh/news/press-release/press-20180828-1.html

1. 主動非被動—採取主動措施。在事前預測風險，以防止隱私侵入事件的發生；隱私設計是事前，而非事後。
2. 隱私為預設設置—在 IT 系統或服務流程中自動內建隱私保護，個人不需要採取任何行動保護隱私。
3. 隱私納入設計—隱私措施納入系統或服務流程的設計與建置當中，讓隱私政策成為設計的重要成分。
4. 全功能整合—確保各種合法利益及目標都能平衡兼顧，以雙贏而非零和的方向進行保護。
5. 整體安全/完整生命週期保護—採取完整的保護策略，可確保個資蒐集、處理、利用、刪除等各階段都能受到保護。
6. 透明公開—讓資訊的蒐集處理利用流程能透明化，讓資料當事人充分知悉。
7. 尊重使用者隱私/以使用者為中心—以資料當事人為中心，確保資料當事人的利益可以獲得充分的保護。

（五）設置資料保護長（data protection officer，DPO）

個資規則新增規定，要求資料管理者及資料處理者應指定一名資料保護長。於資料處理運作中，依其形式、範圍及/或目的，要求廣泛地對當事人採取日常性且系統化監控。若涉及特種個人資料或關於犯罪判斷及犯罪行為之個人資料時，均應任命資料保護長。

資料保護長之任務包括但不限於以下所述：

1. 告知及提供建議給資料管理者或資料處理者；及其處理資料之員工有關他們所負擔之義務；
2. 監督遵守歐盟個人保護規則、其他歐盟或各會員國之資料保護規範、資料管理者或資料處理者之個人資料保護策略，包括職

權劃分、對於參與處理程序人員之教育與教示，及與其相關之審查；

3. 依請求提供隱私衝擊評估（有譯為：資料保護影響評估，data protection impact assessment，DPIA）及監督其實施等相關建議；
4. 與監督機關合作；
5. 作為關於資料處理相關問題與監督機關之聯絡單位。

資料保護長應注意其職業資格，特別於資料保護法令及實務領域之專業知識，及其履行任務能力。相較於「個資指令」，「個資規則」加重資料保護長之責任，除協調歐盟個人資料保護體系有重大意義外，對隱私衝擊評估制度之落實，亦扮演關鍵角色。

（六）大幅提升罰則

「個資規則」為確保規範得以落實，於「個資規則」第 83 及 84 條中，針對違反個資規則之行為，訂定處罰與制裁規定。違反規定者最高可處以 2 千萬歐元或其年度國際總營收 4%之罰鍰。

二、 歐盟個資規則重要內容

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

資規則」重要內容摘述如後，另章節一覽如表 2-4：

表 2-4　歐盟個資規則章節一覽表

章　節	內　容	條號
第一章　總則	定義適用範圍、目的及名詞解釋	§1~§4
第二章　原則	包括個人資料處理原則、處理之合法性、同意條件等	§5~§11
第三章　當事人（資料主體）之權利	第一節　透明度及管道	§12
	第二節　告知事項與個人資料存取	§13~§15
	第三節　更正與刪除	§16~§20
	第四節　拒絕權及自動化個人決策	§21~§22
	第五節　限制	§23
第四章　資料管理者與處理者	第一節　一般義務	§24~§31
	第二節　隱私資料安全	§32~§34
	第三節　資料保護影響評估與事前諮詢	§35~§36
	第四節　資料保護長	§37~§39
	第五節　行為準則及認證	§40~§43
第五章　個人資料傳輸至第三國或國際組織	涵蓋傳輸基本原則、經充分評估傳輸、經適當防護傳輸等	§44~§50
第六章　獨立監理機關	第一節　獨立地位	§51~§54
	第二節　權限、職務及權力	§55~§59
第七章　合作及一致性	第一節　合作	§60~§62
	第二節　一致性	§63~§67
	第三節　歐洲資料保護理事會	§68~§76
第八章　救濟、義務及處罰	---	§77~§84
第九章　特殊情況處理之規範	涵蓋表達與資訊自由、身分證號碼、公共利益等特殊情況下的資料處理	§85~§91
第十章　授權法及施行法	---	§92~§93
第十一章　附則	---	§94~§99

資料來源：本研究整理

（一）規範對象

「個資規則」規範對象，區分為「規範客體」及「適用主體」。在規範客體方面，「個資規則」延續指令規定，限於「**全部或部分以**

自動化方式蒐集、處理或利用的個人資料」，至於以「非」自動化方式蒐集、處理或利用的情形，僅限於「構成檔案系統（filing system）一部分，或『為』構成檔案系統一部分而蒐集、處理或利用的個人資料」才有適用（個資規則第 2 條第 1 項參照）。應說明者，所謂檔案系統的定義，「個資規則」仍延續指令「個人資料檔案系統」的規定，指：「可以特定條件存取的結構化個人資料集合，不論是集中、分散或以其他功能或地理因素散佈者」（個資規則第 4 條第 6 款）。因此，一般零散的紙本資料集合，如不能以一定方式檢索，仍無「個資規則」適用。

適用主體方面，如同指令既有規定，「個資規則」對資料管理者[17]（data controller，亦有譯為資料控制者）及處理者[18]（processor，有譯為受託者）的定義，均包括「自然人、法人，公務機關，機構或其他組織（natural or legal person, public authority, agency or other body）」，並「不以」特定組織型態作為認定適用主體的標準。

「當事人所為單純之個人或家庭活動」不屬「個資規則」範圍（§2.2(c)），主要理由在於：將自然人納入個人資料保護法制的適用範圍內，要求其遵守與一般公司行號、法人或團體相同規範標準，恐與常情有違；執行上也因一般人欠缺必要專業知識與資源，而面臨困難。故在「個資指令」時，即有「自然人純供個人或家庭目的」之排除適用規定。但應注意，所謂「個人或家庭活動」仍不得與職業或商業活動有關，不過隨網際網路發展，尤其各種網路交易平台、影音、社群媒體普及，使「純個人或家庭活動」目的判斷困難，例

[17] 「資料管理者」係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；依照歐盟法或會員國法決定處理之目的及方法，由歐盟法或會員國法律規定控管者或其認定之具體標準（歐盟個資規則§4(7)）。

[18] 「資料處理者」係指代管理者處理個人資料之自然人或法人、公務機關、局處或其他機構（歐盟個資規則§4(8)）。

如：自然人將他人的個人資料、照片或影像放置於社群媒體或影音網站，依照隱私設定程度之不同，最廣可供全世界不特定人瀏覽、轉傳或存取，此一行為對個人資訊隱私之侵犯，恐遠超過其他受規制機關、團體之行為。

（二）擴大個人資料定義

配合網路及通訊科技發展，「個資規則」對「足資識別特定人」資料之識別符號（identifier），增加了位置資料（location data）、線上識別碼（online identifier）等包括透過網路 IP、瀏覽紀錄產生之數位軌跡，以追蹤識別特定當事人身分。新舊法比較詳表 2-5：

表 2-5 「個資規則」與「個資指令」有關個人資料定義比較表

個資規則	個資指令
「個人資料」係指有關識別或可得識別自然人（「資料主體」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人。所謂「足資識別之自然人」係指：「一個可以透過**『識別符號』（identifier）**」，例如：姓名、**識別號碼（identification number）、位置資料（location data）、線上識別碼（online identifier）**，或一項或多項身體、生理、基因、精神、經濟、文化或社會身分特徵等具體因素之識別工具。	「個人資料」係指有關識別(identify)特定自然人或具備辨識可能性的任何資料。所謂**可識別之個人(identifiable person)**是指某一個透過身分證號碼或一項以上之專屬於其人身分之因素，包括其個人之身體、精神、心理、經濟、文化或社會地位，可直接或間接被他人所識別。

資料來源：本研究整理

「線上識別碼」依「個資規則」立法說明，應指由裝置、應用程式、工具或網路協定賦予的（獨特）識別碼，例如：網路協定位置（internet protocol address）、小型文字檔案識別碼（cookies identifier）或其他識別碼（如：無限射頻識別標籤，RFID）。另有關個人（隱私）資料可分為一般個資與特殊（種）個資，圖示如 2-7。

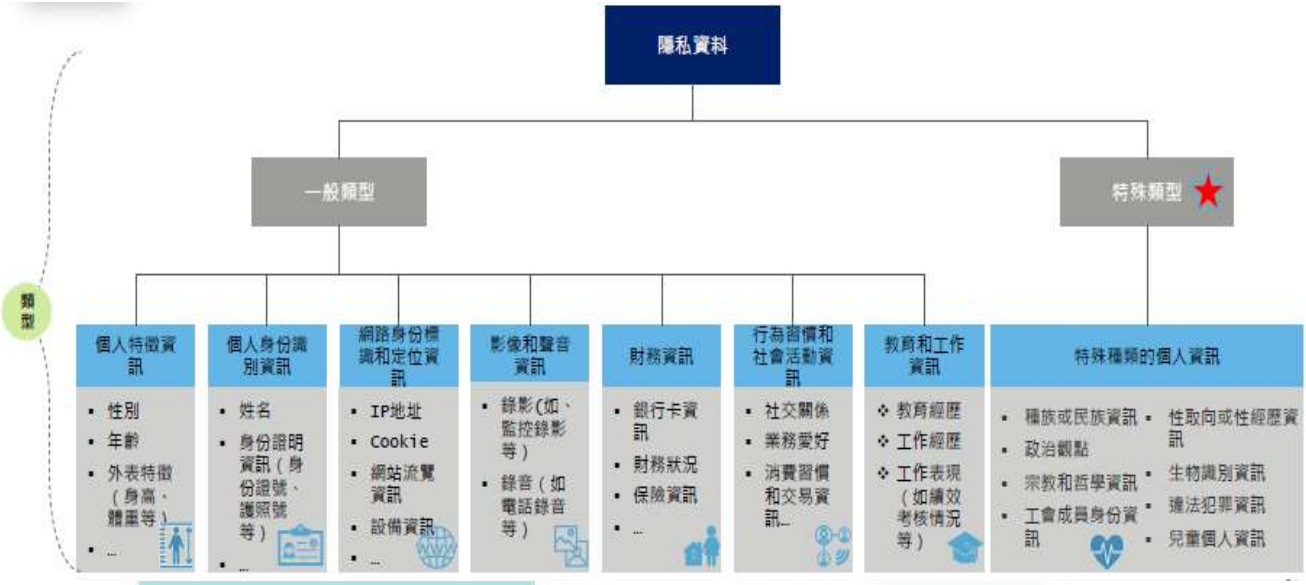


圖 2-7 個人資料類型

資料來源：從歐盟 GDPR 看全球隱私與安全保護發展趨勢，勤業眾信聯合會計師事務所，2018/8

「個資規則」將個人(隱私)資料區分為一般類型與特殊類型，並就不同資料類型區分處理要件。所謂特殊類型之個人資料，指與民族或種族來源、政治見解、宗教或哲學信仰，或所屬工會相關之個人資料，及得明確識別特定人之基因、生物特徵、個人健康或性生活或性傾向資料（個資規則§9.1），前述特殊類型的個人資料原則上不得處理，僅在例外情況下才可處理（個資規則§9.2），設定要件較第 6 條一般類型的個人資料之處理更為嚴格（如例外允許情況：該特殊類型個人資料之處理，係基於公共衛生領域之公共利益，如為防止對健康之跨境嚴重威脅，或為確保醫療保健及醫療產品或醫療設備品質之高標準與安全性而有必要者，並依據歐盟法或會員國法律規定採取適當及具體安全措施保護資料主體之權利和自由）。

（三）強化當事人權利

「個資規則」對資料當事人所賦予之權利，包括 1.接近使用之權利—查詢、閱覽及複製權（right of access）、2.更正權（right of

rectification）、3.被遺忘權/刪除權（right to be forgotten）、4.限制處理權（right to restriction of processing）、5.資料可攜權（right to data portability）及 6.異議權（right to object）。其中「被遺忘權」及「資料可攜權」為本次新增權利，本研究已於本節一、歐盟個資規則主要改變中詳述，於此不再贅述，僅就資料當事人其他權利概述介紹。

1. **接近使用之權利—查詢、閱覽及複製權**（個資規則§15，right of access）

資料當事人有權查詢其個人資料及其處理目的、個人資料之種類、接受者之種類、個資儲存期限；且有權要求更正、移除、限制或反對資料處理。當個資被傳遞至第三國或國際組織時，「個資規則」進一步規定，資料當事人有權取得以下資訊：資料管理者採取之適當安全措施為何、資料預計保存期限或決定保存期限之標準等。

另「個資規則」關於答覆查詢之方式有明確規定，資料當事人以電子方式提出查詢等申請時，資料管理者應以常用的電子格式（commonly used electronic form）查詢或提供相關資訊。

2. **更正權**（個資規則§16，right of rectification）

資料當事人有權要求資料管理者立即更正所持有不正確之個人資料，在與處理目的相符範圍內，資料當事人有權要求將不完整之個人資料補全。

3. **限制處理權**（個資規則§18，right to restriction of processing）

資料當事人於下列情況，有權限制資料管理者處理其個資：

（1）資料當事人質疑其個人資料之正確性，限制處理期間之長短，應使處理者有查證個人資料正確性的充分時間；

（2）處理是違法，且資料當事人拒絕刪除其個資，並要求限制其使用；

（3）資料處理者依處理目的不再需要該個人資料，但該個人資料為資料當事人建立、行使或防禦法律上請求所必須者；

（4）資料當事人依同規則第 21 條對處理提出異議時，在尚未確認處理者是否具有優先於資料當事人權益之正當理由前，資料當事人得主張限制處理其個資。

4. **異議權**（個資規則§21，right to object）

資料當事人對基於公益或資料管理者或第三方之法律利益進行的資料處理，有權提出異議。

（四）加重企業責任

「個資規則」強化對資料處理者（企業、機構）之責任，內容包括 1.隱私保護設計要求（個資規則§25）；2.文件紀錄責任（個資規則§30）；3.個資外洩通報及通知（個資規則§33~§34）；4.個資保護影響評估（個資規則§35）；5.指定資料保護長（個資規則§37~§39）以及 6.提高罰則金額（個資規則§83）。其中「隱私保護設計要求」、「指定資料保護長」及「提高罰則金額」，本研究已於本節一、歐盟個資規則主要改變中介紹，此不再贅述，僅就企業其他責任概述之。

1. 文件紀錄責任（個資規則§30）

員工 250 人以上企業原則上應保存維護相關紀錄，該紀錄應包含下列資訊：

（1） 資料處理者及共同處理者、處理者代表及資料保護長之名稱及聯絡方式；

（2） 處理目的；

（3） 資料當事人類型及個人資料類別之描述；

（4） 個人資料已對其或將對其揭露之接收者類型，包括第三國或國際組織之接收者（the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations）；

（5） 將個人資料移轉至第三國或國際組織，包括指明該第三國或國際組織，且若係第 49 條第 1 項第 2 款所定之移轉者，適當保護措施之書面文件；

（6） 刪除不同類別之個人資料之預設時間上限；

（7） 第 32 條第 1 項所定科技化且有組織之安全措施之概述。

2. 個資外洩通報及通知（個資規則§33~§34）

有關個資外洩通知義務的規定，「個資規則」分別規範對監督機關通報及對資料當事人之通知義務。個資規則第 33 條第 1 項規定，當個人資料外洩，資料管理者應避免不當拖延，並在可能情況下，於知悉事件發生後 72 小時內，通報第 55 條規定的監督機關，但個資外洩不至於對自然人自由與權利產生危險者，不在此限。通報內容包括：

（1）個資外洩事件本質的描述，包括受影響當事人種類及約略人數，外洩個人資料的種類與約略數量；

（2）資料保護長或其他聯絡窗口姓名及聯絡方式；

（3）描述個資外洩可能影響；

（4）描述資料管理者已採取或即將採取的因應措施，包括減輕或緩和個資外洩可能造成不利影響的作法。

另個資外洩向資料當事人的通知則規定於同法第 34 條，當個資外洩可能導致自然人自由或權利的高度風險時，資料管理者應避免不當拖延，將個資外洩情事通知資料當事人，除以淺白文字描述個資外洩情形外，通知內容至少應包括前述第（2）~（4）項資訊。然為減輕資料管理者負擔，同條第 3 項列舉三項豁免通知事由：

（1）資料管理者對外洩的個資已採取適當地技術及組織上保護措施，如加密，使未經授權者無法理解資料內容。

（2）資料管理者事發後採取措施，使所稱當事人自由或權利的高度風險不至於實現。

（3）個別通知須付出不合比例的努力，於此情形下，資料管理者應採取公告或其他類似措施，使資料當事人以相同有效方式知悉通知內容。

3. 個資保護影響評估（Data protection impact assessment，DPIA 個資規則§35）

「個資規則」要求企業須進行「個資保護影響評估(Data Protection Impact Assessments，DPIA)」，用以辨識業務活動中涉及個人隱私權利的風險，並加以衡量、管理與因應，並於蒐集與處理個人資料前，評估該等風險與業務活動必要性與對稱性。DPIA 與許多企業已實施之「隱私影響評估(Privacy Impact Assessments，PIAs」類似，惟 PIAs 並無明確的規範與定義，DPIA 則強化了其內涵與一致性。在啟動影響評估的要件上，「個資規則」第 35 條第 1 項規定，凡特定類型的個人資料蒐集、處理或利用（特別是使用新科技之處理方式），且考量該處理之本質、

範圍、使用情形及目的後，可能對自然人之權利及自由產生高度風險時，資料管理者應先對預計資料活動，可能對個人資料保護的影響進行評估。除前述抽象規定外，第 35 條第 3 項特別要求下列三種具體情形，需進行影響評估：

（1）關於自然人之系統性及大規模的個人特質評估，而該評估是基於自動處理，包含建檔，且基於該評估作成關於該自然人之法律效果或其他重大影響該自然人之決定；

（2）處理大規模之第 9 條第 1 項所稱之特殊類型個人資料，或關於第 10 條所稱前科及犯罪之個人資料；

（3）大規模系統性監督公共場所。

依同條第 7 項規定，評估內涵包括：

（1）對預計進行的蒐集、處理或利用活動及其目的的系統性描述，包括資料管理者主張的合法利益；

（2）蒐集、處理或利用活動與達成目的的必要性與比例性評估；

（3）對資料當事人自由與權利造成風險的評估；

（4）應對風險之方式，包含保護措施、保全措施及確保個人資料保護及符合本規則考慮資料當事人及其他相關人員之權利及合法利益之機制。

（五）限制個資跨境傳輸

資料在各產業內扮演核心角色，近年個人資料處理及儲存行為主要係透過跨境傳輸處理。「個資規則」原則上限制個資跨境傳輸至歐盟以外國家，但在數位經濟蓬勃發展的現今，跨境資料傳輸已是

多數產業營運不可或缺的一部分。因此，「個資規則」在下列三種情況下例外允許傳輸：

1. 具備適足性認定

國家通過歐盟執委會適足性認定（adequacy decision，個資規則§45）：執委會評估該國是否具適足性認定標準有三：

（1）法制環境，對人權與基本自由的尊重與相關國內法規範；

（2）獨立運作的監管機關；

（3）簽訂國際協定或合約。

目前取得歐盟適足性認定 13 個國家或地區分別為：「個資指令」時期的安道爾、阿根廷、加拿大（商業組織）、法羅群島、格恩西島、以色列、馬恩島、澤西島、紐西蘭、瑞士、烏拉圭、美國（隱私盾），與 GDPR 施行後取得適足性認定的日本[19]。我國國發會也在 2018 年 12 月向歐盟遞交自我評估報告，盼後續能儘速展開技術性對話。

2. 具備適當防護措施

依「個資規則」§46，倘歐盟執委會未對資料接收國做出適足性認定，資料管理者或處理者只能在接收方（含資料管理者與處理者）有提供適當防護措施的情況下，方能將個人資料傳輸至第三國。符合規範之適當保護措施包括（個資規則§40、§42、§46~§47）：

（1）標準資料保護合約條款（Standard Contractual Clauses, SCC）

歐盟針對個人資料標準合約條款，發布不同類型範本，如規範歐盟管理者（EU controller）傳送資料到非歐盟或歐洲經濟區管理者（non-EU or EEA controller）；或規範歐盟管

