計畫編號: NCC-Y109-006

109 年委託研究報告

109 年度通訊傳播事業導入隱私保護管理機制與資料加值服務之研析委託研究

期末報告

（匿名版－上冊）

計畫委託機關：國家通訊傳播委員會

中華民國 109 年 12 月

計畫編號: NCC-Y109-006

109 年委託研究報告

PG10904-0134

109 年度通訊傳播事業導入隱私保護管理機制與資料加值服務之研析委託研究

期末報告

受委託單位

財團法人資訊工業策進會

計畫主持人

顧振豪

共同主持人　協同主持人

葉奇鑫　　陳志宇

研究人員

宋佩珊、李沛宸、孫鈺婷、張腕純、劉純妤、

范晏儒、劉芷宜、許嘉芳、周芷瑄

本報告不必然代表國家通訊傳播委員會意見

中華民國 109 年 12 月

目次

表次

圖次

提要

國家通訊傳播委員會（下稱通傳會）身為 APEC CBPR 體系中我國會員經濟體之隱私執法機關（Privacy Enforcement Authority, PEA）之一，因應通傳業者實務需求之必要，透過相關資源輔導其通過 CBPRs 認證，俾提升商譽、增進民眾與消費者之信賴，並助益其推展跨國業務，順利與當地隱私法規或個資保護法遵要求接軌。

通傳會依據我國個資法第 27 條第 3 項規定之授權，訂定「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」，並於 2016 年 11 月 9 日發布，俾督促其所監理之通訊傳播事業保護消費者個人資料及隱私，並積極提升企業組織內部個資法遵度與管理能量，降低罹於刑典或其他法律上責任之風險。

本計畫透過議題研析，輔以規劃針對通傳事業遵循個人資料保護與安全維護執行情形進行調查，以通盤瞭解通傳產業在個人資料、隱私保護與風險控管機制等相關配套，是否符合法規之要求，進而研議資料加值運用之可能性、適法性及適足性之要求與措施。

關鍵詞：個人資料保護法、通訊傳播事業、個人資料保護與管理制度、資料加值服務、國際傳輸

Abstract

As one of the Privacy Enforcement Authorities (PEA) of Taiwan in the APEC Cross Border Protection Rules system (hereinafter CBPRs), The National Communications Commission (hereinafter, NCC) has respond to the practical necessity of communication industry, such as increasing the trust of the public and consumers, supporting them to promote communications businesses, and privacy regulations compliance requirements by making them qualified for the CBPRs certification.

Personal Data Files on November 9th, 2016, in accordance to Paragraph 3, Article 27 of the Personal Data Protection Act, in order to facilitate communications businesses under its supervision to protect consumers' personal data, and actively improves the compliance and management capability of the company's internal laws and regulations to reduce the risk of penalties or other legal liabilities.

Through the analysis of issues, this project is supplemented by a plan to investigate the implementation of personal data protection and security maintenance in the communication businesses, so as to comprehensively understand whether the communication industry are compatible with personal data, privacy protection and risk control mechanisms. The requirements of laws and regulations, and then discuss the requirements and measures of the possibility, legality and adequacy of the value-added use of data.

Keywords: Personal Information Protection Act; communication industry; Personal information protection and administration system; Value-added service; cross-border transfer

第一章 整體說明

第一節 本案緣起

全球經濟環境已隨著科技技術的提升與嶄新的科技應用趨勢，逐漸遠離傳統的經濟型態，並邁入新興數位時代。而在迅速變化的數位時代中，使運用數位科技之產業型態漸漸產生變化，從而帶動全球數位經濟的整體發展。而數位經濟仰賴「資料」驅動，對於資料運用的形式、目的、風險與監管等都與產業發展及應用息息相關，對於通訊傳播產業而言亦復如是。

因此，當資料自由流通已成為國際自由貿易與經濟運作上十分重要的核心時，除有利於跨國業務推動與經濟貿易互動外，其背後深受憂心與矚目之處，則在於如何確實的維護並落實個人資料及隱私安全性。從而，在資料的風險控管機制與相關配套措施上，又應如何調適，使之同時適於產業運用上，並符合法規之要求，已成為全球必須積極面對處理的議題。如歐盟「一般資料保護規則」(General Data Protection Rule, GDPR)於 2018 年 5 月正式施行以來，已多次針對施行狀況進行回顧與檢視。況且已有許多國家針對個人資料保護法制展開翻新工作。以亞太地區為例，至少有日本、韓國、新加坡、印度、澳洲、泰國、馬來西亞、斯里蘭卡等國近年來都宣布（或已經完成）將對國內的隱私相關法令的修正 。

對於我國而言，在忖量符合產業需求之際，個人資料與國際法規要求之平衡與取捨，以及如何加速產業對於個人資料保護與資料加值的適法利用，以促進數位經濟發展，為各界急需處理的問題。我國政府為此除積極與歐盟洽談 GDPR 適足性認定外，另已於 2018 年 12 月躋身亞洲太平洋經濟合作會議下之跨境隱私保護規則體系(Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, CBPRs, APEC CBPRs)之一員，該體系係近年來由美國所大力倡議，呼籲亞洲太平洋經濟合作會議(Asia-Pacific Economic Cooperation, APEC)會員經濟體共同參與。APEC CBPRs 係在尋求企業和社會各界

意見後所制訂的一套體系，以期有效保護個人資料安全，建立消費者、企業和監督管理者對個人資料跨境流動之信任，並促進區域內經濟發展。而 APEC CBPRs 要求參與企業訂定和實施符合 APEC 隱私保護綱領的資料隱私政策。

通傳會身為 APEC CBPR 體系中我國會員經濟體之隱私執法機關(Privacy Enforcement Authority, PEA)之一，實有呼應通傳業者實務需求之必要，善盡監理作為或透過相關資源輔導其通過 CBPRs 認證，俾提升商譽、增進民眾與消費者之信賴，並助益其推展跨國業務，順利與當地隱私法規或個資保護法遵要求接軌。

通傳會既依據我國個資法第 27 條第 3 項規定之授權，訂定「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」，並於 2016 年 11 月 9 日發布，俾督促其所監理之通訊傳播事業保護消費者個人資料及隱私，並積極提升企業組織內部個資法遵度與管理能量，降低罹於刑典或其他法律上責任之風險。

冀望未來能夠透過相關議題之持續研析，輔以規劃針對通傳事業遵循個人資料保護與安全維護執行情形進行調查，以通盤瞭解通傳產業在個人資料、隱私保護與風險控管機制等相關配套，是否符合法規之要求，進而研議資料加值運用之可能性、適法性及適足性之要求與措施。

第二節 需求工作項目

通傳會委託本團隊執行「109 年度通訊傳播事業導入隱私保護管理機制與資料加值服務之研析委託研究採購案（以下簡稱本案）」，依需求書所載，本案共計 8 項工作項目，分別為：

一、辦理通傳會及通傳產業之個資法遵教育訓練及實務專題講座 8 場次

(一)個資法遵教育訓練規劃，北部地區 2 場次及中、南部地區各 1 場次，合計 4 場次，每場次以可容納 100 人以上規模辦理，授課總時數 24 小時以上（並擇一場次錄影存檔送交通傳會使用），相關訓練教材資料電子檔提交通傳會置放於通傳會官網供通傳事業參考使用。

(二)實務專題講座北部地區 3 場次（其中 1 場次，規劃符合頻道、電臺及傳播內容產業之實務案例）及南部地區 1 場次，合計 4 場次，每場次以可容納 50 人以上規模辦理，授課總時數 16 小時以上（擇 2 場次錄影存檔送交通傳會使用），相關訓練教材資料電子檔提交通傳會置放於通傳會官網供通傳事業參考使用。

(三)前揭教育訓練及實務專題講座內容包括個人資料保護法規、個資保護及實務管理機制、案例說明、跨境隱私保護管理機制議題、法律效果及責任等，本計畫將以具備資通訊、傳播、法律及個人資料管理制度稽核實務經驗等專長之專家或學者擔任講師。

二、成立通訊傳播產業個資保護及資料創新運用法制諮詢服務，提供通傳會及通傳事業相關法律意見諮詢，並對其諮詢案例或通傳事業涉及案例等，製作至少 20 則以上適法說明模擬題庫（含電子檔）資料提交通傳會官網問答模擬題庫供通傳事業參考；另彙整通傳會 107 年起至本案同委託案之成果資料、諮詢案例及問答模擬題庫，編寫與設計

「通傳會處理通傳事業個資案例參考手冊」之電子檔，提供通傳會同仁實務執行之參考。

三、依據我國個資法相關規範及參考彙整通傳會 107 年及 108 年同案委託之成果資料（於契約生效後，通傳會提供電子檔給予得標廠商參考），編寫與設計「通傳產業個人資料保護與管理實作指引手冊」1 式（將包含自我評核表、參考指引、程序文件（範例）、參考資料等），彩色印刷 500 本（含電子檔），並於本案執行之實務講座或研討會發放。

四、辦理 15 家通傳事業輔導訪查（談）作業（依據通傳會後續提供輔導業者名單，並與輔導業者召開實施作業方式討論會議後辦理，並將規劃 8 小時以上之作業人力時間）

(一) 依通傳會 107 年及 108 年同案委託之輔導訪查（談）業者之評估結果報告（於契約生效後，依據通傳會提供電子檔），遴選原輔導 10 家通訊傳播事業檢視原評估結果之改善情形，以及協助重新檢視實務上之落實及運作情形。

(二) 新遴選 5 家通傳事業，其實施作業方式，參考前揭同案輔導評估方式，並與輔導業者討論後辦理。

(三) 彙整前揭訪查（談）結果，製成通傳事業個資法遵因應評估報告。

五、舉辦有關通傳事業個資管理機制或資料加值運用相關之研討會 1 場次（北部地區），規劃時數 6 小時以上，場地以可容納 110 人以上規模辦理，並敬邀具備資通訊、傳播、法律及個人資料管理制度稽核實務經驗等專長之專家、學者或產業代表參與，另研討會名稱、舉辦期間及議題內容另規劃提交通傳會確認（包含現場網際網路直播功能及作業）。

六、蒐集與研析 109 年度 2 則以上國際知名組織之個資保護管理機制及資料加值創新應用等議題發展趨勢活動報告【如 IAPP(International Association of Privacy Professionals) 或

Gartner 等級組織】。

七、付費取得或參考使用主要國際研究或顧問機構之經濟發展、產業趨勢、資料運用與個資保護議題報告或資料庫，並自契約生效次月起，每月提供 2 則以上國際資料經濟與個資保護趨勢動態資訊，以及每月提供研究調查摘譯與分析重點資訊 1 篇，檢送通傳會確認後，置放通傳會官網所連結之「國際通傳產業動態觀測」專屬網站，至履約結束日。

八、參考 107 年及 108 年之同案委託成果資料與本案實施情形，評估 3 項通傳產業對資料運用有興趣之服務需求（涉及跨產業之目的事業主管機關權責情形，後續與通傳會討論確認研析項目），進而探討提供商業運用或加值服務過程中，所面臨之障礙與法規適用之疑慮，研擬並提出解決面臨議題之意見討論與諮詢交流平臺機制（參考研析相關國家或專業組織針對該項服務之案例、運作模式及適法性等）及解決方案之建議。

期中報告內容依前揭委託辦理工作項目，已完成以下 5 項部分工作項目：

一、工作項目一（一）：完成通傳會及通傳產業之個資法遵教育訓練 4 場之執行成果紀錄，相關訓練教材資料電子檔已提交通傳會置放於通傳會官網供通傳事業參考使用。

二、工作項目二：成立通傳產業個資保護與資料創新運用法制諮詢服務團隊，並製作適法說明題庫 15 則（含電子檔）資料提交通傳會官網問答模擬題庫供通傳事業參考。

三、工作項目三：完成「通傳產業個人資料保護與管理實作指引手冊」初稿 1 式（定稿後將彩色印刷 500 本（含電子檔），並於本案執行之實務講座或研討會發放）。

四、工作項目四：完成遴選原輔導 7 家次以上通訊傳播事業，檢視原評估結果之改善情形，重新檢視實務落實及運作情形之輔導訪查（談） 結果之評估結果報告。

五、工作項目七：提供 4 月份至 8 月份每月 2 則國際資料經濟與個資保護趨勢動態資訊（共 16 則），以及 1 篇研究調查摘譯與分析重點資訊（5 篇）。

期末報告完成工作項目包含：

一、工作項目一（二）：完成實務專題講座北部地區 3 場次及南部地區 1 場次，共 4 場次（已提交 2 場次錄影存檔送交通傳會使用），相關訓練教材資料電子檔提交通傳會，並置放於通傳會官網供通傳事業參考使用。

二、工作項目二：成立通傳產業個資保護與資料創新運用法制諮詢服務團隊（提供 4 則諮詢），並製作適法說明題庫 24 則（含電子檔）資料，提交通傳會官網問答模擬題庫供通傳事業參考；編寫完成「通傳會處理通傳事業個資案例參考手冊」（電子檔詳參附錄 1）。

三、工作項目三：完成「通傳產業個人資料保護與管理實作指引手冊」定稿，彩色印刷 500 本（電子檔詳參附錄 2），並已於 11 月 10 日本案執行之研討會發放（領取名單詳參附錄 3）。

四、工作項目四：完成輔導 15 家次通訊傳播事業，檢視原評估結果之改善情形，重新檢視實務落實及運作情形之輔導訪查（談）結果之評估結果報告。

五、工作項目五：11 月 10 日舉辦完成「通傳資料應用與法制整備研討會」1 場次。

六、工作項目六：因疫情影響，原規劃國外出差 2 趟 2 人次，經計畫變更為線上參與 3 場 4 人次，完成蒐集與研析 3 份發展趨勢活動報告。

七、工作項目七：提供 9 月份至 11 月份每月 2 則國際資料經濟與個資保護趨勢動態資訊（共 6 則），以及每月 1 篇研究調查摘譯與分析重點資訊（共 3 篇）。

八、工作項目八：評估通傳產業對資料運用有興趣之服務需求，探討提供商業運用或加值服務過程中所面臨之障礙與法規

適用之疑慮，研擬提出解決面臨議題之意見討論與諮詢交流平臺機制及解決方案之建議。

第三節 研究方法

本計畫之實施將依循計畫執行團隊長期所建立的研究方法論進行本專案之相關研究（參見圖 1 計畫研究方法論）。此一研究方法論主要立基於比較法之研究，其實施步驟主要為：確認施政需求（即研究議題）、國際相關政策、法規與措施研析、我國政策與法制現況檢視，以及研提相關之政策、推動措施或法規調適建議。

資料來源：本計畫整理

圖 1 計畫研究方法論

一、確認施政需求

計畫執行團隊於委託研究計畫履約期間將與通傳會密切聯繫合作。於專案執行期間，將隨時配合通傳會就研究主題範圍內之諮詢，依據通傳會之需要，提出相關個案資料蒐

集及研析建議，作為研究工作項目之一部分。另將評估本案工作項目是否需要進行性別統計分析，並將評估結果列入研究報告及說明理由。

二、國際相關政策、法規與措施研析

透過文獻蒐集等方式，檢視追蹤國際產業、政策或法規之趨勢，觀測主題主要如下：

(一)蒐集國際通訊傳播產業資料經濟應用案例，以公私或業者間相互交換資料或是對外開放資料為主，透過案例解析勾畫出整體資料應用的架構。

(二)蒐集國際開放資料法制與政策，分析對於通訊傳播產業資料應用所造成的影響。

(三)就蒐集、案例及法制等資料開始分析、歸納及整理出通訊傳播產業或資料保護之主管機關所採取的相關政策或措施及未來趨勢。

三、我國產業、政策或法規之現況檢視

蒐集我國現行法規及現行做法，提出與國外作法之異同比較分析，預期處理的議題如下：

(一)我國通訊傳播產業於資料加值、資料保護與創新應用服務之資料類型與價值需求。

(二)我國通訊傳播產業於資料加值、資料保護與創新應用在法令限制及挑戰。例如：個人資料、隱私、資訊安全及智慧財產權等議題。

(三)我國主管機關對於推動資料加值、資料保護與創新應用服務可行的措施。

四、研提相關之政策、推動措施或法規調適建議

本於前揭之研究基礎，提出我國如何推動通訊傳播產業資料加值與創新應用之建議，並就本研究重點以主管機關，亦即是通傳會的觀點提出相關具體調適建議，以作為未來政策之參考。

採取前揭之研究方法，有以下之正面效益，首先是可以

掌握委託單位之需求，能為研究方向進行設定與適時調整。其次是可以透過比較法，標竿國際經驗，作為我國推動措施研擬之參考。

最後是透過文獻資料之蒐集，可以掌握國內產業所面臨之問題或政策措施之缺口，同時也可以就所研擬推動之措施廣納意見並凝聚共識，強化相關措施建議之有效性。

第二章 通傳產業之個資法遵教育訓練

第一節 執行成果

一、課程需求

通訊傳播事業個資法遵教育訓練規劃，北部地區 2 場次及中、南部地區各 1 場次，合計 4 場次，每場次以可容納 100 人以上規模辦理，授課總時數 24 小時以上，並提交相關訓練教材資料電子檔。

二、課程目的

協助通訊傳播主管機關輔導我國通訊傳播事業深入瞭解消費者個人資料蒐集、處理及利用之合法性，使業者意識違法蒐集、處理及利用個資之法律效果與責任，以期加強事業個資保護能力，建置健全個資保護與管理制度，降低個資外洩發生之風險；另外本教育訓練將加強分享相關實務案例及查檢經驗，以完善各事業對個人資料保護法遵之作為，提升事業服務之可信賴度，建立健全之服務環境。

三、課程主題

(一) 個資蒐集處理利用合法性判斷技巧；
(二) 違法蒐集處理利用個資的法律效果與責任；
(三) 國內外個資法精選案例解析。

四、課程日期

(一) 109 年 7 月 22 日台北第 1 場
(二) 109 年 7 月 29 日台北第 2 場
(三) 109 年 8 月 12 日台中場
(四) 109 年 8 月 26 日高雄場

五、課程產出

總計產出 2 份教材、台北場課程影像檔，並提供提供公務人員終身學習時數 6 小時或中小企業終身學習護照認可時數 6 小時。

第二節 課程內容

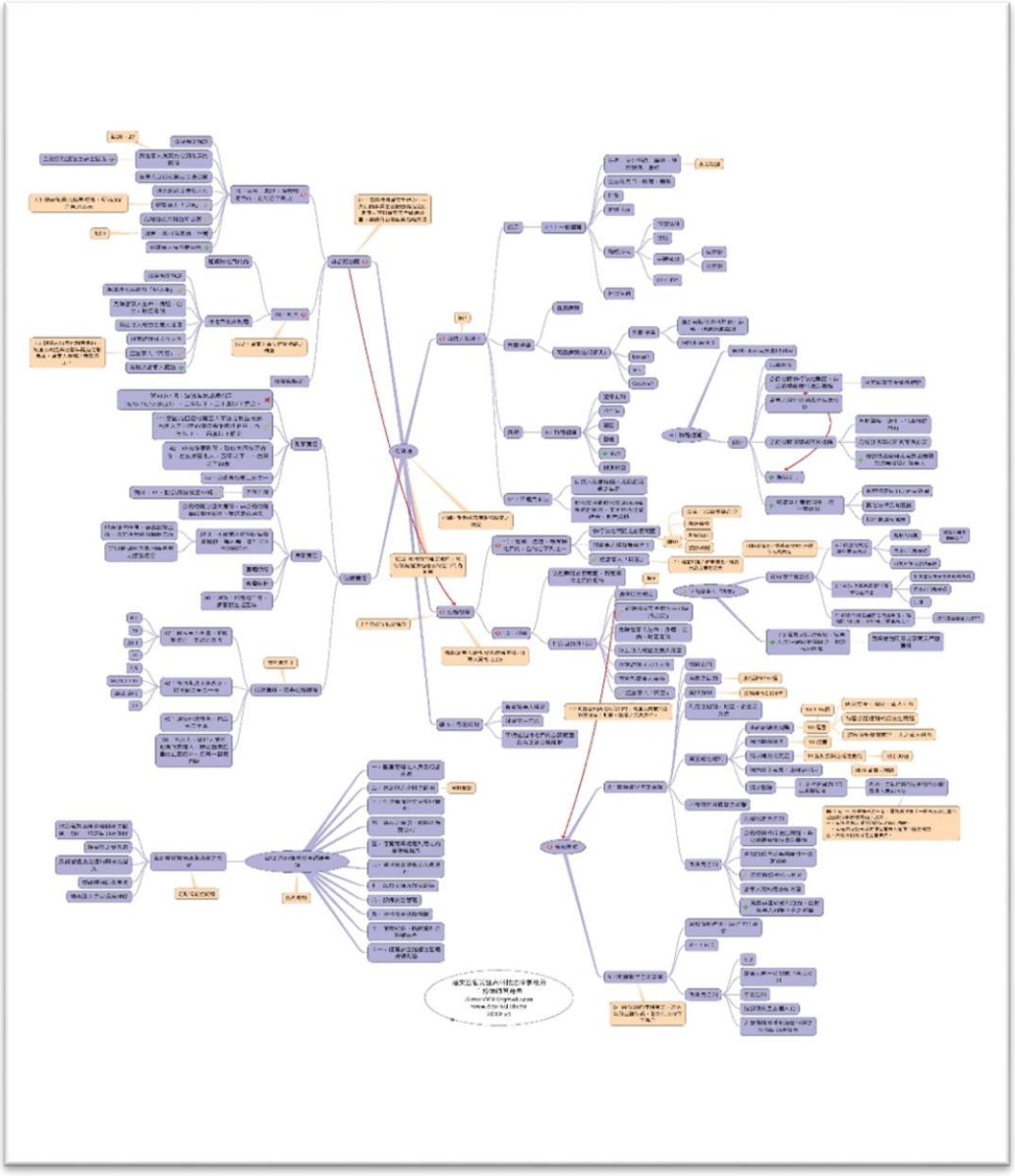
一、主文宣（含議程）

資料來源：本計畫製作

圖 2 109 年通訊傳播事業個資法遵教育訓練 DM

二、課程教材

本案教育訓練由達文西個資暨高科技法律事務所葉奇鑫所長及王慕民合夥律師分別以「個資法心智圖」與「國內外個資法精選案例解析」為題，緊扣課程主題與學員分享法律規範與實務執行經驗。教材節錄如下：



資料來源：本計畫製作

圖 3 個資法心智圖

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

國內外個資法精選案例解析

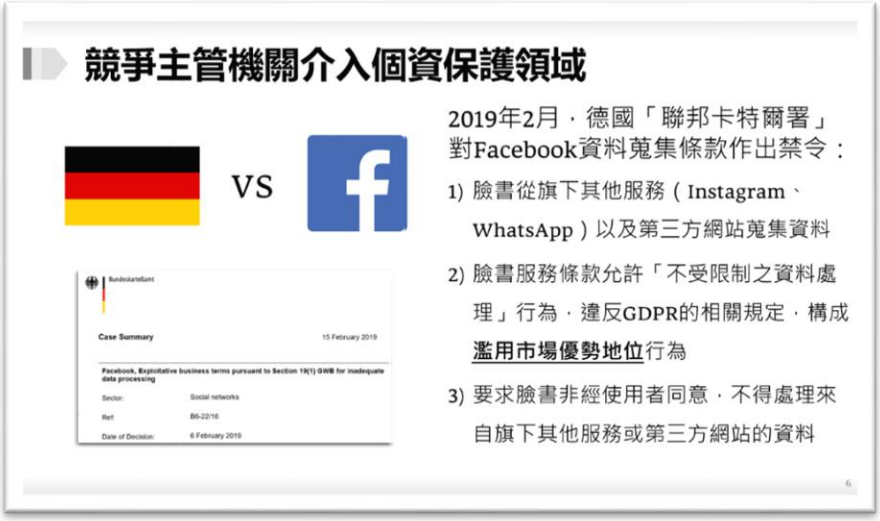
達文西個資暨高科技法律事務所
王慕民 合夥律師

2020/07、08 於通訊傳播事業個資法遵教育訓練

個資法關鍵要素

歐盟5G監理焦點 TOP 3

1) 終端用戶可能無法理解5G應用的強大資訊共享與傳播能力，未能評估對自身的影響
2) 5G帶來的資料經濟，使不同參與者可交換大量終端用戶資訊，用戶可能無從知悉、無從同意
3) 網路安全的重要性大幅提升