[19] https://ec.ltn.com.tw/article/breakingnews/2702576

理者傳送資料到非歐盟或歐洲經濟區處理者（non-EU or EEA processor）。

（2）企業自我拘束原則（Binding Corporate Rules, BCRs）

企業自我拘束原則（BCRs）是由歐盟資料保護工作小組所制訂，允許跨國公司、國際組織和公司集團依歐盟資料保護相關法律進行組織內跨境個人資料傳輸。BCRs 旨在確保一組織或團體內部進行的所有傳輸皆能維持適足的保護水準。每次需要將資料移轉給組織成員時，BCRs 是公司須簽署標準合約條款的一個替代方案。要取得使用 BCRs 之允許，相關公司必須選定一個主要資料保護監管機關，該機關將協調確保其他相關資料保護機關之批准。

（3）行為守則（Codes of Conduct）

鼓勵特定行業、中小企業、微型企業等採行。

（4）驗證機制（Certification）

會員國、監管機關、委員會及執委會應鼓勵建立資料保護認證機制，與資料保護標章及標誌，以證明資料管理者及處理者之處理活動遵從本規則，而微型及中小型企業之具體需求也應納入考慮。

3. 例外條款（個資規則§49）

跨境傳輸應優先採行前述國家層級適足性認定，或企業自主採行適當保護措施方式。於少量、偶發性的傳輸時，可採以下方式：

（1）個資當事人明確同意：告知個資當事人可能的風險後，取得當事人明確同意移轉。

（2）其他必要措施，例如：執行契約所必要、基於公共利益之

重要原因、於個資當事人無法為同意之表示，移轉對其有重要利益保護必要。

第三節　我國個資法與 GDPR 比較分析

我國「個人資料保護法」，簡稱「個資法」，取代電腦處理個人資料保護法，修正條文分別於 2012 年 10 月 1 日及 2016 年 3 月 15 日生效，共 6 章、56 條。我國「個資法」與 GDPR 皆師承經濟合作暨發展組織（OECD）個人資料保護原則，且我國「個資法」研修過程，不少條文意旨參考 GDPR 前身之 Directive 95/46/EC4 相關規定，故 GDPR 與我國「個資法」比較分析時，可發現二者有相似之處。

有關我國個資法架構及主要內容與 GDPR 之重點比較分析如下：

一、 **規範對象與域外效力**：GDPR 適用對象範圍，除歐盟境內設有分支機構之資料管理者及處理者之外，即便資料管理者或資料處理者於歐盟未設分支機構，但跨境提供商品或服務過程中，如有蒐集或處理歐盟居民個人資料，仍應符合 GDPR 規範。

二、 **保護客體—個資定義**：GDPR 第 4 條有關識別或可得識別自然人之任何資訊，並明文涵蓋網路識別碼；我國個資法第 2 條，規範得以直接或間接方式識別該個人之資料，因此，可解釋亦涵蓋網路識別碼。

三、 **當事人權利**：GDPR 第 20 條，規範資料當事人在特定情形下，有權要求以結構的、通常使用的、機器可讀的形式，接收其提供給管理者的資料，並有權將之傳輸給其他管理者，即「資料可攜權」規定，我國個資法並無相關規定。另 GDPR 賦予當事人的權利範圍較我國個資法廣泛，以接近使用權為例，甚至涵

蓋應提供得遠端使用之安全系統供資料當事人使用；且針對自動化處理得行使拒絕權。

四、 **資料管理者義務**：GDPR 第 37 條規定資料保護長（DPO）之設置，我國僅在個資法施行細則第 12 條第 2 項第 1 款有類似規定（配置管理之人員及相當資源），不似 GDPR 規定只要符合特定情況則一定要設置，並設有相關設置條件。另我國個資法並無個資保護設計與預設之規定。

五、 **跨境傳輸**：歐盟境內之個人資料原則禁止跨境傳輸至歐盟以外地區或國家，除非符合下列情況之一，方得為之：（一）擬傳輸地區經評估具備「適當保護水平」（GDPR§45）；（二）資料管理者已提供適當保護措施，包括：1.訂有具拘束力之企業守則、2.採用標準契約條款、3.訂有經核准之行為守則、4.取得資料保護認證或資料保護標章及標誌（GDPR§46）；（三）當事人明確同意；（四）履行契約或依當事人要求，為締約前必要措施；（五）基於重要公共利益之維護；（六）為主張、行使或防禦法律上之請求權所必要；（七）基於保護當事人之重要利益所必要；（八）依法辦理之登記作業，而向公眾提供資訊（GDPR§49）。至於我國個資法第 21 條，我國個人資料跨境傳輸至境外，雖原則上不禁止，惟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，亦得防止我國人之個人資料不當國際傳輸：（一）涉及國家重大利益；（二）國際條約或協定有特別規定；（三）接受國對個人資料之保護未有完善法規，致有損當事人權益之虞；（四）以迂迴方法向第三國（地區）傳輸個人資料規避我國個資法。有關我國個資法與 GDPR 之架構內容與比較詳表 2-6：

表 2-6 我國個資法架構及主要內容與 GDPR 之比較分析

比較項目	我國個資法		GDPR	
規範對象及域外效力	§51	我國公務及非公務機關於境外對我國人民個人資料之蒐集、處理及利用，亦有本法適用。	§3	歐盟境外企業對歐盟境內當事人提供商品、服務或監控其於歐盟內行為，仍有該法適用。
保護客體—個資定義	§2	一般個資：得以直接或間接方式識別個人之資料； 特種個資：病歷、醫療、基因、性生活、健康檢查及犯罪前科等。	§4	一般個資：得以直接或間接方式識別當事人之任何資訊，包括透過網路IP、瀏覽紀錄產生之數位軌跡，並得追蹤識別特定當事人身分。 特種個資：揭露人種、血統、政治意見、宗教、哲學信仰、工會身分、基因、生物特徵、健康相關、性生活或性傾向之資料； 刑事：前科與犯罪紀錄。
當事人權利	§3	➢查詢閱覽權 ➢請求製給複本 ➢補充更正權 ➢拒絕權 ➢刪除權	§15 §16 §17 §18 §20 §21	➢接近使用權 ➢更正權 ➢刪除權 ➢限制處理權 ➢資料可攜權 ➢異議權
資料管理者義務	個資法施行細則§12	➢個資風險評估 ➢配置管理人員 ➢使用紀錄及軌跡資料與證據保存 ➢事故通報及應變措施設備安全管理	§35 §37 §30 §33 ~34 §25	➢個資保護影響評估 ➢設置資料保護長 ➢文件紀錄 ➢知悉個資侵害事故 72 小時內通報與通知 ➢個資保護設計與預設
跨境傳輸	§21	原則允許、例外禁止	§45 ~46 、 §49	原則禁止、例外允許

資料來源：本研究整理

第三章　大數據於金融業之應用現況

近年來因穿戴裝置的興起及網際網路的快速便捷，使資料來源多元化，傳統蒐集之資料由交易生成的數據資料，轉為客戶的生活資料，加以統計技術的複雜化，資料分析得協助企業瞭解客戶需求，應用於預測未來客戶的行為，以改善企業之經營循環，大數據應用大幅改變商業模式，致大數據一詞成為各行各業間的熱門話題。以下就傳統資料分析與大數據應用的差異、大數據於金融業之應用及實際案例加以討論。

第一節　傳統數據與大數據應用的比較

大數據應用之興起，主要是因社群網站、穿戴裝置的流行以及物聯網的發展，產生大量(Volume)的新型態資料，例如社群網站公開的檔案、朋友名單、照片及貼文或是穿戴裝置上傳的即時運動資料等，資料形態呈現多樣化（Variety）且具真實性（Veracity），而通常該資料為連續、不間斷和及時上傳的具時效（Velocity）性的資料。透過大數據分析，協助金融業調整行銷及服務方式，最終替公司帶來利益。

由於資料的多樣化及分析方法的演進，傳統商業智慧的資料分析為事後分析，資料多為因交易生成的量化資料，再透過敘述資料的狀況描述過去發生之事實，再依數據變化瞭解事實發生之原因，透過大數據應用，資料分析透過人工智慧轉為具預測功能的先見之明，係因資料來源變得多元且資料形式不再限制量化資料，圖片、文章、定位點及社群照片等亦是重要的資料來源，透過大數據之應用，能夠協助金融業瞭解顧客以預測行為發生之機率，提供最佳化建議，大幅改變金融業營運模式，提升資料的最終價值（Value）。

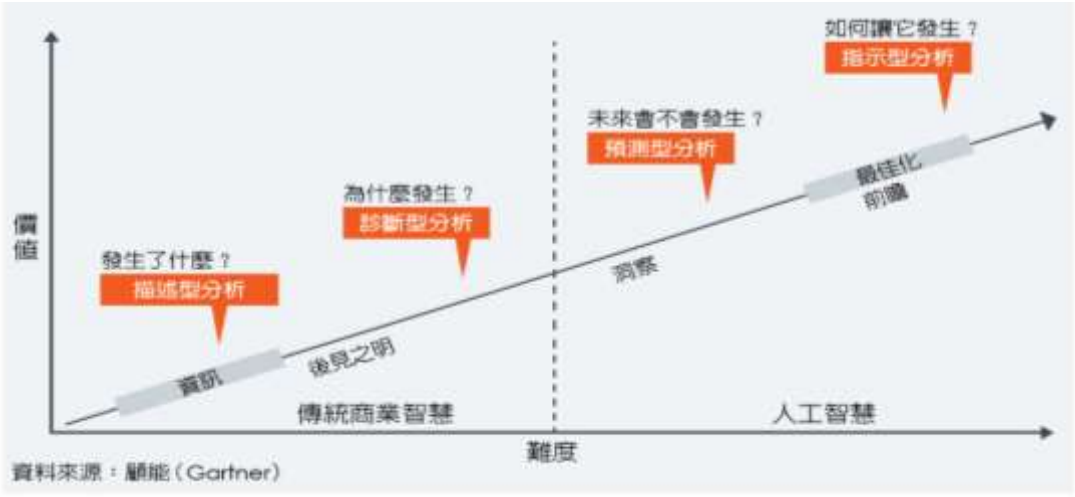


圖 3-1 資料運用分析四階段

資料來源：哈佛商業評論全球繁體中文版
https://www.hbrtaiwan.com/article_content_AR0007025.html

如圖 3-1 依照資料運用的難易度及其開發價值可以分為：描述型分析、診斷型分析、預測型分析及指示型分析，其中描述型分析及診斷型分析屬傳統商業智慧，蒐集的資料多為交易發生後所產生之數據，因此分析方式屬事後且量化資料之分析方式，由於人工智慧及機器運算等複雜統計方法的協助，蒐集的資料不再只是數字資料。

一、描述型分析：為量化分析，描述資料分布狀況及已經發生的事實，即財務報表、庫存表等。

二、診斷型分析：為量化分析，推測數字變化的原因，即同期比較分析等。

三、預測型分析：透過人工智慧，預測未來市場狀況。

四、指示型分析：透過複雜的演算法，提供決策者最佳化的建議，即金融業的理財機器人。

以下就資料蒐集、統計方法及行銷應用等三面向，瞭解大數據應用和傳統資料分析帶來的差異。

一、資料蒐集

傳統資料之蒐集主要以產品為導向，通常是以「行銷」其產品為目的大量蒐集客戶資料，尤其金融機構向來很重視資料蒐集，而蒐集的資料多是客戶主動提供的年齡、性別、年收入及往來情形等可量化的資料。

在大數據應用下，資料蒐集擴大至客戶的生活足跡，每次與客戶接觸蒐集的資訊不再只有金融交易種類、金額等基本資訊，資料蒐集由行銷目的之產品導向轉變為客戶導向，為利瞭解顧客真實需求，以推出滿足顧客需求之商品，蒐集之資料範圍可透過異業合作蒐集涵蓋顧客生活的資料，包含客戶的定位點、興趣偏好等，資料變得容易取得且多元化，以協助瞭解客戶。

資料蒐集之目的、方式、資料形式及資料來源皆發生以下轉變：

（一） 蒐集目的：不具目的性，而是蒐集客戶「生活」資料。

（二） 蒐集方式：需客戶主動提供轉為透過網路銀行、手機 APP 即可蒐集。

（三） 資料形式：由量化資料轉為照片、貼文或是定位資料等非結構性資料。

（四） 資料來源：除了內部資料外，透過異業合作，完整了解客戶的喜好和蒐集客戶生活資料，將客戶的興趣及喜好標籤化。

資料蒐集目的、方式、形式及資料來源的改變，使得營運方式轉為顧客導向。

二、統計方法

傳統統計方式多為事實發生後所蒐集的數字資料，通常多以一段時間（週、月、季、年）為單位來更新資料，此資料即為無法不斷更

新之靜態資料。為了找出數字變化的關係，通常先假設因果關係，再用統計方法驗證是否有顯著關係，隨著電腦的進步，可以短時間蒐集及處理大量的資料，資料更新及運用不再有時間限制，為不斷更新之動態資料。再透過決策樹、人工智慧（Artificial Intelligence，AI）及機器學習（類神經網路）等較複雜的運算方法，轉變為先找出相關聯的變數，再去推測因果關係，而不斷更新及修正機器學習、AI 模型的方式，使資料分析具預測性，能夠協助決策最佳化。統計方式及分析方法的改變，使得資料據預測能力，更具價值。

三、行銷應用

傳統金融業因蒐集的客戶資料有限，以及資料無法即時更新等問題，造成業務拓展通常是以數量取勝，行銷成本偏高，即便想透過分眾行銷提高行銷效率，因無法有效掌握客戶喜好，造成金融業傳統的行銷方式無法引起共鳴，行銷成功率偏低。

在大數據應用下，可以協助金融業者更了解客戶，建構完整的客戶資料，除了了解客戶生活習慣及興趣外，亦可掌握客戶行為、喜好的轉變，預測客戶的需求以客製化廣告，行銷廣告由大量低效率轉變為質量化的精準行銷。行銷步驟依建立客戶輪廓、客戶標籤及行為預測分析如下：

（一）建立客戶輪廓

利用埋追蹤碼至客戶的網頁，分析網頁的程式語言，以蒐集客戶的外部資訊，例如：瀏覽資訊、關注的事項與廣告的互動方式，描繪其生活習慣，透過不斷的更新資料以建立動態且精準的顧客輪廓，從中了解目標客戶喜歡的廣告模式、社群互動及生活習慣等狀況。如圖 3-2 依照意藍科技所提供之案例，顧客輪廓除了基本資料外，包含了

網路互動行為（網站瀏覽時間及社群互動）、點擊廣告行為（點擊廣告的方式、點擊率）、交易行為（定位點、行動裝置資訊）及客戶興趣（網路訂閱）等資料瞭解客戶的日常生活習慣。

圖 3-2 顧客輪廓建立圖

資料來源：http://www.eland.com.tw/20181108.html

（二）客戶標籤

分析客戶瀏覽的網頁、點擊網頁的狀況及停留的時間等，推測其喜好及興趣並進行標籤，依圖 3-3 常見的興趣標籤包括休閒、投資理財、電影及嬰幼兒等，透過標籤可以瞭解主要族群特徵，以投資理財為例，透過客戶分群，分析人群特徵，可以得知每個年齡層注意的理財商品可能有所不同，再進行分眾行銷。

圖 3-3 興趣標籤補充會員資料之示意圖

資料來源：http://www.eland.com.tw/20190220.html

（三）行為預測

分析客戶標籤的轉變，可預測客戶行為，投以客製化行銷廣告。依圖 3-4 客戶標籤由單身轉換為結婚意圖，推測客戶有結婚的想法，且未來可能在桃園買房及求職，即可對客戶提供房貸、車貸或是蜜月旅行社的信用卡優惠資訊。動態標籤分析，可以打破金融業總是被動得知客戶需求、無法及時提供資訊予客戶的困境，大幅提升行銷精準度。

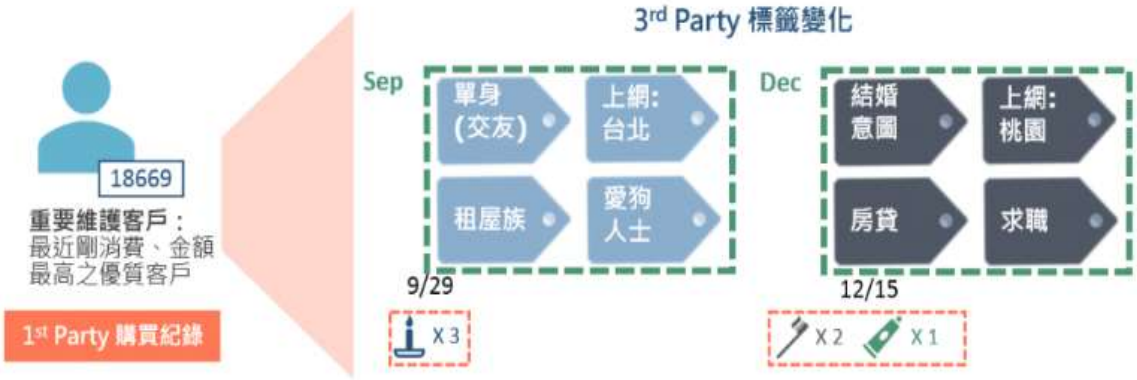


圖 3-4 客戶輪廓

資料來源：http://www.eland.com.tw/20190220.html

如表 3-1 所示，傳統金融業主要透過交易與客戶接觸來蒐集資料，因此資料來源多為客戶的基本資料及往來資料，蒐集目的是以行銷為目的，資料型態為量化資料，資料分析多是描述已發生的業務情況，對於業務狀況的改變通常以邏輯推論出先找出因果關係，再透過統計方法驗證，在大數據架構下，拜資訊進步所賜，蒐集的資料來源變得豐富且多元，可以透過手機 App、網路銀行以及異業合作（社群媒體、第三方資訊業者）等方式蒐集涵蓋客戶的生活得資料，資料型態可以

為一張照片、一篇文章等非結構化的資料，因資料可以不斷的更新因此多為動態資料，而資料量大、多量化、具真實性及時效性的特性，透過複雜的統計方式分析，資料進而具有預測效果，對於過去業務狀況的分析轉為先找出可能相關的原因再以邏輯推測。在行銷應用的部分，透過完整的資料瞭解客戶行為與預測客戶行為，行銷方式轉為低成本高效率的精準行銷。

表 3-1：傳統數據與大數據應用比較

		傳統數據應用	大數據應用
資料蒐集	資料來源	客戶基本資料、往來資料	社群媒體、第三方資訊業者
	蒐集資料目的	為特殊「目的」蒐集	圍繞客戶「生活」蒐集
統計方法	資料型態	量化資料/靜態資料	非結構化資料/動態資料
	分析方式	對歷史資料的描述	具「預測」效果
	變數間的關聯性	以邏輯推測關聯再透過統計方式驗證	先得到有關聯的變數，再找出原因
行銷應用	瞭解客戶	內部資料	內外部資料整合，完整客戶資料
	行銷方式	大眾行銷	分眾行銷
	行銷成效	低效率高成本	精準行銷，高效率低成本

資料來源：本研究整理

第二節　金融業之大數據應用

金融業透過與客戶的業務往來，一直以來都握有龐大的客戶資料庫，惟該資料無法及時更新及維護，屬於靜態的龐大資料，近年網路的普及、穿戴裝置的流行，金融業每次與客戶接觸所得到的資料更多元且可以及時更新，依據 Anurag Singh Bisht, Swadhin Kumar Nayak(2019)[20]將大數據定義為企業與客戶交易、互動和觀察得到的資料，以圖 3-5 得知，傳統 ERP、CRM 和傳統的 Web 應用程式係蒐集和處理結構化的交易數據，而大數據則是擴大範圍至客戶廣告點擊方式、網頁瀏覽時間、社交互動和定位點等互動數據以及穿戴裝置和機器裝置(例如 ATM)回傳之觀察資料運用及分析，使得企業能更瞭解客戶的習慣和喜好，能夠有效率地將蒐集的資料轉換為有價值的營運資料。