資料來源：本計畫製作

圖 4 國內外個資法精選案例解析節錄

三、課程摘要

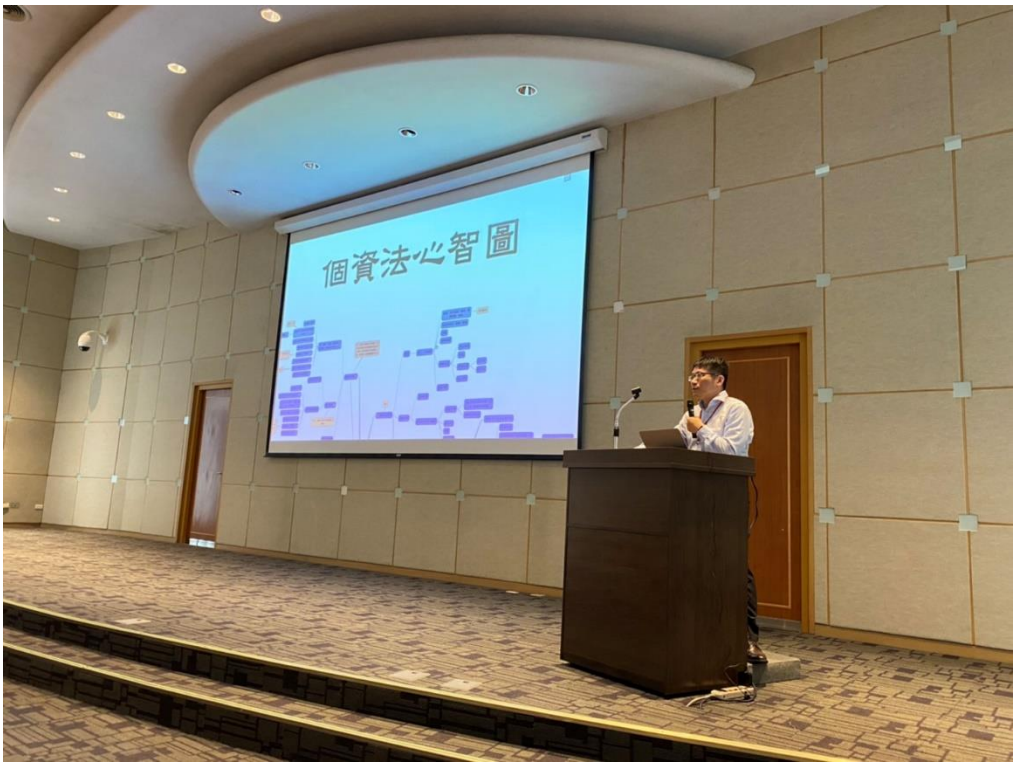
（一)109 年 7 月 22 日：第一場次（台北場）

假集思交通部國際會議中心舉行，總計 127 人報名，實到 106 人，相關課程剪影與說明如下：

1. 現場課程剪影

資料來源：本計畫拍攝

圖 5 國家通訊傳播委員會林簡任技正隆全開場致詞（109.07.22）



資料來源：本計畫拍攝

圖 6 達文西個資暨高科技法律事務所葉奇鑫所長授課（109.07.22）

資料來源：本計畫拍攝

圖 7 達文西個資暨高科技法律事務所王慕民合夥律師授課（109.07.22）

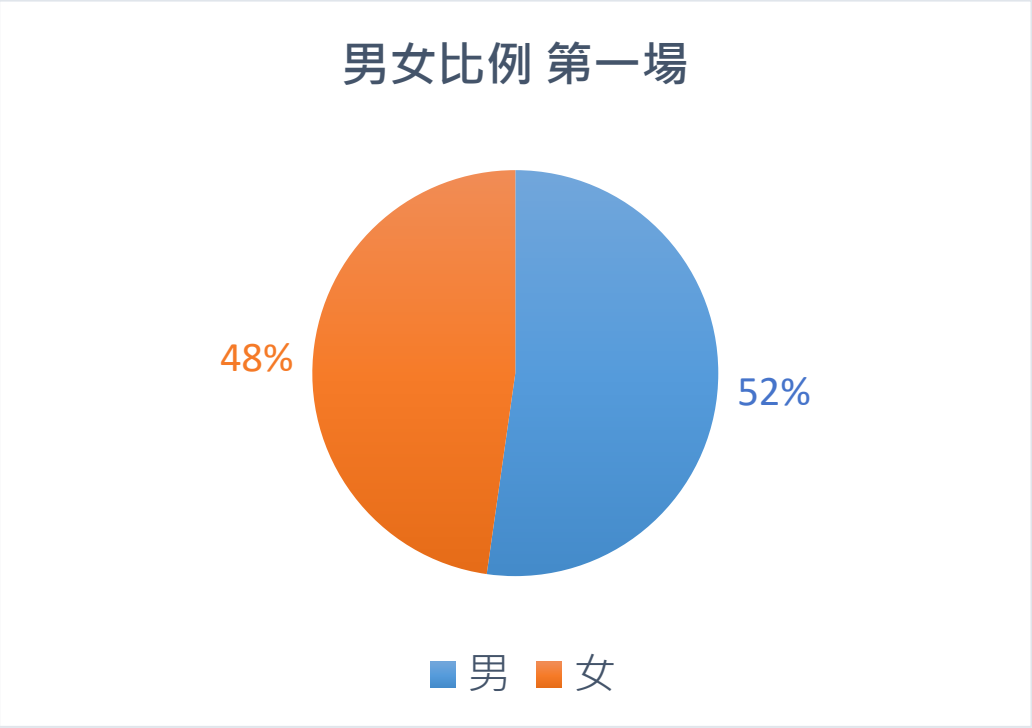
資料來源：本計畫拍攝

圖 8 中堂播放廉政宣導動畫（109.07.22）

2. 參與業者分析

本場次參與業者以傳播業為主，佔整體 43%；職務階層多為一般職員，佔整體 42%；參與動機則以職務需求、公司安排為主，各佔總體 41%、30%。分析圖表如下：

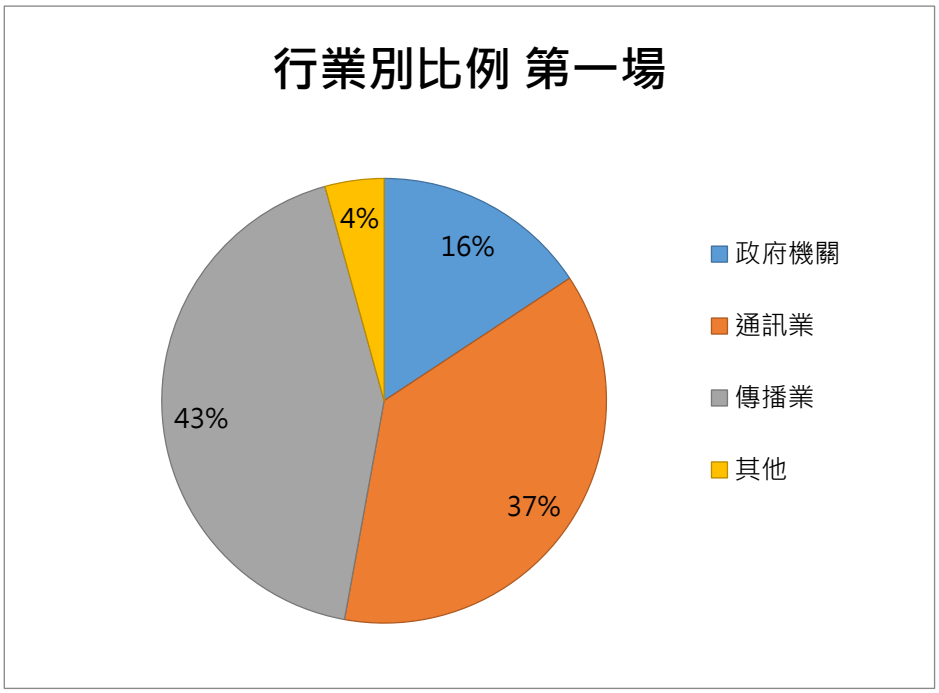
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 9 參與業者性別比例分布（109.07.22）

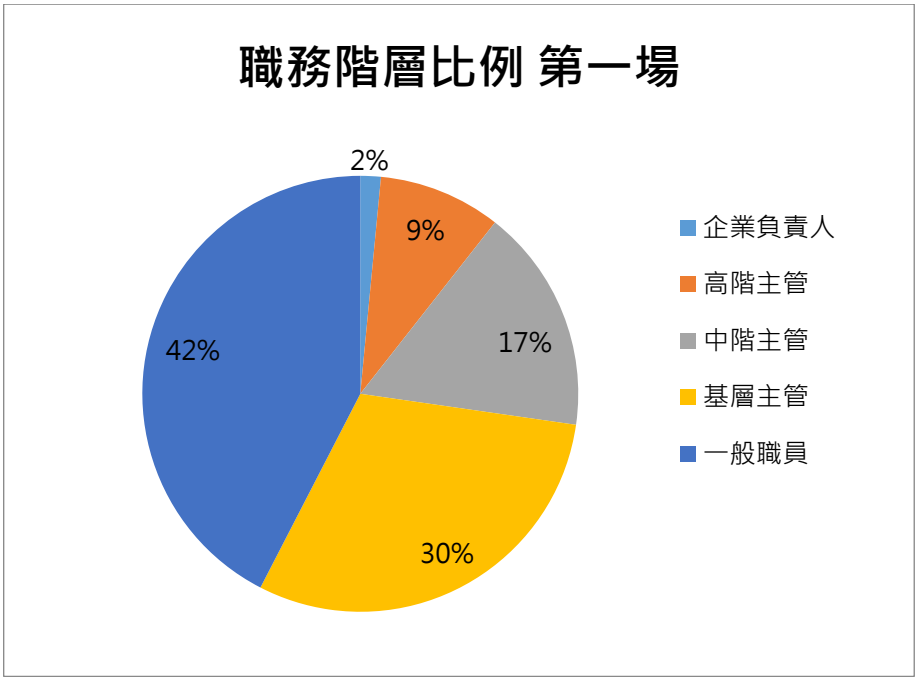
(2) 參與業者行業別比例分布



資料來源：本計畫製作

圖 10 參與業者行業別比例分布（109.07.22）

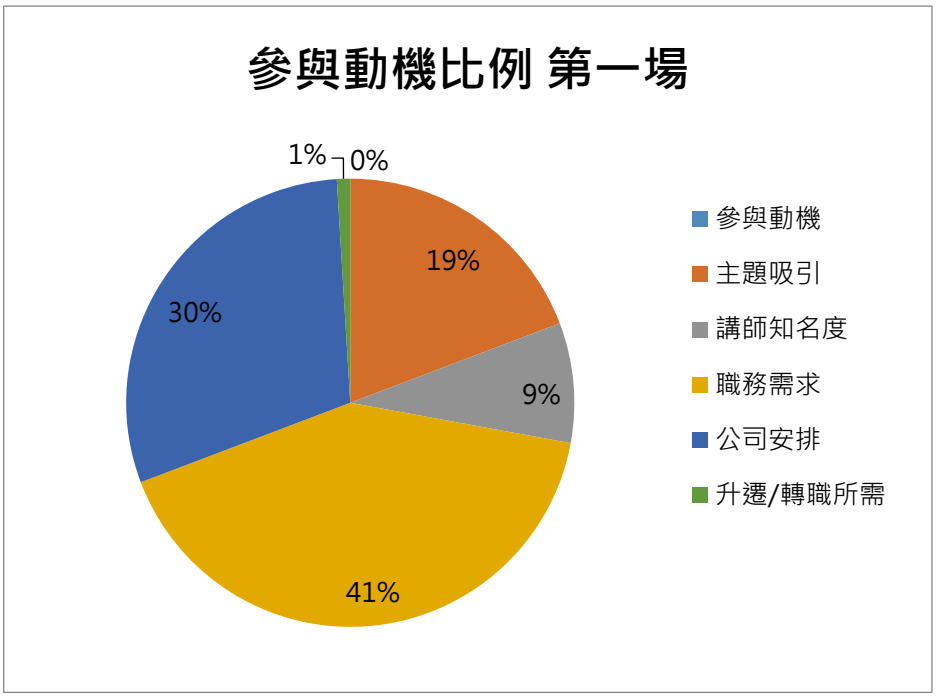
(3) 參與業者職務階層比例分布



資料來源：本計畫製作

圖 11 參與業者職務階層比例分布（109.07.22）

(4) 參與業者參與動機比例分布



資料來源：本計畫製作

圖 12 參與業者參與動機比例分布（109.07.22）

（二） 109 年 7 月 29 日：第二場次（台北場）

假集思台大會議中心舉行，總計 188 人報名，實到 113 人，相關課程剪影與說明如下：

1. 現場課程剪影

資料來源：本計畫拍攝

圖 13 國家通訊傳播委員會林簡任技正隆全開場致詞（109.07.29）

資料來源：本計畫拍攝

圖 14 達文西個資暨高科技法律事務所葉奇鑫所長授課(109.07.29)

資料來源：本計畫拍攝

圖 15 達文西個資暨高科技法律事務所王慕民合夥律師授課（109.07.29）

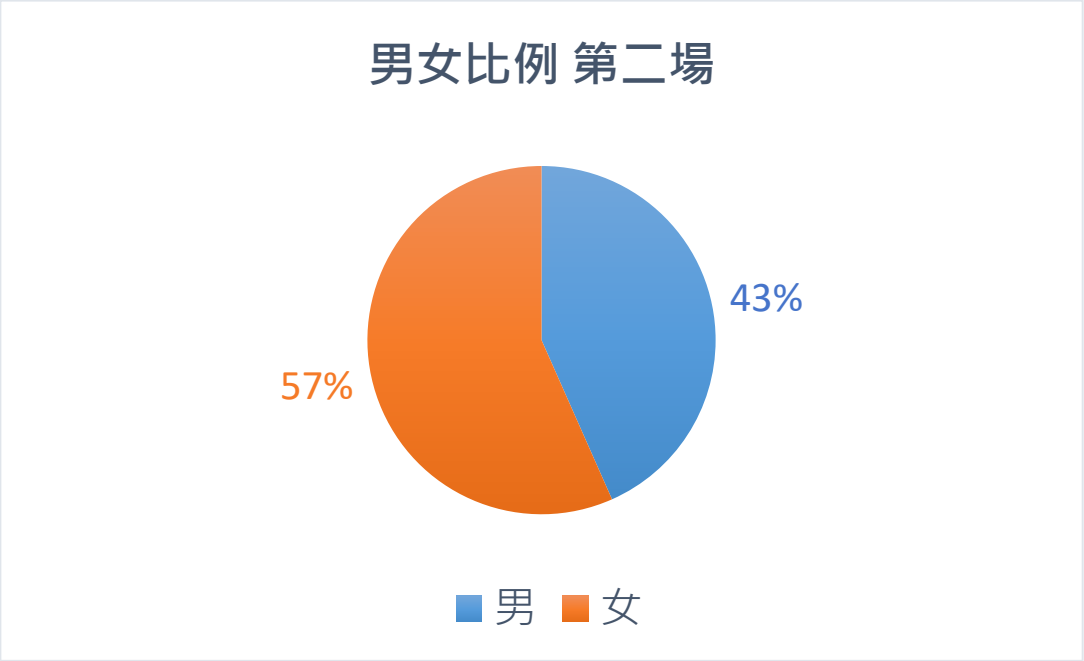
資料來源：本計畫拍攝

圖 16 中堂播放廉政宣導動畫（109.07.29）

2. 參與業者分析

本場次參與業者以通訊業為主，佔整體 45%；職務階層多為一般職員，佔整體 60%；參與動機則以職務需求、公司安排為主，各佔總體 40%、30%。分析圖表如下：

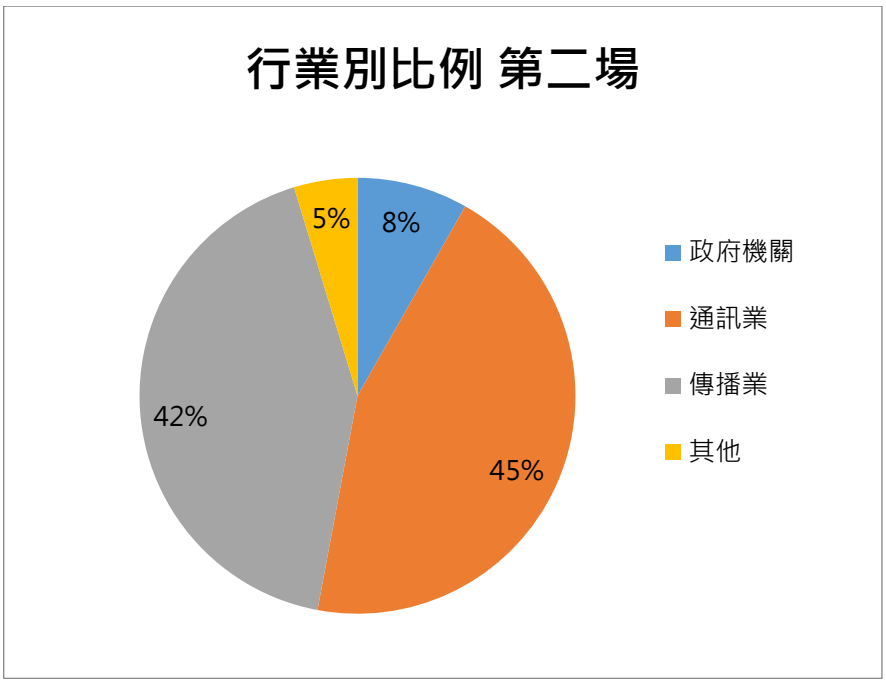
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 17 參與業者性別比例分布（109.07.29）

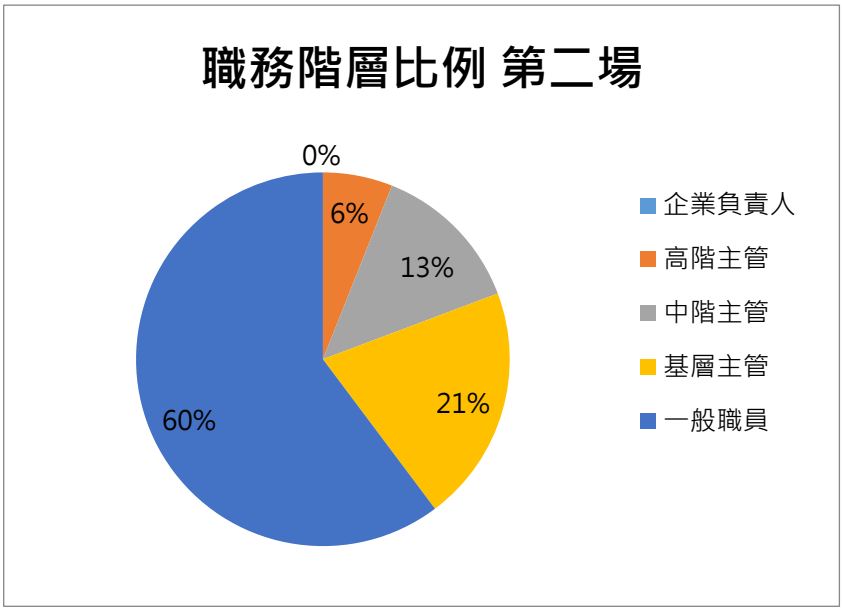
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 18 參訓業者行業別比例分布（109.07.29）

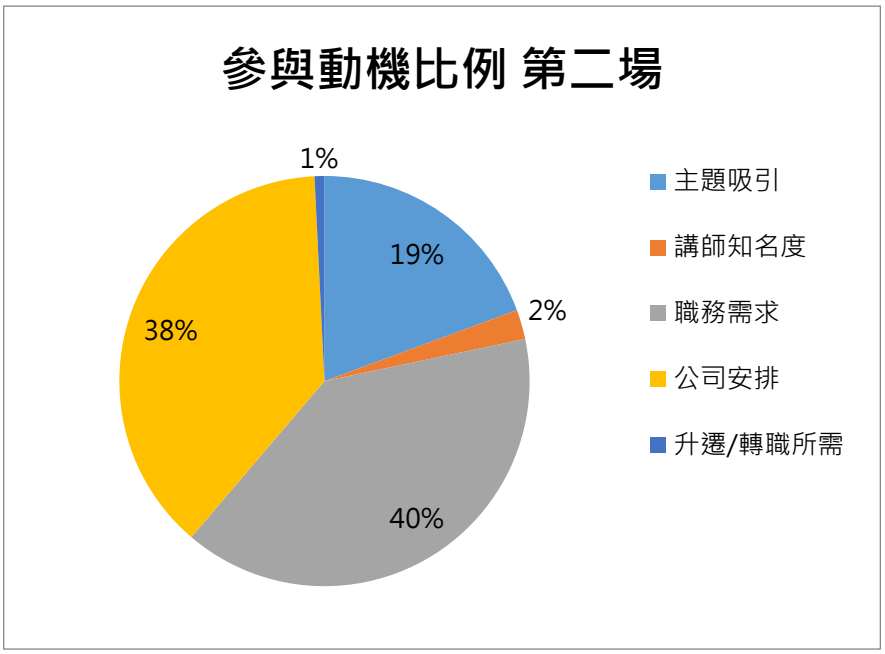
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 19 參訓業者職務階層比例分布（109.07.29）

(4) 參訓業者參與動機比例分布



資料來源：本計畫製作

圖 20 參訓業者參與動機比例分布（109.07.29）

（三） 109 年 8 月 12 日：第三場次（台中場）

假集思台中文心會議中心舉行，總計 62 人報名，實到 50 人，相關課程剪影與說明如下：

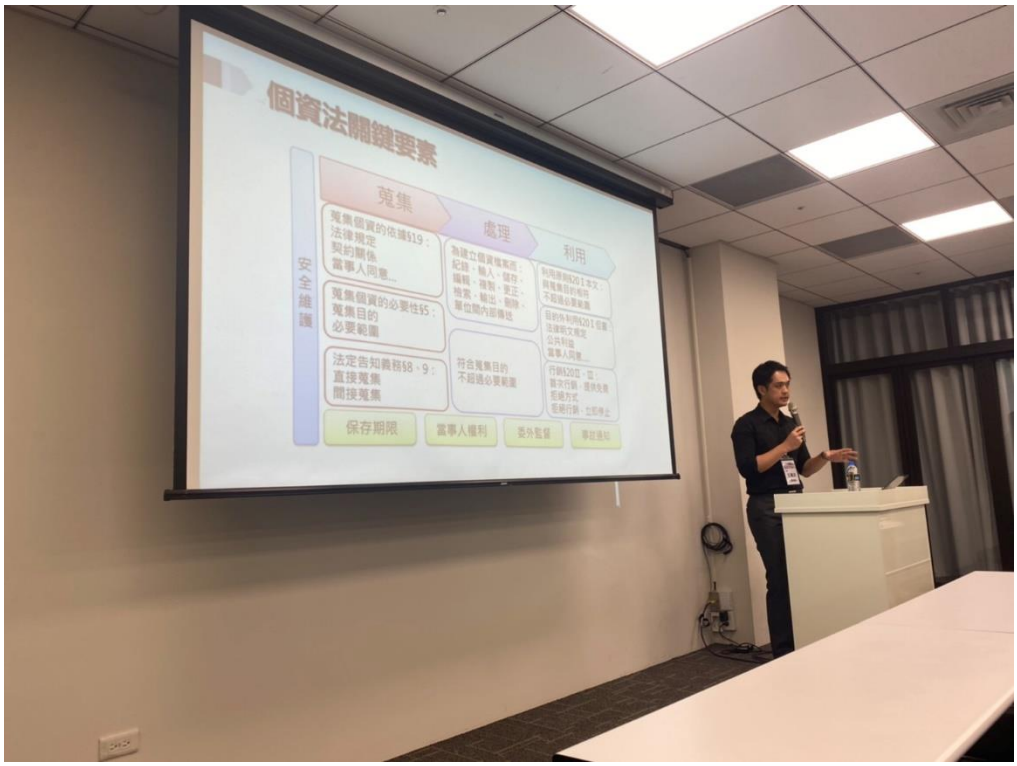
3. 現場課程剪影

資料來源：本計畫拍攝

圖 21 國家通訊傳播委員會林簡任技正隆全開場致詞(109.08.12)

資料來源：本計畫拍攝

圖 22 達文西個資暨高科技法律事務所葉奇鑫所長授課（109.08.12）



資料來源：本計畫拍攝

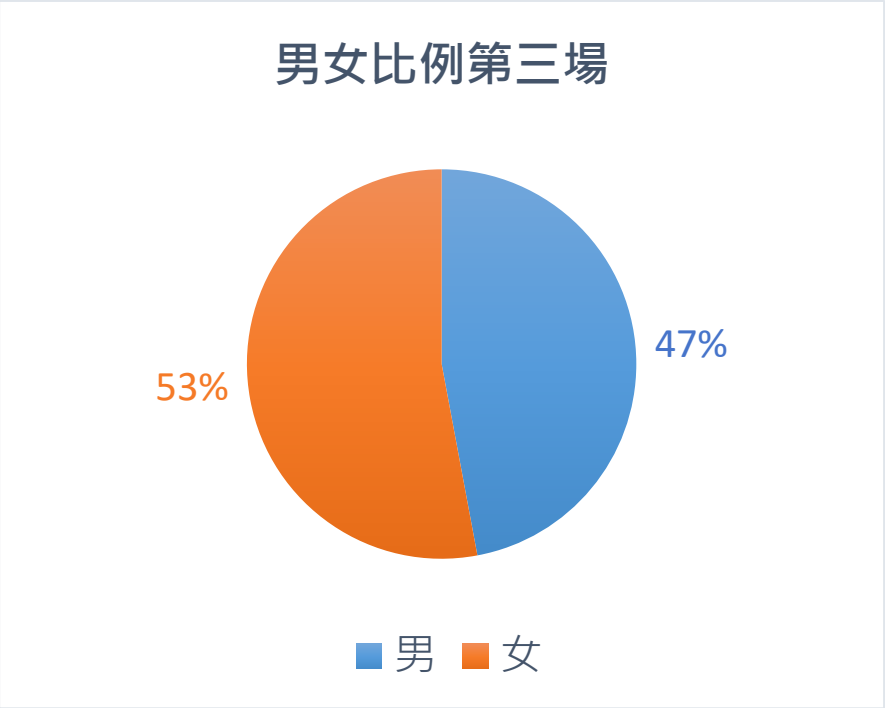
圖 23 達文西個資暨高科技法律事務所王慕民合夥律師授課

（109.08.12）

4. 參與業者分析

本場次參與業者以傳播業為主，佔整體 70%；職務階層多為一般職員，佔整體 59%；參與動機則以職務需求、公司安排為主，各佔總體 34%、45%。分析圖表如下：

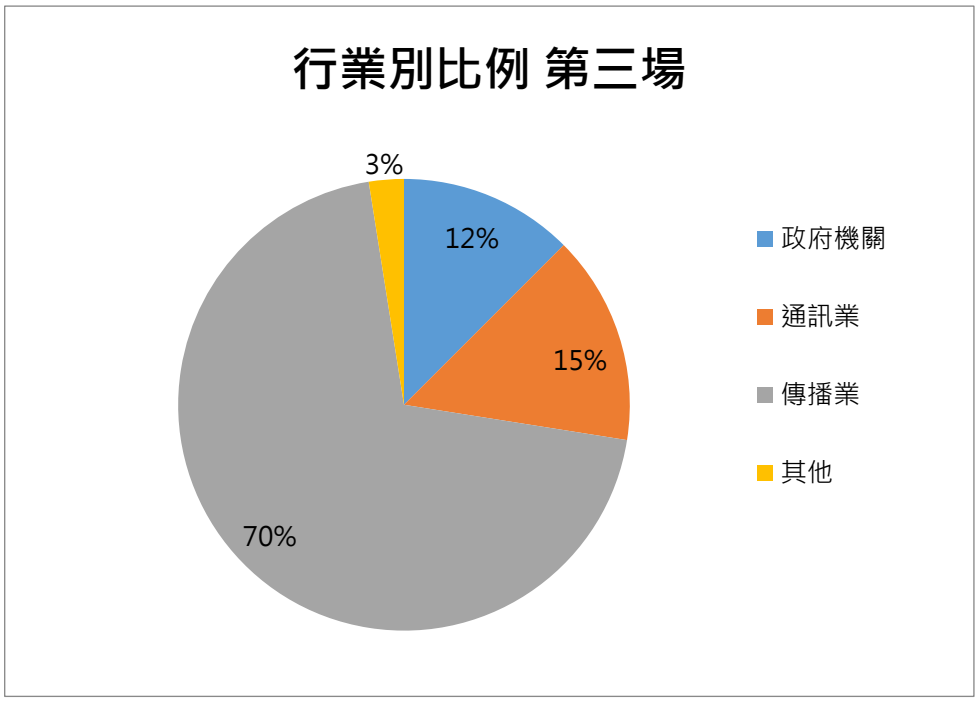
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 24 參與業者性別比例分布（109.08.12）

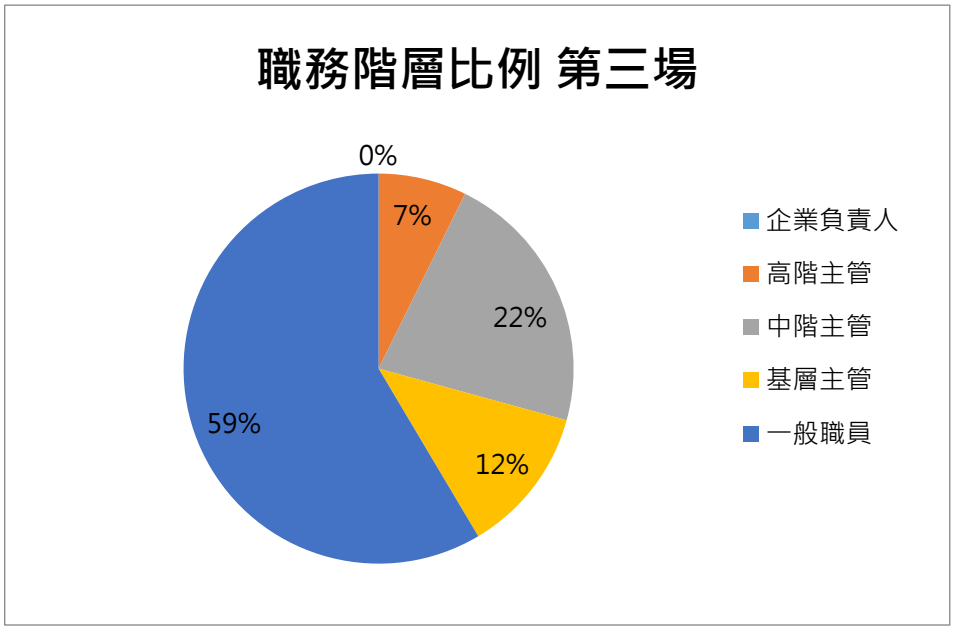
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 25 參訓業者行業別比例分布（109.08.12）