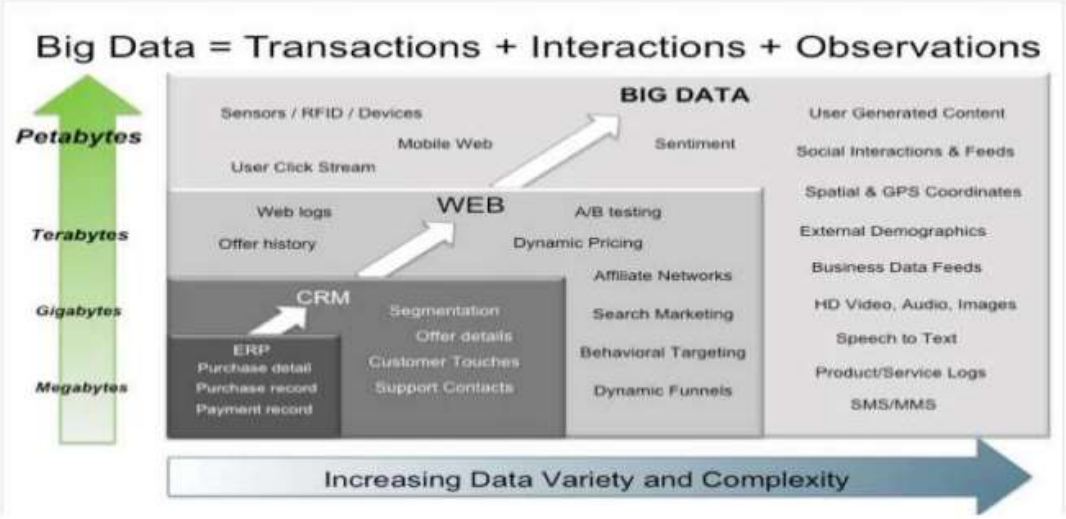


圖 3-5 大數據資料蒐集

資料來源：INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

大數據分析法的應用下，透過 AI、機器學習等複雜的運算法使得金融業從前台的行銷管理、對於商品投資的市場預測、中台的風險

[20] https://www.ijariit.com/manuscripts/v5i1/V5I1-1381.pdf

控管及後台的產品規劃都發生大幅度的轉變。以下就行銷管理、風險控管、產品規劃及投資理財分述金融業之大數據應用。

一、行銷分析

金融業為高度競爭之行業，而各銀行所提供之產品未存在明顯差異，因無法準確得知顧客喜好及行為偏好，大多以大量投放紙本、簡訊及 E-MAIL 等廣告方式增加產品曝光度，過去在行銷領域赫赫有名的 4P 理論，在設計產品時即已設定目標客群（Product），再開始思考銷售通路（Place）、如何定價（Price）及透過促銷強化品牌形象（Promotion），所有的行銷活動是以產品的角度出發，即便設定目標族群，透過性別、年齡等方式做市場區隔，期望分眾行銷能提高行銷效率，惟因客戶資料無法即時更新，無法有效將產品活動傳達予客戶，導致傳統行銷廣告成本高、點擊率卻不高的窘境。

隨著大數據的發展，因瞭解客戶喜好，完整客戶輪廓，使得傳統依性別、職業及年齡等所做的市場區隔不再重要，重要的是客戶是否有興趣，因此衍生出新 4P 行銷理論[21]，以人為出發點，透過大數據分析瞭解客群（People），分析客群的共通點，透過廣告點擊率瞭解數位廣告方式的績效（Performance），依客戶足跡和廣告績效修正及規劃未來廣告方式（Process），再透過不斷分析客戶資料預測消費者行為（Prediction），行銷模式不再是單向由企業向客戶進行，而是企業亦依據客戶行為不斷修正行銷模型的循環，有效率地將行銷模式由大量低效率轉為質化的精準行銷。

[21] https://www.largitdata.com/blog_detail/20190521

二、風險管理

金融業提供的服務幾乎都建立在風險架構上，信用卡、貸款等業務使金融業承受巨大的客戶信用風險，一般的轉帳、存款等交易則存在洗錢及資助資恐或是帳戶盜用等異常交易的問題。

（一）信用風險

信用風險是指金融業借款予客戶，惟客戶無法依照合約準時還款，致金融業有經濟損失。傳統金融業依據授信 5P 原則[22]評估貸款金額及核定利率，首先評估借戶之履行契約的能力（People），再評估借款用途是否合理、合情（Purpose），最重要需評估借戶之還款能力，即需有充足的還款來源（Payment），假設借戶無法履行合約是否須徵提擔保品或保證人（Protection），以及評估貸放後需承擔的風險及預期之報酬，以及借款人未來之發展（Perspective）。以房貸為例，貸款金額高且個人戶僅能提供存摺、薪資單及繳稅證明等財力證明，金融業徵信辦理時參考資料有限，倒帳案件時有所聞。

大數據應用下，考慮客戶的基本資料、行為資料及生活資料，包含教育程度、過去信用狀況、是否結婚及消費偏好等資料運算出信用分數，於貸款前依據信用分數透過大數據模型核定最終貸款金額及利率，於撥貸時透過數位資料的監控，確保其資金用途符合申請目的，貸放後則持續瞭解借戶生活，若是其真實情況與預期有差異則即時調整利率或是將貸放金額降低。金融業在貸款前、中期因瞭解借戶真實生活情形，能夠精準的評估放貸後承擔的風險及預期報酬，在後期亦能持續追蹤客戶行為，防止客戶違約，提升金融業風險控管能力。

[22] https://friap.moeasmea.gov.tw/kn_article.php?nid=111&gid=2

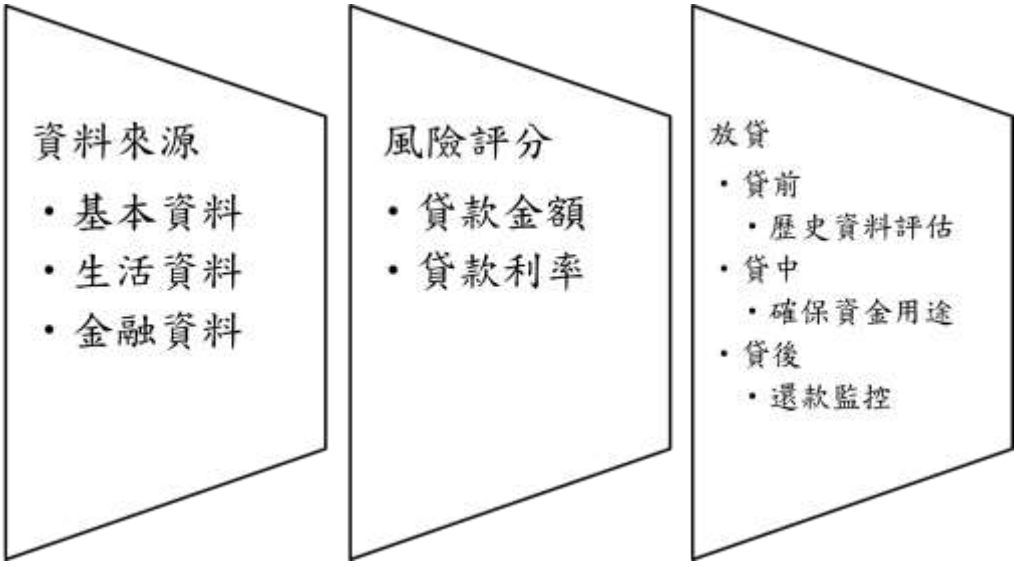


圖 3-6 大數據信用風險控管

資料來源：本研究案整理

（二）異常交易

防制洗錢與打擊資恐指以合法掩飾非法的方式，將非法資金導入合法之金融體系，國際間防制洗錢及資恐罰則趨於嚴格，若金融業違反此條款則會遭受天價罰鍰，且大幅損害企業形象，德意志銀行即因洗錢控管不周於 2017 年間遭罰 4.25 億美元及 4,100 萬美元的天價罰金[23]，依據國際防治洗錢金融行動工作組織（The Financial Action Task Force, FATF）將洗錢分為三個步驟：處置（Placement Stage）、多層化（Layering Stage）、整合（Integration Stage）[24]。

1. 處置階段：將不法所得以現金、購買黃金或賭博等方式置入金融體系。
2. 多層化階段：複雜的匯款轉帳、買賣股票等方式，以複雜的金融交易掩蓋非法資金。
3. 整合階段：非法資金混入合法業務或個人交易，致執法機關難以察覺。

[23] https://www.ettoday.net/news/20181130/1319360.htm
[24] https://www.mjib.gov.tw/EditPage/?PageID=de653765-bcbb-4ba6-b600-795e1ec2acf7

在實務上，傳統金融業透過首先審查客戶身分證明文件確認身分以防止帳戶盜用或是人頭戶的問題，再透過客戶填寫問卷的方式完成認識您的客戶（KYC）/客戶盡職調查（CDD）瞭解個人戶的職業和財務狀況，最後審查交易文件是否合理及合法，若是有疑似洗錢及資恐疑慮的交易則婉拒交易並通報法務部調查局。惟透過客戶填寫問卷的方式無法避免客戶刻意欺瞞的問題，且一般的電腦程式僅能提供簡單變數的偵測，例如：大額、匯款地等異常警示，對於人頭戶的冒用、執行交易的合理性以及及時發生的新聞事件仍需耗費人力審核，而金融機構每日的交易量龐大，造成金融業法律遵循風險及人力成本大幅提高。

在大數據的架構下，透過客戶輪廓，可以瞭解客戶活動的地點、職業及交易狀況等，協助審核客戶資料的真實性，且透過自然語言分析方法，瞭解新聞內容對相關帳戶及時提出警示，AI、機器學習能將交易地點、帳戶特性及交易方式等變數列入運算，偵測帳戶異常及異常交易，以中國非現金支付為例[25]，若客戶為小學學歷、無瀏覽網頁的紀錄，近一週開始頻繁閱讀線上英文新聞、瀏覽外語網站，則會被認為是帳戶盜用或是人頭戶，將其帳戶列為警示帳戶禁止其轉帳交易。若客戶每日的帳戶金額都以小額支付為主，今日卻有大筆金額入帳，且帳戶所有人準備將該筆金額轉出，則有洗錢嫌疑，系統將顯示異常交易警示。

三、產品規劃

金融機構規劃產品時多以商品為導向，未符合消費者需求，致商品難以有效推廣，另外，商品訂價方式常以年齡、性別、職業及年收入等客觀條件分類訂價，以保險商品為例，大眾化的訂價方式未考慮

[25] https://kknews.cc/zh-tw/tech/yareb2k.html

每個人的生活習慣、背景及居住地等不相同，可能造成道德風險問題，即保險公司無法避免駕駛人在購買汽車保險後，降低駕車的謹慎程度，致駕駛風險提高，保險公司因而低估風險，而謹慎駕駛人卻因保費不平等，選擇不購買汽車保險。

因科技的進步及穿戴裝置的興起，現今金融業者可以透過手機 App 或是物聯網蒐集顧客行為，依據Wang(2018)[26]在大數據架構下，金融商品衍生出依使用者行為模式來訂價之使用者基礎保險（User Based Insurance,UBI）以及大數據保單（Big-Data Based Insurance, BBI）。其中 UBI 保險即是依據消費者的健康狀況、開車習慣及生活習慣做為保險訂價時的參考，而 BBI 則是依大數據分析算出最適保費，例如：退運險。依圖 3-7 可知透過內部原始的保險資料配合外部資料，形成數據資料庫，再透過客戶畫像分析，瞭解客戶行為模式，推出以客戶行為計費的 UBI 保險，以及透過人群分析，瞭解客戶需求推出符合顧客生活所需的保險，再以大數據算出最適保費的 BBI 保險。

26 http://www.tigf.org.tw/UpFile/ResearchTopicsFile/%E6%88%91%E5%9C%8B%E4%BF%9D%E9%9A%AA%E6%A5%AD%E9%87%91%E8%9E%8D%E7%A7%91%E6%8A%80%E7%99%BC%E5%B1%95%E8%B6%A8%E5%8B%A2%E4%B9%8B%E9%A2%A8%E9%9A%AA%E7%AE%A1%E7%90%86%E5%8F%8A%E7%9B%A3%E7%90%86%E6%A9%9F%E5%88%B6%E7%A0%94%E7%A9%B6_%E6%9C%9F%E6%9C%AB%E5%A0%B1%E5%91%8A.pdf

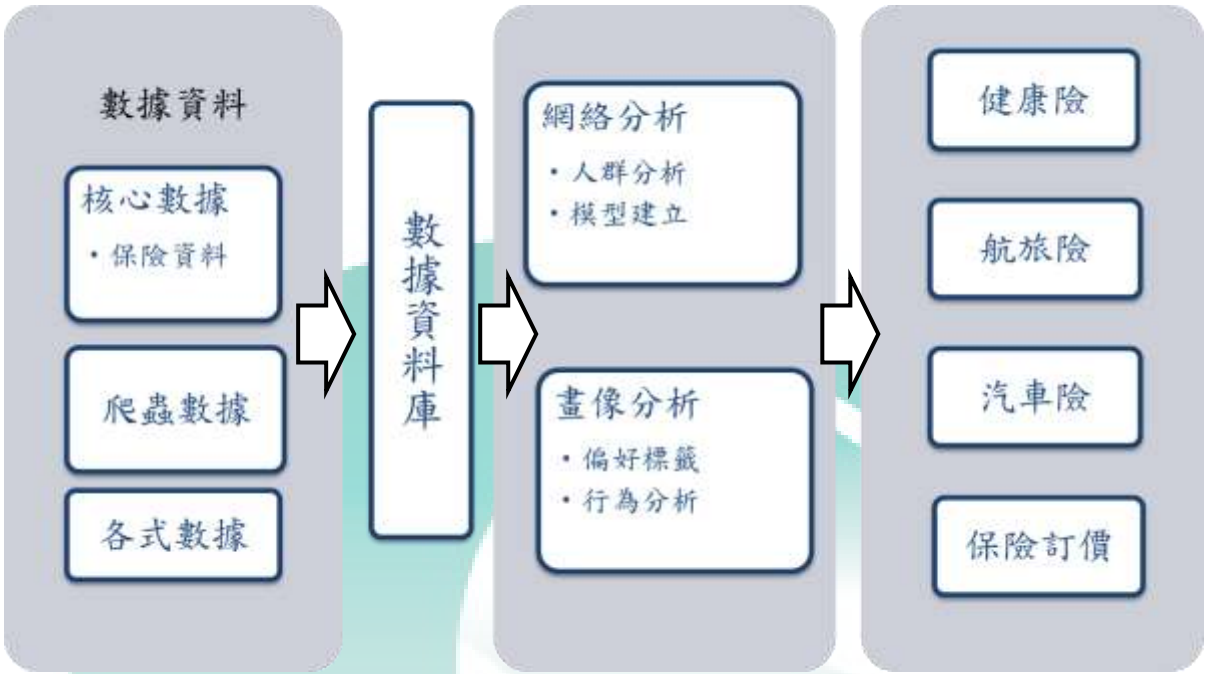


圖 3-7 大數據應用於產品規劃及訂價

資料來源：本研究案整理

四、投資理財

傳統金融業為培養專業的理財顧問，耗費巨額成本大量舉辦課程及鼓勵理財顧問考取證照以精進專業知識，致理財顧問多服務金字塔頂端的消費者，一般消費者無法享受理財顧問的服務，然而，金融市場瞬息萬變，受到各國政經情勢影響，各種投資決策多仰賴理財專員主觀判斷及經濟數據的輔助，人為判斷的不理性行為及經濟數據多為落後資料，造成理財專員無法長遠平穩地提供效率投資決策。

在大數據應用下，透過資料分析能提供股價預測及總體經濟預測予理財專員參考，Johan Bollen, Huina Mao, Xiao-Jun Zeng(2010) 提到，股票市場是遵循效率市場理論，唯有「新聞」才會影響股價，過去及現在的股價都無法預測未來股價，然而許多篇研究也發現，這些「新聞」有些領先指標可以先看出端倪，因此 Johan Bollen 將 2008 年 2 月 28 日至 12 月 19 日（9,853,498 條推特，約 270 萬用戶發布）的推

文分成平靜（Calm）、警覺（Alert）、肯定（Sure）、重要（Vital）、善良（Kind）和快樂（Happy）等 6 個面向衡量情緒，將觀察到的情緒與 3~4 天後的道瓊工業指數變動情形比較，發現以情緒預測道瓊工業指數上升或下降的準確度為 87.6%。

理財機器人目前發展較快為美國，最早於 2008 年即出現 Betterment、WealthFront 及 Vanguard 等理財機器人，依據 RoboAdvisorPros.com 資料統計[27]，至 2019 年 9 月底美國已有超過 200 家的業者推出理財機器人服務，管理的總資產約 5000 億美元，依據證券暨期貨月刊第三十七卷第一期[28]，美國的理財機器人主要分為兩類，一類為以金融業為背景，ETF 發行商所推行的理財機器人，例如：Vanguard、貝萊德，另一類則為金融科技公司推行的理財機器人，沒有金融業背景當作後盾，如 Betterment、WealthFront。在美國，理財機器人透過 ETF 的多元化標的提供客戶理財建議，透過 AI、機器學習篩選標的有效分散風險，提供目標報酬下最低波動度的投資組合，整個決策流程少有人為參與，除了降低人為的決策偏誤也大幅降低「人」的成本，致理財機器人的顧問費用較傳統的理財顧問費用為低。惟依據 Friedberg（2019）[29]討論消費者對於理財機器人與人類理財顧問的想法，其中 88%的受訪者希望技術能協助人類，而不是取代人類，另外，有 85%的受訪者較喜歡與人類的理財財務顧問打交道，而 Betterment 為解決高淨值資產客戶子女海外遊學基金、稅務等特殊問題，自 2018 年推出真人理財顧問服務搭配機器人理財的服務。

[27] https://www.roboadvisorpros.com/

[28] 證券暨期貨月刊第三十七卷第一期，淺談機器人理財在台灣未來之發展

[29] https://www.roboadvisorpros.com/fintech-news-robo-advisor-news/

表 3-2：美國理財顧問的形式

	傳統理財顧問	理財機器人	理財顧問及理財機器人
理財顧問形式	真人提供建議	AI 提供資產配置建議或自動化投資	真人及 AI，以 AI 建議當作輔助，最後依人為判斷提供建議。
收費	高	低	中（真人諮詢以”時”計費）

資料來源：本研究案整理

第三節　金融業應用大數據之案例

傳統金融業蒐集的客戶資料，主要為客戶申辦業務時主動提供的基本資料及往來業務資料，而該資料通常未及時更新，致建立的客戶資料庫不夠大也不夠完整，依圖 3-8，隨著大數據的發展，透過連結客戶生活的方式蒐集及分析資料，改變金融業的營運模式，因瞭解客戶偏好因此可以大幅提升行銷效率，也可以對顧客做較精準的信用評分，再規劃產品時可以依顧客喜好提供服務。

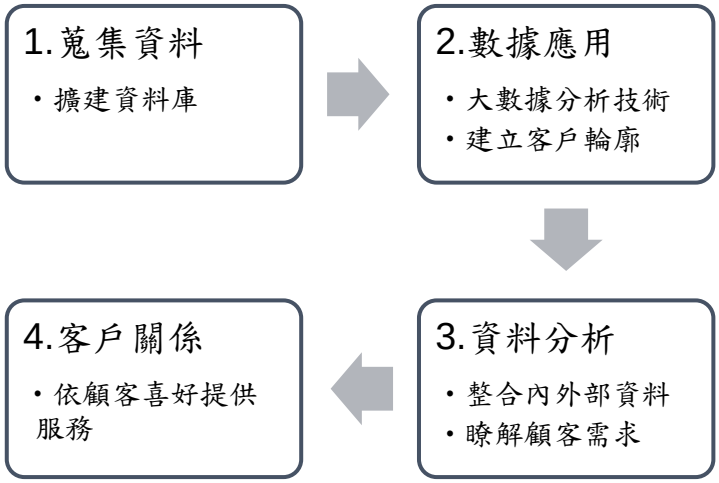


圖 3-8 金融業數據應用

資料來源：本研究案整理

一、　行銷分析

（一）Richart 數位帳戶

在 Fintech 浪潮下，為了提供客戶更便利的金融服務，擴大客群以及蒐集更多有別於傳統的資料，台新銀行推出 Richart 數位帳戶，

透過提升生活便利性[30]、高優惠及低門檻[31]和連結生活圈[32]等方式提供客戶有別於以往的顧客體驗，吸引客戶目光，根據金管會統計，Richart 數位帳戶於 2018 年底市占率高達 50%，為市占率最高之數位帳戶[33]。

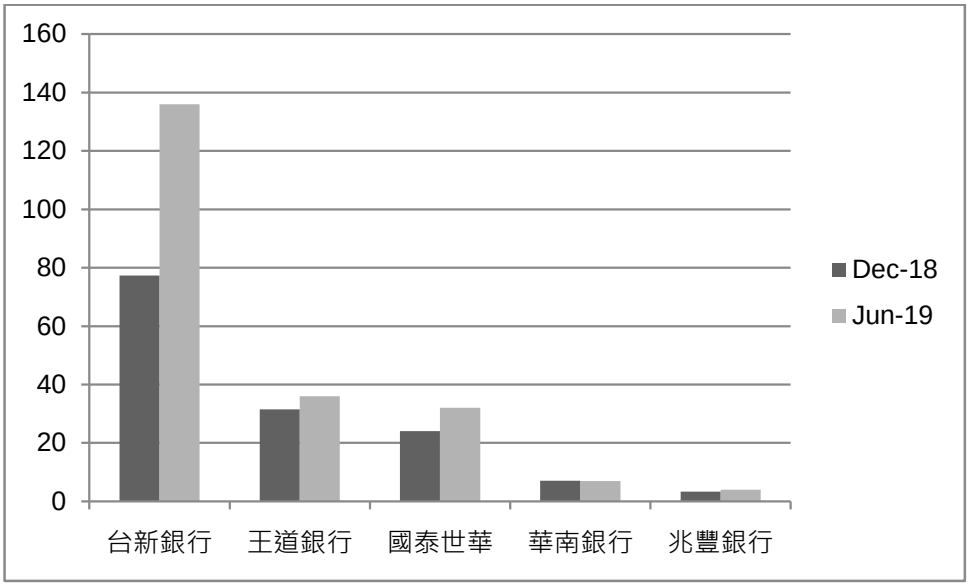


圖 3-9 數位帳戶市占率前五名銀行家數

資料來源：金管會，本研究案整理

傳統網路銀行僅能提供帳務資料核對、帳務轉帳及信用卡餘額查詢等傳統銀行業務功能，數位帳戶則標榜盡可能減少客戶至實體分行等待的時間，任何服務透過網路即可完成，亦將客戶生活所需的金融服務整合至一個 App，依遠見雜誌 2018 年 10 月號的訪問可知，台新銀行的目標客群為頻繁使用行動裝置的青年世代，透過金融服務融入生活吸引客戶，除了傳統銀行業務外，透過該 App 即能購買旅平險、以 10 元銅板投資基金及消費記帳等功能，近期亦推出「麻吉指數」，客戶參與服務的程度越高則麻吉指數越高，指數越高越能享特定優惠，例如折抵貸款利率。Richart 提供青年世代有別於以往的金融體驗，

30無卡提款、尋找 ATM 及記帳功能。

31活期儲蓄存款 1%（臺灣銀行 0.2%）、10 銅板買基金（一般至少 3000 元）。

32推薦朋友優惠、手機號碼轉帳功能。

33截至 2018 年底國人開立數位存款帳戶數突破 150 萬戶，戶數最多是台新銀行 Richart 達到 77.3 萬戶。

將金融業務與客戶的「生活」做連結，由圖 3-9 可知台新銀行之市占率及客戶成長率一直位居第一，大量吸引客戶擴建資料庫，而客戶每次操作 App 的資料皆被整合描繪出「全視角的客戶圖像」。將全視角的客戶圖像加以分析標上各種興趣、習慣及需求等標籤，利用數據分析將客戶分群，投以個人化的廣告，根據今周刊統計，台新銀行透過精準行銷方式吸引卡友進一步成為財富管理會員的比例較一般客戶多出 5 成。

（二） 純網銀

金管會於今（108）年 7 月底核准三家純網銀執照，分別為連線銀行、將來銀行及樂天銀行，純網銀沒有傳統銀行的客戶資料，亦沒有實體分行據點，主要提供線上服務，造成「獲客」較為困難，因此策略通常為向母集團或股東的會員推廣，將手中握有的會員資料透過大數據應用推展業務，連線銀行在日本的母公司 LINE Financial 業已開發出個人信用評等系統 LINE Score，有其社群軟體在台灣約 2,100 萬的會員基礎，亦有行動支付（LINE PAY）的先行優勢，LINE Bank 籌備處表示，未來將應用 AI、大數據及各式金融科技，提供民眾安心及創新的金融服務。將來銀行則有股東全聯實業的會員消費資料，其策略為服務傳統銀行未服務到的客群（主婦、學生）、透過大數據運算推出客製化的商品及透過異業合作打造生活生態圈。樂天銀行其背後樂天集團於日本擁有約 1 億名會員，集團服務涵蓋食、衣、住、行及育樂，會員只需申請一個帳號即能享有集團內所有服務的會員優惠，透過會員消費資料集團為每位會員打造「CustomerDNA」[34]，以日本樂天音樂為例，其樂天音樂用戶與樂天全體用戶的年齡、性別組成看似未有差異，惟深入了解「CustomerDNA」，則會發現相較於普

[34] https://adsales.rakuten.co.jp/business/special/2018_10_kitagawa_mizogami.html

通用戶，樂天音樂用戶購買書籍高近三倍、有很多遊戲買家和許多音樂用品買家，日本樂天銀行亦運用「CustomerDNA」，依照金融服務的屬性配合大數據分析，對會員進行個人化廣告投放，致廣告點擊增加 778%[35]、廣告播放率增加 356%，大幅提高行銷效率。而樂天集團於 2008 年進入臺灣，會員人數逐年增加，其中信用卡發行量更超過 50 萬張，未來將移植日本樂天銀行之經驗來臺灣發展純網銀業務。

二、 風險管理

（一）ZestFinance

ZestFinance 為美國一家網路貸款公司，該公司透過機器學習模型貸款予無信用評分或信用破產致無法向銀行借貸的客戶，以及協助金融機構達成在不增加風險的情況下增加貸放業務。傳統歐美銀行通常採用性別、出生地、職業等基本資料將每個人簡單地用信用計分卡的方式評分，美國的 FICO 評分於申請房貸、信用卡、車貸等業務時廣泛地被參考，銀行審核貸款申請時，依據 FICO 信用評分[36]將客戶分成 10 個借款級別，FICO 信用評分越高，借款級別越高而信貸利率越低，惟 FICO 提供的是一個計算信用評分的公式，因此若未與金融機構往來 6 個月以上，則會沒有信用評分無法與銀行借貸，在美國約有 15%的人沒有信用評分。ZestFinance[37]蒐集客戶的繳款記錄、社群網路資料資訊，甚至客戶填寫表格時的大小寫習慣等資料，透過建立信用模型評估客戶信用風險核予貸款金額與利率，ZestFinance 認為傳統 FICO 評分同一借款級別的人違約風險可能不盡相同，因原始信用評分衡量的變數不夠多錯估客戶風險，如圖 3-10 所示，透過機器學習信用模型評估客戶風險，使用約 7,000 個變數建構模型，除了蒐集

[35] https://www.ithome.com.tw/news/130383
[36] https://gigaom.com/2013/07/31/peter-thiel-leads-20m-round-for-zestfinance/
[37] https://www.zestfinance.com/blog/how-machine-learning-helps-underwriters-grow-without-risk

原始的信用計分卡所採用的資料外，透過不斷將借款人重新分類找出其變數之間的相互作用，其中 ZestFinance 發現表格填寫月收入 7,500 美元的客戶其違約率越低[38]，超過 7,500 美元則違約率越高，顛覆傳統借貸思維，其亦聲稱其還款率比傳統方法高出 90%，透過機器學習有效降低核貸的風險，達到新增核准貸款未增加風險或是減少風險的目標。

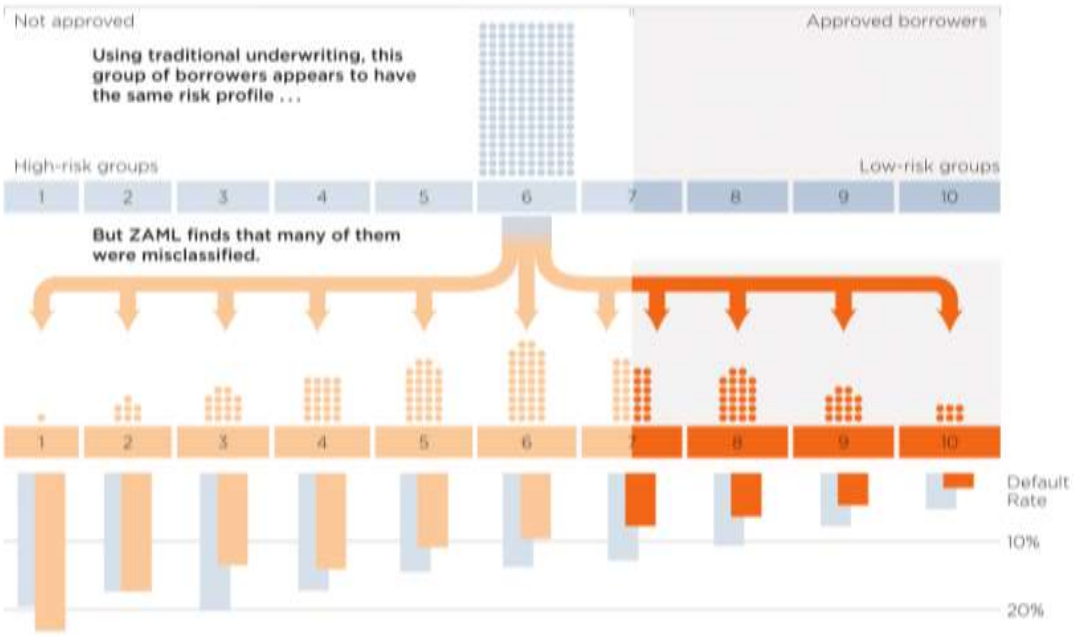


圖 3-10 機器學習信用模型

資料來源：
https://www.zestfinance.com/blog/how-machine-learning-helps-underwriters-grow-without-risk

（二） 芝麻信用

芝麻信用為金融獨角獸之一的螞蟻金服提供的第三方信用服務，由於中國大陸非現金支付的快速發展及網路購物的流行，阿里巴巴集團幾乎擁有所有中國人民生活上的各種大數據資料，螞蟻金服和中國互聯網協會曾在 2016 年發布的白皮書提到，「讓每一個中國人都有信用評分，讓信用等於財富。」的構想。依據芝麻信用官網介紹，芝

[38] https://bigdatafinance.tw/index.php/finance/risk-management/169-zestfinance

麻信用的資料主要來自於互聯網，涵蓋學歷、人脈及生活習慣等因素，其將評分資料分成信用歷史[39]、行為偏好[40]、履約能力[41]、身份特質[42]及人脈關係[43]五個構面來評分，分數則大致分成五個等級，分數越高則表示信用越良好。如圖 3-11 芝麻信用是一種循環式的信用資料評分，客戶借款後，每個月有準時還款紀錄，即能提高信用評分，提高信用評分後，客戶即可再透過較高的信用評分享有更優惠的貸款利率，是一種循環式的機制，可以督促民眾在享受任何信用服務前，衡量自己的能力所及。

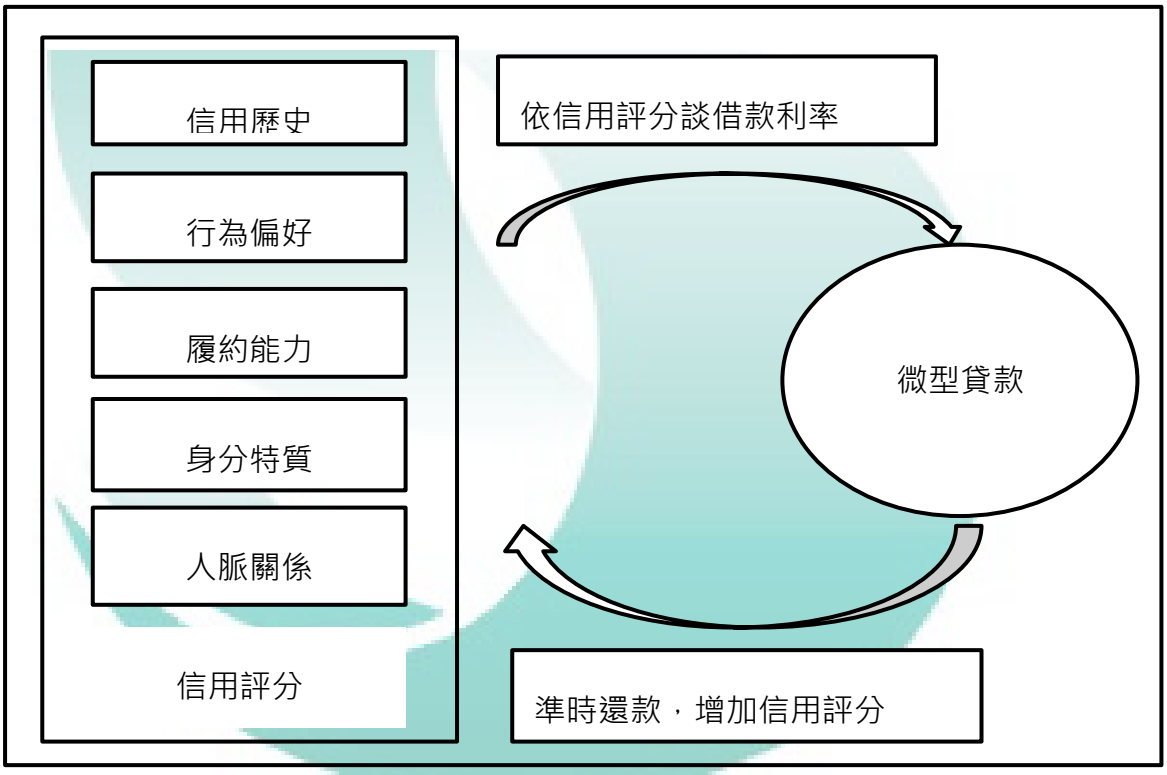


圖 3-11 信用評分

資料來源：本研究案整理

[39]過往信用賬戶還款記錄及信用帳戶歷史。

[40]生活偏好及穩定性。

[41]類似財力證明。

[42]個人基本訊息，例如：學歷、職業等訊息。

[43]考量為「物以類聚」，往來好友、校友等都會納入評分。

三、產品規劃

（一）Oscar

KPMG 於 2016 年發表《全球金融科技 100 強》報告[44]，其中第 3 名為 Oscar，該公司是於美國成立的科技保險公司，經營方式是以消費者的角度出發，提供客戶完整且便利的醫療流程，訂價方式則是依照消費者的狀況訂定因人而異的保費，除了提供消費者保險商品亦整合線上醫療的服務。為利大數據分析，該公司在建立資料庫時，將來自不同醫院的病歷及醫師的診斷報告等進行資料規格統一，透過與專業醫師的合作，釐清不同醫生的診斷用詞，將各醫院的病歷及醫師診斷報告內容統一。在線上醫療的部分，該公司與各地區專業醫生合作，消費者透過手機 App 即可在線上與醫生進行免費地諮詢，Oscar 透過手機的定位功能推薦該區域合作之專業醫生，也追蹤客戶是否按時回診。該 App 整合線上查詢醫師門診時間、預約掛號及電子處方箋等功能，另外，為了養成消費者良好的運動習慣，推廣預防勝於治療的觀念，App 也會記錄運動手環紀錄心跳數、運動公里數等，最後，將資料庫資料、客戶身體狀況和生活習慣及風險綜合評估，訂定出一套因人而異地訂價方式。

（二） 眾安保險

眾安保險為一家網路保險公司，為 KPMG 於 2016 年發表《全球金融科技 100 強》報告[45]之第 5 名，依照客戶生活需求提供適用於各個生活場景的小型保險，例如：考量電子商務的興起，繁瑣的退貨流程及費用造成買家的負擔，因此與電子商務平台業者合作，分析電子商務平台的大量退貨歷史資料，於 2013 年推出與電商平台合作的「退

[44] https://assets.kpmg/content/dam/kpmg/tw/pdf/2017/02/fintech-100-zh.pdf
[45] 同上

運險」。另外，該公司觀察到客戶時常錯過傳統旅平險的投保時間（通常為飛機起飛前 24 小時），透過即時航班的分析，與通訊軟體合作，保險的購買及理賠皆透過通訊軟體完成，而保險的保費與理賠金額會因為購買時間、購買的班次和及時機場狀況而出現不同金額，與傳統保單最大的不同在於即使已經得知航班延遲亦可投保，投保時間為航班起飛前四小時至延誤發生後二小時，大幅提升便利性。

（三） 泰安產險

泰安產險與鴻海集團旗下的創星物聯推出臺灣首張 UBI（Usage-Based Insurance）車險，即依據駕駛的「行車里程、駕駛時段、駕駛習慣」等三大面向來調整保費，透過 App 或 OBDII 追蹤紀錄駕駛人的駕駛習慣，包含記錄時速、駕駛時段、行駛里程、急煞頻率及急轉彎頻率等，該保費除了因人而異地制訂外，每年因駕駛行為的回傳及分析亦會有所調整。

四、投資理財

（一）貝萊德

1. 股價預測

中國股票市場為世界最具影響力的市場之一，貝萊德[46]為了能向市場投資者提供有用訊息，運用大數據資料分析人流量及衛星圖預測市場動向，再使用人工智慧及機器學習技術協助投資者篩選標的。由於中國市場散戶投資人的總交易量佔總市場約 80%-90%，因此貝萊德追蹤微博等社群媒體，以一篇發文訊息為單位，運用自然語言處理技術透過語意分析、討論熱度、關鍵字搜尋等匯總大量文字訊息追蹤

[46] https://www.blackrock.com/ae/intermediaries/themes/investing-in-asian-equities/big-data-asian-investments

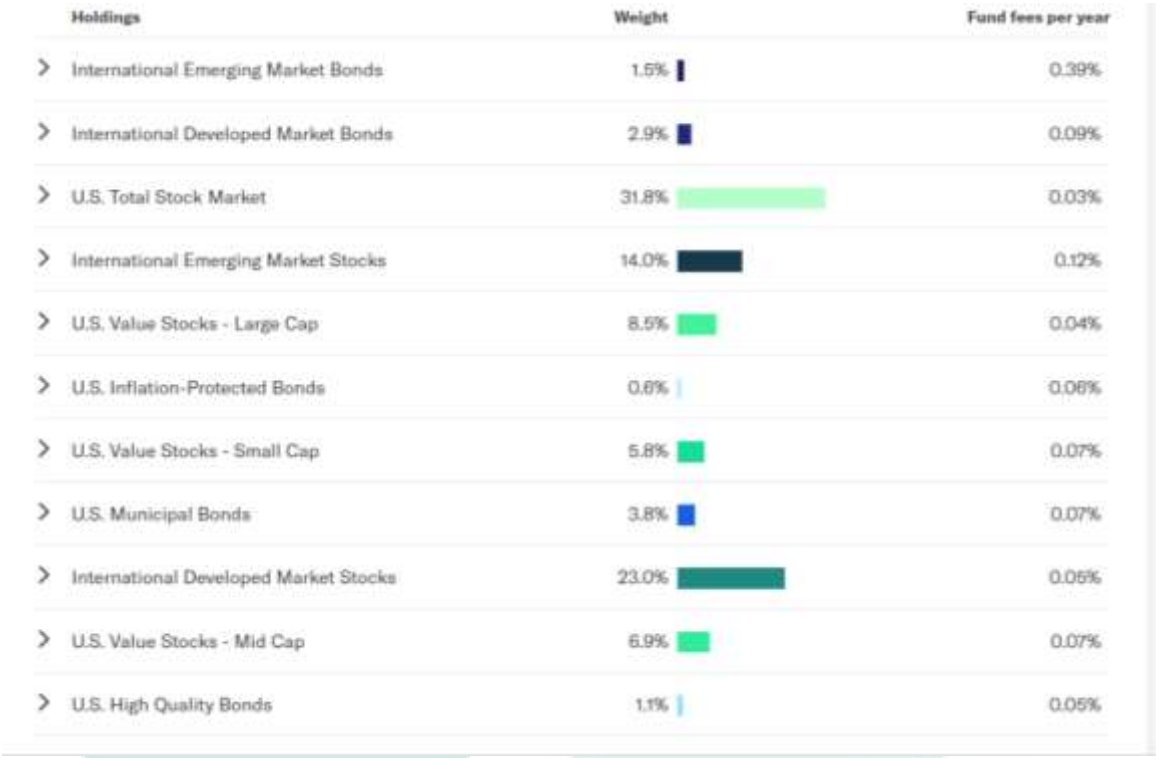
市場民眾的情緒及關注焦點，例如：哪間公司討論度大增，及某間公司的盈利情形預測等。