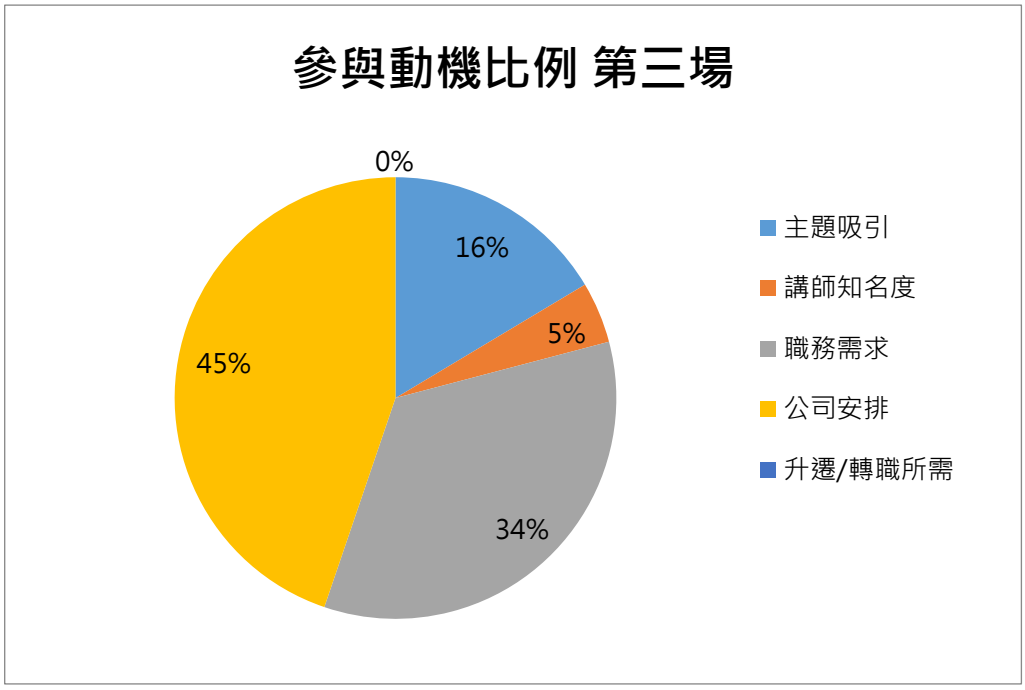
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 26 參訓業者職務階層比例分布（109.08.12）

(4) 參訓業者參與動機比例分布



資料來源：本計畫製作

圖 27 參訓業者參與動機比例分布（109.08.12）

（四） 109 年 8 月 26 日：第四場次（高雄場）

假集思高雄亞灣會議中心舉行，總計 68 人報名，實到 54 人，相關課程剪影與說明如下：

5. 現場課程剪影

資料來源：本計畫拍攝

圖 28 國家通訊傳播委員會林簡任技正隆全開場致詞(109.08.26)

資料來源：本計畫拍攝

圖 29 達文西個資暨高科技法律事務所葉奇鑫所長授課（109.08.26）

資料來源：本計畫拍攝

圖 30 達文西個資暨高科技法律事務所王慕民合夥律師授課（109.08.26）

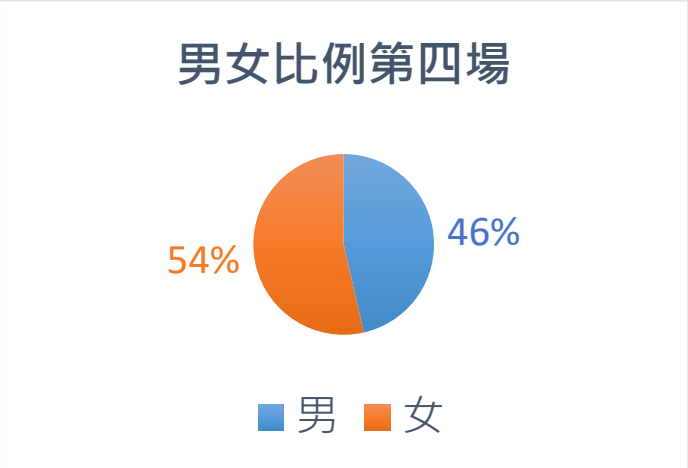
資料來源：本計畫拍攝

圖 31 中堂播放廉政宣導動畫（109.08.26）

6. 參與業者分析

本場次參與業者以傳播業為主，佔整體 72%；職務階層多為一般職員，佔整體 41%；參與動機則以職務需求、公司安排為主，各佔總體 35%。分析圖表如下：

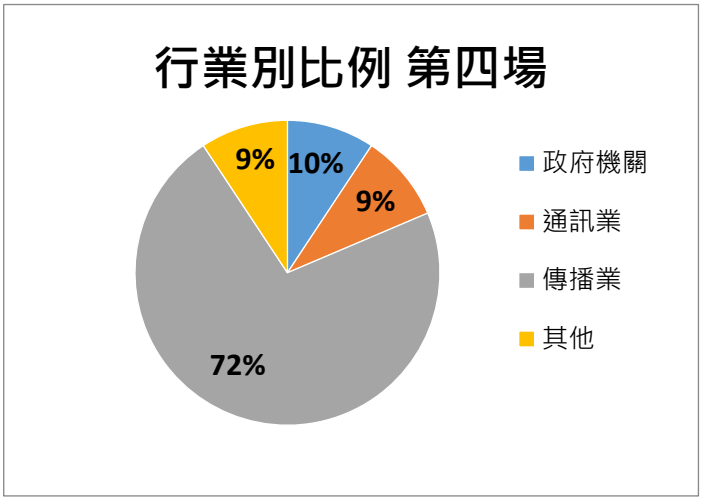
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 32 參與業者性別比例分布（109.08.26）

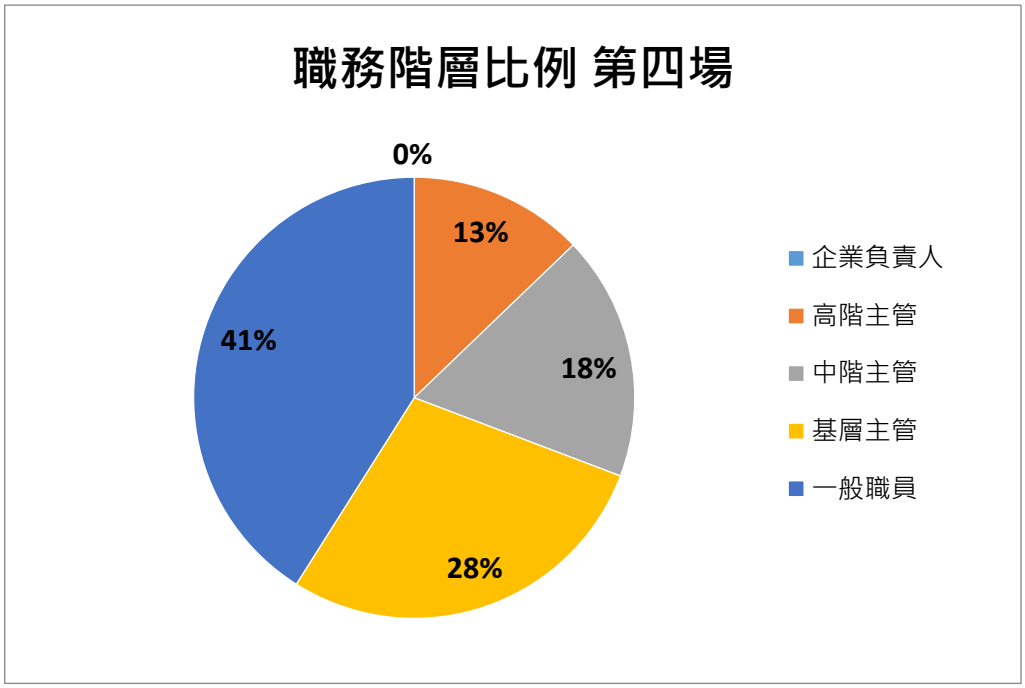
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 33 參訓業者行業別比例分布（109.08.26）

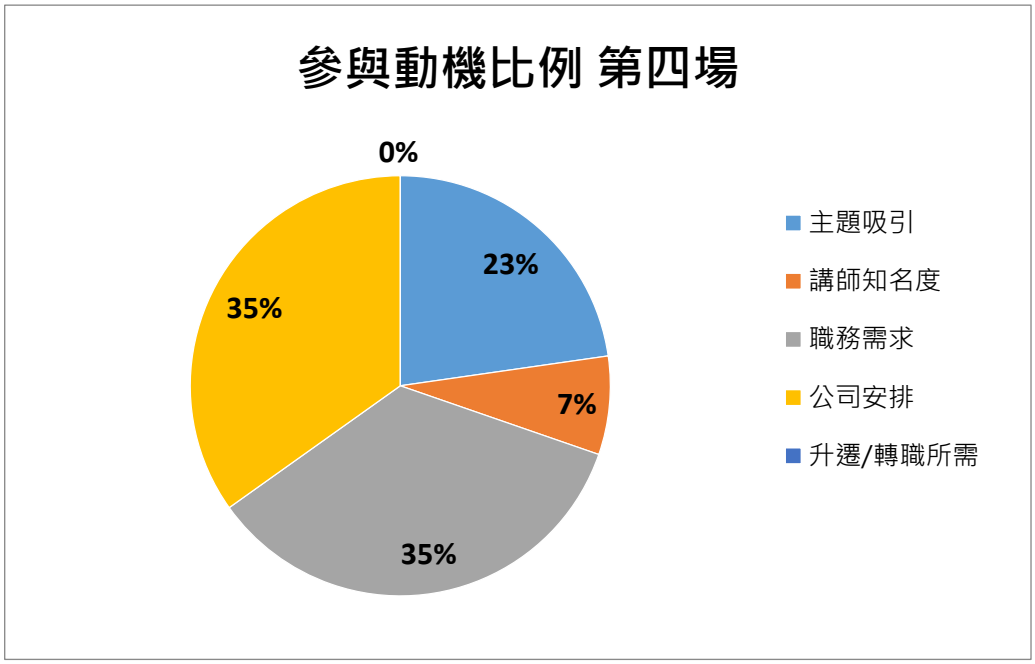
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 34 參訓業者職務階層比例分布（109.08.26）

(4) 參訓業者參與動機比例分布

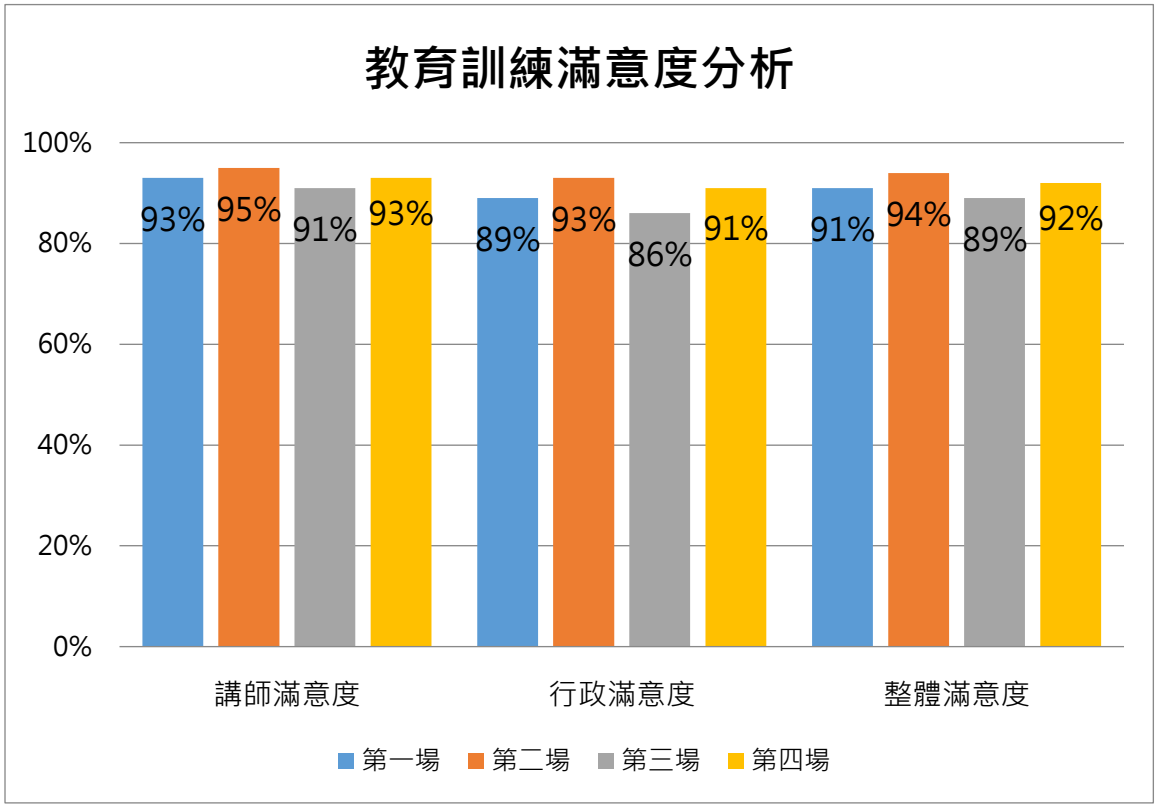


資料來源：本計畫製作

圖 35 參訓業者參與動機比例分布（109.08.26）

第三節 成果統計

本案 4 場教育訓練總報名人數為 443 人，實到總人數為 323 人，共回收 252 份問卷，其中有效問卷為 247 份，整體平均滿意度為 92%（計算方式為講師滿意度佔整體 50%、行政滿意度 50%）。茲將分析圖表及各場次學員回饋羅列如下：



資料來源：本計畫製作

圖 36 教育訓練滿意度分析圖

表 1 教育訓練學員回饋：最有幫助的主題

最有幫助的主題	
1.	何謂個資?如何判斷是否違法?
2.	個資利用合法性判斷技巧
3.	違法蒐集處理利用個資法律效果與責任
4.	個資心智圖的使用
5.	個資法心智圖幫助本人分辨更加了解
6.	案例分析，心智圖解說
7.	掌握法規近況
8.	個資法架構
9.	個資法案例
10.	違法蒐集處理利用個資法律效果與責任
11.	個資保護風險評估及承受能力
12.	媒體採訪拍攝對個資的問題
13.	提升個資管理知識能力
14.	精選案例解析
15.	個資法心智圖
16.	個資蒐集處理合法性判斷技巧
17.	電信事業個資實例解說

18.	個資隱私
19.	個資蒐集處理利用合法性判斷技巧
20.	客服部分
21.	個資法關鍵要素，個資法心智圖分析
22.	特定目的消失刪除侵害利益
23.	增加法律學習的廣度及實務訓練
24.	個資與稽核

資料來源：本計畫製作

表 2 教育訓練學員回饋：想深入了解的主題

想深入了解的主題	
1.	案例分享
2.	去識別化主題
3.	個資裁罰案例
4.	個資函釋探討
5.	國內外個資法精選案例
6.	未來修法方向
7.	何謂管理
8.	公開資料蒐集與個資法的關聯
9.	5G 時代，資料經濟加值應用的實例分享
10.	個資上雲端服務的安全與合規要求
11.	違法蒐集處理利用個資法律效果與責任
12.	歐盟 GDPR 實務規範，我國電信事業應遵守個資法案例實務
13.	個資保護實際案例資料
14.	解決個資技術方案
15.	違法蒐集處理利用個資法律效果與責任
16.	網路詐欺相關法條

17.	IT 技術安全
18.	傳播事業的大數據應用
19.	雲端服務大數據個資法關鍵要素跟安全性管理
20.	5G 相關、歐盟差異
21.	特定產業之個資法建議及案例分享
22.	網路釣魚詐欺涉及之個資法律問題
23.	個資安全實務
24.	隱私政策法規之撰寫實務
25.	針對第四台個資防護
26.	法令規定保存期限、資料的存廢價值
27.	智財相關、職場個人權益保障蒐證

資料來源：本計畫製作

第三章 通傳產業之實務專題講座

第一節 執行成果

一、課程需求

通訊傳播事業個資實務專題講座規劃，北部地區 3 場次及南部地區 1 場次，合計 4 場次，每場次以可容納 50 人以上規模辦理，授課總時數 24 小時以上，並提交相關訓練教材資料電子檔。

二、課程目的

針對通訊傳播事業舉辦個資實務專題講座，將邀請擔任國家發展委員會個資法諮詢委員的達文西個資暨高科技法律事務所葉奇鑫所長到場，講授目前國發會為取得 GDPR 適足性認定並因應國內需求而推動個資法修法之趨勢；再藉由探討個資加值應用法規、跨境隱私議題研析等，期使各事業得深入瞭解我國實務運作現況與進入全球市場後可能面臨的挑戰與規範，熟稔通傳事業運用資料加值之風險及因應作法；並將於特別場探討有關頻道、電臺及傳播內容產業之個資實務案例。

三、課程主題

（一） 通傳事業資料加值案例研析；
（二） 個資法之修法趨勢初探；
（三） 特別場：傳播事業的大數據應用；傳播業務中的同意、去識別與個資管理。

四、課程日期

（一） 109 年 9 月 16 日台北第 1 場
（二） 109 年 9 月 23 日台北第 2 場
（三） 109 年 9 月 30 日高雄場
（四） 109 年 10 月 7 日台北特別場

五、課程產出

總計產出 4 份教材、台北場課程影像檔，並提供公務人員終身學習時數 4 小時或中小企業終身學習護照認可時數 4 小時。

第二節 課程內容

一、主文宣（含議程）

資料來源：本計畫製作

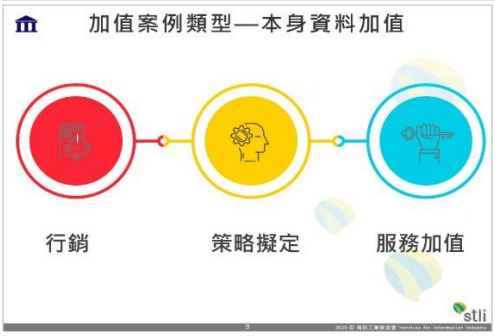
圖 37 109 年通訊傳播事業個資實務專題講座 DM

資料來源：本計畫製作

圖 38 109 年通訊傳播事業個資實務專題講座（台北特別場）DM

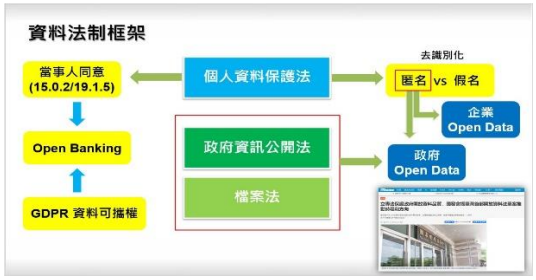
二、課程教材

本案專題講座邀請資策會科法所的宋佩珊副主任及達文西個資暨高科技法律事務所葉奇鑫所長分別以「通傳事業資料加值案例研析」與「個資法之修法趨勢初探」為題，與學員分享加值案例與未來修法趨勢；台北特別場則邀請資策會數位服務創新研究所的徐毓良副主任及達文西個資暨高科技法律事務所王慕民合夥律師分別以「傳播事業的大數據應用」與「傳播業務中的同意、去識別與個資管理」為題，與學員分享數據應用與案例分享。教材節錄如下：



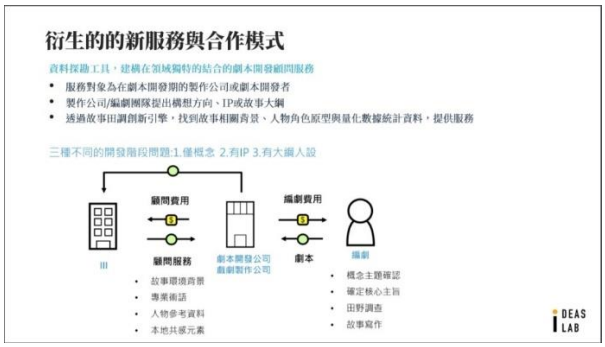
資料來源：本計畫製作

圖 39 通傳事業資料加值案例研析節錄



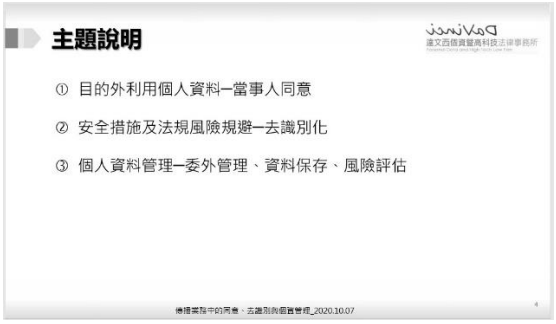
資料來源：本計畫製作

圖 40 個資法之修法趨勢初探節錄



資料來源：本計畫製作

圖 41 傳播事業的大數據應用節錄



資料來源：本計畫製作

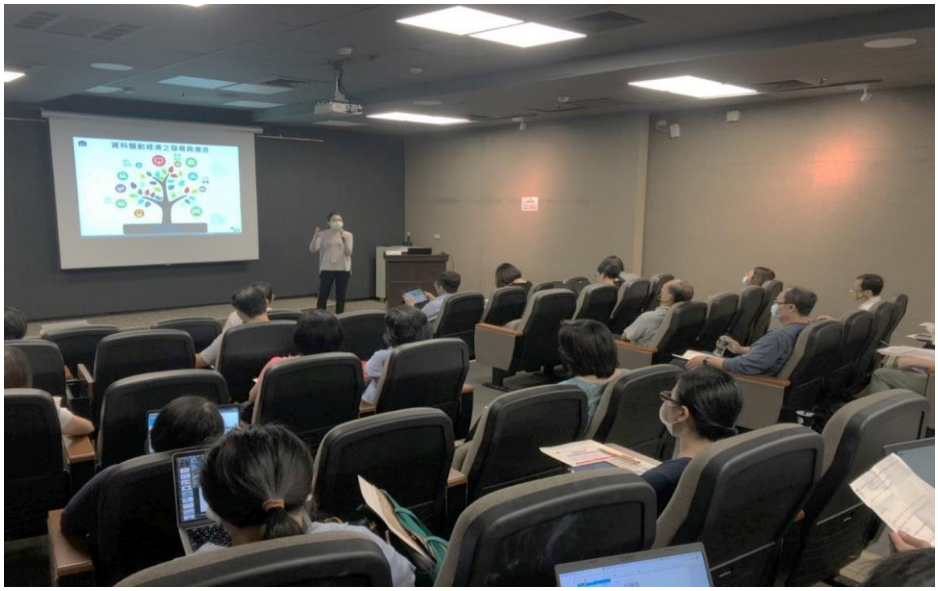
圖 42 傳播業務中的同意、去識別與個資管理節錄

三、課程摘要

(一)109 年 9 月 16 日：第一場次（台北場）

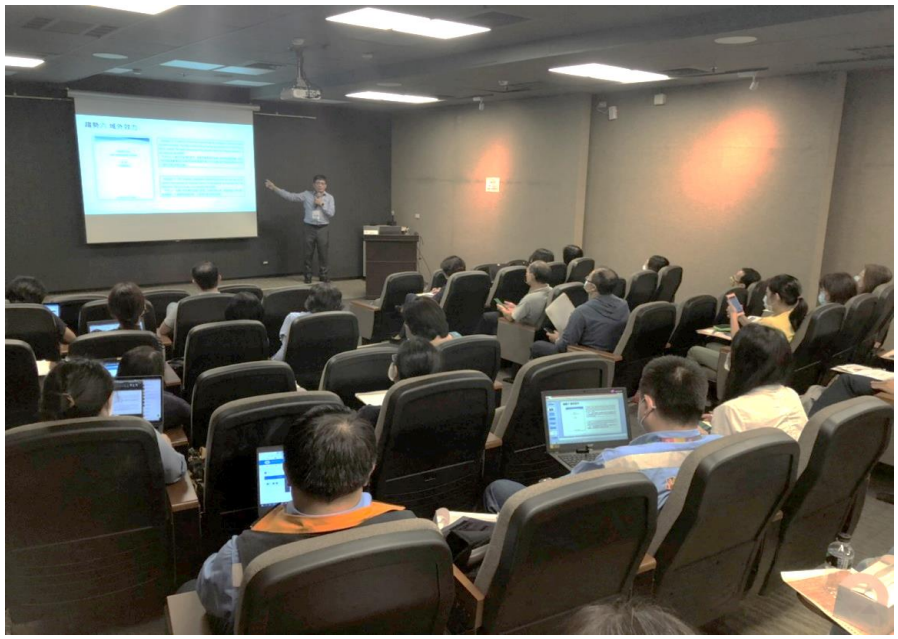
假集思台大會議中心舉行，總計 82 人報名，實到 55 人，相關課程剪影與說明如下：

1. 現場課程剪影



資料來源：本計畫拍攝

圖 43 資策會科法所宋佩珊副主任授課（109.09.16）



資料來源：本計畫拍攝

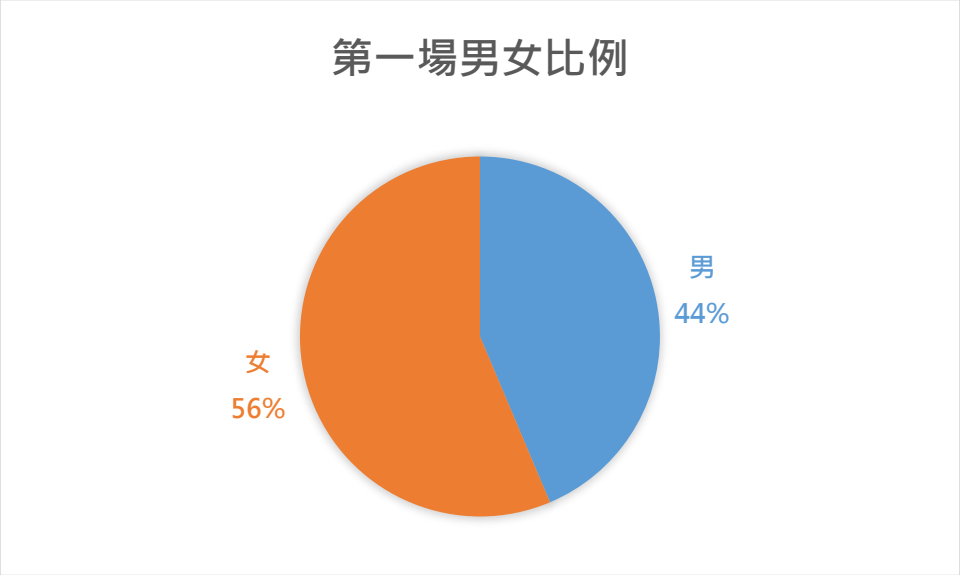
圖 44 達文西法律事務所葉奇鑫所長授課（109.09.16）

2. 參與業者分析

本場次參與業者性別比例以女性居多，佔整體56%；行業別以通訊業為主，佔整體 47%；職務階層多為一般職員，佔整體 48%；參與動機則以公司安排、職務需求為主，各佔總體 44%、39%。分析