2. **總體經濟預測**

以前市場主要透過中國政府官方發表的「宏觀經濟領先指數」來預測中國的經濟發展，該宏觀經濟領先指數包含了 18 種經濟數據，其中有輕工業總產值、一次能源生產總量、鋼產量、鐵礦石產量及新開工項目數等18項經濟數據,為了能獲得中國工業活動的及時情況，貝萊德透過衛星技術掃描圖像，每 30 分鐘左右拍攝一次，掃描圖像中建造工廠金屬框架的“金屬度”以及比較來自工廠的卡車的移動來預測經濟發展，這些圖像資料的補充使得市場對經濟發展的預期不再依賴官方所提供的歷史數據。這些影像除了可以觀察總體經濟，透過觀察特定地區的實質活動，將個別公司的實質活動及財報比較，也可以評估及預測特定公司短期內的發展。

（二） **Betterment**

為全球第一家推出理財機器人之新創公司,2008 年於美國成立，提供線上投資諮詢服務，有別於以往僅考量客戶的風險偏好、收入、投資目標等，其認為亦需考慮達到投資目標客戶所需承受之風險，因此改以投資目標、投資期間長短及資金運用方式設定風險承受程度，透過人工智慧模型分析提供客戶客製化的投資建議,其首先提出債券與股票的建議比率，再提出細項的投資標的(如圖 3-12)，投資人對於投資建議可調整債券與股票的比率，惟對於細項的投資標的無法調整。



Holdings	Weight	Fund fees per year
International Emerging Market Bonds	1.5%	0.39%
International Developed Market Bonds	2.9%	0.09%
U.S. Total Stock Market	31.8%	0.03%
International Emerging Market Stocks	14.0%	0.12%
U.S. Value Stocks - Large Cap	8.5%	0.04%
U.S. Inflation-Protected Bonds	0.6%	0.06%
U.S. Value Stocks - Small Cap	5.8%	0.07%
U.S. Municipal Bonds	3.8%	0.07%
International Developed Market Stocks	23.0%	0.06%
U.S. Value Stocks - Mid Cap	6.9%	0.07%
U.S. High Quality Bonds	1.1%	0.05%

圖 3-12 Betterment 提供的 30 歲、年收入 30,000 美金的投資建議

資料來源：Betterment 官網

（三）阿發總管

阿發總管是由「鉅亨買基金」平台與工研院合作推出的理財機器人，主要投資一般基金，提供無信託管理費、無收顧問費的收費架構，首先投資人需填寫基本資料以了解自己風險屬性，阿發總管會寄一封預估投資組合波動度及股票報酬率的報告，設定預期的年化報酬率後，阿發總管即會推薦基金組合，在未來若是市場有變動，阿發總管會啟動「再平衡」機制，寄電子郵件提醒投資人是否接受理財機器人建議調整投資標的。而阿發總管的投資標的多為主動式基金，並非 ETF 被動式基金，無法達理財機器人降低門檻及帳管費之精隨。

（四）富邦理財悍將

富邦理財悍將是由富邦證券推出，配合客戶的投資屬性推薦投資組合，若是配息 ETF 則會直接將股利再投資 ETF 以創造複利效果，

而不是傳統的利息直接返還，投資標的則皆為富邦證券推出的 ETF，該商品雖提供 ETF 當作投資標的，得協助客戶降低管理費，惟其商品選擇性不高，無法達到有效分散風險之原則。

現有的理財機器人相較於傳統理專有三大優勢，1.低管理費，2.低波動，3.低門檻，透過投資被動式基金 ETF 而達成低管理費的目標，而透過大數據分析及模型的建立，理財機器人會組合出可以有效分散風險、低波動及有最佳報酬的組合，傳統投資人的資產需到達一定程度才會配有理專提供理財建議，理財機器人大幅降低人力，因此大幅降低使用理財建議服務的門檻。

第四節　大數據應用的隱憂

大數據已成為時下流行的話題，拜科技所賜，大數據應用賦予資料「預測」的能力，大幅提升資料價值，公司行號對於大數據的應用更是趨之若鶩，為了蒐集大量資料，許多社群平台透過免費的星座運勢、心理測驗等方式吸引用戶同意其資料的蒐集，惟實際蒐集的範圍可能包含於平台上的數位足跡，用戶總是在不知不覺中交出自己的個人資料，資料取得成本低廉且容易，大部分的用戶並不瞭解資料被應用的範圍以及目的，近年來發生多起操作大數據「預測」功能的爭議事件，致社會開始思考大數據的糖衣下，是否隱藏著個人資料保護及資料濫用的負面隱憂。

一、 資料濫用

一般人視為溝通情感管道的社群平台，成為商業行為中最易取得資料的主要來源，在過去幾年中，社群媒體及資訊科技公司已著手將蒐集來的個人數據資料商業化，該數據資料可能包含可以直接識別的

資料，這些堪稱是現代監視狀態的資料可能會帶來龐大的個人資料保護安全疑慮外，然而，這些資料的使用「目的」也造成巨大的道德疑慮。

（一）操縱輿論

2018 年 3 月 Facebook 發生個資大量洩漏的「劍橋事件」[47]，起因於 2014 年間某心理學家以研究為目的，透過心理測驗應用程式吸引約 2.7 萬的 Facebook 用戶使用，該應用程式主要蒐集用戶於 Facebook 上的數位足跡及個人資料，資料內容涵蓋居住城市，閱讀文章的內容及瀏覽習慣等，之後，該批資料被賣給一間第三方資料公司，該公司透過 2.7 萬名用戶的朋友網絡，取得超過 5,000 萬名的使用者個人資料，而該批資料被發現運用於政治操作引爆資訊戰，影響美國總統大選及英國脫歐，該公司是透過建立一套心理分析模型[48]，以「心理變數」預測選情，透過社群活動製造假新聞試圖影響選民的意識形態，甚至造成美國人種分裂的疑慮，引發英國及美國政府要求 Facebook 提供如何取得、儲存以及保護使用者個人資料的相關資料。

（二）商業壟斷

在大數據架構下，企業透過數據資料瞭解客戶及改善服務來吸引客戶，與客戶的互動將帶來新的資料，再透過新資料調整其服務的循環稱為數據網絡效應[49]（Data Network Effect），致世界市場由 Facebook、Google、Amazon、阿里巴巴及騰訊等擁有龐大的數據資料的公司來領導，透過其握有的資料讓集團業務多元發展，造成無形的進入障礙，中小型的科技公司難以相抗衡。2019 年 7 月歐盟認為 Amazon 因擁有

[47] https://www.ithome.com.tw/news/121879
[48] https://global.udn.com/global_vision/story/8662/3039672
[49] http://www.cier.edu.tw/site/cier/public/data/178-087-093-%E5%9C%8B%E9%9A%9B%E7%B6%93%E6%BF%9F-%E7%BE%85%E9%88%BA%E7%8F%8A.pdf

電商平台及零售業者的雙重角色，其有將其電商平台的客戶行為資料、買賣雙方資料及競爭對手資料等運用於大數據分析，以預測消費者行為，致其有壟斷市場違反歐盟的市場競爭規範的疑慮，因此對亞馬遜公司展開調查。

依據 TechCrunch 的 2019 年 1 月的報導，Facebook 自 2016 年起以每月支付 20 美元的報酬吸引 15-35 歲的青年安裝「Research」應用程式，Facebook 即可透過應用程式蒐集用戶的網路流量、網路足跡蒐集資料，甚至求用戶提交於電商平台的消費資料，計畫將這些資料用於商品評估、評估併購計畫以及規劃產品，雖然該應用程式因違反 Apple 商店的隱私權規範被迫下架，而此次事件為人詬病的是 Facebook 蒐集資料的方式是對於不諳世事的青年以金錢的方式誘使其在網路世界被高度監控，不過仍可發現，目前網路世界巨頭所擁有的資源是其他中小型公司難望其項背的。

（三）數據監控

芝麻信用在中國使得每個人都可以享受金融服務，信用分數越高除了可以享受優惠的貸款利率，不需任何財力證明即可申請盧森堡、日本及新加坡的簽證[50]，或是入住飯店免押金的服務，若是信用分數較低的民眾，除了無法借信貸外，甚至無法購買機票，然而該信用評分項目多元，除了過去的信用資料外，是否時常搬家、日常生活圈及往來的朋友等都是信用評分項目之一，鋪天蓋地的資料來源，在什麼時間做什麼事皆可透過數位足跡監控，致民眾為了得到較高的分數，會「優化」其行為模式符合官方標準，刻意避免出現不良行為，甚至被官方引導至特定的行為。另外，信用評分也會受到朋友圈的影響，

[50] https://buzzorange.com/techorange/2017/06/07/zhima-credit/

造成民眾只願意與信用評分較高的朋友互動，分數較低的弱勢的族群更不易累積其信用分數，無形中將民眾階級化，造成社會的不公平。

二、 運算偏誤

大數據應用下，大量的資料透過 AI、機器演算的複雜統計方式，可以協助人類做決策，金融業用 AI 及機器演算來評估商品定價、客戶的保費、貸款利率以及貸款額度，以及理財機器人，然而，卻有越來越多的例子發現，其實 AI 的發展尚未成熟，也會發生決策的偏誤。

過去美國白宮運用過去犯罪者的資料進行大數據分析[51]，希望透過大數據分析協助司法人員判斷「風險評估分數」，而該分數可能影響保釋金、服刑期間，若風險評估分數較高代表其再犯罪機率也較高，因此會影響法官的最終判決，但是該大數據分析卻也被證實，存在著對有色人種的偏誤，該分析結果認為有色人種的再犯機率是白人的兩倍，造成種族歧視的偏誤及社會的不公平。

紐西蘭移民署[52]自 2016 年起藉由辦理簽證時蒐集新移民的年齡、性別、種族、信用資料、身體狀況及犯罪紀錄等資料，以此建立一個模型預測該移民是否會造成紐西蘭社會成本增加，若是該模型出現有疑慮者，則會拒絕發新簽證或是拒絕入境，其中一位印度裔移民即因為模型預測其可能有乳癌的家族病史而拒絕申請簽證，惟該婦女家族沒有任何乳房病變的病史，該偏誤也引發紐西蘭被抨擊是否移民政策存在著種族歧視的問題。

由上述的例子可知，在科技的發達下，大數據大幅度改變我們的生活，惟目前大數據的應用仍存在著一些負面隱憂，近幾年 AI 技術的進步，當社會大眾期待自駕車成熟的智慧生活時，卻也在 2018 年

[51] https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=8311&pages=1
[52] https://buzzorange.com/techorange/2018/08/21/how-big-data-and-ai-will-develop/

5 月發生自駕車撞死行人的事件，顯見目前科技仍有進步空間。近年來，也有一些金融業者發現，由於金融市場的影響因子過於複雜，大數據、人工智慧等方式仍無法精準預測未來經濟走勢，現階段的發展還是需要人類做最終的判斷。

AI 及機器學習的進步，需要不斷多元、大量的「新」資料去優化模型，然而這些分析的結果及使用目的對於商業可能帶來龐大的利益，對於社會也可能帶來巨大的影響，因此更該去探討的是這些提供資料的民眾，是否瞭解其資料被蒐集的範圍以及運用的目的及運用方式，而歐盟於 2018 年實施的 GDPR 即認為須將個人資料的權力還權於民，擴大了個資保護的範圍，加強了資料所有權、可攜權、可刪除權等概念，增加個資對於國際傳輸、自動化設備運用的相關規範。

第四章　金融大數據未來發展與個資保護新趨勢

根據歐盟 GDPR 規定，個資定義範圍擴大至透過自動化方式蒐集的任何形式資料，包括個人喜好、興趣、定位、健康及經濟狀況等資料，在蒐集個資時需當事人明確、具體及充分的指示，若以口頭同意或是預設同意蒐集個資的作法皆不符規定。

在大數據浪潮下，從商品設計、服務提供及風險控管皆涉及運用自動化方式蒐集及處理個人資料，然而金融業不應讓個人資料保護限縮其科技面的創新。

第一節　金融大數據未來發展—OPEN BANKING

銀行的客戶資料也屬大數據重要一環，近年來金融科技（Fintech）風起雲湧，也興起開放銀行（Open Banking）聲浪，使金融大數據可做更多元的創新加值運用。「開放銀行」是銀行透過應用程式介面（Application Programming Interface；API），將客戶資料分享給第三方服務提供者，讓第三方服務提供者（Third-party Service Provider，TSP）可將銀行客戶資料加值運用，開發新的產品服務。

開放銀行的重要性，在於改變金融數據資料「所有權」和「使用權」的主從關係。過去客戶的帳戶資料、金融數據，儼然是銀行獨自擁有的資產；客戶要查詢自己的信用卡帳單、存款往來紀錄等歷史數據，有些銀行動輒收取高額服務手續費，金融消費者只能忍痛接受。由於開放銀行實施，讓金融消費者取得自身資料的自主權；即在客戶授權下，第三方服務者可藉由銀行提供的 API 取得客戶資料。甚至透過第三方服務者的協助，將金融消費者不同銀行的資料整合分析，提供調整建議，使金融消費者可做最佳資產配置、最適負債組合等有利的理財規劃，實質上達成金融消費者數據的可攜性。

本研究以下參考國立政治大學金融科技研究中心「台灣開放銀行政策研究報告」之內容，探討開放銀行與個資保護、各國開放銀行監理機關、資料開放種類與範圍、GDPR 與 PSD2 比較及我國現況發展。

一、 開放銀行與個資保護

客戶與銀行因往來關係而產生的資訊，包含客戶基本資料、帳戶、消費、轉帳、貸款等數據，這些數據對新興金融科技業者，在進行金融服務研發的分析上相當重要。銀行雖然有系統地保存這類資料，但因資料更新成本高往往未加以更新。新興金融科技業者無法有效掌握大數據，以至難與大型金融機構競爭，然而這種情況在開放銀行的潮流下將漸被扭轉。

各國推動開放銀行的背景不同，其中澳洲的發展脈絡是希望落實「消費者資料權」（Consumer Data Right，CDR），提升消費者對個人資料的控制，進而增加消費者的便利性與選擇。而銀行產業是 CDR 推動下的第一個試驗對象，澳洲政府乃修正「競爭與消費者法」（Competition and Consumer Act 2010）作為實施消費者資料權的基礎，並在同一架構下推動開放銀行，希望藉此改變零售銀行市場由某些銀行宰制的現象。

英國則因零售銀行市場競爭不足，由九大銀行業者掌控，高度集中，消費者面臨銀行轉換成本過高、個人及企業戶之現金往來帳戶收費結構不透明，及中小企業商品選擇有限等問題。因此，競爭及市場管理局（Competition and Market Authority，CMA）提出四大補救措施，其中開放銀行 API 是最關鍵的補救措施之一，透過修法方式，由 CMA 強制九大銀行於 2018 年 1 月，將內部資料透過開放 API 授權給第三方業者使用，一方面提升消費者選擇，便於消費者轉換帳戶選擇

對其最有利產品，一方面降低新進業者的市場進入障礙，達到提升市場競爭效果。

歐盟的推動背景與英國類似，主要植基於金融海嘯後全球強化銀行體系信任度，及金融科技實現普惠金融的浪潮，希望透過銀行資料開放與共享，讓支付機構及相關新興金融服務業者與傳統銀行業者處於平等的競爭態勢。因此，修改「支付服務指令 2」[53]（Payment Service Directive 2，PSD2），提供一個跨歐盟各國的支付架構平台，協助導入金融科技應用，並規範必要的技術與管理。

至於亞洲鄰近的香港與新加坡，不若前述國家有較嚴重的零售銀行市場競爭問題，其推動背景除國際趨勢外，更希望與產業目標互補，且協助銀行業者利用開放銀行商機，在妥適管理第三方業者治理流程的前提下，有機地形成多樣化創新發展的金融服務生態圈。以新加坡為例[54]，基於成為亞太地區智慧金融中心之戰略考量，篩選出候選應用程式介面建議清單，鼓勵國內外業者針對候選應用程式的具體類別投入及發展，策略性地透過導入國際資源補足國內產業不足。

綜觀前述，澳洲與英國、歐盟實施開放銀行的背景稍有差異，和香港新加坡情況更是不同。澳洲是從「消費者資料權」出發，原預計

---

[53] 歐盟最早於 2007 年即宣布單一歐元支付區支付服務指令（Payment Service Directive, PSD），目的在調和歐盟區與歐洲經濟區內各國不同的支付規範與作業標準。使消費者在單一歐元支付區（Single Euro Payments Aera, SEPA）及歐洲經濟區內各國皆能使用帳戶轉帳、直接扣款及卡片支付等工具，進行各種付款。因應新科技型態發展，2013 年 7 月提出歐盟支付服務指令修正案（revised Payment Service Directive, PSD2），PSD2 主要目的在為統合歐盟內部的電子支付市場提供法律基礎，使歐盟內部的跨國支付如同單一國家內的支付同樣簡單，2015 年 10 月歐洲議會通過，2016 年 1 月 13 日生效，歐洲經濟區內 31 國（歐盟會員國及冰島、挪威、列支敦士登）需在 2018 年 1 月 13 日前將 PSD2 內國內法化。

[54] 新加坡金融管理局（MAS）於 2015 年成立金融科技與創新團隊，除了連結銀行與金融科技新創產業外，也對數位銀行、開放銀行等議題進行政策制定與協助。相較於歐盟的強制性措施，新加坡金融監理機構採取建置政策架構以及鼓勵的性質推動。因此 MAS 與新加坡銀行公會（ABS）於 2016 年頒布 Finance-As-AService API PlayBook，詳細制定金融業 API 發展策略，並鼓勵銀行參與開放 API。截至 2018 年底，MAS 開放 42 支 API 供查詢金融業公開資訊，並督導新加坡的銀行，包含星展、華僑、花旗、渣打銀行等，共開放 313 支 API。

今(2019)年 7 月要求澳洲四大銀行(Common Bank、ANZ、Westpac、NAB，市佔率高達 95%）開始第一階段資料開放，但對客戶資料保護仍是四大銀行目前最關注議題，Westpac 曾表達：「將原先存在銀行高資安規格的資料，移轉到資安規格較不嚴謹的第三方機構，很有可能將客戶資料暴露於新的風險中。」因資安架構有所疑慮進而延遲至明（2020）年 2 月再進行開放銀行第一階段。

可見金融科技創新與隱私保護，在大數據浪潮的推展下皆不可偏廢，是主管機關與業者須不斷權衡思考的心中尺。

二、 各國資料開放種類與範圍

資料開放的種類與範圍方面，各國作法不同。就資料類型而言，至少可區分為以下四類：產品資料(Product Data)、帳戶資料(Account Data）、交易資料（Transaction Data）及整合性經轉換後資料（Aggregated and Transformed Data）等。另外，各國也將資料依權限分為唯讀資料（Read Data）及可編輯資料（Write Data），進而決定資料開放範疇是否僅限於唯獨資料，抑或及於可編輯資料。

借鏡澳洲以「消費者資料權」出發的開放銀行背景，闡述該國資料開放的作法。澳洲將資料分為五大類加以討論：消費者資料（Customer-provided Data）、交易資料（Transaction Data）、加工資料（Value-added Customer Data）、整合性資料（Aggregated Data）及產品資料（Product Data），分述如下：

（一） 消費者資料（Customer-provided Data）

消費者資料是客戶直接提供給銀行的資料，例如：客戶地址、電話等聯絡資料、申請貸款時客戶提供自身財務狀況資料等，屬於得開放之資料。金融消費者擁有指定移轉權限，消費者得要求銀行

將自身曾向該銀行提供的所有資料予其他同業銀行或第三方業者。但提供銀行的資料限以電子形式記錄；若涉及個人身分驗證時，消費者則不得指示將該資料提供予其他同業或第三方業者。

（二）交易資料（Transaction Data）

消費者於銀行交易之資料，如：存取款記錄、帳戶餘額、利息收入、利息費用等，皆為得開放之資料。

（三）加工資料（Value-added Customer Data）

銀行根據客戶原始資料加工後所產生的附加價值資料，對了解消費者有幫助，如：消費者信用評等、對消費者資產與收入查驗，經加工後消費者帳戶資料。此種加工後的資料，係銀行透過分析消費者交易資料所歸納，屬於銀行創建的新資料，不屬於開放資料範疇。

（四）整合性資料（Aggregated Data）

指銀行整理多個消費者資料後所創建的集體或平均數據資料，如：按各產業別區分的平均帳戶餘額，目前不屬於開放資料範圍。

（五）產品資料（Product Data）

各家銀行業者對其金融產品的資料，例如：產品名稱、費用、消費者身分要求等，然而因各家銀行資料分散且格式不一致，使消費者難在不同競爭者間比較產品優劣，因此開放銀行要求的乃是應用一個共同的資料儲存、公開標準，將產品資料提供給所有參與成員，提升資料可用度。