圖表如下：

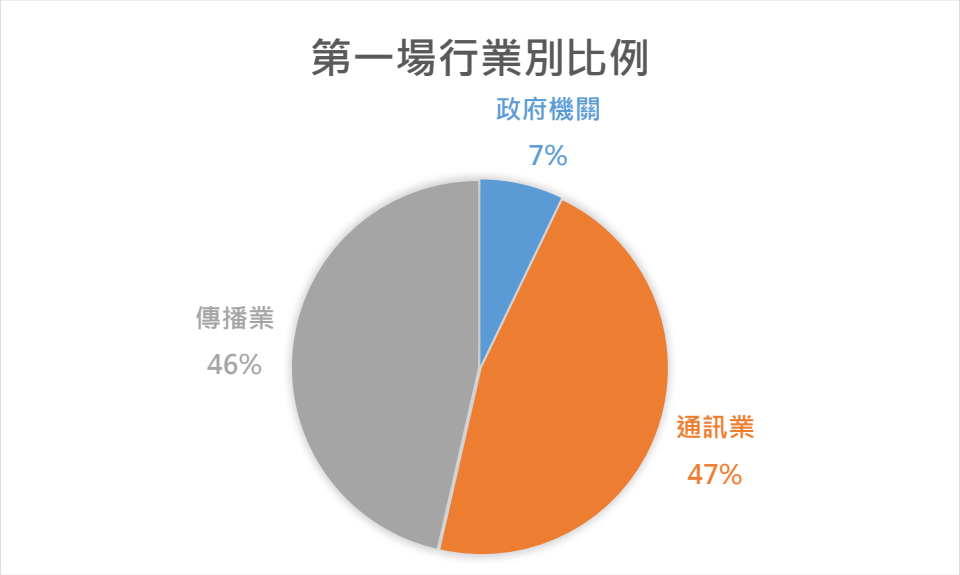
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 45 參與業者性別比例分布（109.09.16）

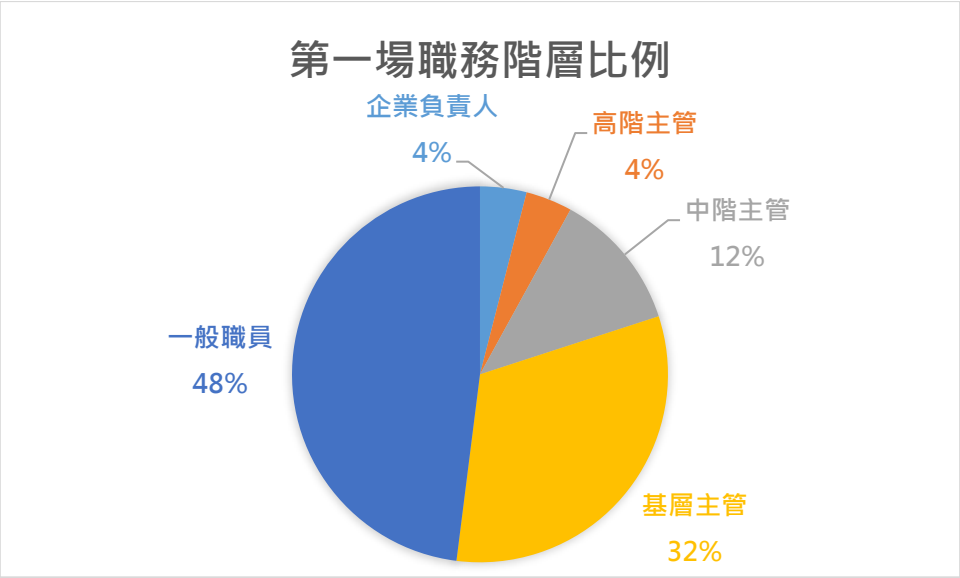
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 46 參與業者行業別比例分布（109.09.16）

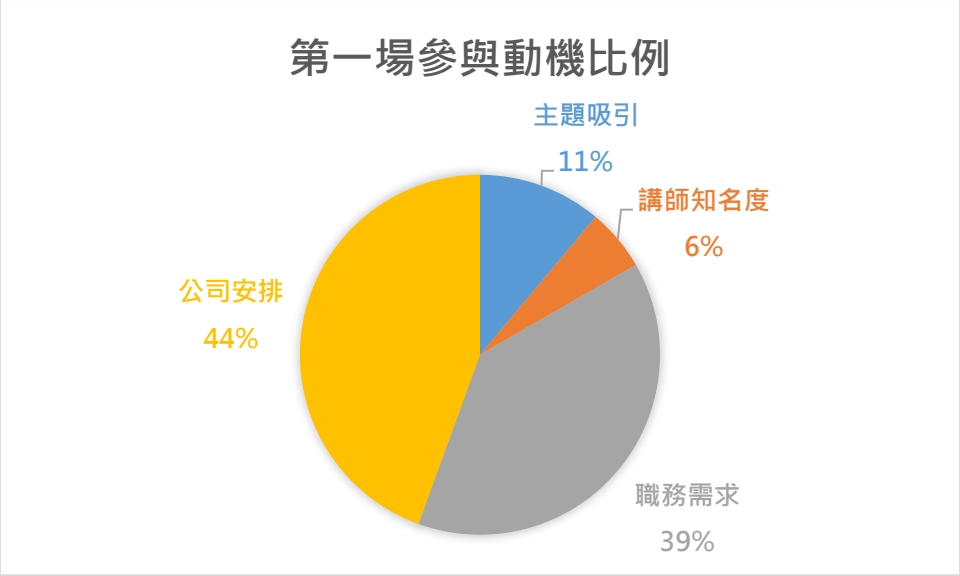
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 47 參與業者職務階層比例分布（109.09.16）

(4) 參訓業者參與動機比例分布



資料來源：本計畫製作

圖 48 參與業者職務階層比例分布（109.09.16）

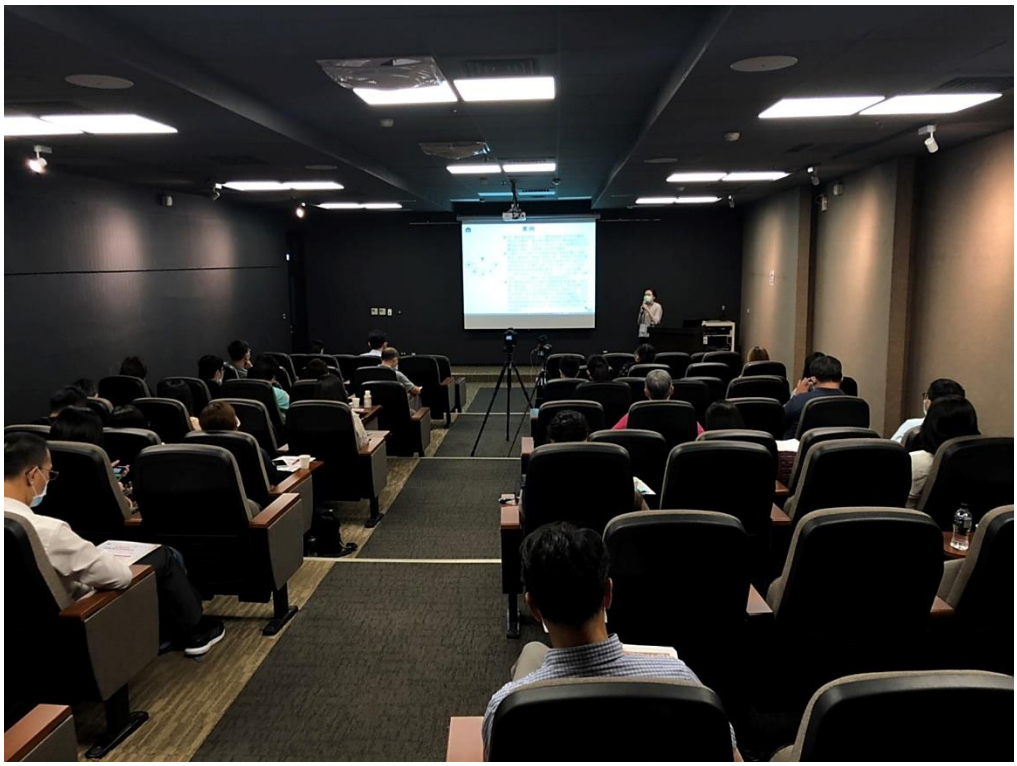
（二)109 年 9 月 23 日：第二場次（台北場）

假集思台大會議中心舉行，總計 83 人報名，實到 40 人，相關課程剪影與說明如下：

7. 現場課程剪影

資料來源：本計畫拍攝

圖 49 通傳會林簡任技正隆全開場致詞（109.09.23）



資料來源：本計畫拍攝

圖 50 資策會科法所宋佩珊副主任授課（109.09.23）

資料來源：本計畫拍攝

圖 51 達文西法律事務所葉奇鑫所長授課（109.09.23）

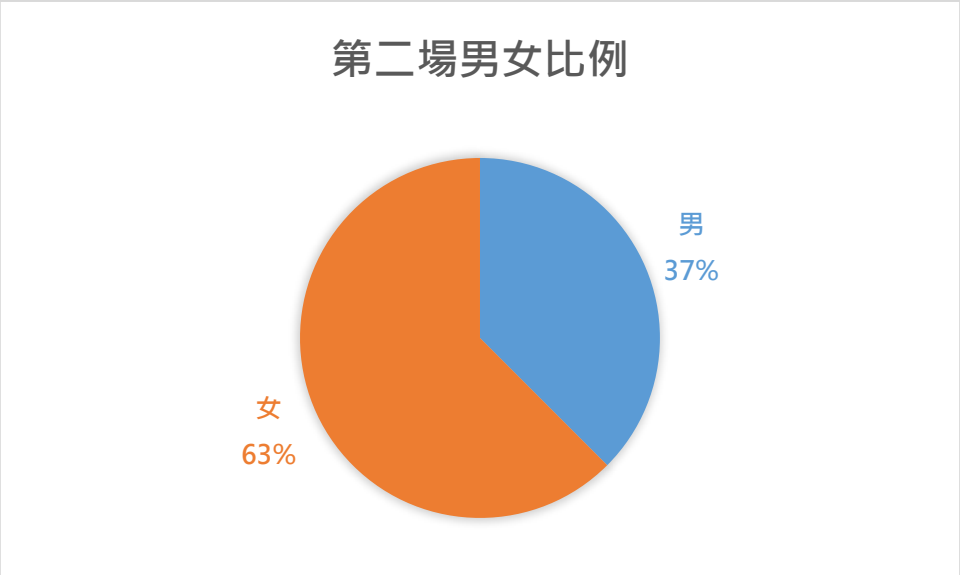
資料來源：本計畫拍攝

圖 52 中堂播放廉政宣導動畫（109.09.23）

8. 參與業者分析

本場次參與業者性別比例以女性居多，佔整體63%；行業別以傳播業為主，佔整體64%；職務階層多為一般職員，佔整體42%；參與動機則以職務需求、主題吸引為主，各佔總體32%、26%。分析圖表如下：

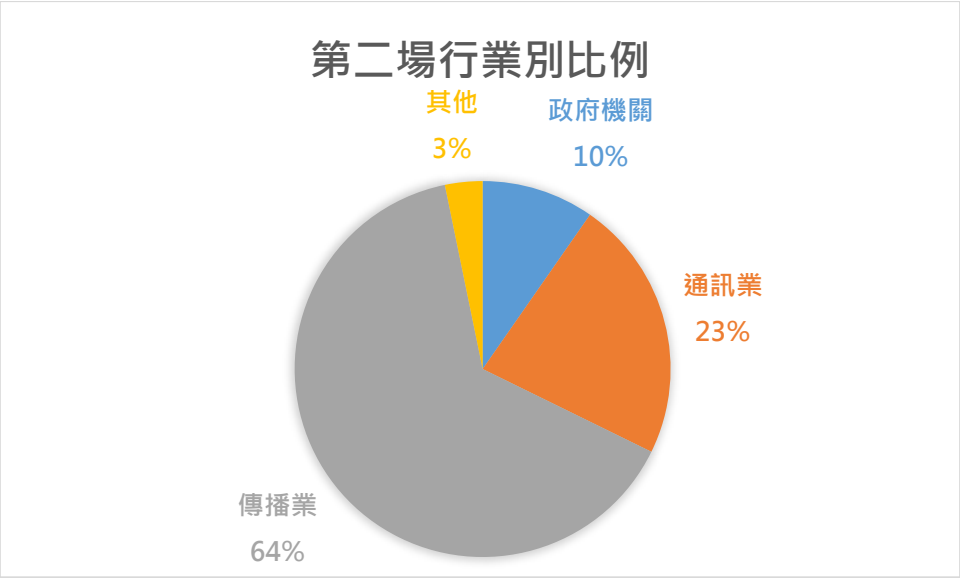
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 53 參與業者性別比例分布（109.09.23）

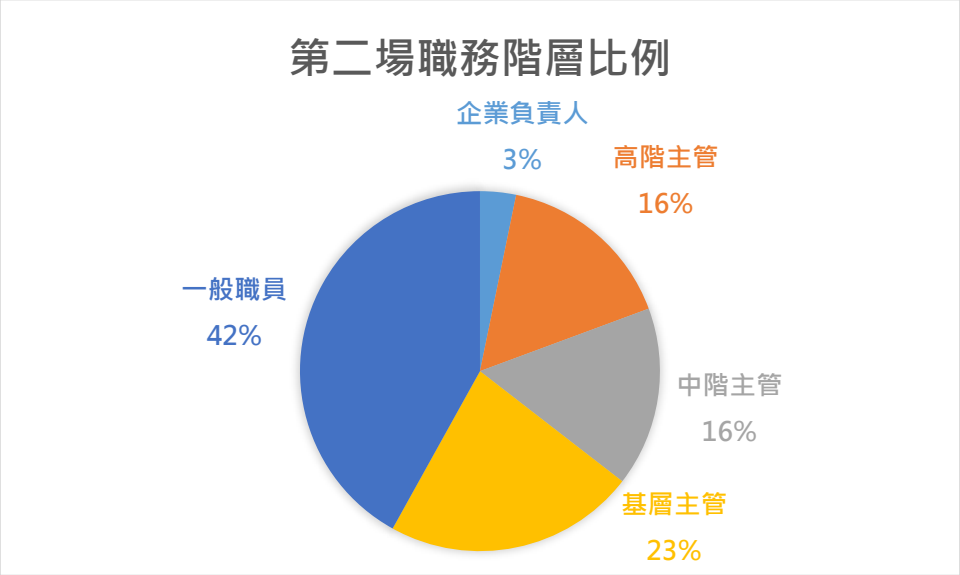
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 54 參與業者行業別比例分布（109.09.23）

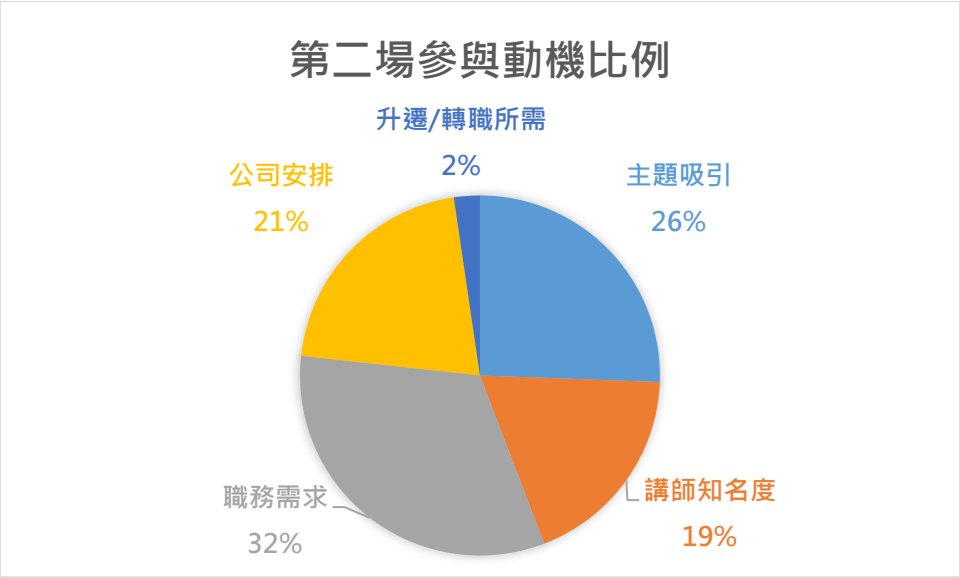
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 55 參與業者職務階層比例分布（109.09.23）

(4) 參訓業者參與動機比例分布



資料來源：本計畫製作

圖 56 參與業者職務階層比例分布（109.09.23）

(三)109 年 9 月 30 日：第三場次（高雄場）

假集思高雄亞灣會議中心舉行，總計 58 人報名，實到 45 人，相關課程剪影與說明如下：

1. 現場課程剪影

資料來源：本計畫拍攝

圖 57 通傳會林簡任技正隆全開場致詞（109.09.30）

資料來源：本計畫拍攝

圖 58 資策會科法所李沛宸經理授課（109.09.30）

資料來源：本計畫拍攝

圖 59 達文西法律事務所葉奇鑫所長授課（109.09.30）

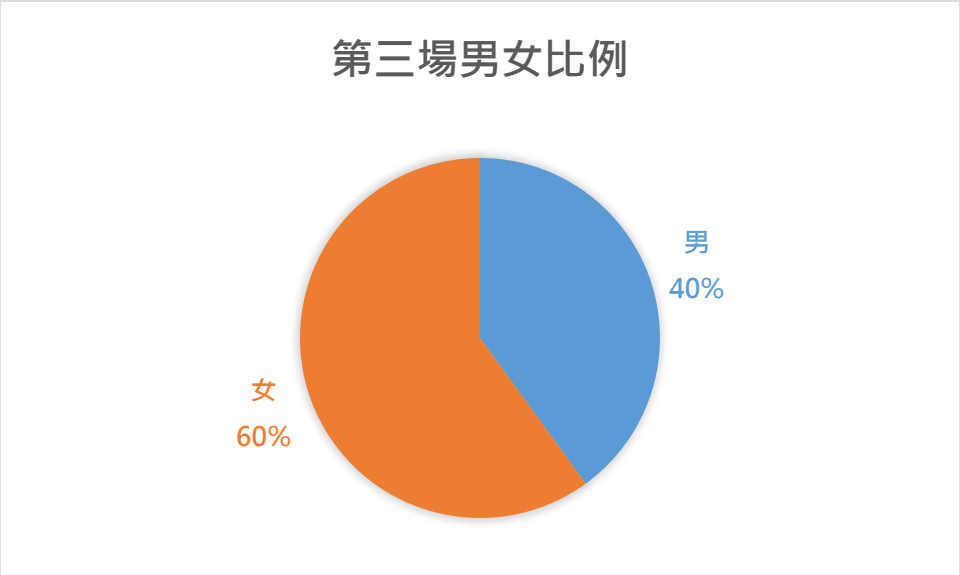
資料來源：本計畫拍攝

圖 60 中堂播放廉政宣導動畫（109.09.30）

2. 參與業者分析

本場次參與業者性別比例以女性居多，佔整體60%；行業別以傳播業為主，佔整體48%；職務階層多為一般職員，佔整體47%；參與動機則以公司安排、職務需求為主，各佔總體47%、35%。分析圖表如下：

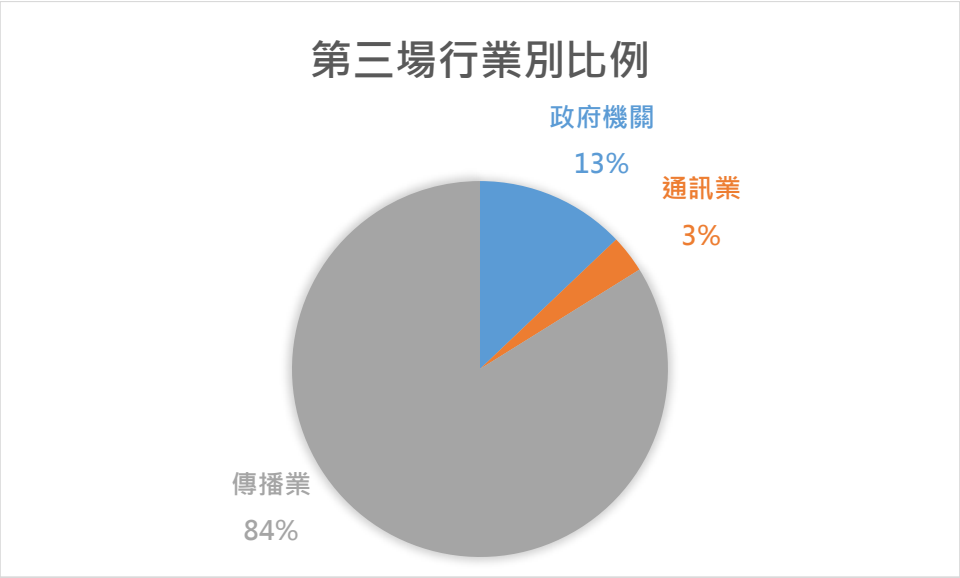
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 61 參與業者性別比例分布（109.09.30）

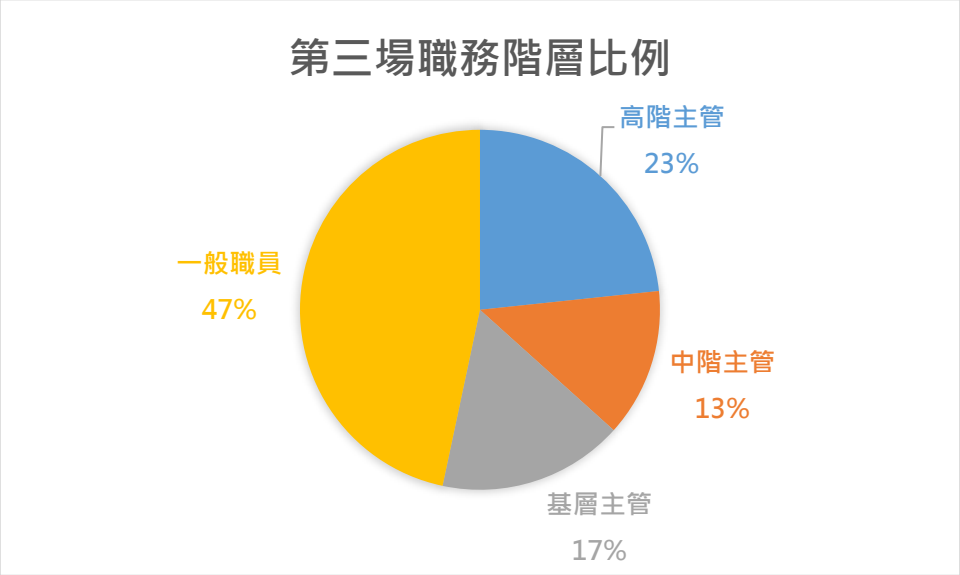
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 62 參與業者行業別比例分布（109.09.30）

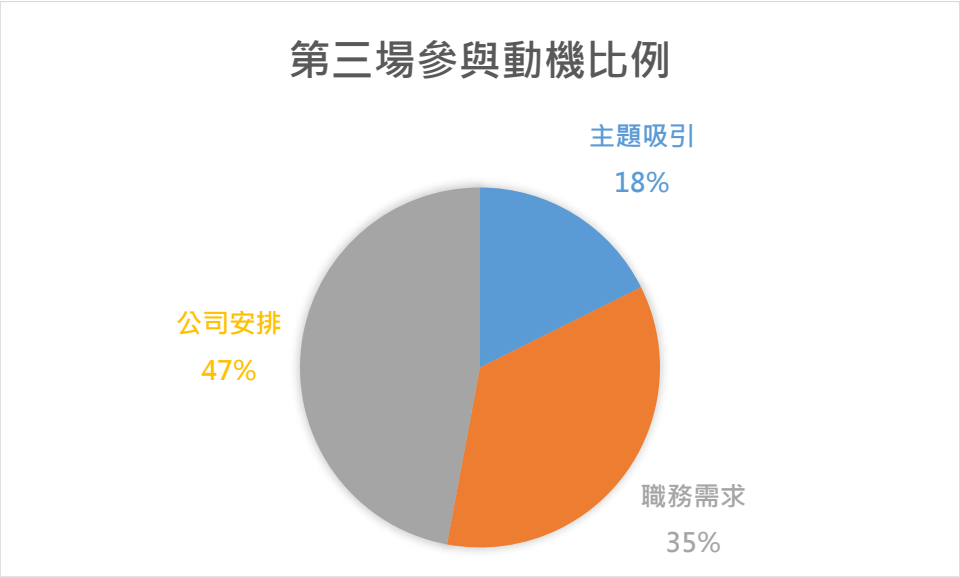
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 63 參與業者職務階層比例分布（109.09.30）

(4) 參訓業者參與動機比例分布



資料來源：本計畫製作

圖 64 參與業者職務階層比例分布（109.09.30）

（四)109 年 10 月 7 日：第四場次（台北特別場）

假集思台大會議中心舉行，總計 82 人報名，實到 55 人，相關課程剪影與說明如下：

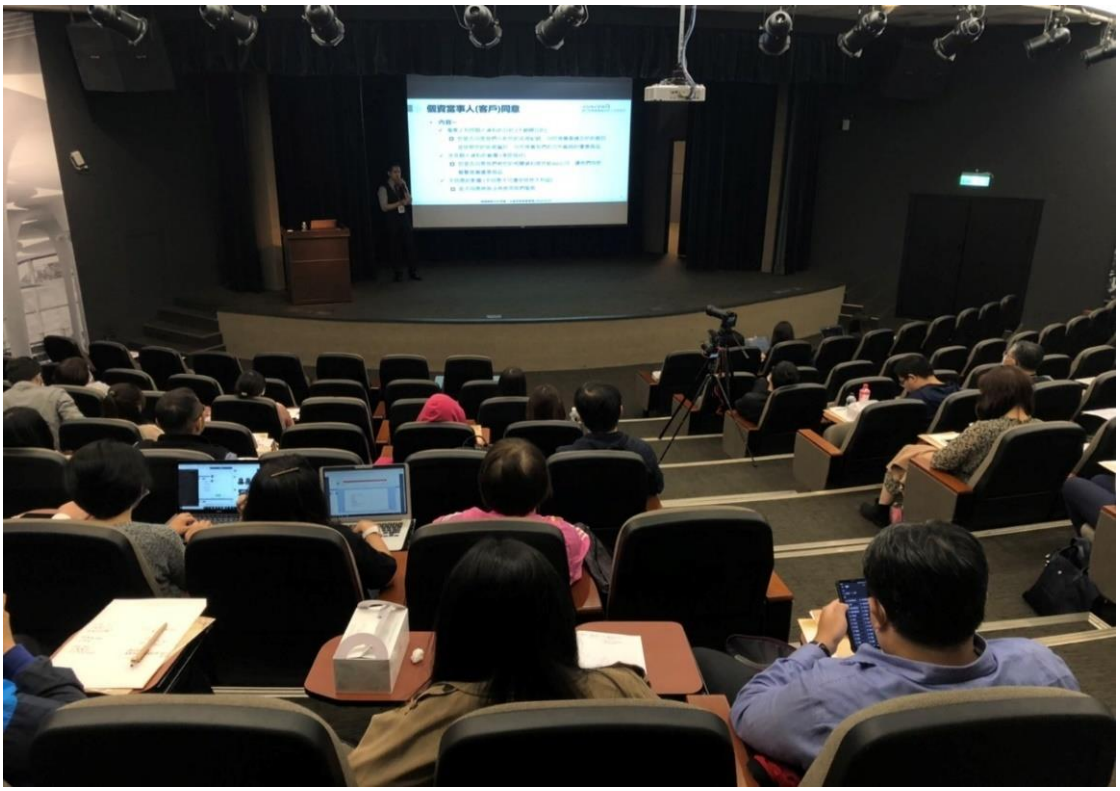
1. 現場課程剪影

資料來源：本計畫拍攝

圖 65 通傳會陳簡任視察書銘開場致詞（109.10.07）

資料來源：本計畫拍攝

圖 66 資策會服創所徐毓良副主任授課（109.10.07）



資料來源：本計畫拍攝

圖 67 達文西法律事務所王慕民合夥律師授課（109.10.07）

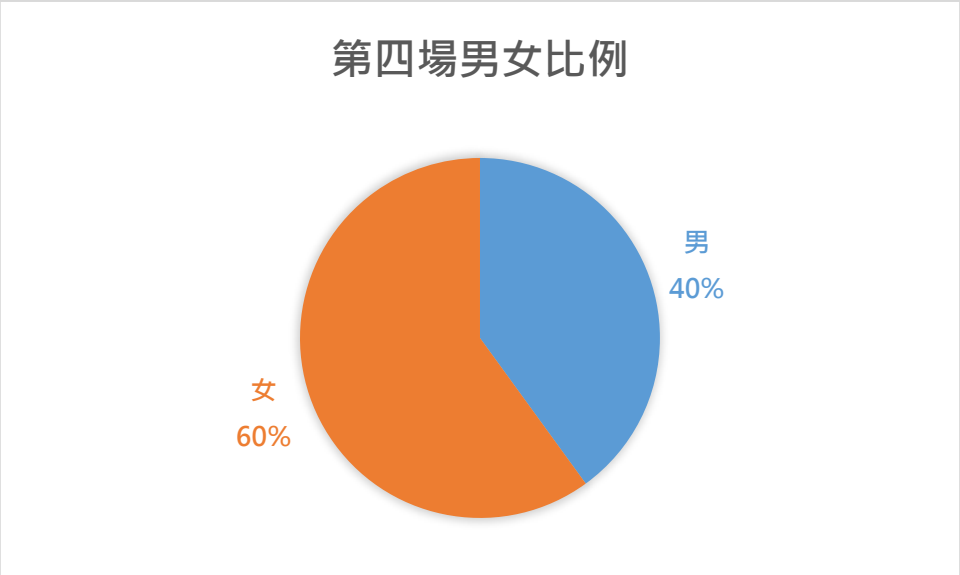
資料來源：本計畫拍攝

圖 68 中堂播放廉政宣導動畫（109.10.07）

2. 參與業者分析

本場次參與業者性別比例以女性居多，佔整體60%；行業別以傳播業為主，佔整體 59%；職務階層多為一般職員，佔整體 38%；參與動機則以職務需求、公司安排為主，各佔總體 38%、34%。分析圖表如下：