各國主管開放銀行的監理機關及資料開放的種類與範圍稍有不同，本研究整理歐盟、英國、澳洲、香港與新加坡作法如表 4-1：

表 4-1 各國開放銀行監理機關及資料開放的種類與範圍比較表

	歐盟	英國	澳洲	香港	新加坡
法律依據	支付服務指令(Payment Service Directive 2)	2017 支付服務法(Payment Services Regulations 2017, PSRs 2017)	競爭與消費者法(Competition and Consumer Act 2010)	外匯基金條例、銀行業條例	新加坡金融管理局法(Monetary Authority of Singapore Act)
主管機關	歐洲銀行監理機關	1. 金融行為監理總署(Financial Conduct Authority, FSA)為支付服務法監理機關； 2. 支付系統監理機構(Payment Systems Regulator, PSR)負責支付相關監理	財政部(Treasury)	香港金融管理局(Hong Kong Monetary Authority, HKMA)	新加坡金融管理局（Monetary Authority of Singapore, MSA）
開放資料種類	NA	1. 唯讀資料 2. 可編輯資料	1.唯讀資料	1.唯讀資料	NA
開放資料範圍	1. 帳戶資料 2. 交易資料	1. 最初開放：銀行總行/分行地點、營業時間、個人及企業經常帳戶價格、利息、中小企業界貸款條件等(2017/3 前透過 Open Data API 建置完成) 2. 開放個人及企業金融帳戶交易資料(2018/1 前建置完成)	3. 消費者資料 4. 交易資料 5. 產品資料	分四階段開放 1. 產品與服務資訊 2. 訂閱與新申請產品/服務 3. 帳戶資訊 4. 交易資訊	NA

資料來源：國立政治大學金融科技研究中心「台灣開放銀行政策研究報告」本研究整理

三、 PSD2 與 GDPR

開放資料(Open Data)與大數據(Big Data)皆涉及「資料」(Data)，因此二者常被混淆。根據英國 2012 年發布的「開放資料白皮書」，開放資料指的是資料可以被任何人接觸（Availability and Access），且可重製（指資料修改）、機器可讀（machine-readable）的資料格式，最重要的是，「沒有」任何使用或散布的限制。因此開放資料意涵重在「開放」兩字，是一種強調開放及資料共享的態度。而大數據重點在分析高頻率獲取、大量、各種結構與類型的資料，是獲取「價值」的一種架構和技術，強調的是大量資料的商業價值或社會價值。二者關係可參圖 4-1：

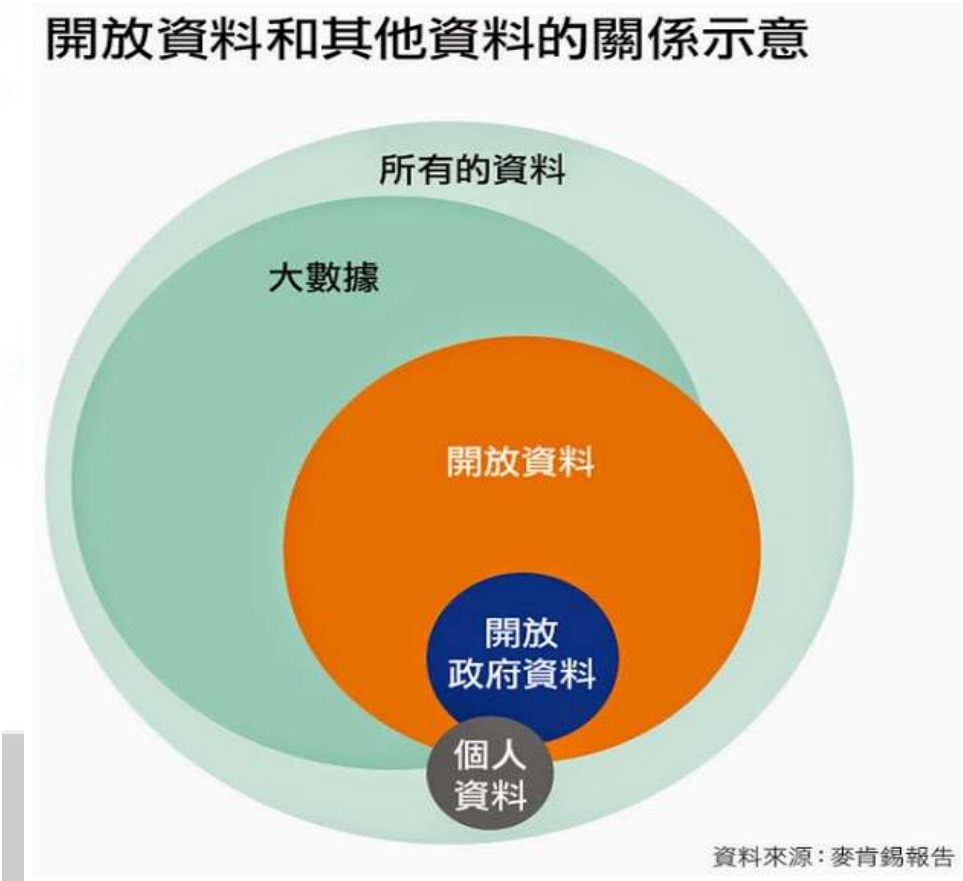


圖 4-1 開放資料與大數據關係圖

資料來源：https://www.bnext.com.tw/article/33242/BN-ARTICLE-33242

歐盟 2018 年 1 月實施支付服務指令（PSD2），在客戶明確同意使用的原則下，規定金融機構必須讓第三方機構（Third Party Payments, TPPs）存取客戶的金融消費相關數據，屬於開放資料範疇。因此，「支付服務指令」（PSD2）目標在創造個人資料的接觸[55]；「一般個人資料保護規則」（GDPR）目標則是個人資料的保護，使消費者更容易了解其個人資料在何處被使用，並讓消費者對其使用提出異議。儘管兩項法令的目標不相同，但資料的處理及使用，都取決於資料主體（消費者）的明確同意[56]。

PSD2 第 94 條規定：為了特殊目的處理個人資料須符合歐盟的資料保護規範，即金融業在推行業務時，若遇矛盾處應不違反 GDPR 規定。然而，在業務執行中較多討論的模糊地帶，包括靜默方資料處理及「明確同意」[57]。

（一） 靜默方資料處理：銀行的轉帳業務中，通常由 A 轉給 B，若 A 同意由支付服務商處理其個人資料，屬靜默方 B 之被動交易資料（Silent Party Data），支付服務商可運用整合嗎？依據 PSD2 第 66 條，成員國應確保付款人有權利用支付服務商提供之服務，第 67 條，成員國應確保支付服務用戶有權利能夠得到帳戶訊息的服務。GDPR 6（1）提到若合乎合法利益，允許第三方使用且運用資料。惟合乎合法利益該如何定義？GDPR 6（4）提到如果處理目的不是蒐集個人資料的目的、不是基於資料主體的同意，也不是基於聯盟或成員國法律，應確定用於其他目的的處理與最初蒐集個人資料目的相符。綜觀以上，除

[55] 透過接觸帳戶規則，PSD2 可獲取消費者或支付服務使用者（PSUs）的財務資料。PSD2 允許第三方機構進入支付市場且提供新帳戶資訊及支付啟動服務。以上服務分別由帳戶資訊服務提供商（AISPs）及支付啟動服務提供商提供。

[56] https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2

[57]

非靜默方處理資料之目的能夠符合當初蒐集目的，否則支付服務商進一步處理靜默方資料並不合理。

（二）明確同意：PSD2 及 GDPR 中皆提到運用個人資料時，需當事人明確同意，根據 PSD2 94（2）提到成員國應允許支付服務商處理必要的個人資料，以預防詐騙及協助調查，而支付服務商只能在客戶「明確同意」下處理和保留個人資料，惟 PSD2 並未說明明確同意之定義，依據歐盟資料保護監督機關（European Data Protection Board，EDPB）解釋，PSD2 所指的明確同意並非單指客戶同意處理資料，而是指系統使用者須明確同意資料予系統提供商為特定目的使用，是一種合約關係，若依照 GDPR6 解釋，能夠合法處理資料的行為包括為履行合約而處理資料的行為，因此與支付服務提供商簽訂合約時，客戶應充分了解個人資料將被處理之目的，並必須明確同意這些條款，而這些條款應與合約中其他事項明確區分開來。

事實上，關於「消費者同意」，PSD2 與 GDPR 的內涵稍有不同，比較如表 4-2：

表 4-2 PSD2 與 GDPR 同意內涵之比較

同意內涵	PSD2	GDPR
1.消費者同意資料處理出於自由意願且有特定目的	✓	✓
2.消費者被告知有撤回同意的權利	✗	✓
3.個人機敏資料或跨境傳輸，需有消費者明確同意	✓	✓
4.消費者明確要求資料處理及共享	✓	✗
5.同意表示自動到期	✓	✗
6.同意須清楚、明確及被告知	✓	✓

資料來源：
https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2

四、 我國現況

國內 Open Banking 採取香港模式，以不修法方式進行，由銀行與第三方服務公司（TSP）合作推動。在三階段的開放措施中，首先第一階段是「公開資料查詢」，以非交易面的金融產品為主，例如房貸利率、信用卡商品等。第二階段是「消費者資訊查詢」，須獲得客戶授權，TSP 業者可提供帳戶整合服務，例如將同一客戶在五家銀行的房貸、存款、基金投資等資訊一併整合。第三階段是「交易面資訊」，在客戶同意下開放交易與支付，TSP 業者可在整合帳戶後，直接透過 App 連結帳戶扣款、支付、調整或撥付帳戶資金。

「開放銀行」是金管會 2019 年重點工作項目之一，並委託財金資訊公司就銀行得開放的業務研擬 Open API 之共同資安及技術規範，打造一個資料開放的平台促進銀行與第三方業者合作。今年 7 月金管會首度揭露第一階段開放 API 的標準，由 13 家參與的銀行提供非消費性的資料，例如存款利率、信用卡優惠及貸款利率等資料，而首個 OPEN API 應用的 APP 是「麻布記帳」，符合財金公司制定的資安與技術標準，第一階段麻布記帳除了提供基本的現金消費記帳功能、儲存電子發票功能外，亦將消費者在 13 家銀行的存款資料、信用卡資料及貸款資料整合，透過麻布記帳可以一目了然每家帳戶的餘額、每筆信用卡的刷卡金額及各家信用卡繳費時間，除了提供消費狀況分析，將每筆費用及存款轉為負債與資產，讓消費者了解自己的資產狀況。

第二節　個資保護新趨勢

一、 國際 ISO27001 個資管理規範

國際標準組織(International Organization for Standardization，ISO）2005 年 10 月 15 日公布 ISO27001 資訊安全標準(Information Security Management Systems，ISMS)，所稱 Systems，與一般慣用的資訊系統、網站系統不同，較貼切的解釋應為管理規範、作業流程與文件表單。在 ISMS 範疇內，資訊被當作一項有價值的資產，需受到適切保護。ISO27001 主要是以建立、實作、運作、監視、審查、維持及改進資訊安全管理系統之模型，共有 11 個控制領域、39 個控制目標及 133 個控制點（參圖 4-2），藉由各項控制措施確保組織的資訊安全。

資料來源：https://www.cc.ntu.edu.tw/chinese/spotlight/2010/a99010.asp

圖 4-2 ISO27001 控制領域

由於個資保護有許多措施仍屬於資訊安全範圍，因此許多企業仍以導入 ISO27001 作為因應個資法的策略。對企業而言，雖然要投入不少人力物力，但導入認證有以下好處：首先，可採用業界成熟的管

理制度和經驗，減少企業自行摸索的耗損；其次，透過第三方驗證單位證明企業卻有落實善良管理之責；最後，企業可透過認證建立內部共識，讓員工學習同一套管理制度以建立共同的管理觀念和思維。

企業組織通過 ISO27001 認證，若要強調個資保護議題，似乎較為簡單，至少已有第三方之稽核保證，但應同時檢視相關之技術配套是否足夠。建議企業組織可根據自身業務特性，從個人資料保護持續改善管理流程、個人資料保護與安全、設備管理、系統開發及委外管理等方面訂定細部管理措施，徹地落實個人資料保護。

二、 英國 IASME 對 TSP 業者之資安與個資標準認證[58]

ISO27001 對資源匱乏的中小型企業（Small and medium-sized enterprises，SMEs）來說較為複雜，而英國 IASME 是提升中小型企業網路安全的資訊保證標準，不僅標準較為簡單且價格適中。英國於 2009-10 年對 IASME 模式進行研究。IASME 於 2010-11 年開發並試用，定期對其進行修訂，以適應中小企業風險環境的變化。

IASME 治理標準與國際標準使用相同的實施模式，包括 PDCA（計劃-執行-檢查-行動）原則和提供管理框架的資訊安全標準（ISMS）。該標準是國際標準 ISO27001 的可負擔且可實現的替代方案。

IASME 治理標準涵蓋以下資訊安全主題：1.管理安全；2.資訊資產；3.雲端服務；4.風險管理；5.資料保護（包括 GDPR）；6.人員；7.安全政策；8.物理環境；9.防火牆及網路閘道；10.安全配置；11.營運管理；12.使用者帳號；13.管理權限；14.惡意軟體防護；15.漏洞掃描；16.監控；17.備份及還原；18.事件管理；19.業務連續性。

[58] https://en.wikipedia.org/wiki/IASME

三、 GDPR 違規案例

GDPR 施行已超過一周年，搜尋引擎巨擘 Google 即因違反 GDPR 而遭裁罰鉅額罰鍰，除具指標意義外，也是歐盟會員國對嚴格執行 GDPR 的態度展現。此外，NOYB（None Of Your Business）團體於今(2019)年 1 月 21 日在奧地利提交另一份申訴，這次是針對 Amazon、Apple、Spotify、Netflix 及 YouTube 等影音串流媒體服務業者，就渠等未能提供充足的額外訊息，例如個資當事人的資料將會被傳輸、分享給哪些特定人，或是未能即時回應個資當事人針對該等資訊或是其個人資訊存取的請求（後者即是所謂「當事人權利行使」的違反）。

從前述裁罰案例可得知，適用 GDPR 的企業在法遵上，應注意監督者不再僅是政府或主管機關等公權力，商業交易往來對象甚或市場消費者，亦有可能透過類似 NOYB 的個資保護團體進行行政申訴或團體訴訟。企業日後恐無法再存有「我們並非大型企業，應不致遭主管機關盯上裁罰」的心態，因為在 GDPR 的監督及執行上，係著重在從個資當事人的視角出發，尤其在個人資料保護意識高漲的歐盟各國，更是如此。

（一） Google

1. 案例事實

該案是由法國兩大民間團體「NOYB（None Of Your Business，其宗旨口號就是：”My Privacy is none of your Business”）」以及「LQDN（La Quadrature du Net）」，於 2018 年 5 月 25 日及 28 日 GDPR 甫施行後，立即向法國資訊及自由委員會 CNIL（Commission Nationale de l'Informatique et des Libertés）所提出之申訴；其中，LQDN 還受高達 10,000 名權利

受害者委任。CNIL 於接收該等申訴並確認其具有管轄權後，旋即於同年 9 月就本案進行在線檢查（online inspections），以分析 Google 用戶瀏覽模式，佐以用戶使用 Android 手機建立 Google 帳戶時所得接觸之文件，確認 Google 在個資蒐集、處理及利用程序上，有無違反法國當地個資法規以及 GDPR 之相關規定。

最終，CNIL 於今(2019)年 1 月 21 日作出處分，認定 Google 在對用戶進行個人化廣告行為（ads personalization）時，就其所蒐集的個人資訊，並未有公開處理的透明度、充足資訊以及有效的同意，對其處以高達 5,000 萬歐元的罰鍰（依照 GDPR 規定，就罰鍰之裁處，最高可達 2,000 萬歐元或是違法公司全球營業額的 4%，本案 CNIL 明顯是以後者來計算罰鍰）。

2. CNIL 認定違反 GDPR 部分

（1） CNIL 認為 Google 並未提供充足且透明的個資處理相關資訊予其用戶

包括一些基本的資訊，例如 Google 蒐集個資以進行處理的目的、個資儲存的期間、哪些蒐集來的個資將用於個人化廣告行為上等訊息，散見在不同的分頁文件及連結中，用戶無法輕易且直覺性地獲得相關資訊。此外，部分個資處理資訊即便有提供，也不一定清晰詳盡，常有用戶無法全盤了解其個資處理行為的內容。舉例而言，Google 告知用戶其處理、利用個資的目的，常過於籠統且含糊，而在蒐集的個資種類告知上，亦有相同問題；更嚴重的是，

Google 甚至未向用戶告知，部分蒐集來的個資，將留存的期間。

（2） CNIL 認為 Google 自用戶所取得的個資蒐集、處理及利用的同意，恐非有效同意

理由包括：一、CNIL 發現 Google 用戶在同意前，並未接受到完整且充足的告知。例如承前所述，Google 就個人化廣告行為的個資處理相關資訊，散見在不同文件中；然而，個人化廣告行為其實會同時在 Google 眾多服務、網頁及應用程式中（如搜尋引擎、Google 地圖、YouTube 等）進行，其就特定用戶所各自蒐集來的資訊，會進行合併分析及處理，如果 Google 未就此情形向用戶進行充分告知，則用戶作出零散、個別的同意是否有效，即有疑慮。其二，CNIL 發現 Google 自用戶蒐集來的同意，並不具體明確。舉例來說，在使用者創建 Google 帳戶的過程中，其必須點選「我同意 Google 的使用者條款」以及「我同意 Google 依其隱私權政策處理我的個資」等方框，才能成功創立 Google 帳戶，亦即使用者為建立 Google 帳戶，必須一次性地概略同意所有 Google 的使用者條款及隱私權政策。然而，GDPR 所要求的「同意」，必須係個資當事人清楚確認其同意的內容及行為，且不容有模糊的餘地，故上開等同「預設點選」的「強迫同意」方框（pre-ticked boxes），即與 GDPR 要求個資當事人針對不同個資蒐集處理目的有「具體」同意的精神有違。從而在本案中，由於個資處理的合法基礎之一，是基於個資當事人「有效的」同意，故

CNIL 認為 Google 未取得用戶有效同意即使用相關個資進行個人化廣告行為，已有違反 GDPR 的規定。

（3） GDPR 相關規定

GDPR 有關「同意」的合法性要件認定係規定在第 7 條中，要求個資當事人必須就其個人資料處理，在受充分告知下，進行具體肯定、自由明確及非屬模糊的指示，始為合法的同意。此外，如果單次同意涵蓋到不同目的的個資處理行為，必須確認個資當事人就該等同意均有上述合法的同意。

實務上較容易產生問題的是「視為同意」、「強迫同意」的情形。由於 GDPR 前言已載明，就單純沉默、預設選項為同意或不為表示的情況，皆不應構成 GDPR 規定中所稱的同意，所以如在相關個資告知文件中使用「您如使用本公司所提供之服務（例如：創建帳戶），即視為您已同意本公司的使用者條款及個資處理利用之隱私權政策」等用語條款，即有違背 GDPR 的意旨。

3. Google 案例中，歐洲法院對「被遺忘權」看法

2016 年 Google 因拒絕在全球搜尋結果中刪除敏感資訊，遭法國資訊及自由委員會（CNIL）裁罰 10 萬歐元（10.9 萬美元）[59]。之後 Google 對法國要求將「被遺忘權」（刪除權）擴及全球的命令提起告訴。2019 年 9

[59] 2011 年一位西班牙男子一狀告上法院，要求當地報章雜誌，刪除十幾年前，他因財務危機，名下房屋遭出售的訊息。他認為，由於他早已還清債務，而當時報導有損他名聲，期望藉由法律保障他的隱私權。這項法律案件緊接著進入歐洲最高法院審理，當時法院作出判決，判定該男子訴求有理，認為 Google 有協助移除「已過時且不相關訊息」的義務。這項判決正式使「被遺忘權」成為歐洲地區公民的權利之一。目前 Google 採用「地理隔離」的方式，讓在歐洲境內的人，無法上網存取這些已申請通過的被遺忘的資訊，但在歐洲地區以外的人，仍可透過 Google 的搜尋引擎接觸這些資訊。

月 24 日歐盟最高法院駁回法國當局要求，判定 Google 只需在歐洲境內刪除敏感的個資搜尋結果，不必在全球網域刪除[60]。

（二） 英國航空（British Airways）

2018 年 9 月，英國航空因網站和行動 App 遭駭，導致透過 ba.com 網站連上公司系統的用戶都被導向至詐騙網站，並遭攻擊者取得用戶資訊，包含姓名、住家地址、Email、信用卡、旅客訂位代號等資訊，高達 38 萬筆網路交易受到影響。

英航於個資外洩事故發生後，主動告知英國資訊委員辦公室（the Information Commissioner's Office, ICO），ICO 調查後發現這起個資外洩事件從 2018 年 6 月就發生，英國航空是在事情發生 3 個月後才主動告知。另外，認為英國航空的個資系統缺乏嚴謹的安全防護，包含顧客登入資訊、信用卡支付資訊、顧客機票資訊等都不夠安全。根據 GDPR 罰則，ICO 以英航 2018 全年營收的 1.5%計算，判處 1.83 億英鎊（約新臺幣 70 億元），成為 GDPR 上路以來最嚴厲處分，比先前 Google 遭重罰 5 千萬歐元（約新臺幣 7 億元）更高出數倍。

四、 臺灣產業因應 GDPR 具體做法

（一） 金融業

1. 金融業於歐盟地區設立情形

（1）銀行：6 家本國銀行於歐盟境內設置 7 分行及 1 子行，當地分行或子行處理歐盟自然人個資流程，須完整遵循

[60] https://udn.com/news/story/7088/4066211

GDPR 及相關法規規定；此外，我國總行就取得之歐盟自然人資料相關處理運用方式亦應遵守 GDPR 規定。

（2）保險:2 家保險公司於歐盟境內設置 8 家特殊目的公司，然該等公司並非從事保險業務，除少數當地員工個資外，未涉及蒐集歐盟居民個資，經評估可不適用 GDPR 規定。

（3）證券：2 家證券公司於歐盟境內設置 2 家子公司，其營運模式係轉介客戶至其他海外子公司開戶，且以法人戶為主，除少數當地員工個資外，原則不碰觸客戶個資。

2. 銀行業因應措施

（1）歐盟有分支機構之銀行業因應

A. 強化隱私資料保護

a. 配合 GDPR 進行內部作業規範調整；

b. 檢視網路資安防護系統；

c. 建置個資外洩時之通報系統。

B. 資料處理程序調整

a. 檢視隱私資料蒐集、處理與利用的要件，包括：清楚、積極之同意、法定蒐集要件，配合調整相關契約條款；

b. 委託/諮詢外部顧問/律師提供專業協助處理，並依 GDPR 原則簽署同意遵循當地資料保護規範。

C. 進行個資盤點：包括歐盟個資人數、業務範圍及是否適用 GDPR 之評估。

D. GDPR 規範比較

a. 完成法規差異分析；

b. 評估建置個人資料可攜權、被遺忘權、限制權之機制；

c. 禁止犯罪前科資料之處理。

E. 跨境傳輸因應：簽署 SCC（Standard Contractual Clauses）或申請 BCRs（Binding Corporate Rules）

F. 設置資料保護長:4 家已完成設置;1 家雖不設置 DPO，但於倫敦設置連絡窗口。

（2）歐盟未有分支機構銀行業因應

本國銀行雖於歐盟未設有分支機構，若其業務涉及對歐盟境內自然人提供商品或服務，仍有 GDPR 適用。相關因應措施包括：

A. 由總行或委託相關顧問公司協助進行差異性分析及影響範圍，並就個資蒐集、處理程序及個資當事人權例告知事項，研修銀行個資同意書範本等相關規章。

B. 取得歐盟自然人個資之銀行均已辦理法規差異分析，且完成網路資安防護措施之檢視，並已參加相關教育訓練。

（二） 百貨業--台北 101

臺灣指標性地標之一台北 101，每年有超過 1,000 萬人次的國際旅客造訪，無論是觀景台、購物商場，都使台北 101 會接觸到歐洲公民的個資，GDPR 施行後，台北 101 因應的具體作法如下：

1. 取得個資認證—BS10012：2017

台北 101 在 2015 年已經拿到 BS10012：2009 個資認證，在全世界隱私保護不斷提升下，面對歐盟 GDPR 施行，今（2019）

年又取得英國新版個資保護認證 BS10012：2017 以為因應。更難得的是，101 將個資保護認證的範圍擴展到全組織，並不像許多企業僅以資訊部門作為取得 BS10012 的主要認證範圍，亦即包含 101 購物中心、觀景台等業務單位的個資使用均全盤納入，表示 101 每個部門所蒐集、處理和利用到的各種個資及相關資訊流都有跡可循。

2. 設置資料保護長（Data Protection Officer，DPO）及全員教育訓練

台北 101 完成個資認證後，即設置資料保護長，由法務主管擔任。接下來就是在組織中傳遞個資保護概念，即透過個資管理小組（各部門代表）發布相關訊息，讓員工瞭解歐盟對於個資保護的相關規範。為增加員工對個資管理辦法熟悉度，每年有相關個資測驗，並針對不及格者複試與輔導，這種測驗無論正職、約聘人員都要參加，未來希望擴及場域內外包的保全、清潔人員。

另外，定期進行事故通報演練，製作演練腳本與情境，員工一開始可試著依腳本練習，熟悉後就知道事故發生時，該打電話給誰，誰接到電話後要向誰報告，如何處理事件調查反應，以及是否要通知當事人或對外發布新聞稿。

值得注意的是，除內部員工外，101 也要求委外廠商配合，一開始委外廠商對個資保護的態度，覺得不重要也不積極，101 會採引導方式，將個資保護要求列於委外合約中，簽署保密切結書，同時每年執行一至二次的委外檢查，並將委外廠商的個資保護執行程度列為後續合作的考量。

3. 每年全組織兩次個資盤查

個資盤點的執行上，重點在於強化整體資訊流的識別，101 個資管理辦法要求每年兩次個資盤點。當個資進入 101 後，先識別出所涉及的單位，雖然個資盤點時，是以部門的主要業務流程盤點，若盤點部門拿到的是二手資料，就要問誰是第一手？下一手又是誰？如此才能將全公司的資訊流串起來，並檢視那些部門涉及這些個資的處理流程。

個資盤點需依個資生命週期進行檢視，才能掌握完整的個資動向與個資的安全防護，像是個資實際擁有的人與處理單位，還有如何提供給第三人或委外廠商等面向。

4. 新系統導入隱私保護設計概念

GDPR 將隱私保護預設（Privacy By Design）的概念置於規範中，台北 101 過去沒有這種觀念，因此系統開發是屬於事後因應，未來只要有 IT 新系統上線或系統更新版本，就會將資料保護的概念納入相關系統設計考量。

5. 徹底執行客戶被遺忘權

對於當事人刪除個資的請求，台北 101 也提供相應管道，只要提出的理由合理，便會透過一定程序將所有資料刪除，包括存在系統及連結到資料庫等之當事人個資。企業在個資蒐集上，可能用於不同地方，如行銷與合作推廣等，一旦客戶要求刪除時，可能刪除了主檔，但其他地方是否也一併刪除，就成為企業挑戰，此時，對於資訊流（應用軌跡）的掌握就很重要。

不過企業若是依據其他法律規定蒐集或使用個資，企業就有權拒絕使用者的刪除要求。因此，101 執行個資盤點時，會

要求員工列出蒐集此項個資的依據，若是依法蒐集也會有保存年限，並在個資盤點的保存期限項目特別標註，如此一來，可快速識別出那些資料是企業有權拒絕刪除者。

（三） 科技業--群暉科技

總部位於臺灣的群暉科技，是屬於網路儲存設備業者（NAS），包括臺灣、美國、澳洲、日本甚至歐盟都有龐大客戶群，也提供相關私有雲服務。GDPR 施行後，群暉科技因應的具體作法如圖 4-3，說明如後：

資料來源：https://www.ithome.com.tw/news/123462

1. 個資盤點

個資盤點主要是蒐集使用者的個資及流向，跨部門進行，包括產品、研發、人資、財會、資訊、客服等總共 10 個部門，同時進行包括臺灣總公司和歐洲分公司的個資盤點。執行個資盤點最關鍵任務，就是明確確認當初公司取得消費者個資時的使用目的為何？並檢視公司目前個部門擁有的個資是否仍符合當初蒐集目的？一旦發現當初蒐集目的已不存在，相關個資須在安全情況下不再利用，包括刪除個資都是可行方式。另外，

個資盤點時也須確認蒐集的管道和使用用途是否合法，個資當事人是否被告知個資使用目的，其他像是資料存放的安全性、存放時間、存取管控機制及風險評估等，都是公司進行個資盤點時須考量環節。

GDPR 將線上識別碼（如 IP 位址、Cookies 等）視為個人資料的一環。而群暉科技提供的 NAS 產品，其中有一項服務是協助使用者找尋內網的 NAS 設備，客戶須允許存取 IP 位址才能使用這項服務。該公司盤點各部門擁有的個資時，就提供上述這項服務時，須因應 GDPR 規範有所調整，因此，群暉科技就會跳出新版的使用者同意個資使用條款，要求使用者允許群暉科技蒐集相關 IP 位址，以提供可搜尋內網 NAS 設備的服務。

2. 影響評估與流程優化

進行影響評估時，公司須從資料內容、敏感度、是否加密等面向分析，如何進一步做到流程優化。例如：在資料蒐集部分，須確認是否已取得當事人同意授權；資料應用上，是否符合最小權限原則，避免過度使用當事人個資；資料保存部分，須透過系統整合，做到自動化處理，以減少人為因素帶來的誤差；最後在資料追蹤上，須謹記尊重當事人被遺忘權的處置方式，不是所有個資都可被搜尋引擎永遠記住。

3. 稽核

群暉科技資安政策規定，每半年須進行稽核自評一次，除自評外，也會委由公正第三方業者進行內部相關稽核。另外，群暉科技於總部及歐盟分公司皆指定資料保護長（DPO），因

應個資保護，群暉科技原本即有資料管理委員會（Data Management Committee），配合 GDPR 施行，共納入三個組織—產品資安應變小組（Product Security Incident Response Team，PSIRT）、IT 部門及產品管理部門等，各部門均有種子成員參與該委員會，也負責因應 GDPR 相關事項。

第五章 結論與建議

綜合前述各章內容，本研究除就金融大數據未來發展及個資保護趨勢提出結論外，另針對資產管理業者業務發展上可能碰觸之個資保護提出可行建議。

第一節 研究結論

一、 大數據應用徹底改變人類生活

數位時代，資訊是繼土地、人力、資本後的新生產資源，無論政府、企業、個人都深受影響。現今因資料量急速成長、儲存設備成本下降、軟體技術進化及雲端環境成熟等客觀條件具備，使資料分析從過去洞悉歷史進化到預測未來，開創前所未見的商業模式。

僅僅 10 年，我們就見證從類比到數位的轉變，而下一個 10 年，資料力量帶來的改變將無可限量。據 IDC 估計，2025 年全球將創造和複製高達 163zettabytes 的資料量（達 1 萬億 gigabytes），是 2016 年產生資料量的 10 倍之多。從自駕車到人形機器人，從智慧個人助理到智慧家庭裝置，我們周遭的世界正經歷根本上變化，改變著我們的生活、工作和娛樂方式。

二、 大數據應用改變金融業營運模式

大數據應用下，透過不斷更新客戶的資料，能精準評估客戶的信用狀況與預測客戶行為模式，降低金融業的營運風險及成本。各家金融業因目標族群的不同，利用各自建立的大數據模型預測客戶行為，預期將發展出獨特的產品及服務。

「開放銀行」（Open Banking）是金融大數據未來發展趨勢，其重要性在於改變金融數據資料「所有權」和「使用權」的主從關係。

銀行透過 Open API 方式將客戶資料分享給第三方服務提供者，讓第三方服務提供者（Third-party Service Provider，TSP）可將銀行客戶資料加值運用，開發新的產品服務。然而，銀行對開放既有資料均存有資安疑慮，我國作法是由財金資訊公司研擬 Open API 之共同資安及技術規範，打造一個資料開放的平台促進銀行與第三方業者合作。

三、 大數據應用雖便利卻有負面影響

大數據應用下，雖帶給人們生活便利，卻也帶來蒐集資料及資料運用的負面隱憂，例如：有不肖業者為了蒐集更多資料以金錢誘使青少年販賣其網路個資、將資料濫用於操縱人心企圖影響社會輿論、運用於監控人民行為、演算偏誤造成歧視或是握有大量資料的跨國網路平台利用大數據築起高牆壟斷市場等，顯見在大數據應下猶如雙面刃，提升人們生活品質卻也可能造成人心的不安及社會的不公平。

四、 大數據應用與個資保護不可偏廢

大數據應用是追求資料開發的價值最大化，而個人資料保護的最終目的則在保障個人資料的自主控制，兩者價值各異。資訊科技不斷進步，各種資訊設備與網路連結，使每個人隨時隨地可產生、傳遞、分享並處理訊息，個人隱私問題也格外受重視。隱私是讓人們決定何時、以什麼方式、將多少個資料向他人傳達的權利，而隱私保護的相關規範是建立在個人對資料管控的需求上，例如「最小蒐集原則」及「目的限制原則」等。但這二原則在大數據時代中，資料蒐集最小化可能不再是保護隱私的一種方式，而當隱私與其他社會價值（包括公共衛生、國家安全、法律執行、環境保護以及經濟效率等）相互權衡時，就必須確保資料處理的合法性。

五、 資料安全是未來關鍵基礎

IDC（國際數據資訊，International Data Corporation）於”Data Age 2025”中針對資料如何深化對世界影響，提出五大趨勢，其中一項提到「安全是關鍵的基礎」。隨著嵌入式感測器數量增加，資料在不知不覺中被擷取，個資外洩情形增加，2018 年全球發生許多個資洩漏大事，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，而 Google 也因違反「一般個人資料保護規則」（General Data Protection Regulation，GDPR）遭 5 千萬歐元重罰，可見大數據時代，個資保護已是當前最受重視的關鍵議題。

六、 歐盟 GDPR（一般個人資料保護規則）是近期個資保護較為積極的立法例

（一）特色

1. 為統合各會員國間對個人資料保護之法規範標準，2016 年 4 月 27 日歐洲議會通過「一般個人資料保護規則」（General Data Protection Regulation；GDPR），因考量該新法規影響層面深遠，特將該法生效日期延後兩年，於 2018 年 5 月 25 日生效並於歐盟境內實施，正式取代 1995 年「個人資料保護指令」（1995 Data Protection Directive 95/46/EC）。
2. 具直接規範效力：無須透過各會員國國內立法程序轉換，該規範可直接適用於歐盟成員國。
3. 適用範圍擴大：只要對歐盟境內居民為個人資料的蒐集、處理或利用，無論是否設置據點於歐盟；亦不問提供商品或服務是否有償，皆有 GDPR 適用，故影響範圍廣泛。

4. 高罰則：違反規定者最高可處以 2 千萬歐元或其年度國際總營收 4%之罰鍰。
5. 限制個資跨境傳輸：數位經濟蓬勃發展下，跨境資料傳輸已是多數產業營運不可或缺的一部分，當具備適足性認定或有適當防護措施時，GDPR 例外允許跨境傳輸。

（二）重點

1. 擴大個資定義：配合網路及通訊科技發展，GDPR 對「足資識別特定人」資料之識別符號（identifier），增加了位置資料（location data）、線上識別碼（online identifier）等數位軌跡，至於「線上識別碼」，應指由裝置、應用程式、工具或網路協定賦予的（獨特）識別碼，例如：網路協定位置（internet protocol address）、小型文字檔案識別碼（cookies identifier）或其他識別碼（如：無限射頻識別標籤，RFID）。
2. 明確當事人同意：資料當事人的同意，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。此外，若當事人同意是以書面聲明為之，而該書面同時包含其他事項，則當事人同意的部分，須與其他事項清楚分離，並以清晰可理解、易於接近、清楚並淺白的文字呈現。
3. 新增被遺忘權、資料可攜權：本次新增的當事人權利，皆是當事人自主控制權利的具體展現。「被遺忘權」（刪除權）是在特定情況下，當事人有權要求資料管理者立即刪除其個人資料。「資料可攜權」即當事人移轉個人資料的權利。
4. 明訂隱私保護設計（Privacy by Design，PbD）概念：所謂隱私保護設計（Privacy by Design）或隱私保護預設（Privacy by

Default)，是要求企業或組織從設計系統開始就應包含隱私資料保護的應用，不再是事後追溯的補充性應用，換言之，事先將隱私保護構想嵌入 IT 系統和業務流程設計中。

5. 明訂資料保護長：GDPR 要求資料管理者及資料處理者應指定一名資料保護長。於資料處理運作中，依其形式、範圍及/或目的，要求廣泛地對當事人採取日常性且系統化監控。

（三）我國個資法與 GDPR 比較

我國「個人資料保護法」，簡稱「個資法」，共 6 章、56 條。我國「個資法」與 GDPR 皆師承經濟合作暨發展組織（OECD）個人資料保護原則，且我國「個資法」研修過程，不少條文意旨參考 GDPR 前身之 Directive 95/46/EC4 相關規定，二者無論在個資定義、當事人權利、資料管理者義務等皆有類似規定，較不同者，在跨境傳輸部分，我國個資法原則允許跨境傳輸，例外才禁止；而 GDPR 則剛好相反。另外，我國個資法中尚無「資料可攜權」及「隱私保護預設」的概念。

第二節　研究建議

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。

本研究最終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（問卷內容詳附錄二）。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) 1.進行資料盤點，並刪除蒐集目的不存在資料	13	1	0
(2) 2.設置資料保護專責單位(人員)	12	2	0
(3) 3.訂定個資外洩時通報程序	14	0	0
(4) 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

近來駭客利用資訊漏洞進行的網路攻擊事件層出不窮，金融業、證券業時有所聞，資訊安全已成組織中的重要課題。強化組織資訊安全的可行做法，包括取得相關資安認證，如 ISO27001、英國 IASME 資安認證等；另有可能從組織架構調整中獲得改善，以本研究所舉台北 101 及群暉科技的例子，在組織架構上皆有所調整：台北 101 設置資料保護長（DPO），由法務主管擔任，並由各部門代表組成個資管理小組，由個資管理小組發布個資相關訊息，讓員工瞭解個資保護的相關規範。而群暉科技於總部及歐盟分公司皆指定資料保護長，此外，該公司亦設有資料管理委員會（Data Management Committee），配合 GDPR 施行，並納入三個組織—產品資安應變小組（Product Security Incident Response Team，PSIRT）、IT 部門及產品管理部門等，各部門均有種子成員參與該委員會，也負責因應 GDPR 相關事項。

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各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

從 Google 違反 GDPR 案例中，資產管理業者亦應避免重蹈「強迫同意」的覆轍。為取得資料當事人就個資處理利用的同意，不少業者會在網頁上使用彈出式視窗，並加上聲明同意的勾選方框欄位，以作為個資當事人已為同意的證明；然而，從上開 Google 案例中可知，若是在 App 程式、網頁等使用者界面設計上，要求使用者須勾選相關同意選項後，始得進行下一個動作或流程的話，即有落入 GDPR 所禁止的「強迫同意」情形的風險。所以，資產管理業者如要在服務或產品的 App 程式或網頁上，避免在預設選項設計上違反 GDPR 相關規定，即不應將此種同意選項設計成產品或服務提供的必要條件，亦即縱使使用者未予勾選，仍應保留得令其繼續後續流程的可能性（但可跳出相關視窗，確認使用者是否不欲同意，或僅是漏未勾選）。然而，若是相關產品或服務必須取得使用者同意，始可能進行後續提供的話，即須於使用者未勾選同意或勾選不同意時，彈出說明視窗，詳為說明為何使用者不同意相關個資處理利用，即無法提供後續服務的關聯性。

「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更的進行個資盤點，才能更嚴謹有效率地掌握個資動向，確實做好個資保護。

結語

本研究針對「個資保護規範下之大數據現況運用與未來發展」，彙整國內外文獻與國際趨勢，並召開產官學座談會，深入分析重要發展面向，並提出相關研究建議，希望能協助台灣資產管理業者掌握世界個資保護規範潮流，權衡業務執行與法遵成本，在兼顧產業發展與個資保護下，尋求有效的最佳解決方案。