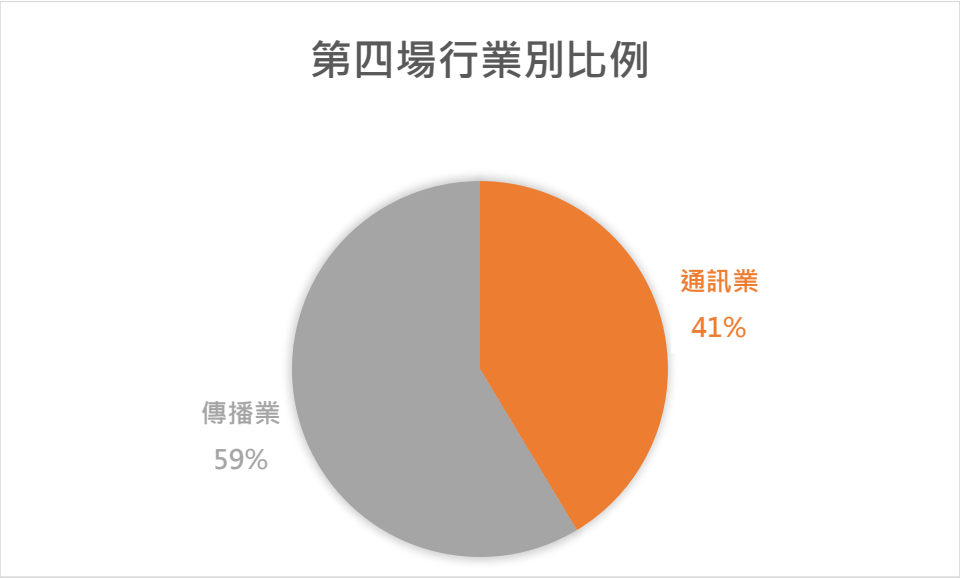
(1) 參訓業者性別比例分布



資料來源：本計畫製作

圖 69 參與業者性別比例分布（109.10.07）

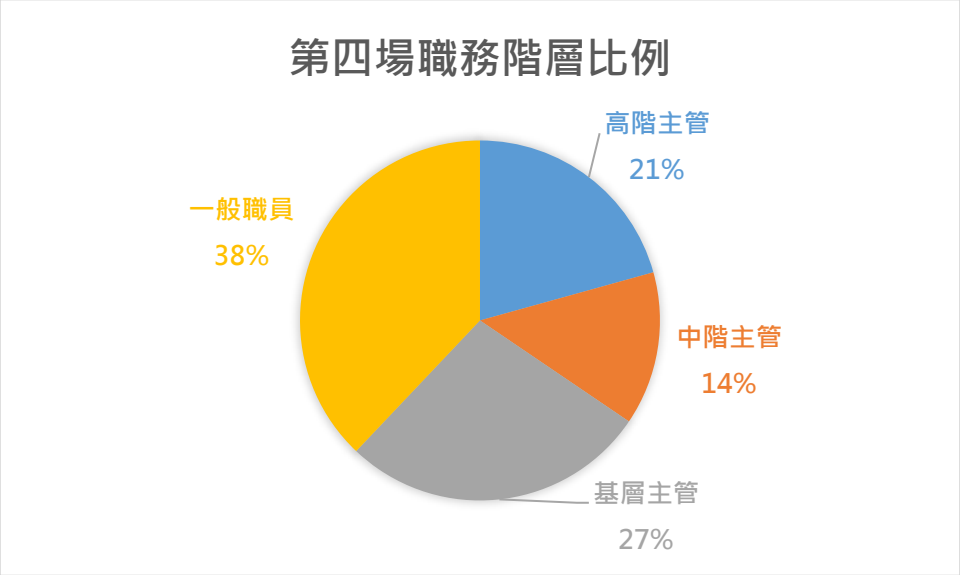
(2) 參訓業者行業別比例分布



資料來源：本計畫製作

圖 70 參與業者行業別比例分布（109.10.07）

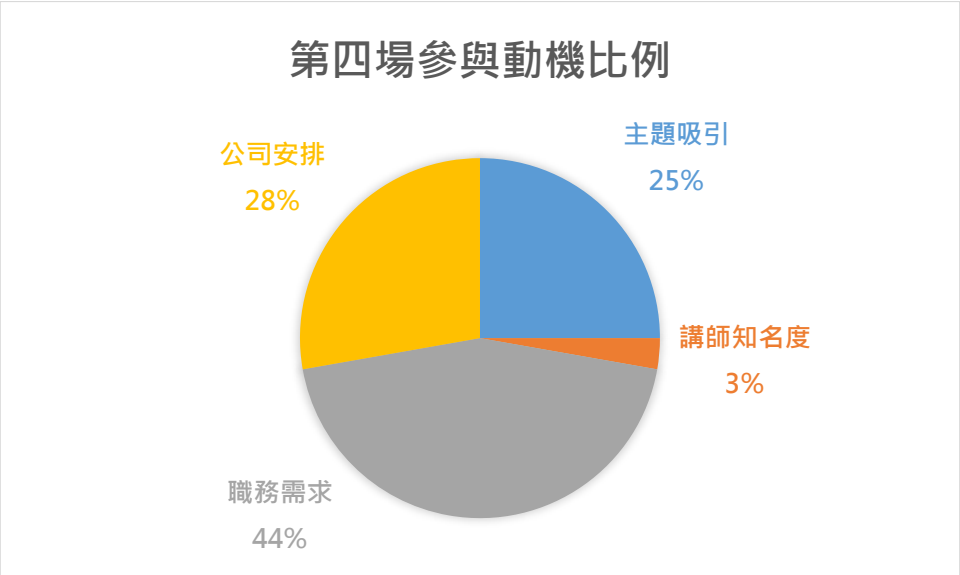
(3) 參訓業者職務階層比例分布



資料來源：本計畫製作

圖 71 參與業者職務階層比例分布（109.10.07）

(4) 參訓業者參與動機比例分布

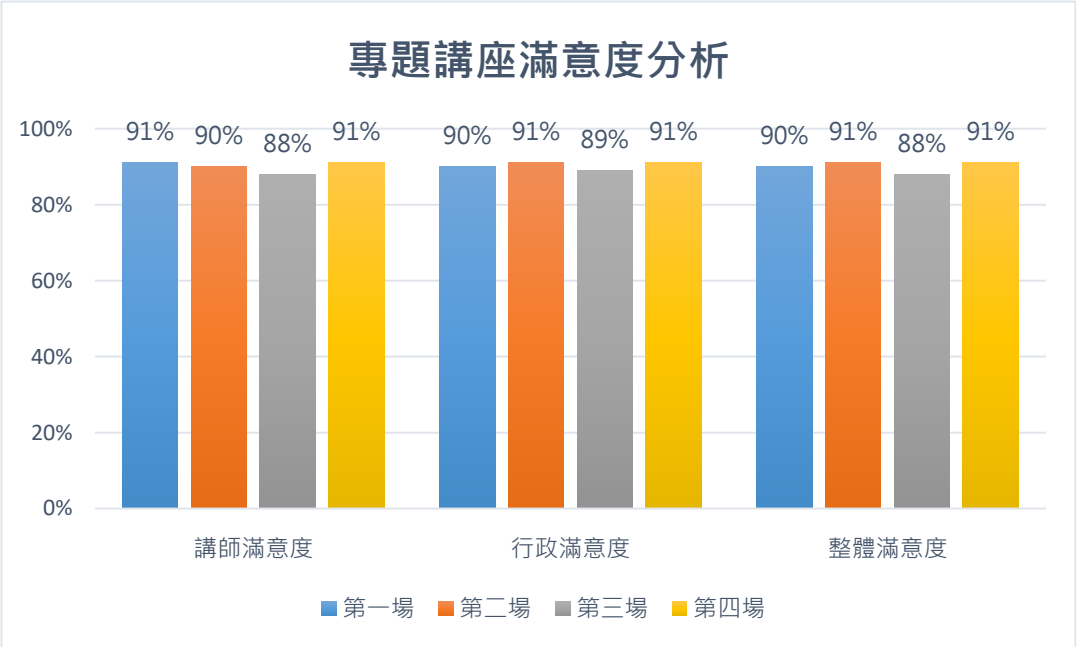


資料來源：本計畫製作

圖 72 參與業者職務階層比例分布（109.10.07）

第三節 成果統計

本案 4 場專題講座總報名人數為 305 人，實到總人數為 195 人，共回收 127 份問卷，其中有效問卷為 121 份，整體平均滿意度為 90%（計算方式為講師滿意度佔整體 50%、行政滿意度 50%）。茲將分析圖表及各場次學員回饋羅列如下：



資料來源：本計畫製作

圖 73 教育訓練滿意度分析圖

第四章 通傳產業法制諮詢、問答模擬題庫與參考手冊

第一節 通傳產業個資保護及資料創新運用法制諮詢

一、諮詢服務團隊

本案由達文西個資暨高科技法事務所所長葉奇鑫律師率同王慕民律師、吳彥欽律師及林廷憶法務助理，組成通訊傳播業務個資法律議題諮詢服務團隊，並特設諮詢服務電子郵件信箱 davinci-qa@davinci.idv.tw 及專線 02-3365-3437，供通傳會及通傳業者就通訊傳播業務涉及個人資料保護法適用與解釋之相關議題提出諮詢。

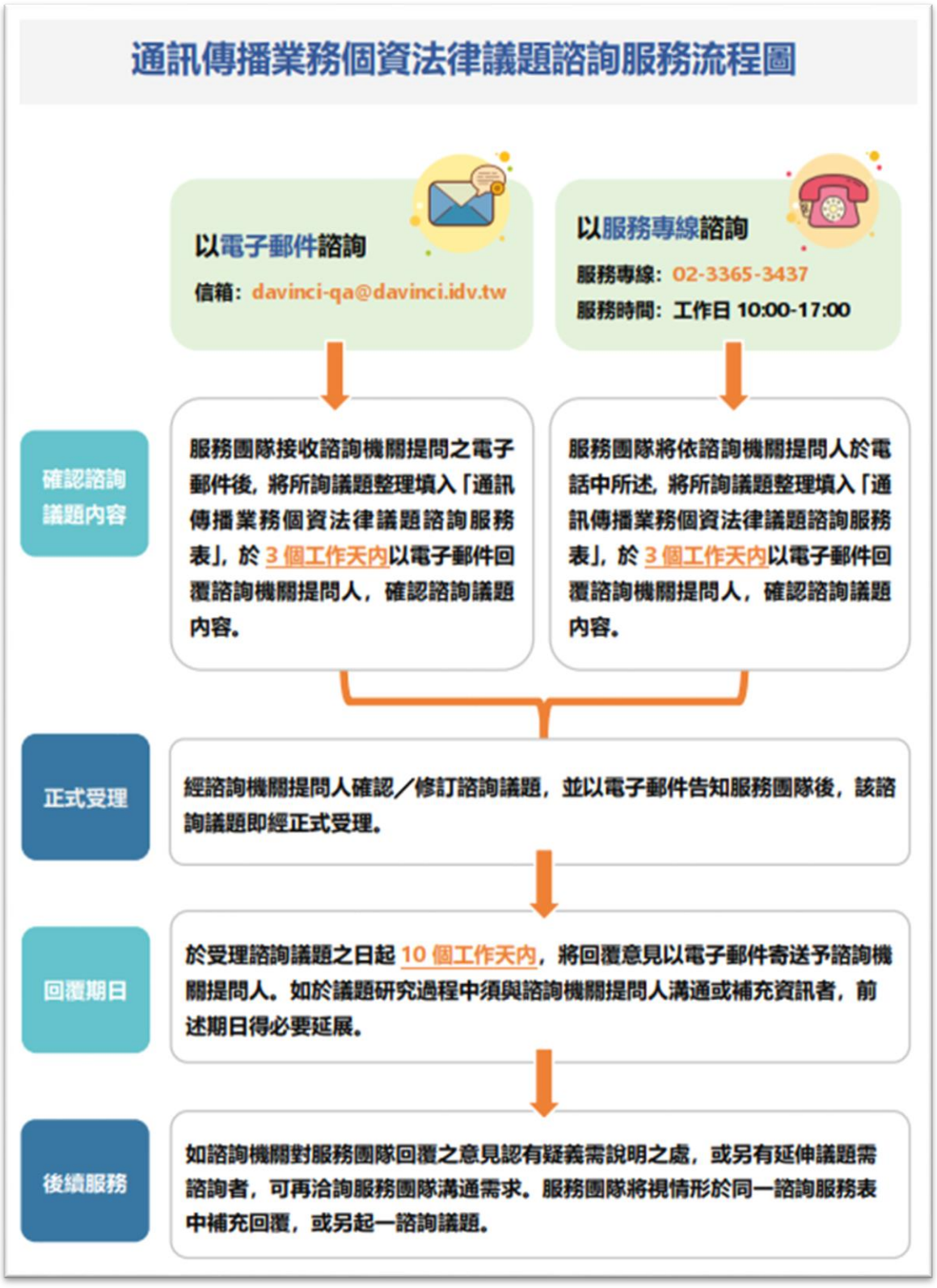
二、諮詢議題受理與回覆流程

（一）以**電子郵件**諮詢：

1. 服務團隊接收諮詢機關提問之電子郵件後，將所詢議題整理填入「通訊傳播業務個資法律議題諮詢服務表」，於 3 個工作天內以電子郵件回覆諮詢機關提問人，確認諮詢議題內容。
2. 經諮詢機關提問人確認/修訂諮詢議題，並以電子郵件告知服務團隊後，該諮詢議題即經正式受理。
3. 服務團隊將於受理諮詢議題之日起 10 個工作天內，將回覆意見填入「通訊傳播業務個資法律議題諮詢服務表」，以電子郵件寄送予諮詢機關提問人。如於議題研究過程中須與諮詢機關提問人溝通或補充資訊者，前述期日得必要延展。
4. 如諮詢機關對服務團隊回覆之意見認有疑義需說明之處，或另有延伸議題需諮詢者，可再洽詢服務團隊溝通需求。服務團隊將視情形於同一諮詢服務表中補充回覆，或另起一諮詢議題。

（二）以**服務專線**諮詢：

1. 諮詢機關提問人可於工作日上午 10 點至下午 5 點以服務專線進線，洽廖又萱法務提出諮詢議題。
2. 服務團隊將依諮詢機關提問人於電話中所述，將所詢議題整理填入「通訊傳播業務個資法律議題諮詢服務表」，於 3 個工作天內以電子郵件回覆諮詢機關提問人，確認諮詢議題內容。
3. 後續流程同前述 2 至 4。
4. 諮詢服務流程圖略表如下：



資料來源：本計畫製作

圖 74 通訊傳播業務個資法律議題諮詢服務流程圖

三、 諮詢議題彙整

（一）諮詢編號：109050003-001

諮詢機關	OOOO
聯絡人	OOO
單位／職稱	OOO
email	OOOO

諮詢議題：

本公司與客戶擬簽署契約，其中有關個人資料之約定為：「甲方如因○○○服務之執行而須蒐集、利用或處理乙方客戶、供應商、員工、經理人、董事或顧問之個人資料者（下稱個人資料），除應符合個人資料保護法之相關規定外，並應採取合理適當之安全保密措施。未經乙方事前書面同意，甲方不得再授權第三人蒐集、利用或處理個人資料。」就此約定於我國個人資料保護法上，是否有規範不足或範圍過大之疑慮，請貴事務所提供法律意見。

回覆意見：

一、按《個人資料保護法》第 27 條規定：「***非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。***」次按同法第 4 條規定：「***受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。***」

二、查　貴公司所提之諮詢議題係　貴公司與客戶簽定合作契約時，客戶特別要求　貴公司簽署一份「保密切結書」，其中有關個人資料之約定，若　貴公司受客戶委託執行之業務涉有蒐集、處理或利用客戶、供應商、員工、經理人、董事或顧問等個人資料，依前開《個資法》第 4 條規定，受委託機關即　貴公司之權利義務，視同委託機關，故　貴公司亦應符合《個資法》相關規定。

三、除　貴公司應依照前開《個資法》第 27 條規定，採取合理適當之安全保密措施（適當之安全措施），防止相關個人資料被竊取、竄改、毀損、滅失或洩漏之外，更約定了　貴公司若未經客戶同意，不得再將涉及個人資料之業務複委託予第三人，此亦符合《個資法施行細則》第 8 條第 2 項規範個資委外監督事項中關於複委託之約定。

四、準此，**客戶要求　貴公司所簽訂的「保密切結書」，其中有關個人資料之約定，均係依照前開《個資法》等相關規定所擬定，如　貴公司與客戶簽署該「保密切結書」則係於法有據。**若　貴公司與客戶間合作內容涉及個人資料者，建請　貴公司務必依照該「保密切結書」有關個人資料之約定辦理，必須遵守《個人資料保護法》相關規定，並採取適當安全維護措施，且在未經客戶同意前，不得將與個人資料有關之業務再複委託予第三人。

（二）諮詢編號：109050003-002

諮詢機關	OOOO
聯絡人	OOO
單位／職稱	OOO
email	OOOO

諮詢議題：

電信業者之法務人員於撰寫隱私權政策時，為避免疏漏，將經法務部公告之個人資料保護法特定目的中可能與其業務相關者，例如：○四○行銷、○六九契約、類似契約或其他法律關係事務、○七二政令宣導、○八一個人資料之合法交易業務、○八五旅外國人急難救助、○九○消費者、客戶管理與服務等，均列為其隱私權政策中之「特定目的」。

倘電信業者將所有經法務部公告之個資法特定目的，均列入該公司之個資告知聲明，是否符合個資法規範？

回覆意見：

一、 按個人資料保護法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」

二、 查電信業者為了提供客戶電信服務，與客戶成立電信服務契約，以個人資料保護法第 19 條第 1 項第 2 款的「與當事人有契約或類似契約之關係，且已採取適當之安全措施」作為蒐集個資的法律依據，則依此契約關係蒐集客戶個人資料之特定目的，即不應逸脫電信業者履行電信服務契約之範圍。

三、惟題旨所述，電信業者之法務人員於撰寫隱私權政策時，為避免疏漏，將經法務部公告之個人資料保護法特定目的中可能與其業務相關者都寫入隱私權政策，但題旨中諸如「○七二政令宣導」、「○八一個人資料之合法交易業務」、「○八五旅外國人急難救助」

等特定目的似均與電信業者履行電信服務契約無正當合理之關聯，如電信業者依據此等特定目的進而蒐集個人資料，將導致電信業者過度蒐集個資，逾越必要範圍，違反個人資料保護法第 5 條規定。

四、由此可知，倘電信業者主張將所有經法務部公告之個資法特定目的均列入公司個資告知聲明，並據此蒐集客戶之個人資料，此時電信業者將因過度蒐集個人資料，違反個人資料保護法第 5 條規定。

（三）諮詢編號：109050003-003

諮詢機關	OOOO
聯絡人	OOO
單位／職稱	OOO
email	OOOO

諮詢議題：

若本公司將個資予以可逆的擬匿名化，再提供給配合廠商，對廠商來說該資料無從直接或間接識別特定個人，但本公司得以重新識別，請問「本公司提供廠商可逆的擬匿名化資料」及「廠商處理、利用這些可逆的擬匿名化資料」等行為是否適用個資法規範？

回覆意見：

一、法務部（時為我國個資法解釋主管機關，現為國發會）103 年 11 月 17 日法律字第 10303513040 號函釋略以：「個人資料運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍。」由此可知，去識別化之個人資料因無法直接或間接識別特定人，不是個人資料，不適用個資法。

二、查貴公司將客戶個人資料以「可逆的擬匿名化」方式進行處理，實

務上較常稱為「假名化資料」(我國個資法雖未規定「假名化」之定義，但概念上仍得透過解釋個資法第 2 條第 4 款規定「編輯」之處理行為)。**假名化資料對貴公司而言，由於仍得以透過對照表或解密工具等與其他資料的對照、組合、連結，重新識別特定個人，因此仍屬個人資料，適用個資法規範。**

三、次查，若貴公司將該假名化資料提供予配合廠商，應區分廠商與貴公司之關係而區別認定：

1. **如配合廠商為「個資委外廠商」**

   依個資法第 4 條規定，委外廠商視同委託者，因此，針對「貴公司提供廠商可逆的擬匿名化(假名化)資料」及「廠商處理、利用這些可逆的擬匿名化(假名化)資料」等行為，貴公司須留意貴公司委託廠商利用資料之行為是否與蒐集目的相符，以符合個資法第 19 條、第 20 條規定，並應將資料進行可逆的擬匿名化(假名化)一事視為安全維護措施。

2. **如配合廠商為「合作廠商」(第三人)**

   (1) 可逆的擬匿名化(假名化)資料對貴公司而言仍屬個人資料，貴公司將該資料提供(利用)予第三人，仍應以個資法第 20 條檢視合法性。

   (2) 至貴公司諮詢題旨雖假定該可逆的擬匿名化(假名化)資料對廠商而言無從識別特定個人，但實務上，**假名化資料恐存有遭重新識別的風險，需視提供的資料具體內容而定。**舉例而言，如貴公司僅將客戶資料中如姓名、身分證號等身分識別資訊以假名化方式編碼，但仍保留其他屬性資料，例如性別、生日、地址、消費紀錄等，且未搭配其他去識別技術(例如抑制、隱匿、泛化、聚合等)，便提供予廠商，此作法在實務上其實不必然達到去識別化的效果，廠商如與自己保有之資料(欄位可能包含廠商消費者的性別、生

日、地址）比對，便有可能勾稽兩資料而識別特定個人。

(3) 因此，如貴公司提供合作廠商的資料僅單純假名化處理，未搭配其他去識別技術，該資料很有可能仍具識別性，即廠商的蒐集、處理與利用行為均應適用個資法規範。

（四）諮詢編號：109050003-004

諮詢機關	OOOO
聯絡人	OOO
單位／職稱	OOO
email	OOOO

諮詢議題：

公司因門號申裝業務蒐集用戶個人資料，假若因營業需要，擬將用戶的地址資料進行業務行為分析，如果已依據公司的內規進行管理與保護，是否有違個人資料管理法？在管理上有無特別需要留意之處？

回覆意見：

一、 貴公司蒐集用戶的個人資料，必須具備（正當的）蒐集目的，而貴公司分析用戶的地址，涉及「利用」個人資料的行為，依照個人資料保護法第 20 條第 1 項規定，原則上必須「與蒐集目的相符」才可合法利用（除非符合但書允許的例外事由之一）。至於判斷「蒐集目的」是否正當，則須視　貴公司「蒐集個人資料的法律依據」而定（個人資料保護法第 19 條）。

二、 依諮詢議題所示，如　貴公司因門號申裝業務蒐集用戶的個人資料，應是與用戶成立服務契約，即　貴公司是以個人資料保護法第 19 條第 1 項第 2 款規定的「與當事人有契約或類似契約之關係，且已採取適當之安全措施」，作為蒐集用戶個人資料的法律依據。在此契約關係下，貴公司對於用戶個人資料的「蒐集目的」應該與「履行該服務契約」有合理關聯，才能符合蒐集目的正當

性。

三、 目前除公務機關以「調查、統計與研究分析」作為其法定職務外，我國實務尚未對於「企業分析用戶個人資料之行為是否與『履行服務契約』有合理關聯而具備正當性」多所著墨。然而，如企業為市場調查、改善服務、作出商業決策等目的而內部分析用戶的個人資料，應可認為是為增進服務品質而與履行服務契約有合理關聯，且再輔以適當有效的安全維護措施，應不致對用戶的（資訊）隱私權產生額外風險，且亦不致超出用戶的合理隱私期待，則企業分析用戶個人資料的利用行為應與蒐集目的相符而合法。惟若企業分析用戶個人資料之目的是為對外提供資料給第三者，則此目的恐較難主張與「履行服務契約」有合理關聯，將逾越用戶的隱私期待，並對用戶的（資訊）隱私權造成額外風險。

四、 因此，諮詢議題所示行為是否合法，仍應視　貴公司分析用戶地址資料的具體目的而定，此與　貴公司是否依內規為管理與保護並無必然關聯（但採取適當的安全措施以管理與保護用戶資料，乃　貴公司於個人資料保護法規範下的法定義務）。

五、 此外，貴公司於最初向用戶蒐集個人資料時，也應留意須依個人資料保護法」第 8 條第 1 項規定，向用戶明確告知「蒐集個人資料之目的」(以及其他法定應揭露事項)。

六、 至如　貴公司有意對第三者提供用戶的個人資料，除依個人資料保護法第 20 條第 1 項但書檢視有無「目的外利用個人資料」的例外合法事由外（例如第 6 款的「經當事人同意」)，尚可評估可否使用各種技術（抑制、隱匿、泛化、聚合等)，將擬提供的資料有效的去識別化，以此不受個人資料保護法的拘束（例如提供統計數據，或將資料表內的姓名、身分證號等獨特識別符碼刪除，另遮蔽用戶地址中的門牌號碼，或僅模糊呈現用戶居住城市與行政區域等)。

（五）諮詢編號：109050003-005

諮詢機關	OOOO
聯絡人	OOO
單位／職稱	OOO
email	OOOO

諮詢議題：

請問隱私的定義?與個資法有關個人資料定義之差異為何?

回覆意見：

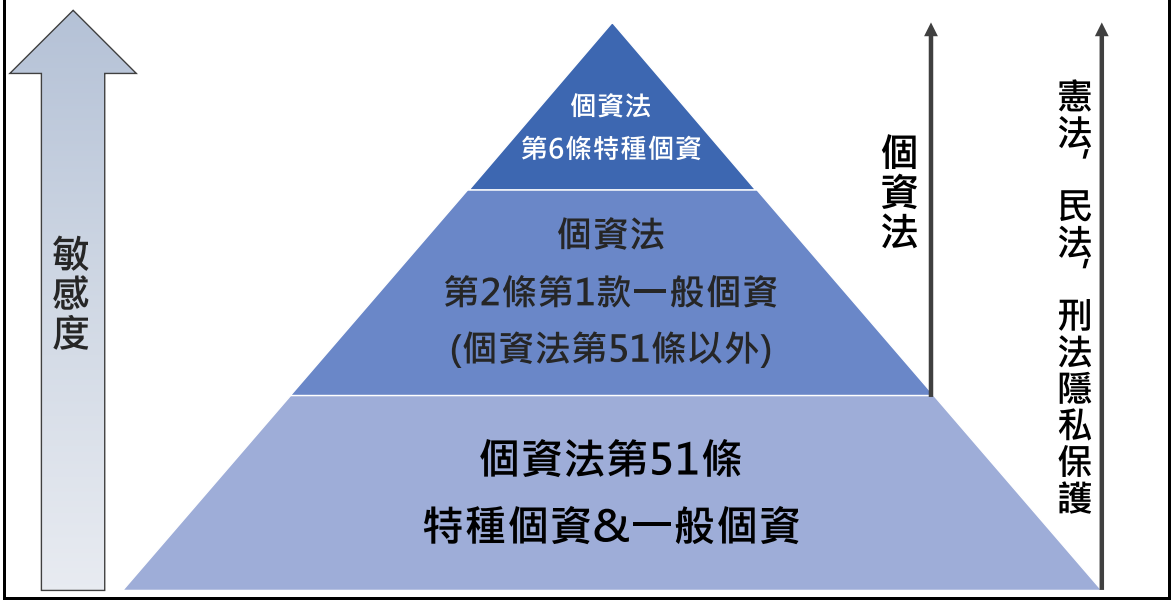
一、依照我國實務發展，一般認為「隱私」是指「私領域自主不受侵擾的狀態」，而「隱私權」則指個人於其私人生活事務領域，享有獨自權利，不受不法干擾，免於未經同意之知悉、公開妨礙或侵犯之權利（最高法院 106 年度台上字第 2674 號民事判決參照），即「保持私領域自主不受侵擾狀態的權利」。此項權利乃維護人性尊嚴、個人主體性、人格發展之完整所不可或缺，屬於憲法第 22 條所保障的自由權（司法院釋字第 585 號解釋參照）。此外，隱私權亦屬民法第 195 條所明文保護之人格權之一種。

二、如果依照隱私的內涵細部分類，可再略分為「身體隱私」、「空間隱私」、「通信隱私」、「資訊隱私」等類別，並由各種法律規範建構保護框架，例如刑法竊聽竊錄罪（保障身體隱私、通信隱私）、「刑法」侵入住居罪（保障空間隱私）等。

三、其中，「個人資料保護法」所保護者為資訊的隱私，即憲法所保護之隱私權，包括個人自主控制個人資料之資訊隱私權，也就是「人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」（司法院釋字第 603 號解釋參照）。由此可知，個人資料保護法第 2 條第 1 款所定義之「個人資

料」，乃作為「隱私」之下位概念受憲法保護。

四、從個資保護之視角釐清「隱私」與「個人資料」關係之實益在於，若「個人資料」因個人資料保護法第 51 條而被排除於該法適用範圍之外，仍可作為廣義之「隱私」而依民法、刑法等法律之有關規定而尋求保護與救濟，具體如下圖所示。



第二節 問答模擬題庫

一、 109 年 4 月模擬問答

問題(一)
A 有線電視業者在官方網站提供「留言版」功能，並將「姓名」、「電話」、「地址」等欄位加註*號，為留言者必填欄位。A 業者應如何確保「蒐集」個資行為符合《個人資料保護法》規範？
結論
一、A 業者應在網站留言版區塊的醒目位置揭露法定必要資訊（個資法第 8 條的應告知事項），或記載要旨並提供完整內容的網頁連結，以此滿足業者的告知義務，並取得留言者的知情同意。 二、此外，業者也應檢視所要求提供的資料有沒有超過蒐集目的之必要範圍，若該筆資料對蒐集目的之達成沒有幫助，業者列為必填欄位即可能構成逾越必要範圍的違法蒐集行為。
說明
一、業者蒐集留言者個資的法律依據應為「經當事人同意」 (一) 業者在官方網站留言版蒐集留言者的個人資料，首先須依《個人資料保護法（以下簡稱個資法）》第 19 條第 1 項檢視蒐集個資的法律依據。 (二) 由於「單純留言」與「線上申辦」不同，在後者情形，申辦人與業者間乃是「在契約成立前，為商議訂立契約之目的，所進行之接觸行為」，依照個資法施行細則第 27 條第 2 項第 1 款規定，雙方存有「類似契約之關係」，因此符合個資法第 19 條第 1 項第 2 款的要求，業者可主張「與當事人有類似契約之關係，且已採取適當之安全維護」作為蒐集個資的法律依據。 (三) 然而「單純留言」的留言者，因不是客戶，與業者間可能不存

在這樣的契約或類似契約關係。因此，業者較保險的作法應是在網站留言版區塊，利用適當的文字揭露以設計「知情同意」機制，主張個資法第 19 條第 1 項第 5 款「經當事人同意」為合法蒐集個資的依據。

二、合法的同意以揭露法定資訊為前提

(一) 依個資法第 7 條第 1 項規定，合法的同意是指「當事人經蒐集者告知個資法所定應告知事項後，所為允許的意思表示」。因此，業者要以「經當事人同意」作為蒐集留言者個資的法律依據，就必須在網站留言版區塊的醒目位置，以適當方式揭露個資法第 8 條第 1 項規定的「應告知事項」，包含：

1.A 業者名稱；

2.蒐集之目的；

3.個人資料之類別；

4.個人資料利用之期間、地區、對象及方式；

5.當事人依第三條規定得行使之權利及方式；

6.當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

(二) 雖然應告知事項項目繁多，但在「留言版」的背景下，由於蒐集目的理論上僅為「答覆留言事項」，利用個資的方式亦不複雜，因此以文字撰寫應不至於冗長而干擾使用者體驗。

(三) 如果業者以一份涵蓋全業務（包含網站留言版）的「隱私權政策（或類似名稱文件）」記載應告知事項，內容較為繁複，不便將其全文與留言板置於同一頁面，則依照個資法施行細則第 16 條規定，以「言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式」都是合法的告知方式，業者亦可選擇在留言版醒目位置記載應告知事項的要旨，並附上完整隱私權政策（或類似名稱文件）的連結，

供留言者點選閱讀。

三、若業者蒐集的資料超過必要範圍，仍然違法

(一) 依個資法第 5 條規定，個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

(二) 因此，縱使業者合法經留言者同意而蒐集個人資料，但若所蒐集的資料超過留言者同意的目的之必要範圍，仍然是違法蒐集個資的行為。

(三) 如果 A 業者蒐集留言者資料的目的是為「答覆留言事項」時，似乎只要蒐集留言者的姓名及電話即可達到目的，A 業者將「地址」欄位加上*號列為必填欄位，恐怕已經超過必要範圍。

問題(二)
未成年人向電信公司申辦手機門號，需檢附未成年人及法定代理人之雙證件，但未成年人身分證明文件可能是戶口名簿或戶籍謄本，其中含有第三人個人資料，電信公司能否蒐集這些文件？
結論
未成年人向電信公司申辦手機門號需檢附未成年人及法定代理人之雙證件，而未成年人身分證明文件可能是戶口名簿或戶籍謄本，其中雖涉及第三人的個人資料，惟為了維持該文件的真正性、完整性，且該文件是訂定電信契約所必要蒐集之資料，電信公司得蒐集含有第三人個人資料之戶口名簿或戶籍謄本。
說明
(一) 未成年人向電信公司申辦手機門號，電信公司蒐集未成年人及法定代理人之雙證件，應依照《個人資料保護法》第 19 條第 1 項第 2 款及第 20 條規定，在訂定電信契約的情形下，在電信業務之特定目的範圍內，蒐集必要的個人資料。

(二) 雖然過去並無函釋直接說明電信公司是否能蒐集未成年人及法定代理人之雙證件，但參照法務部 103 年 4 月 1 日法律決字第 10300058290 號有關保險理賠蒐集涉及第三人個人資料的函釋意旨，「當受益人申請身故保險金時，保險公司為了調查被保險人是否確實身故，因而蒐集被保險人之除戶戶籍謄本。雖然其中含有非客戶之其他戶籍成員的個人資料，但為維持該文件（戶籍謄本）之真正性、完整性，且該文件是保險理賠所必要蒐集之文件，因此受益人向保險公司申請身故保險金時，保險公司得蒐集涉及第三人個人資料之文件。」由此可知，**為維持文件之真正性、完整性，且該文件是履行契約所必要蒐集之文件時，契約相對人可以蒐集含有第三人個人資料之文件。**

(三) 因此，未成年人向電信公司申辦手機門號，需檢附未成年人及法定代理人之雙證件，而未成年人身分證明文件可能是戶口名簿或戶籍謄本，雖然涉及第三人的個人資料，惟參考前開函釋意旨，為了維持該文件的真正性、完整性，且該文件是未成年人訂定電信契約所必要蒐集之資料，電信公司得蒐集含有第三人個人資料之戶口名簿或戶籍謄本。

問題(三)
政府機關以「細胞廣播」方式同時發送訊息至特定區域內所有手機，是否符合個資法規範？
結論
政府機關以「細胞廣播」方式同時發送訊息至特定區域內所有手機，不需使用個人資料即可發送，故不適用個資法。
說明
(一) 政府機關透過「災害訊息廣播平台」發送「細胞廣播（Cell Broadcast）」訊息，經網路傳送我國行動通訊業者所建置之細

胞廣播控制中心（Cell Broadcast Center，CBC），再由業者於指定區域的基地台以細胞廣播的方式發送告警訊息，則基地台訊號涵蓋範圍內的手機用戶（終端設備）即可收到此告警訊息。

(二) 細胞廣播因不受行動網路流量限制，適合在緊急災害發生時對手機用戶進行通報，其優點簡要例示如下[1]：

1.可於短時間（10 秒內）對數百萬用戶發出告警訊息；

2.手機接收到告警訊息時，會發出特殊告警聲響、振動；

3.發送對象可涵蓋於特定區域範圍內的國際漫遊用戶；

4.告警訊息中可置入網頁連結，亦可更新前次訊息通報之情況；

5.不需個人資料，例如用戶身分或 MSISDN（Mobile Station International Subscriber Directory Number），即可發送。

(三) 綜上所述，政府機關以「細胞廣播」方式同時發送訊息至特定區域內所有手機，不需使用個人資料即可發送，故不適用個資法。

二、 109 年 5 月模擬問答

問題(一)
電信門市是否可量測來客之體溫？
結論
量測體溫為蒐集一般個人資料之行為，而維護員工及其他來客之健康安全，符合個資法第 19 條第 1 項第 6 款「為增進公共利益所必要」之要件，故電信門市可量測來客體溫。
說明
一、體溫是一般個人資料，非特種個資 電信門市量測所得之來客體溫，並非依照《個人資料保護

[1] 維基百科「Cell Broadcast」條目，網址：https://en.wikipedia.org/wiki/Cell_Broadcast

法施行細則》第 4 條第 5 項規定由醫事人員「以醫療行為施以檢查所產生之資料」，可知體溫非屬個資法第 6 條規定之「特種個資」，而是一般個人資料，合先敘明。

二、量測體溫屬蒐集個人資料之行為

量測體溫但不做成紀錄，是否屬《個人資料保護法》第 2 條第 3 款規定「以任何方式取得個人資料」之「蒐集」行為或有爭議。其他國家之個資保護主管機關如英國 ICO[2]、瑞士 FDPIC[3]、法國 CNIL[4]、比利時 DPA[5]等，於討論防疫措施之個資保護事宜時，均認定「量測體溫或詢問身體症狀」是蒐集個人資料，故本文亦認為量測體溫係屬蒐集個人資料之行為。

三、量測來客體溫屬「為增進公共利益所必要」，符合個資法規範

在防疫的迫切需求下，由於發燒為罹患新冠肺炎的症狀之一，而新冠病毒又具有極強大的傳染力，因此，為維護員工或是其他來客的健康安全，電信門市對來客量測體溫，可主張個資法第 19 條第 1 項第 6 款規定「為增進公共利益所必要」為法律依據。

四、此外，中央流行疫情指揮中心於近日（5/28）發布「實聯制措施指引」，為兼顧個資保護與疫調需求，電信門市如基於防疫目的蒐集民眾個人資料，應明確告知當事人包含蒐集機關、目的、個人資料項目、利用期間、利用對象及方式、當事人依個資法可請求的權益及不同意提供時的影響，並應指定專人辦理並善盡資料保護責任，最多存放 28 天，之後必須刪除或銷毀等，詳情請參閱衛生福利部疾病管制署網址：

[2] https://ico.org.uk/for-organisations/data-protection-and-coronavirus/，最後到訪為 2020 年 5 月 4 日。

[3] https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-216122139，最後到訪為 2020 年 5 月 4 日。

[4] https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles，最後到訪為 2020 年 5 月 4 日。

[5] https://www.autoriteprotectiondonnees.be/covid-19-et-traitement-de-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-sur-le-lieu-de-travail，最後到訪為 2020 年 4 月 1 日。

https://www.cdc.gov.tw/Bulletin/Detail/h4JHDHTxkceidB1NzV9EKA?typeid=9

問題(二)
傳播事業是否可調查員工之旅遊史、接觸史？
結論
傳播事業調查員工之旅遊史、接觸史等個人資料，符合個資法第 19 條第 1 項第 1 款或第 6 款之要件，且該調查仍應受個資法第 5 條必要範圍原則之限制。
說明
一、旅遊史或接觸史是個人資料 依照個資法第 2 條第 1 項規定，旅遊史或接觸史涉及員工的社會活動與家庭、社會關係，屬於員工的個人資料。傳播事業調查員工的旅遊史、接觸史，即是蒐集、處理個人資料的行為。 **二、調查員工之旅遊史、接觸史，符合個資法第 19 條第 1 項第 1 款或第 6 款之要件** (一) 傳播事業調查員工之旅遊史、接觸史，係依據勞動部職業安全衛生署按《職業安全衛生法》第 6 條第 3 項授權之《職業安全衛生設施規則》所發布的「因應嚴重特殊傳染性肺炎（武漢肺炎）職場安全衛生防護措施指引」第四點規定：「二、勞工應做好自主管理，保持手部清潔消毒，落實使用肥皂勤洗手、呼吸道衛生與咳嗽禮節、遵守社交禮節及保持社交距離，避免前往列為國際旅遊疫情建議等級第三級之地區旅遊、避免接觸野生動物。若出現發燒、咳嗽等身體不適，請速就醫，告知醫師旅遊史、職業史、接觸史及是否群聚，並主動告知雇主及配合各項防疫管制措施。」由此可知，傳播事業調查員工的旅遊史或接觸史，可能符合個資法第 19 條第 1 項第 1 款「法律明文規

定」之要件。

(二) 不過，有論者認為，勞動部職業安全衛生署所發布的「因應嚴重特殊傳染性肺炎（武漢肺炎）職場安全衛生防護措施指引」是行政指導，不是法律授權之法規命令，並不符合個資法第 19 條第 1 項第 1 款「法律明文規定」之要件，惟調查員工的旅遊史或接觸史可幫助傳播事業掌握工作場所的潛在病毒傳染風險，可據以辨別該員工是否違反居家隔離或居家檢疫的規定，對所有員工甚至是訪客的健康安全均有所助益，亦符合個資法第 19 條第 1 項第 6 款「為增進公共利益所必要」之要件。

三、調查員工之旅遊史、接觸史應受個資法第 5 條「必要範圍」的限制

此外，傳播事業調查員工的旅遊史或接觸史，仍應受個資法第 5 條「必要範圍」的限制，例如：中央流行疫情指揮中心曾於 4 月時公告建議「清明連假期間曾前往特定 11 處人潮擁擠景點旅遊之民眾」應進行 14 天的自主健康管理，傳播事業欲調查員工旅遊史時，僅需確認員工「有無」前往經指揮中心公告之特定景點旅遊，即可安排員工遠距工作，而無須再進一步詢問其同行旅客的年籍資料等，如此便能符合個資法第 5 條必要範圍之原則。

問題(三)
傳播事業如何確保遠距工作之資訊安全？
結論
建議傳播事業檢視現有資訊安全政策有無包含「遠距工作」項目，並可參照《個人資料保護法施行細則》第 12 條第 2 項規定及下述說明調整或訂定之。
說明

一、依照個資法第 27 條規定，維護個人資料的安全，是傳播事業的法定義務[6]。進行遠距工作時的個資或資安保護，對大部分傳播事業來說可能都是一項新挑戰，建議傳播事業可先檢視既有的資訊安全政策有無包含「遠距工作」項目，再視情形調整或訂定。

二、依《個人資料保護法施行細則》第 12 條第 2 項規定，傳播事業可採取 11 項適當安全維護措施[7]，本文參考澳洲資訊委員辦公室（Office of the Australian Information Commissioner, OAIC）「評估已改變的工作環境下的隱私風險：隱私衝擊評估（Assessing privacy risks in changed working environments: Privacy Impact Assessments）」之意見[8]，提供數點關於遠距工作的評估建議如下，完整建議內容請詳參網址 https://www.davinci.idv.tw/news/769：

(一) 組織治理：組織有無建立包含員工遠距工作的資安政策？（細則§12II（6）資安管理及人員管理）

(二) 資通訊安全：員工能夠使用私人裝置遠端存取系統嗎？組織針對這些私人裝置採取哪些技術上與程序上控管措施，以降低安全風險？（細則§12II（6）資安管理及人員管理）

(三) 存取安全：組織有無考量在員工的終端裝置內安裝遠端刪除程式，以便在裝置遺失或遭竊時刪除個人資料？（細則§12II（8）設備事故管理

[6] 請參《個人資料保護法》第 27 條第 1 項：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」。

[7] 請參《個人資料保護法》第 12 條第 2 項：「前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善」。

[8] 見澳洲資訊委員辦公室，https://www.oaic.gov.au/privacy/guidance-and-advice/assessing-privacy-risks-in-changed-working-environments-privacy-impact-assessments/，最後到訪為 2020 年 5 月 25 日。

(四) 安全管理：因應遠距工作的安排，現有計畫中有關通知事故或可疑事故的方式需要調整嗎？（細則§12II（11）個人資料安全維護之整體持續改善）

(五) 實體安全：組織是否考慮主動採取措施以確保員工家中有適當的實體安全維護（例如考慮以現場或遠端方式持續抽查員工家中環境，檢視員工的遠距工作環境安全）？（細則§12II（9）資料安全稽核機制）

三、 109 年 6 月模擬問答

問題(一)
中央流行疫情指揮中心以「類細胞簡訊」技術發送簡訊至特定手機（例如磐石艦確診案例足跡提醒簡訊），是否符合《個資法》規範？
結論
衛福部成立的中央流行疫情指揮中心以「類細胞簡訊」技術發送確診案例足跡提醒簡訊，係以「確診者停留點的周遭基地台」為基礎，請電信業者提供曾在同一時間和該基地台交換過訊號的手機號碼，以一般簡訊方式傳送警示訊息，此為執行衛福部的法定職務「預防或控制傳染病疫情的發生或蔓延」所須，未逾越必要範圍，其蒐集、處理個資的行為符合《個資法》第 15 條第 1 款「執行法定職務必要範圍內」，利用個資的行為符合同法第 16 條本文「於執行法定職務必要範圍內為之，並與蒐集之特定目的相符」等規定。
說明
一、行動電話號碼及位置資訊為個人資料。 (一) 行動電話號碼本身雖僅係一串數字組合，並無特定識別性，但一旦與其他個人資料如姓名、國民身分證統一編號、特徵及其他社會活動資料相互比對、組合、連結及勾稽結果，即得以間接方式識別特定自然人（臺灣臺北地方法院 103 年度北小字第

1360 號民事判決意旨參照），依照《個資法》第 2 條及《個人資料保護法之特定目的及個人資料之類別》規定，行動電話號碼為 C001 識別類之個人資料。

(二) 雖然「位置資訊」未明列於我國《個資法》第 2 條或法務部公告的《個人資料保護法之特定目的及個人資料之類別》之類別內，法院實務亦尚未對此表示意見。惟若藉由「位置資訊」（足跡）與其他資料進行連結、交叉、比對，而可能得以間接識別特定人，再參照歐盟 GDPR 第 4 條第 1 款規定[9]，亦明訂位置資訊（location data）是個人資料，是應將位置資訊認定為《個資法》第 2 條規定之個人資料為宜。

二、 中央流行疫情指揮中心蒐集、處理及利用民眾行動電話號碼及位置資訊係為執行法定職務所必要。

(一) 中央流行疫情指揮中心由衛生福利部成立，而無論依《傳染病防治法》或為本次新冠肺炎制定的《嚴重特殊傳染性肺炎防治及紓困振興特別條例》規定，「預防或控制傳染病疫情的發生或蔓延」當然為衛福部的法定職務[10]。

(二) 在題示情形，衛福部中央流行疫情指揮中心取得民眾的行動電話號碼及位置資訊以發送足跡通知簡訊，提醒民眾留意自身健康狀況，此手段有助於達成防疫目的（適當性）；而發送簡訊乃目前最快速、有效的提醒方式，在此範圍內僅取得行動電話號碼（不包含民眾其他個資如姓名、通訊地址等）與位置資訊（辨別需否發送提醒簡訊），乃對民眾最小侵害之手段（必要性）；且所追求防疫控制的重要性與發送簡訊之手段間也符合比例原則（衡平性）。

[9] 詳參國家發展委員會網站：https://www.ndc.gov.tw/Content_List.aspx?n=F98A8C27A0F54C30。

[10] 例如《傳染病防治法》第 7 條「主管機關應實施各項調查及有效預防措施，以防止傳染病發生；傳染病已發生或流行時，應儘速控制，防止其蔓延」，或《嚴重特殊傳染性肺炎防治及紓困振興特別條例》第 7 條「中央流行疫情指揮中心指揮官為防治控制疫情需要，得實施必要之應變處置或措施」。

(三) 因此，衛福部中央流行疫情指揮中心採用「類細胞簡訊」技術，向特定時間經過特定區域的民眾發送足跡提醒簡訊，其蒐集、處理個資的行為符合《個資法》第 15 條第 1 款「執行法定職務必要範圍內」，利用個資的行為符合同法第 16 條本文「於執行法定職務必要範圍內為之，並與蒐集之特定目的相符」等規定。

問題(二)
傳播事業如遇個人資料外洩等個資事故，是否應通報個資當事人或主管機關？
結論
傳播事業如遇個人資料外洩等個資事故，應依照《個資法》第 12 條、《個資法施行細則》第 22 條及《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 4 條等規定，以適當方式即時通知個資當事人，其通知之內容應包括「個人資料被侵害之事實」及「已採取之因應措施」；如個資事故情節重大，將危及傳播事業正常營運或大量當事人權益之情形時，應立即通報國家通訊傳播委員會。
說明
一、傳播事業如遇個人資料外洩等個資事故，應依照《個資法》第 12 條、《個資法施行細則》第 22 條及《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 4 條等規定履行法定義務。 二、依《個資法》第 12 條及《個資法施行細則》第 22 條規定，當傳播事業違法導致個人資料外洩等事故發生時，應在查明後以適當方式即時通知個資當事人，該「適當方式」包含以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使

當事人知悉或可得知悉之方式為之。通知的「內容」則應包含「個人資料被侵害之事實」及「已採取之因應措施」。

三、原則上，傳播事業應該「主動」、「個別」通知個資受侵害的當事人，避免個資當事人的損害發生或擴大(例如即時變更密碼、留意詐騙電話等)。但若主動個別通知將花費過鉅時（例如個資被侵害者的人數甚多)，傳播事業始得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

四、此外，如個資事故情節重大，將危及傳播事業正常營運或大量當事人權益之情形時，依照《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 4 條第 2 項及第 3 項規定，傳播事業應即通報國家通訊傳播委員會。

問題(三)
客戶向電信公司網路門市申請攜碼後又取消，電信公司應如何處理該客戶之個人資料始符合《個資法》規範？
結論
客戶於電信公司網路門市辦理攜碼後又申請取消，此時電信公司未能與客戶成立電信服務契約，該客戶所留存之個人資料，除有《個資法》第 11 條第 3 項但書規定之情形外，電信公司應主動或依當事人之請求刪除、停止處理或利用該等個人資料。
說明
一、按《個資法》第 11 條第 3 項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」。當客戶於網路門市辦理攜碼（NP）時，電信公司原依「經營電信業務與電信加值網路業務」等特

定目的，基於「與當事人有契約或類似契約之關係」向客戶蒐集、處理其個人資料（《個資法》第 19 條第 1 項第 2 款規定參照）。

二、惟若客戶又因故向電信公司取消辦理攜碼，導致該電信服務契約未成立，此時，電信公司為履行契約而蒐集個人資料之特定目的已不存在。

三、雖然過去並無函釋直接說明電信公司應如何處理未成立契約之客戶個人資料，但仍可參照法務部 104 年 9 月 7 日法律字第 10403509510 號及金融監督管理委員會 105 年 2 月 2 日金管保壽字第 10410938020 號等函釋意旨：「有關保險業因保險契約未成立或有其他未完成保險交易之因素，其所留存未承保保戶之個人資料，除有個人資料保護法第 11 條第 3 項但書規定之情形外，應主動或依當事人之請求刪除、停止處理或利用該等個人資料。」

四、由前開函釋意旨可知，若客戶因故取消辦理攜碼，導致該契約未成立時，電信公司因履行契約而蒐集個人資料之特定目的已不存在，準此，除有《個資法》第 11 條第 3 項但書規定（因執行職務或業務所必須或經當事人書面同意者）之情形外，電信公司應主動或依當事人之請求，刪除、停止處理或利用該等個人資料。

四、 109 年 7 月模擬問答

問題(一)
客服人員因與來電客戶發生爭執，竟將客戶的行動電話號碼於比價優惠網站上公開，請問該客服人員之行為有無違反個資法？雇主於個資法上有何責任？
結論

客服人員將來電客戶的行動電話號碼於網路上公開，可能違反《個資法》第 20 條第 1 項規定，構成目的外利用個人資料的違法行為。該客服人員的雇主為客戶個人資料的蒐集者，依《個資法》第 29 條第 1 項規定，將承擔損害賠償責任。

說明

一、行動電話號碼為個人資料。

(一) 有論者主張，行動電話號碼本身僅係一串數字組合，並無特定識別性，不是個人資料。

(二) 惟曾有法院實務認為，行動電話號碼雖然乍看之下僅為一連串之數字，但該號碼之持有人於當時僅有 1 人，對某特定人具有專屬性、獨特性，以其為憑據直接即可與該人連結而識別出特定個人[11]。

(三) 法院見解亦有認為，如將行動電話號碼與其他個人資料（例如：姓名、國民身分證統一編號、特徵及其他社會活動資料）相互比對、組合、連結及勾稽結果，即得以間接方式識別特定自然人[12]。

(四) 又我國個資法主要係參考歐盟 1995 年個人資料保護指令（下稱 95 指令）制定，關於個人資料之定義亦與 95 指令相仿。參考歐盟法院（CJEU）2016 年判決（Case C-582/14）亦明確指出，所稱「個人資料」，並未要求所有足使特定資料主體被識別之資料都必須由同一人掌握，例如保有動態 IP 位址（dynamic IP address）資料之服務提供者得以可能、合理之方式，透過其他網路服務提供者取得對照、組合之資料識別特定資料主體，即可認定動態 IP 位址屬於個人資料[13]。

(五) 準此，行動電話號碼應得以直接或間接方式識別該號碼使用

[11] 參照臺灣高等法院臺南分院 105 年上易字第 393 號刑事判決意旨。
[12] 參照臺灣臺北地方法院 103 年度北小字第 1360 號民事判決意旨。
[13] 參照國家發展委員會 109 年 7 月 24 日發法字第 1090015912 號函釋。