參考資料

1. 彭金隆、陳俞沛、孫群，「巨量資料應用在台灣個資法架構下的法律風險」，載於臺大管理論叢第 27 卷第 2S 期，2017 年 5 月
2. 葉志良，「大數據應用下個人資料定義的檢討：以我國法院判決為例」，載於資訊社會研究，2016 年 8 月
3. 法務部「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告，2016 年 12 月 30 日
4. 「台灣開放銀行政策研究報告」，國立政治大學金融科技研究中心，2019 年
5. 淺談機器人理財在台灣未來之發展，證券暨期貨月刊第三十七卷第一期
6. 從歐盟 GDPR 看全球隱私與安全保護發展趨勢，勤業眾信聯合會計師事務所，2018 年 8 月
7. 一次搞懂大數據(上) https://www.bnext.com.tw/article/35807/bn-2015-03-31-151014-36
8. 【GDPR 施行後的法遵議題】深度剖析隱私工程 https://www.ithome.com.tw/news/127226
9. 因應歐盟 GDPR 掌握隱私保護設計制度七原則， https://www.pwc.tw/zh/news/press-release/press-20180828-1.html
10. INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY
11. https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf
12. https://www.seagate.com/www-content/our-story/trends/files/data-age-2025-white-paper-traditional-chinese.pdf
13. https://eugdpr.org/the-regulation/

14. https://ec.ltn.com.tw/article/breakingnews/2702576
15. https://www.hbrtaiwan.com/article_content_AR0007025.html
16. http://www.eland.com.tw/20181108.html
17. http://www.eland.com.tw/20190220.html
18. https://www.largitdata.com/blog_detail/20190521
19. https://friap.moeasmea.gov.tw/kn_article.php?nid=111&gid=2
20. https://www.ettoday.net/news/20181130/1319360.htm
21. https://www.mjib.gov.tw/EditPage/?PageID=de653765-bcbb-4ba6-b600-795e1ec2acf7
22. https://kknews.cc/zh-tw/tech/yareb2k.html
23. https://www.roboadvisorpros.com
24. https://www.roboadvisorpros.com/fintech-news-robo-advisor-news/
25. https://adsales.rakuten.co.jp/business/special/2018_10_kitagawa_mizogami.html
26. https://www.ithome.com.tw/news/130383
27. https://gigaom.com/2013/07/31/peter-thiel-leads-20m-round-for-zestfinance/
28. https://www.zestfinance.com/blog/how-machine-learning-helps-underwriters-grow-without-risk
29. https://assets.kpmg/content/dam/kpmg/tw/pdf/2017/02/fintech-100-zh.pdf
30. https://www.blackrock.com/ae/intermediaries/themes/investing-in-asian-equities/big-data-asian-investments
31. https://www.ey.com/en_gl/banking-capital-markets/how-banks-can-balance-gdpr-and-psd2
32. https://en.wikipedia.org/wiki/IASME

附錄一

財團法人中華民國證券暨期貨市場發展基金會召開

「個資保護規範下之大數據現況運用與未來發展」

期末諮詢會議紀錄

紀錄：陳恩儀、汪宛臻

時間：108 年 10 月 30 日（星期三）上午 9 時 30 分

地點：台北市南海路 3 號 9 樓會議室

主席：政治大學金融科技研究中心王教授儷玲

出席：

金融監督管理委員會證券期貨局古組長坤榮、

政治大學風管學系彭教授金隆、

永豐投信林董事長弘立、簡副總經理妤倫

野村投信王總經理伯莉

勤業眾信會計師事務所曾副總經理韵

列席：本基金會研究處

葉處長淑玲、陳副處長莉貞、陳研究員恩儀、汪中級專員宛臻

壹、 主席致詞：(略)

貳、 研究報告簡報：(略)

參、 與會人員發言摘錄

王教授儷玲

希望這研究的貢獻可以回饋到金融市場及資產管理業者，大家可以暢所欲言。

林董事長弘立

一、 投信投顧以資本額或員工人數而言，算是小型金融機構，不論是符合 ISO27001、設立獨立的 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，對於投信投顧業者都是龐大的法遵壓力。

二、 以經濟效益方面分析，由於法律遵循通常會更改整個作業流程，大幅墊高成本，例如：FATCA 條款，投信投顧業者如果沒有金控母公司的協助導入作業流程，投信投顧業者是難以獨自負擔該成本。

三、 以業務方面分析，目前業務分為兩大項目，會計及股務，會計帳就是投資評價，股務則是客戶申贖資料，客戶可以直接透過投信顧業者直接申贖，或是透過券商及銀行等代理業者申贖，若是透過代理業者申贖，則客戶個資的蒐集、處理及運用等相關個資保護責任則是在銀行端或是券商端。

四、 綜觀以上幾點，投信投顧業者會為了減輕法遵壓力，可能會有兩個反應，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之業務量，僅專心做資產管理這部分。

王教授儷玲

一、 關於個資保護之規範或修法趨勢並不是一致性的標準架構，而是分級架構。以投信顧業者來說，若提供投資策略的服務或是銷售商品的策略是透過銀行及券商銷售，並未直接碰到客戶個人資料，或是碰到的客戶資料也透過金控加以整合的話，所要遵守的個資保護規範就不需要像銀行這麼嚴謹。

二、 個資保護的議題可從兩個面向來看，(一)在個資保護下的資安問題，(二)對於參與者的個資議題，例如：個資處理是否包含間接資料？個資儲存是否存放於雲端等？

三、 參考世界其他國家之發展趨勢，目前已發展出多個資料中心(Data Center)，由資料中心處理資料後供業者使用，能提供業者蒐集、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。另外，也發展出一種標準化的平台，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。

四、 就個資保護規範來說，是提供一個明確的規範來讓大家遵循，以分級管理的角度，可以協助資料釋放其價值，也協助業者在資安程序的標準化時更符合個資保護的規範。

彭教授金隆

一、 剛剛在聽報告時一直有一個疑問，這篇報告為什麼是提供給資產管理業者做參考，後來才知道這是資產管理人才培育與產業發展基金委託辦理的研究，建議在研究報告中的研究目的可以稍微提到。

二、 個資法依遵循程度可以分為三種：

(一) 形式上的遵守：金融機構避免受罰為目的，例如個資法第 8 條，必須在蒐集時完成下列的說明，因此在金融機構常常簽一些我們不太懂的東西，客戶並不了解實質內容及其權利。

(二) 實質上的遵守：金融機構避免被告為目的，例如沒有經過同意即使用客戶資料、沒有將客戶資料刪除等致對方受到損害，對金融業而言因為作業程序是標準化且重複的，因此只要爆

發一件觸法事件，代表的是一大串的事件違法，而且罰責是一案一罰，對於金融業而言這也是相當可觀的。

(三) 積極的遵守：以合法且合理的角度出發，創造出價值，要做到這個程度，前面兩種也必須滿足，因此建議可以務實地提醒投信投顧業者是不是有什麼沒有做到，或是什麼該加強的。

三、 報告的結論與建議有點像是提醒，建議結論與建議應該要大膽、再具體化且可以有進一步作為的建議，例如：

(一) 在我國個資法架構下推動可攜權之修法，若從投信投顧之角度該如何推動可攜權。

(二) 個資法第 21 條規定，首次行銷時應以免費的方式告知客戶如何停止使用個資，以及個資法第 54 條規定，過去間接得到的資料，下次再使用時，需通知客戶得到資料的來源等，這兩條在實務上是難以遵守的，市場上也難以看到大家對這些條文有所反應，或許也可以納入建議。

(三) 「同意」絕對是未來個資保護的重點，現在已經有很多人發現常在不自覺的情況就「同意」對方使用個資，而在未來若客戶主張其權益受損時，該怎麼證明客戶曾經同意的軌跡，或許也可以請教同業在實務上怎麼解決且在報告中提出建議。

(四) 個資法屬於普通法，只要其他法律另有規定，個資法需要讓步且遵守其他法律之限制，因此只要主管機關願意發布相關函令，個資法某些較為模糊的問題就可以解決。而該議題也牽涉到個資保護的主管機關不明，我們只知道目的事業的主管機關，以金融業來說是金管會，而國發會是推動 GDPR 取

得適合度的主政單位，惟對於法律的解釋是透過法務部解釋，再加上，普遍認為目的事業主管機關才了解該行業，因此對於金融業來說，面對個資疑義時，金管會認為其只是目的事業主管機關，無權解釋個資保護法，國發會認為目的事業主管機關比較了解應該金管會解釋，而法務部認為主政機關是國發會其無權解釋，因此，現在個資的解釋都需要等到法院的判例，而法院判例少之又少。建議報告中也可以提到關於主管機關的問題，其實若是金管會願意負擔解釋的責任，對於金融業在遵守法律促進保護客戶資料方面會有一大進展。

王教授儷玲

政大目前已成立一個有關 Open Banking 資安與個資保護的研究團隊，之前也辦過法規座談會，彭老師這些建議是彙整了我們的座談會及研究後整個團隊的一些明確的想法。其實個資保護議題涵蓋範圍滿大的，雖然這次的報告只專注在資產管理業者，但是從高齡化社會需求，以及 OPEN BANKING 會從支付走到投資再走到保險，資產管理業者應該都是市場上重要的角色，在這個角色下，如何讓個資保護及大數據的價值增加，是一個重要的議題。而我個人認為個資保護議題也會是這三年金融市場的重要議題，政大將協助教育宣導以及政策落實。其中再強調一些重點，且回應彭教授所講的：

(一) 主管機關的明確授權部分，其實有一些前例可循，像是現在在推動的 OPEN API，雖然目前僅是提供銀行業一些標準化的規範和架構，但是未來也是可以應用到保險業以及資產管理業，證期局以及保險局也可以瞭解，哪些東西可以替業者爭取，以及如何管理業者，提供業者一些標準規範，對於主

管機關而言，也可以透過標準化的規範及架構調整其監理的程度。

(二) 在「同意」方式部分，舉例來說，在醫療的部分，以前病人的病歷資料是屬於醫院的，現在可以透過健保卡及健康存摺跨醫院傳輸病人的用藥以及診斷資訊，病人可以透過 APP 設定授權資料給哪一家醫院以及授權的時間長短，還有授權的資料包含哪些資料，這些軌跡、資料的保存及應用，甚至是稽核的部分，其實健保已經有實行先例。今天討論的僅是法律規範，之後還有實行的部分，要如何實行、遵守法律時成本會不會過高等問題，金融業其實可以透過科技來解決的，就如同剛剛所提到，未來台灣有可能走的是資料處理中心，透過去識別化的模式，用共享方式大幅降低業者資料處理的成本，使一些有成本考量的業者可以減輕負擔，甚至，也可以用區塊鏈的模式，自動化且不會被竄改內容的方式來做一個共享平台，相信共享平台的建立，對業者而言法律遵循及稽核成本可以下降，對消費者而言可以清楚知道其授權形式、時間及內容等，平台的建立相信在未來三年到五年可以蓬勃發展，促進金融業生態圈的建立。

彭教授金隆

建議本報告如果可以有一小段，針對資產管理業者個資使用的痛點，如此才能針對未來個資的解決方案提出具體建議。例如了解資產管理業者認為個資法哪些條文是窒礙難行？又或是適用 GDPR 有哪些做不到？找出問題後，再來思考有哪些解決方案，如此研究會更聚焦。

王教授儷玲

是否可用簡單問卷嘗試了解業者使用大數據及遵循個資法方面有何痛點？至少可以彙整業者的一些看法。未來就有機會針對這些痛點，聚焦討論出可行的解決方案。

林董事長弘立

一、 我估計若用問卷詢問投信業者，可能會有一半答不出來。癥結在於業者對個資法內容有多了解。

二、 剛提到病歷，引發我想起投資的全貌在金融業，一個投資人可能在銀行、保險、證券、投信都有投資部位。

王教授儷玲

這就是整合帳戶的概念，Open Banking 第二階段會處理，第二階段會開放 account information，當然首先要取得資料所有人的同意，TSP 業者就可以處理，整合後就可以看到同一客戶在不同金融機構所有帳戶資料，是可以從 Open Banking 進展到 Open Finance。

林董事長弘立

大家都在構思如何提供消費者最好及最適的 solution，但目前只能看到自己帳戶內的資料，無法掌握同一客戶在不同金融機構的投資。

王儷玲教授

Open Banking 就是要解決這個問題，未來分析完後也需要下單、支付，到第三階段後才能全部完成。明年會是 Open Banking

第二、三階段較大進展的一年，其中也有許多資安與個資問題，如果未來二、三階段完成後，後續對資產管理業者的影響也會很大。

王總經理伯莉

一、 或許業者對於個資、GDPR 規範都不是太清楚，我個人經歷是從銀行、保險到投信，感覺證券投信業者在個資、AML 等方面，是走在銀行、保險之後。投信業者擁有的個資相較於其他金融機構的確較少，也比較單純，因為投信核心業務是資產投資與管理，有個資的部分，主要是直銷或網路下單的公司，項目僅限於聯絡資料、資產規模、風險胃納等個資，不需要知道太多客戶的個人資料。因此，在個資法、AML 等規範下，投信要遵循和銀行、保險相同標準會耗費過多成本且壓力大，尤其投信資本相對小，人員編制也少，因此，如果同時要符合這麼多法規上的要求時，確實需要一些協助與體諒，如果今天同業間有一個平台，可以幫忙大家做一些 study，整理出一些簡單作法，讓業者了解可以如何馬上適用，也不需大量的系統建置，相信對業者幫助會很大。

二、 我們有直銷也有通路業務，兩者的客戶還是不太一樣，某些直銷客戶是蠻喜歡和投信往來的，投信在乎的是 AUM，我們和客戶往來長期就是在乎他的 AUM，不希望客戶經常進出，著重資產配置與長期增長。但通路客戶就有些不同，客戶、通路和資產管理業者的 KPI 是不同的，甚至會有衝突。如果因適法要求（KYC、AML、GDPR 等）要增加許多成本，甚至犧牲直銷客戶，從大環境來看，這是非常可

惜的。照理說，應給客戶不同選擇。法規立意甚佳，但若執行時造成業者業務拓展的窒礙，或業者因高門檻而犧牲掉部分業務，都是必須要衡量的。

三、 GDPR 對消費者保護確實周延，以 Privacy by Design 概念來說，要求業者在系統設計之初就要導入隱私保護概念，對已有的系統該如何調整以因應這個概念，工程都會相當浩大，若真要導入這種概念，建議應給予業者緩衝期，因系統的更新或調整是耗費時間人力，甚至要排擠掉既定工作。

四、 GDPR 給予消費者遺忘權，金融業牽涉許多往來資料，是否可任由消費者主張要刪除就可刪除？其中考量點可能還蠻多的，有時我們會發現有些糾紛是在數年之後，接獲法院通知，因訴訟紛爭要調多年前的往來資料，如果按照 GDPR 到底要保留還是不保留這些資料？另外我們也的確會碰到一些利用消保法、個資法規範，在金融機構間興訟的消費者，如果毫無限制地允許消費者要求刪除相關資料，有時會削弱金融機構保護自己的立場。

五、 理財機器人部分，管理標的的確不多，我們是希望理財機器人的標的愈多愈好，但有法規上限制，目前只允許業者自行發行的基金、總代理基金，否則必須和其他總代理業者簽訂銷售契約，成為銷售機構後才能將其他總代理業者的基金納入標的，門檻是有限制。如果能放寬將台灣註冊過的基金或 ETF，經投信業者自行研究認為可納入該公司理財機器人的投資標的中，則其投資理財的效果一定會更好。

王教授儷玲

緩衝期與遺忘權也是未來法規修改上的重點。回到個資法，可攜權和遺忘權究竟要規定在個資法，抑或透過主管機關相關規範處理，是兩種不同層次，一是進立法院修法，這應該是賦予資料可攜權及遺忘權的基本架構，另一是被賦權後，回到金融市場運作，金管會需要對因應大數據使用及個資處理規範。遺忘權對紛爭處理上，到底如何做法是對業者公平的？Open Banking 討論時也有相關問題，所有 TSP 業者(科技公司)是可以協助金融機構資料處理，只是這些資料要不要儲存？TSP 業者(銀行委外單位）的資安如何？如果產生爭議時，這些消費爭議是否還是由金融評議中心處理？因為評議中心只處理金管會管轄的機構，Open Banking 下爭議處理包不包括 TSP 業者？爭議處理也會回到消費者資料是否可毫無限制地要求刪除？從監理機關角度來看會要求投信業一定要保留資料，該資料就不能因個人意願去除。回到剛才彭老師提到的,個資法下的基本授權,無論可攜權或遺忘權，賦權後未來在資產管理業者的處理上，金管會還是必須要有相關規範，如果這些相關規範很嚴謹的話，因為是主管機關要求的，就可以不違反個資法，也就不會是消費者說要執行遺忘權就可以執行的。

彭教授金隆

被遺忘權在第 11 條規範很嚴謹，因法律或業務所必須者，可不刪除。業務所必須是很有彈性的，而法律則是主管機關監理上要求，如主管機關要求契約結束後幾年內須保存該紀錄等，則可

不必遵循被遺忘權。法務部也做出解釋，只要政令目的依然存在，則可不必刪除。

王教授儷玲

因此被遺忘權並不會凌駕監理目的之上。或許未來我們要做的不只是消費者(投資人)的教育宣導，還包括對金融機構與第三方服務公司(TSP)的教育，未來可以朝向和顧問諮詢公司、資安保護認證公司合作，對金融機構及 TSP 做一些教育訓練。

林董事長弘立

我補充一下王總經理提到的爭議紛爭事件，許多並非來自金融界問題，往往是兄弟爭產或個人欠稅，因此保存相關資料，後續並非因交易問題，而是客戶私人因素配合法院必須調閱相關資料。

曾副總經理韵

一、 建議研究動機部分，強化表達本研究是針對資產管理業者做出相關建議。

二、 以 Open Banking(Open Finance)發展來看，勢必會對我國個資法產生需要調適的狀況，或許從本研究整理出的諸多趨勢中，加入相關業者在適用個資法（甚或 GDPR）的痛點，可作為未來修改個資法時的重要參考。

三、 針對資產管理業者較為特殊的部分可以建議：

（一）個資法施行至今，對資產管理業者有無困難點？

（二） Fintech 浪潮下，會產生許多 new business model，導致資產管理業者有所改變，例如 Privacy by Design，倘若業者已

符合個資法，當未來如有新業務，建議可將 Privacy by Design 及去識別化概念加入。

古組長坤榮

一、 投信業者 39 家，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極大，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，並考量其可行性與必要性。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規定。

二、 除問卷外，也可直接訪談業者，了解困難點並提出解決方案。

王教授儷玲

會議結論

一、 報告建議部分，會重新整理。業者意見部分，採雙軌進行：（一）問卷方式：大數據使用與個資規範所遇到的困難點？回收後加以分析彙整；（二）訪談方式：透過訪談具代表性業者，可較深入了解業者的痛點。

二、 分級管理是大家共識，依照規模、營運模式、對資料處理需求有不同設計。

散會（上午 11 時 40 分）

附錄二

敬啟者：

本基金會受「資產管理人才培育與產業發展基金」委託進行「個資保護規範下之大數據現況運用與未來發展」研究。

為瞭解 貴公司保護客戶資料的相關作法;及業務執行/推展上是否因個人資料保護法相關規限制，而有窒礙難行之處。煩請 貴公司指派專人協助依 貴公司實際狀況，勾選適當答案。本問卷結果僅供研究分析，不就個別意見對外發表。懇請 台端詳實填答，以確保研究之品質，非常感謝您的參與及合作。

填妥後煩請回傳證基會研究處

聯絡人：陳恩儀(02)23574358 Email:angel@sfi.org.tw

敬祝

身體健康 萬事如意

證券暨期貨市場發展基金會敬上

1. 請問貴公司執行業務時，針對涉及蒐集、處理及利用個人資料時，在個人資料保護上，是否有進行以下程序？

(1)☐本公司目前尚未蒐集或處理個人資料

(2) 進行個人資料盤點，並刪除蒐集目的已不存在的資料？

☐有 ☐無 ☐不清楚

(3) 設置個人資料保護專責單位（或人員）？

☐有 ☐無 ☐不清楚

(4) 訂定個資外洩時之通報處理程序？

☐有 ☐無 ☐不清楚

(5) 是否定期或不定期舉辦「個資保護」員工教育訓練？

☐有　　☐無　　☐不清楚

2. 有關個人資料蒐集處理及利用，涉及「當事人同意」事項時，請問 貴公司取得當事人同意有何窒礙難行之處（如：網路金融服務比率提升）？

☐有（請說明困難之處及可能的建議解決方式）

_____

☐無

☐不清楚

3. 個人資料保護法相關規範是否對 貴公司業務推展上或實務執行產生困擾？

（請說明原因並舉例說明哪些不方便的情境及希望開放之條文）

_____