人，符合《個資法》第 2 條第 1 款對於個人資料之定義。（法務部公告之《個人資料保護法之特定目的及個人資料之類別》也將行動電話列為 C001 識別類之個人資料）

二、客服人員因與來電客戶發生爭執，將客戶的行動電話號碼於網路上公開，違反《個資法》第 20 條第 1 項「目的內利用個資」之規定。

(一) 客服人員蒐集來電客戶之行動電話號碼的特定目的應為「消費者、客戶管理與服務」，依《個資法》第 20 條第 1 項規定，除非符合該項但書的例外情形[14]，客服人員僅可在該特定目的之必要範圍內利用個人資料。

(二) 惟若客服人員因與來電客戶發生爭執，將客戶的行動電話號碼於網路上公開，此利用個資之行為顯已逾越上述蒐集客戶行動電話號碼的特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個資之行為，且應不符合任一例外情形。

三、客服人員的雇主為客戶個人資料的蒐集者，須承擔受雇人違法的民事損害賠償責任。

(一) 於題示情形，客服人員的雇主始為客戶個人資料的蒐集者，依《個資法》第 29 條第 1 項規定[15]，應由雇主對客戶承擔損害賠償責任。

(二) 惟如雇主能證明無故意或過失者，例如雇主已按《個資法》第 27 條規定採行「適當安全措施」，即同法施行細則第 12 條所規定，包括配置管理之人員及相當資源、資料安全管理及人員管理、認知宣導及教育訓練、設備安全管理、資料安全稽核機制

[14] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

[15] 個人資料保護法第 29 條第 1 項：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

等，則或可依《個資法》第 29 條第 1 項但書之規定而免責。

問題(二)
電信公司受保險公司委託，發送生日優惠權益簡訊予行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，請問電信公司有無違反個資法？
結論
電信公司受保險公司委託，發送生日優惠權益簡訊予行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，已逾越當初簽訂電信服務契約所載明之特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個人資料之行為。
說明
一、電信公司與行動電話用戶簽訂電信服務契約時，其蒐集、處理個人資料之特定目的為「經營電信業務與電信加值網路業務」，依《個資法》第 20 條第 1 項規定，除非符合該項但書的例外情形[16]，電信公司僅可在該特定目的之必要範圍內利用行動電話用戶之個人資料。 二、若電信公司受保險公司委託，發送生日優惠權益簡訊予行動電話用戶，並將回傳簡訊之行動電話號碼提供給保險公司，此利用個人資料之行為顯然已經逾越上述特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個資之行為，且應不符合任一例外情形。 三、實務上曾發生電信公司於電信服務契約所載之特定目的外，利用行動電話用戶之個人資料，且未經當事人同意，發送某保險

[16] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

公司之行銷簡訊，並將回傳簡訊之行動電話號碼提供給某保險公司，此舉被國家通訊傳播委員會認定違反《個資法》第 20 條第 1 項規定，並依同法第 47 條第 3 款及行政罰法第 25 條規定，分別核處罰鍰新臺幣 30 萬元、5 萬元，合計新臺幣 35 萬元[17]，併予敘明。

問題(三)
電信公司未將已離職員工之個人資料(聯絡方式)自工作群組移除，仍繼續寄送工作訊息予已離職員工，有無違反個資法？
結論
電信公司於員工離職後，應主動刪除或停止其個人資料之處理或利用，如電信公司繼續利用其個人資料寄送工作訊息，將違反《個資法》第 11 條第 3 項有關停止利用個資之規定，構成違法利用個人資料之行為。
說明
一、按《個資法》第 11 條第 3 項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」[18]。 二、因此，當員工離職時，電信公司除有《個資法》第 11 條第 3 項但書規定之情形外，應主動或依當事人之請求刪除、停止處理或利用其個人資料。 三、若電信公司於員工離職後，未將已離職員工之個人資料(例如：

[17] 詳參 104 年 9 月 23 日國家通訊傳播委員會第 662 次委員會議紀錄。

[18] 併參個人資料保護法施行細則第 20 條：「本法第 11 條第 3 項所稱特定目的消失，指下列各款情形之一：一、公務機關經裁撤或改組而無承受業務機關。二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。三、特定目的已達成而無繼續處理或利用之必要。四、其他事由足認該特定目的已無法達成或不存在」；第 21 條：「有下列各款情形之一者，屬於本法第 11 條第 3 項但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由」。

電話、E-mail 等）自工作群組移除，仍繼續寄送工作訊息予已離職員工，此時電信公司並無任何《個資法》第 11 條第 3 項但書所列之情形，顯已違反該規定。

四、實務上曾發生電信公司不慎利用已離職員工之個人資料分派工作等情事，國家通訊傳播委員會即認定違反《個資法》第 11 條第 3 項規定，並依照同法第 48 條第 2 項限期於 1 個月內改正並提報改善計畫[19]，併予敘明。

五、 109 年 8 月模擬問答

問題(一)
消費者於申辦電信門號前，欲得知未來提前解約時應返還之補貼款數額，電信業者便要求消費者先提供姓名、生日、身分證字號及雙證件影本等個人資料才能查詢，是否符合《個資法》規範？
結論
消費者於申辦電信門號前，欲得知未來提前解約時應返還之補貼款數額，惟電信業者要求先提供姓名、生日、身分證字號及雙證件影本等個人資料才能查詢，顯已逾越提供查詢所需之必要範圍，與《個資法》第 5 條規定之比例原則不符。
說明
四、《個資法》第 19 條第 1 項規定，非公務機關對個人資料之蒐集或處理應有特定目的，且應符合「與當事人有契約或類似契約之關係，且已採取適當之安全措施」等情形[20]。

[19] 詳參 107 年 8 月 15 日國家通訊傳播委員會第 817 次委員會議紀錄。

[20] 個人資料保護法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

五、消費者與電信業者間申辦電信門號程序尚未完成時，雙方顯然未成立契約關係，惟兩者間是否成立前述「類似契約關係」，應依照《個資法施行細則》第 27 條規定來判斷是否符合「契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為」或「契約因無效、撤銷、解除、終止而消滅或履行完成時，為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為」等情形[21]，而使業者得以蒐集、處理消費者之個資。

六、另按《個資法》第 5 條規定，個資之蒐集、處理或利用，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯[22]。故電信業者蒐集、處理或利用個資之行為，縱符合《個資法》規定，仍應留意「比例原則」之要求，不得逾越特定目的之必要範圍。

七、題示情形中，如消費者欲得知未來提前解約時應返還之補貼款數額，電信業者即要求消費者先提供姓名、生日、身分證字號及雙證件影本等詳細個資，方才協助查詢，而未提供前開個人資料，即無從得知「補貼款數額」。此時業者蒐集消費者個資之範圍，顯已逾越提供查詢所需之必要範圍，與《個資法》第 5 條規定之比例原則不符[23]。

問題(二)
電信業者接獲客戶對某通訊行之申訴後，將載有客戶個資之申訴單

[21] 個人資料保護法施行細則第 27 條：「本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者：一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。」

[22] 個人資料保護法第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」

[23] 法務部 106 年 08 月 24 日法律字第 10603511520 號函釋參照。

轉傳給與執行申訴業務無關之通訊行人員，是否違反個資法？
結論
電信業者將載有客戶個資之申訴單，傳送給與執行申訴業務無關之通訊行人員，違反《個資法》第 20 條第 1 項規定，構成目的外利用個人資料的違法行為。
說明
依《個資法》第 20 條第 1 項規定，電信業者於客訴流程中蒐集、處理客戶個人資料之特定目的為「消費者、客戶管理與服務」，除有符合該條項但書之例外情形外[24]，電信業者僅可於特定目的之必要範圍內利用客戶之個人資料。 題示情形中，電信業者收到客戶對某通訊行之客訴資料，應交由其負責客訴之承辦人員處理，相關個人資料不應提供給非負責處理申訴業務之人員。電信業者卻將客訴資料（包含客戶個人資料）轉傳給與執行申訴業務無關之通訊行人員，即已逾越上述特定目的，違反《個資法》第 20 條第 1 項規定，構成目的外利用個資之行為，且不符合該條項但書任一例外情形。 實務上，類似題示情形之案例，電信業者將載有客戶個資之申訴單，未經去識別化即傳送予被申訴之通訊行人員，因該通訊行人員並非該電信業者處理申訴業務之負責人員，曾被國家通訊傳播委員會認定違反《個資法》第 20 條第 1 項規定，並依同法第 47 條第 3 款核處罰鍰新臺幣 10 萬元[25]，併予敘明。

問題(三)

[24] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益。」

[25] 詳參 106 年 1 月 4 日國家通訊傳播委員會第 730 次委員會議紀錄。

傳播事業可否將客戶個人資料提供給印刷廠印製帳單？如何辦理委外監督？
結論
傳播業者委託印刷廠印製客戶帳單，此時印刷廠蒐集、處理及利用個資之行為，適用《個資法》第 4 條之規定，視同委託機關即傳播業者所為，傳播業者則應依《個資法施行細則》第 8 條規定，對印刷廠進行適當的委外監督。
說明
傳播業者委託印刷廠印製客戶帳單，將客戶個資提供予印刷廠，而印刷廠收受個人資料後加以處理、利用，依照《個資法》第 4 條規定[26]，視同委託機關（傳播業者）所為。 傳播業者應依《個資法施行細則》第 8 條規定第 1 項及第 2 項規定，對受託者（即印刷廠）為適當之委外監督，監督內容應至少包含下列事項: 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 受託者就第十二條第二項採取之措施（亦即適當安全維護措施）。 有複委託者，其約定之受託者。 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 委託機關如對受託者有保留指示者，其保留指示之事項。 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。 個資保護實務的「委外監督」，分為事前、事中及事後監督作業，分述如下： 事前監督：傳播業者與印刷廠簽訂委託契約時，應於委託契約中將「個資保護及委外監督條款」寫入合約，以要求印刷廠配合辦理，

[26] 《個資法》第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

此為委外監督之事前作業。

事中監督：傳播業者應依照《個資法施行細則》第 8 條第 3 項規定，定期依照前述監督內容確認印刷廠的執行情形，並將確認結果紀錄之，此為委外監督之事中（稽核）作業。

事後監督：當委託關係中止或解除時，傳播業者應確認印刷廠已將相關個人資料刪除、銷毀，或是已全數返還予傳播業者，避免個資有外洩風險，此為委外監督之事後作業。

另依《個資法施行細則》第 8 條第 4 項規定，印刷廠僅得於傳播業者指示之範圍內，蒐集、處理或利用個人資料，印刷廠若認傳播業者之指示有違法《個資法》等相關規定，應立即通知傳播業者。

倘印刷廠於受託範圍內違反《個資法》規定，導致個資當事人權益受損，若個資當事人向傳播業者求償，此時依照《個資法》第 4 條規定，受委託機關（印刷廠）之權利義務視同委託機關（傳播業者），故傳播業者須按《個資法》第 29 條第 1 項規定對個資當事人負損害賠償責任[27]，併此敘明。

六、 109 年 9 月模擬問答

問題(一)
電信業者為踐行我國個資法第 8 條課予的「告知義務」，在提供予電信服務客戶之隱私權政策中，揭露欲蒐集之個人資料包含「家庭情形」、「移民情形」、「旅行遷徙」、「職業」、「收入」等，如業者果真向電信服務客戶蒐集上述資料，是否符合個資法規範？
結論

[27] 個資法第 29 條第 1 項：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

電信業者向客戶蒐集「家庭情形」、「移民情形」、「旅行遷徙」、「職業」、「收入」等個人資料，與業者提供客戶電信服務之特定目的無正當合理關聯，可能構成過度蒐集個人資料，違反「個資法」第 5 條規定。
說明
個人資料保護法第 5 條規定:「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」 電信業者與客戶成立服務契約之特定目的是提供客戶電信服務，所欲蒐集之個人資料即應依前述規定，與「提供電信服務」之特定目的間有正當、合理之關聯。 若電信業者未取得客戶之「家庭情形」、「移民情形」、「旅行遷徙」、「職業」、「收入」等個人資料，仍然可以正常提供客戶電信服務，則上述個人資料即與電信業者提供客戶電信服務之特定目的無涉，缺乏正當、合理之關聯。 因此，前述之個人資料與電信業者提供電信服務之特定目的無正當合理關聯，過度蒐集個人資料，不符比例原則，違反「個資法」第 5 條規定。

問題(二)
電信業者主張「○六七信用卡、現金卡、轉帳卡或電子票證業務」、「一○七採購與供應管理」、「○八五旅外國人急難救助」、「一二七募款」為特定目的而蒐集電信服務客戶之個人資料，是否符合個資法規範？
結論
題旨所示「○六七信用卡、現金卡、轉帳卡或電子票證業務」、「一○七採購與供應管理」、「○八五旅外國人急難救助」、「一二七募款」等

目的似與電信業者提供客戶電信服務之契約無關，可能構成過度蒐集個人資料違反個資法第 5 條規定。
說明
依個人資料保護法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」 電信業者為了提供客戶電信服務，與客戶成立電信服務契約，以個資法第 19 條第 1 項第 2 款的「與當事人有契約或類似契約之關係，且已採取適當之安全措施」作為蒐集個資的法律依據，則依此契約關係作為蒐集客戶個人資料之特定目的，所蒐集之個資即不應逾越電信業者履行電信服務契約之範圍。 但題旨所述的「○六七信用卡、現金卡、轉帳卡或電子票證業務」、「一○七採購與供應管理」、「○八五旅外國人急難救助」、「一二七募款」等，屬於法務部訂定「個人資料保護法之特定目的及個人資料之類別」之特定目的，實務上常見記載於電信業者的隱私權政策中，但這些特定目的均與電信業者履行電信服務契約無正當合理之關聯。 因此，電信業者主張上述特定目的而蒐集客戶之個人資料，因與履行電信服務契約無關，將導致電信業者過度蒐集個資，不符合比例原則，違反個資法第 5 條規定。

問題(三)
電信業者員工違反公司資安規定，以未經公司核准之隨身碟存取公司電腦中的客戶個人資料，如因此發生個資侵害事故（例如使電腦中毒致客戶資料遭駭，或隨身碟遺失致客戶資料遭竊取），該電信業者是否違反個資法？
結論

電信業者員工以非公司核准之隨身碟存取公司電腦中之客戶個人資料致個資侵害事故發生，即便業者已制定資安規範禁止該行為，但若未採取其他實務上合理可行的措施避免該行為的發生，則仍有遭認定違反個資法第 27 條第 1 項規定，未對客戶個人資料採行適當之安全措施的可能。
說明
依個人資料保護法第 27 條第 1 項規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」因此，電信業者對其員工存取客戶個資之行為，應採行適當之安全措施，例如參考個資法施行細則第 12 條第 6 款「資料安全管理及人員管理」之措施，訂定使用公司之電腦設備所應遵循的資安相關規定。 然而，即便電信業者已制定資安規範，倘員工仍違反規定，使用未經核准之隨身碟儲存客戶個人資料，並因此造成個資侵害事故，此時無法直接認定業者是否已採行適當之安全措施。 如實務上有其他合理可行的措施，可在實作上避免此事故發生（例如業者封鎖員工電腦使用 USB、系統設定無法匯出客戶之個人資料、或在員工匯出客戶個資時，在系統出現提醒文字，告知員工務必循公司程序申請使用經核准的無惡意程式、加密隨身碟等），則業者不一定能僅以「已制定資安規範」來證明其已善盡適當安全維護的責任。

七、 109 年 10 月模擬問答

問題(一)
通傳業者員工發送電子報時違反公司資安規範，未將電子報以密件副本方式傳送予客戶，使所有收件人均得知其他收件人的電子郵件信箱，致個資侵害事故發生（如客戶電子郵件信箱資訊遭未經授權之不當利用），是否違反個資法？

結論
通傳業者員工未以密件副本方式將電子報發送至其眾多客戶電子郵件信箱，致個資侵害事故發生，即使業者已制定資安規範禁止該等行為，但未採取其他實務上合理可行之措施避免該等行為發生，則仍可能遭認定違反個資法第 27 條第 1 項規定，未對客戶個資採行適當安全維護措施。
說明
依個人資料保護法第 2 條之定義，通傳業者之客戶電子郵件信箱屬客戶個人之「聯絡方式」，因此屬於個人資料。 另依個資法第 27 條第 1 項規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」通傳業者以其保有之客戶電子郵件信箱資料發送電子報給客戶，即應採行適當之安全措施，例如參考「個資法施行細則」第 12 條第 2 項第 5 款規定，訂定個人資料如電子郵件信箱蒐集、處理及利用之內部管理程序。 然而，即便通傳業者已制定相關規範，其員工仍違反規定，於發送電子報時未將所有收件者均列為密件副本，並因此造成個資侵害事故，此時無法直接認定業者是否已採行適當之安全措施。 如實務上存有其他合理可行措施可避免此事故發生（如直接由系統設定於發送電子報時，所有收件者均須列於密件副本欄位方能寄出等），則業者不一定能僅以「已制定資安規範」來證明其已善盡適當安全維護的責任。

問題(二)
電信業者將客戶個人資料提供予資產管理公司催收欠費，是否違反個資法？
結論

電信業者委託資產管理公司對客戶催收欠費，將客戶個人資料（姓名、電話、欠費金額等）提供給資產管理公司進行催收，依個資法第 4 條規定，資產管理公司處理、利用個人資料之行為，均視同電信業者所為；且電信業者仍然是基於客戶管理、催繳欠費等特定目的之必要範圍內，將客戶個人資料提供給資產管理公司，符合個資法規範；電信業者亦應依個資法施行細則第 8 條規定對資產管理公司進行適當的委外監督及稽核 。
說明
依個資法第 4 條規定：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」因此，電信業者委託資產管理公司辦理催繳費用等，該資產管理公司即適用個人資料保護法規定，並視同委託機關（即電信業者）。 電信業者委託資產管理公司之行為，仍然是基於客戶管理、催繳費用之特定目的而提供欠費客戶個人資料給資產管理公司，由資產管理公司向客戶催繳欠費，應仍屬特定目的內利用個資行為，符合個資法第 20 條第 1 項本文規定。 電信業者亦應依照個資法施行細則第 8 條規定，對資產管理公司進行適當的委外監督，至少應於事前約定下列事項： (一) 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (二) 受託者就第十二條第二項採取之措施。 (三) 有複委託者，其約定之受託者。 (四) 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 (五) 委託機關如對受託者有保留指示者，其保留指示之事項。 (六) 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

此外，依個資法施行細則第 8 條第 3 項規定，電信業者應於委託期間定期確認資產管理公司執行之狀況，並將確認結果留下紀錄，以此落實委外監督責任。

問題(三)
電信業者致電予已表明拒絕行銷之客戶，推廣新電信資費方案，是否違反個資法？
結論
電信業者之客戶倘已明確表示拒絕電信業者電話行銷，電信業者應立即停止對其行銷，否則即違反個資法第 20 條第 2 項規定。
說明
依據個資法第 19 條、第 20 條規定，電信業者於「經營電信業務與電信加值網路業務」或「行銷」等特定目的之必要範圍內，得蒐集、處理或利用客戶個人資料。題旨所述業者致電客戶，是為推廣新的電信資費方案，此利用個資之行為符合「行銷」之特定目的。 但依個資法第 20 條第 2 項規定：「非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。」倘客戶事前已明確向電信業者表示拒絕業者利用其個人資料行銷，此時電信業者則應立即停止這樣的行銷行為，如業者仍致電該客戶推廣其新的電信資費方案，即違反前述規定。 此外，個資法第 20 條第 3 項亦規定：「非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。」因此，當電信業者第一次以電話方式向客戶推廣其產品或服務時，也應告知客戶其有拒絕行銷的權利及行使方式，並且代客戶支付行使權利的費用（例如提供免付費電話或提供回郵信封等）。

八、 109 年 11 月模擬問答

問題(一)

通傳業者員工於電話中蒐集首次申辦服務的客戶之個人資料，是否應踐行個資法規定的告知義務，向該客戶揭露業者蒐集個資的目的、利用個資的方式、當事人權利及其他法定應告知資訊？如何執行？
結論
通傳業者員工於電話中蒐集客戶的個人資料，應依個資法第 8 條規定，向客戶揭露法定應告知資訊。實務上可考量以播放錄音搭配分層告知的方式執行。
說明
一、依照個資法第 8 條規定，原則上通傳業者向客戶蒐集個人資料時，應明確告知下列資訊：「1.機關名稱。2.蒐集之目的。3.個人資料之類別。4.個人資料利用之期間、地區、對象及方式。5.當事人得行使之權利及方式。6.當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」此為個資法課予蒐集個資機關的法定告知義務。 二、又依照個資法施行細則第 16 條規定，上述資訊的「告知方式」包含「言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式」。 三、由以上規定可知，通傳業者履行告知義務的方式，只要足以使客戶知悉或可得而知應告知的內容即可，並沒有其他限制。 四、通傳業者透過電話蒐集個人資料時，實務上可由接線員工以口語敘述方式，向客戶說明應告知資訊。不過，完整的應告知資訊內容恐較繁複，通傳業者應可考慮採用播放錄音搭配分層告知的方式履行告知義務，即以預先錄音提供應告知資訊的簡要內容，並向客戶說明可以何種方式取得完整資訊，例如官網上的特定網頁、以簡訊將官網上載有完整應告知資訊的網址發送給客戶，或以電子郵件方式寄給客戶詳閱等，應均符合個資法

施行細則第 16 條規定。

問題(二)

通傳業者若將已終止服務契約之客戶資料永久保存，是否違反個資法？

結論

客戶終止服務契約，依照個資法第 11 條第 3 項規定，如通傳業者蒐集該客戶個人資料的特定目的已消失，即應主動或依客戶之請求，刪除、停止處理或利用該客戶的個人資料。

說明

一、個資法第 11 條第 3 項本文規定:「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料」。所謂「特定目的消失」，依照個資法施行細則第 20 條規定，是指下列情形之一:「1.公務機關經裁撤或改組而無承受業務機關。2.非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。3.特定目的已達成而無繼續處理或利用之必要。4.其他事由足認該特定目的已無法達成或不存在」。

二、通傳業者為「履行服務契約」或「履行法定義務」等特定目的蒐集客戶的個人資料，當客戶終止服務契約後，該特定目的可能已達成或已不存在（但若因客戶尚欠費未繳，應視為履行服務契約的特定目的仍存在），此時除非有個資法第 11 條第 3 項但書「因執行職務或業務所必需或經當事人書面同意」的情形，否則通傳業者即必須履行前述刪除個資的義務。此處所謂「因執行職務或業務所必須」，依照個資法施行細則第 21 條規定是指下列情形之一:「1.有法令規定或契約約定之保存期限。2.有理由足認刪除將侵害當事人值得保護之利益。3.其他不能刪除

之正當事由。」

三、實務上，通傳業者可能依照適用的法規不同，而對不同的個人資料負有保存一定期限的義務(例如依照電信事業用戶查詢通信紀錄及帳務紀錄作業辦法第 4 條規定，電信事業應將通信紀錄及帳務紀錄自紀錄發生時起保存至少一年，供用戶查詢)，不過，法規通常僅要求業者保存資料的最低期限，並未明定最長期限，以保留一定彈性。

四、因此，通傳業者在客戶終止服務契約後，若要繼續甚至永久保存客戶的個人資料，必須嚴格檢視是否有上述個資法第 11 條第 3 項但書和個資法施行細則第 21 條規定的例外情形。

五、然而，如果通傳業者考量系統內資料無法單筆刪除，或是需要分析客戶曾經留下的資料（紀錄）也可考慮以適當匿名技術對個人資料加工，讓保存的資料無法再用以識別特定客戶身分（包含業者自己也無法還原、識別)，以此達到去識別化的效果，該資料即不受個資法規範。

問題(三)
電信業者員工違反公司規定，於公司電腦安裝即時通訊軟體，傳送客戶雙證件影本等個人資料，致個資侵害事故發生（如不慎誤傳予友人導致客戶個資外洩)，該電信業者是否違反個資法？
結論
電信業者員工未經許可，於公司電腦自行安裝即時通訊軟體，並用以傳送客戶雙證件影本等個人資料，致個資侵害事故發生，即使業者已制定資安規範禁止該等行為，但未採取其他實務上合理可行之措施避免該等行為發生，則仍可能遭認定違反個資法第 27 條第 1 項規定，未對客戶資料採行適當安全措施。
說明

一、依照個資法第 27 條第 1 項規定，電信業者保有個人資料檔案，「應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」。個資法施行細則第 12 條第 2 項並提出 11 項安全措施，供業者參照執行。

二、因此，電信業者蒐集客戶雙證件影本等個人資料，即應採行適當之安全措施，例如參考個資法施行細則第 12 條第 2 項第 5 款規定，訂定個人資料蒐集、處理及利用的內部管理制度；或是依照第 6 款規定，訂定資料安全管理及人員管理程序；甚至依照第 8 款規定，訂定設備安全管理政策。

三、然而，即便電信業者已制定相關規範，若其員工仍違反規定，自行於電腦安裝即時通訊軟體，用以傳送客戶證件資料，並因此造成個資侵害，此時不一定可直接認定業者是否已採行適當之安全措施。如果實務上有其他合理可行措施可避免此事故發生（例如以系統設定限制電腦裝置使用者安裝軟體時，要求管理員權限，而一般員工無法自行安裝通訊軟體等），則業者不一定能僅以「已制定相關規範」來證明其已善盡適當安全維護之責。

第三節 通傳會處理通傳事業個資案例參考手冊

本團隊彙整通傳會自 107 年起至本案同委託案之成果資料、諮詢案例及問答模擬題庫，依照個資保護相關重要主題編寫「通傳事業個資案例參考手冊」，分為「個人資料定義」、「必要範圍」、「特定目的外利用」、「委外監督」、「告知義務」、「當事人權利」、「安全維護」、「事故通報」、「屆期刪除」9 篇，每篇均有相關法規及案例分析，共 25 題常見問題模擬題庫，供通傳會處理通傳產業個資案例參考，詳參附錄 1：通傳會處理通傳事業個資案例參考手冊。

第五章 通傳產業個人資料保護與管理實作指引手冊

第一節 手冊編撰執行及方式

一、 手冊目的

為協助我國通傳事業業者，有效建置個人資料保護法與管理制度，避免個資事故之發生，進而導致通傳事業用戶個人資料外洩，當事人受損害例如電信詐騙之情形。同時考量訪查過程中發現業者對於法令認識不足，實務上更無法依循個資法遵之要求，對於如何建置個人資料保護與管理制度仍有其盲點，其於鑑別個資風險或處理個資事故之基本程序仍有待精進之需求，本計畫依據我國個資法通傳產業相關規範，編寫與設計「通傳產業個人資料保護與管理實作指引手冊」。

二、 手冊內容

手冊主要參考範圍包含：第一，我國個人資料法制相關規定（包含個人資料保護法、個人資料保護法施行細則、國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法及法務部、國家發展委員會歷年函釋）。第二，我國常見個人資料管理標準（包含國家標準29100、台灣個人資料保護與管理制度 TPIPAS、英國標準協會BS10012 等）。第三，本研究案例年訪查實例。以及我國個人資料保護管理制度專書等內容。計畫執行團隊以自身多年來執行個人資料法制研究及個人資料保護管理制度建制及驗證經驗，綜合上述資料撰擬指引手冊。希望藉由實做指引手冊，能協助通訊傳播業者建立自身個資管理制度，完善個人資料之管理。

本手冊編纂方式，係以我國個人資料保護法及一般個人資料管理制度常見之「PDCA 方法論」為基礎。協助業者從個人資料保護之計畫、執行、檢討、改進與計畫終止等不同階段，完善個人資料管理制度。具體內容區分為以下六個部份：第一、前言；第二、個資安全維護系統建置；第三、Plan—規劃與建置；第四、Do—執行與落實；第

五、Check and Action—查核與改進；第六、End—使用目的不存在之後該怎做；第七、附錄與參考文獻。

手冊內容特別針對個人資料保護法、個人資料保護法施行細則及國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法三份規範中皆有觸及的「適當安全維護措施」加以說明。為了使得者以實務操作解度閱讀能更容易理解，手冊中將適當安全維護措施的11 項要素分別內入 PDCA 個階段，並在 PDCA 的個階段下進一步以執行時序方式排列，適當安全維護措施要素區分為四個步驟：第一步驟：配置適當的管理人員及資源；第二步驟：界定個人資料檔案盤點的範圍；第三步驟：建立個人資料風險評估及管理機制；第四步驟：訂定個人資料安全維護規定。藉由具操作順序性的內容安排，白話的文字說明，佐以案例及注意事項提醒，讓使用者易讀易懂易操作，以達協助業者落實個資管理規範之目的。

詳細內容請參考附錄 2：通傳產業個人資料保護與管理實作指引手冊。

第二節 手冊印刷發送執行情況

手冊於 10 月中旬由計畫團隊完成手冊書稿內容後，及交付廠商進行編輯印刷，編輯過程中歷經二次校稿修正，最終如期於 11 月 10 日研討會前完成手冊 500 本印製，並於研討會上發送給參與之廠商及相關從業人員。研討會當天共發送手冊 187 本，相關佐證詳參手冊領取名單。計畫結案交付之手冊本數為 313 本。

一、 手冊印製時程

表 3 手冊印製時程

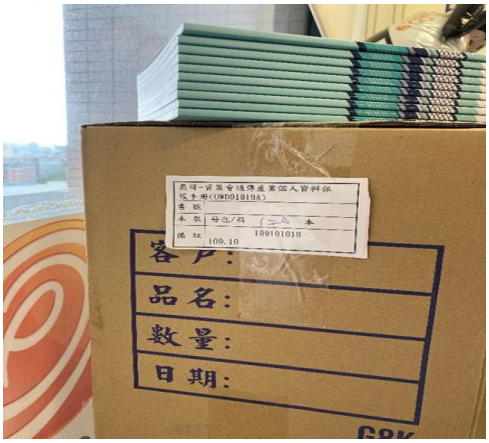
		一	二	三	四	五	六	日
		10/5	10/6	10/7	10/8	10/9	10/10	10/11
Week 1	科法			進稿		國慶日		
	奧得				編排設計	編排設計(加班)	編排設計(加班)	編排設計(加班)
		10/12	10/13	10/14	10/15	10/16	10/17	10/18
Week 2	科法		一校	一校			二校	二校
	奧得	編排設計			修改	修改		
		10/19	10/20	10/21	10/22	10/23	10/24	10/25
Week 3	科法		定稿	數位樣確認				
	奧得	修改	數位樣製作	製版	印刷製作	印刷製作	印刷製作(加班)	印刷製作(加班)
		10/26	10/27	10/28	10/29	10/30	10/31	11/1
Week 4	科法							
	奧得	印刷製作	印刷製作	印刷製作	交貨			

資料來源：本計畫製作

二、 手冊交付

資料來源：本計畫拍攝

圖 75 手冊交貨總量紀錄



資料來源：本計畫拍攝

圖 76 手冊交貨紀錄

三、 手冊領取名單

詳參附錄 3 領取名單（同研討會簽到表，共 19 頁）。

第六章 通傳事業輔導訪查（談）作業

第一節 輔導訪查（談）

一、 執行內容及方式

（一）五大電信業者

1. 門市抽查及當事人權利行使抽查（各業者 2 小時）

為確保電信業者有效將個資管理措施落實予所營門市，本團隊將以秘密客方式對 5 大電信業者門市抽查，確認門市人員是否於業務流程確實履行個資法中的告知義務，向消費者揭露法定應告知資訊。

另本團隊亦將以秘密客方式向 5 大電信業者分別行使個資法中的當事人權利（例如查閱個資、申請複製本，或請求停止利用行銷、請求刪除等），確認輔導對象是否依法准駁消費者行使之權利。

2. 實地訪查（各業者 6 小時）

本團隊將與 5 大電信業者個別安排一日實地訪查，訪查內容包含：

(1) 秘密客抽查結果說明

由本團隊向輔導對象說明前項秘密客執行門市抽查與當事人權利行使抽查之結果，並請輔導對象提供意見或持續追蹤（如有不足之處）。

(2) 108 年輔導訪查改善結果檢視

本團隊將按本案於 108 年對個別電信業者針對個資管理制度的輔導訪查發現，彙整對應之訪查項目表，於實地訪談期日兩周前寄送予輔導對象聯絡人供先行備妥改善說明與證據，並於訪查當日提出，供本團隊確

認具體現況。

(3) 產品／業務個資適法性訪查

本年度實地訪查注重特定產品／業務的個資適法性，本團隊將與委託機關與輔導對象事前取得共識，擇定輔導對象涉及使用者個資或隱私之重要產品／業務作為訪談標的（例如 5G 產品、智慧家庭物聯網服務、行動應用程式 app、委外業務等），並於實地訪談期日兩周前將對應之訪查項目表寄送予輔導對象聯絡人供先行準備，於訪查當日由本團隊訪查人員確認標的之個資適法性，確保輔導對象的說、寫、做一致性。

（二）MSO 與有線電視業者

1. 個資蒐集告知聲明範本與同意方式說明（各業者 2 小時）

本團隊將以輔導訪談方式，邀集 5 大有線電視多系統經營管理業者出席會議，由本團隊說明個資蒐集告知聲明範本內容，以及有線電視業者取得當事人同意蒐集、利用個人資料之實務做法參考。

2. 實地訪查（各業者 6 小時）

本團隊將與 5 大有線電視多系統經營管理業者個別安排一日實地訪查，訪查內容包含：

(1) 108 年輔導訪查改善結果檢視

本團隊將按本案於 108 年對個別有線電視多系統經營管理業者針對個資管理制度的輔導訪查發現，彙整對應之訪查項目表，於實地訪談期日兩周前寄送予輔導對象聯絡人供先行備妥改善說明與證據，並於訪查當日提出，供本團隊確認具體現況。

(2) 委外業務訪查

有線電視多系統經營管理業者與地方有線電視業者間，就寬頻業務消費者資料具有委託（共享）之關係，涉及個人資料之委外蒐集、處理與利用。本年度訪查將著重委外業務之控管，並將事前與委託機關與輔導對象協調，將實地訪查安排於受託之有線電視業者處所，以利實地訪查。本團隊將實地訪談期日兩周前將對應之訪查項目表寄送予輔導對象聯絡人供先行準備。

（三）新增輔導對象

本案新增 5 間輔導對象，由委託機關於獨立系統有線電視業者、電視購物頻道業者、廣播電台業者中擇定。另由於為首次輔導，訪查（談）內容宜包含：

1. 個資蒐集告知聲明範本與同意方式說明（各業者 2 小時）

可與前述 5 大有線電視多系統經營管理業者會議合併，由本團隊說明個資蒐集告知聲明範本內容，以及業者取得當事人同意蒐集、利用個人資料之實務做法參考。

2. 告知聲明檢視／管理制度訪查（各業者 6 小時）

本團隊將與輔導對象安排一日實地訪查（談），首先檢視輔導對象現有個資告知聲明於法律上的完整度，並提出建議；再依輔導對象事前填寫回覆之個資保護管理制度自評表，搭配所提出之證據逐一訪查個資保護之成熟度。

二、 輔導訪查對象

本年度將執行 15 家次業者（包含 5 間電信事業、5 間有線電視事業、5 間電視購物頻道事業）的輔導訪查（談）報告與紀錄（依委託單位規劃，於各別報告或紀錄中隱匿受訪對象之識別資訊）。

三、 執行流程與期日

（一）說明會議

於本工作項規劃書奉核後，本團隊於 7 月 9 日、7 月 10 日舉辦輔導訪查（談）說明會議，第一場邀集 5 大電信業者出席，第二場邀集 5 大有線電視多系統經營管理業者及本年度新增輔導對象出席，本團隊除說明輔導訪查（談）執行方式外，亦一併說明個資蒐集告知聲明範本內容，以及業者取得當事人同意蒐集、利用個人資料之實務做法。

（二）約定期日

本團隊已分別與受訪對象約定實地訪查（談）期日，為預留本團隊秘密抽查及個別製作訪查項目表時間，是規劃於自 7 月份末周開始，以每周 1 至 2 間業者輔導之進度安排，於期中報告前至少依約完成 7 間業者的輔導訪查（談）。

（三）訪查項目表

本團隊將依前述說明，於實地訪查（談）個別輔導對象期日兩周前，提供訪查項目表供輔導對象先行準備，並於當日按所列項目執行訪查，確認輔導對象的說、寫、做一致性。

表 4 訪查項目表

國家通訊傳播委員會 109 年度通傳事業個資保護輔導訪查 查檢項目表		受訪業者： 受訪日期： 受訪地點： 受訪業務：
編號	查檢內容	法律依據&原則
查檢項目 1：個人資料背景		
1.1	受訪業務有哪些蒐集個人資料的	N/A

	管道（方式）？例如門市、網站、電話、APP 等。	
1.2	受訪業務蒐集哪些個人資料？除當事人在契約（或申請文件）上填寫之資料，以及申辦業務當下自行提供的資料之外，是否將來在當事人使用該服務的過程中仍另外蒐集其他資料？例如電信服務取得使用者位置資訊、有線電視服務取得使用者收視紀錄、電視購物服務取得使用者瀏覽商品紀錄等。	個資法第 5 條、第 6 條 & 公平性、必要性、正當合理、特種個資限制
查檢項目 2：蒐集&處理個人資料的合法性		
2.1	受訪業務蒐集、處理個人資料之特定目的為何？	個資法第 19 條第 1 項
2.2	受訪業務蒐集、處理個人資料的法律依據為何？例如基於契約關係、當事人同意等。	個資法第 6 條（特種個資）、第 19 條第 1 項
2.3	如受訪業務蒐集、處理個人資料之法律依據為「與當事人間有契約或類似契約關係」，受訪業務蒐集個人資料之特定目的是否與該契約間有正當合理關聯？	個資法第 5 條 & 正當合理關聯
2.4	如受訪業務蒐集、處理個人資料之法律依據為「經當事人同意」： 2.4.1取得同意之方式為何？ 2.4.2可否針對不同目的分別表示同意？ 2.4.3當事人得以何種方式撤回同意？是否與取得同意之方式相同簡易？	個資法第 7 條第 1 項、第 3 項、第 4 項 & 知情同意
2.5	是否依個別蒐集個人資料的管道（方式），明確向當事人揭露個資法規定之必要資訊？揭露方式為	個資法第 8 條、第 9 條 & 透明性

	何？		
2.6	經由受訪業務所取得之個人資料，除供受訪業務使用之外，是否提供公司內其他業務（人員）存取使用或內部傳輸給其他業務同仁？如有，該其他業務之目的為何？是否與蒐集個人資料之目的相符？		個資法第 6 條（特種個資）、第 19 條第 1 項
查檢項目 3：利用個人資料的合法性			
3.1	受訪業務是否將個人資料提供予公司以外之第三方，或以任何方式供第三方存取？如有：		N/A
	3.1.1	目的為何？是否與受訪業務取得當事人個人資料之目的相符？如不相符，公司合法於目的外利用個人資料之法律依據為何？	個資法第 20 條第 1 項本文、但書 & 目的限制
	3.1.2	如公司以「經當事人同意」作為目的外利用個人資料之法律依據，是否明確向當事人告知新目的、利用資料範圍及不同意的影響後，取得當事人同意？同意之方式為何？可否撤回同意？撤回之方式為何？	個資法第 7 條第 2 項 & 知情同意
	3.1.3	公司與該第三方之關係為何？以何種方式確保該第三方合法蒐集、利用當事人之個人資料（包含該第三方應依個資法第 9 條規定，向當事人揭露法定資訊）？如何約定雙方權利義務？	個資法第 20 條第 1 項本文、但書 & 目的限制
3.2	受訪業務是否需要將當事人之個人資料公開？		個資法第 20 條第 1 項本文、但書

			& 目的限制
3.3	受訪業務是否需要利用當事人之個人資料向當事人聯繫或寄送資訊？		個資法第 20 條第 1 項本文、但書 & 目的限制
3.4	受訪業務是否利用當事人之個人資料向當事人行銷？如有：		N/A
	3.4.1	行銷之商品或服務為何？與受訪業務有何關聯？例如該商品或服務為受訪業務的優惠或更新資訊，或該商品或服務與受訪業務無關？	個資法第 5 條 & 正當合理關聯
	3.4.2	首次向當事人行銷時，是否提供拒絕接受行銷之方式，且無須支付任何費用？	個資法第 20 條第 3 項
	3.4.3	當事人尚有其他何種方式，可對行銷表示拒絕？	個資法第 3 條、第 11 條第 3 項 & 當事人權利保障
	3.4.4	當事人表示拒絕接受行銷後，公司將如何處理？	個資法第 20 條第 2 項
3.5	受訪業務將於何段期間利用當事人之個人資料？如無特定期間，則決定期間長短之標準為何（例如契約存續期間）？		個資法第 11 條第 3 項
3.6	受訪業務是否將當事人之個人資料傳輸之中華民國境外？		個資法第 21 條
3.7	受訪業務是否需要分析當事人之個人資料？或受訪業務取得之個人資料將由公司其他業務/部門分析？如有：		N/A
	3.7.1	分析目的是否為對當事人標註屬性，以供行銷或推送其	個資法第 20 條第 1 項本文、但書

		他資訊之用？	& 目的限制
	3.7.2	分析目的是為產出不具識別性之結果提供第三方或內部使用（包含對當事人行銷或推送其他資訊）？	
	3.7.3	分析目的是為產出可識別個別當事人之結果提供第三方或內部使用（包含對當事人行銷或推送其他資訊）？	
	3.7.4	是否彙整其他業務所取得之同一當事人個人資料分析？	
查檢項目 4：保存個人資料的合法性			
4.1		受訪業務所需保存當事人之個人資料的期間為何？如無特定期間，則決定期間長短之標準為何（例如契約存續期間）？	個資法第 11 條第 3 項
4.2		公司如何界定受訪業務蒐集當事人個人資料之特定目的已達成或已不存在，而依法須主動或依當事人請求刪除資料？	
查檢項目 5：當事人權利行使的合法性			
5.1		當事人得以何種方式向公司就受訪業務取得之個人資料行使個資法中的當事人權利？	個資法第 3 條、第 10 條、第 11 條 & 當事人權利保障
5.2		如當事人請求停止利用個資，公司將如何處理當事人之個人資料？	個資法第 11 條第 3 項
5.3		如當事人請求刪除個資，公司將如何處理當事人之個人資料？	
查檢項目 6：委外監督的合法性			
6.1		受訪業務是否委託公司以外之第三方蒐集、處理或利用當事人之個	個資法第 4 條

	人資料？例如委外印製帳單、委外寄送商品、委外客服、委外電訪、委外裝機、委外雲端儲存資料、委外資料分析等？	
6.2	如有，公司是否及如何對受託者執行事前、事中、事後之監督管理？	個資法施行細則第 8 條
查檢項目 7：事故通知的合法性		
7.1	因受訪業務而保有之個人資料，曾否發生遭竊取、洩漏、竄改、毀損、滅失或其他侵害（例如遭濫用或誤用）？	個資法第 12 條、個資法施行細則第 22 條
7.2	如有，公司當時是否以適當方式即時通知受害之當事人？如何通知？	
7.3	公司現行有效之個人資料事故通知相關管理程序為何？	
查檢項目 8：安全維護措施的適當性		
8.1	請提供現行有效之個人資料管理制度或安全計畫文件，例如個人資料檔案安全維護計畫、資訊安全維護管理辦法，或其他相關規範。	個資法第 27 條、個資法施行細則第 12 條

資料來源：本計畫製作

第二節 小結

一、 通傳事業個資法遵因應評估報告

本團隊期中執行 7 間、期末執行 8 間，共執行 15 間通傳業者個資保護輔導訪查（5 間電信事業、5 間有線電視事業、5 間電視購物頻道事業），儘將主要訪查發現摘要如下：

1. 大型電信事業之個資保護制度與資訊安全措施之落實均較領先，同仁普遍具備個資保護與資訊安全之法規遵循意識。惟因事業體大，業務繁多，除本次訪查鎖定的行動寬頻業務（客戶資料流程）之外，尚有其他電信與加值服務，可取得同一特定客戶的多種個人資料（使用服務所產生之紀錄）。仍須留意在其他業務中的個人資料串接整併（可能供作大數據分析、線上行為追蹤、輪廓側寫、分群貼標等用途）的適法性。
2. 有線電視業者屬多媒體系統經營者之集團下關係企業，經集團安排，在個資保護制度與資訊安全政策方面均遵循多媒體系統經營者的統一規定，但具體落實程度仍須定期確認，避免說、寫、做不一致性。且因集團事業存有業務互相委託情事，涉及個人資料的委託蒐集、處理或利用行為。有線電視業者與所屬的多媒體系統經營者間就個資委託事項如何互為監督、稽核，宜由主管機關續為留意訪查。
3. 新開播的電視購物頻道業者因仍處於開發商品與客戶市場階段，在個資保護與資訊安全方面仍有不足，整體法規遵循意識尚未完整建立，應仍有賴主管機關持續追蹤輔導。
4. 多數業者仍未全面落實法定告知義務，包含無個資告知聲明、蒐集目的與必要性不明、隱私權政策之明確性不足或疊床架屋等。
5. 多數業者之安全維護措施不足，恐有資安風險，包含仍使用不安全之電腦作業系統、帳號密碼管控待加強等。
6. 多數業者與個資委外廠商（物流、資料儲存、資料處理）普遍

就個資保護事項未約定完整的監督權利義務，尤未約定委託事項執行完畢後的資料刪除、銷毀（多表示以口頭或文字告知廠商，但如未以契約約定為廠商義務，究責上較有難度）。

7. 少數業者利用個人資料之適法性尚有疑慮，包含目的外利用個人資料（提供客戶個資予關係企業）所取得之當事人同意未完全符合法定要件、未於首次對客戶行銷時，提供表示拒絕接受行銷之方式等。
8. 少數業者個人資料保存未訂定適當保存期限，或是保存期限屆至未依規定銷毀或刪除。

二、 電信事業個資告知義務秘密客抽查報告

本團隊另針對五大電信事業進行個資告知義務秘密客抽查，茲將各電信業者抽查結果整理如下：

1. OOOO：
   (1) 本次抽查人員申辦預付卡過程中，門市人員蒐集、處理抽查人員之個人資料，並未積極向抽查人員揭露個人資料保護法第 8 條規定的應告知事項，亦未告知或提醒於何處可取得相關資訊。但申請書 B 欄第 8 點記載「立同意書人/法定代理人/代理人已知悉個人資料告知事項」，恐與實際情形不相符合。
   (2) 另申請書 B 欄第 7 點提供勾選是否同意接受優惠或服務訊息之選項，似表示該公司以「經當事人同意」作為利用個人資料行銷之依據。然而門市人員未向抽查人員說明須請勾選以表達意願，更在系統中於申請書 B 欄第 7 點預設勾選同意，此同意非屬當事人所為之意思表示，應屬無效。
2. OOOO：

   本次抽查人員申辦行動寬頻試用專案過程中，門市人員蒐集、處理抽查人員之個人資料，並未積極向抽查人員揭露個人資料保護法第 8 條規定的應告知事項，亦未告知或提醒於何處

可取得相關資訊。但申請書記載「本人已知悉 OOOO 依個人資料保護法第 8 條告知事項」，恐與實際情形不相符合。

3. OOOO：

(1) 申辦過程中，OOOO 服務中心門市人員向抽查人員收取身分證件前後，均未告知有關蒐集個資的法定應告知事項，亦未提出任何有關隱私權保護政策及個人資料使用同意事項之書面或電子畫面等供抽查人員檢視。

(2) 抽查人員簽名時，電子簽名板上除申請表外，已列有個人資料使用同意書的字體，此記載貌似代表抽查人員只要簽名後即同意 OOOO 使用個人資料，惟使用範圍及內容抽查人員卻一概不知。

4. OOOO：

本次抽查人員申辦行動寬頻試用專案過程中，門市人員蒐集、處理抽查人員之個人資料，除已踐行個資告知聲明外，並就該蒐集行為取得當事人同意，應以符合個人資料保護法第 8 條等相關規定。

5. OOOO：

本次抽查人員申辦行動寬頻試用專案過程中，門市人員蒐集、處理抽查人員之個人資料，雖於櫃檯桌面貼有個人資料保護法第 8 條規定的應告知事項，但並未積極向抽查人員提醒促請閱讀。

第七章 通傳事業個資管理機制或資料加值運用研討會

本計畫依約舉辦有關通傳事業個資管理機制或資料加值運用相關之研討會 1 場次。研討會規劃時數為 6 小時，並提供現場及網際網路直播參與兩種選項。邀集具備資通訊、傳播、法律及個人資料管理制度稽核實務經驗等專長之專家、學者或產業代表參與。執行摘要如下：

第一節 執行摘要

一、研討會需求與目的

近年全球數位轉型浪潮愈趨炙熱，舉凡物聯網、大數據、人工智慧相繼蔚為顯學，各國對通傳資料經濟價值之重視度節節攀升。然而各界推動資料加值的過程中，往往礙於若干適法性疑慮，因而躊躇不前影響發展進程。本計畫規劃之「通傳資料應用與法制整備」研討會，旨在參考其他先進國家資料經濟生態系之創新發展趨勢，並針對我國通傳事業相關法規進行深入探討與分析。研討會討論議題、初步資料或結論及與會者回饋等，俱可供通傳會未來監理施政參酌。

本次研討會目標對象為第一類電信事業、第二類電信事業、有線廣播電視系統經營者及有線電視節目播送系統、電視事業、直播衛星廣播電視服務事業、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業、其他對個資管理與資料加值運用有興趣之通傳事業。

二、研討會主題

本次研討會內含三大主題場次，第一場次將聚焦於「通傳產業資料應用與法制研析」，從宏觀角度探討通傳產業資料蒐集後，將巨量資料方法進行分析，或透過數位加值方法處理時，可能面臨的法制爭議，及可行的處理方案。第二場次「通傳產業資料應用與法遵運作」，則接續第一場次的議題，由微觀角度深入剖析通傳產業應用資料在實務層面衍生之法遵議題，譬如通傳產業跨產業之目的事業主管機關權

責與法規調適，及資料法遵風險之落實與消費者保護等等。第三場次則因應今年度疫情席捲全球的情況，以「通傳資料應用與疫情防制議題研析」為主軸，從「減災」、「調適」等兩個面向，探索「科技防疫」、「在家工作」趨勢下引發的個資隱私保護議題。

三、研討會日程與地點

會議時間：2020 年 11 月 10 日（二）9:00-17:10

會議地點：集思交通部國際會議廳 3 樓

表 5 研討會活動議程

時間	與會人員	
09:00-09:40	貴賓報到	
09:40-10:00	開幕致詞	國家通訊傳播委員會 陳耀祥主任委員 財團法人資訊工業策進會科技法律研究所 王偉霖所長
【場次一】通傳產業資料應用與法制研析		
10:00-12:00	主講人	財團法人資訊工業策進會科技法律研究所 孫鈺婷專案經理
	主持人	財團法人資訊工業策進會科技法律研究所 顧振豪副所長
	與談人	國家通訊傳播委員會 鄧惟中委員
		國家發展委員會 李世德參事
		東吳大學法律系 余啟民副教授
		景翊科技股份有限公司 陳奕廷總經理
		意藍資訊股份有限公司 楊立偉董事總經理
		財團法人工業技術研究院產業科技國際策略發展所 趙祖佑總監
12:00-13:20	午餐時間	
【場次二】通傳產業資料應用與法遵運作		
13:20-15:10	主講人	達文西個資暨高科技法律事務所

		王慕民合夥律師
	主持人	達文西個資暨高科技法律事務所 葉奇鑫所長暨主持律師
	與談人	國立臺北大學經濟系 郭文忠教授
		國立政治大學 法律系 劉定基副教授
		凱擘股份有限公司法務法規室 林雅惠處長
		遠傳電信法務法規暨採購群 李和音資深副總經理
		財團法人資訊工業策進會科技法律研究所 林冠宇組長
15:10-15:30	休息時間	
【場次三】通傳資料應用與疫情防制議題研析		
15:30-17:10	主講人	財團法人資訊工業策進會科技法律研究所 王德瀛專案經理
	主持人	財團法人電信技術中心 陳人傑主任
	與談人	國家通訊傳播委員會 孫雅麗委員
		中國文化大學法律學系 李寧修教授
		中原大學財經法律學系 江耀國教授
		中華電信股份有限公司法律事務處 鍾國強法務副總
		理律法律事務所 曾更瑩合夥律師
		財團法人資訊工業策進會科技法律研究所 宋佩珊副主任

資料來源：本計畫製作

四、研討會參與情況分析

（一）現場與會人員數（簽到表詳參附錄 3）

表 6 研討會現場與會人員數

活動報名人數	194 人
研討會當天出席與會人員	
貴賓、講師	17 人
與會來賓	163 人 (包括實際報到 148 人及現場報名 15 人)
出席總計	180 人

資料來源：本計畫製作

（二）Youtube 觀看人數

Youtube直播網址：
https://www.youtube.com/watch?feature=youtu.be&v=dSGwH3mICdc

表 7 研討會 Youtube 觀看人數

當天上線最高流量	56
12/7 影片觀看數	857 次

資料來源：本計畫製作

（三）活動問卷分析

本次研討會活動分為現場參與及網路直播參與兩部分，故活動問卷分為線上及線下兩部分蒐集並分別進行分析。

1. 現場參與

回收有效問卷數：37 份

現場參加總人數：163

表 8 研討會整體評價統計表

	議題符合性	書面資料合適性	時數分配之適當性	環境之配合度
分數	4.35	4.14	4.16	4.43
總分(平均)	4.27			

資料來源：本計畫製作

表 9 行政服務評價統計表

	活動事前之各項服務	活動現場之各項服務
分數	4.22	4.22
總分(平均)	4.22	

資料來源：本計畫製作

表 10 活動訊息管道統計表

訊息管道	國家通訊傳播委員會發送公文	科技法律研究所電子報	科技法律透析期刊廣告	來自網路媒體網站訊息或電子報	活動宣傳海報或DM
總計（份）	28	8	1	4	1

資料來源：本計畫製作

2. 網路直播

回收有效問卷數：5 份

表 11 研討會整體評價統計表

	議題符合性	書面資料合適性	時數分配之適當性	直播平台滿意度
分數	4.8	4.8	4.8	4.4
總分(平均)	4.7			

資料來源：本計畫製作

表 12 行政服務評價統計表

	活動事前之各項服務	活動現場之各項服務
分數	4.6	4.6
總分(平均)	4.6	

資料來源：本計畫製作

表 13 活動訊息管道統計表

訊息管道	國家通訊傳播委員會發送公文	科技法律研究所電子報	科技法律透析期刊廣告	來自網路媒體網站訊息或電子報	活動宣傳海報或DM
總計（份）		2	1	1	1

資料來源：本計畫製作

五、研討會行政照片紀錄

資料來源：本計畫拍攝

圖 77 研討會議程看板

資料來源：本計畫拍攝

圖 78 研討會報到桌配置

資料來源：本計畫拍攝

圖 79 研討會會場指引

資料來源：本計畫拍攝

圖 80 研討會講台布置

資料來源：本計畫拍攝

圖 81 研討會會場布置

資料來源：本計畫拍攝

圖 82 研討會會議資料

（詳參附錄 4：研討會會議手冊）

資料來源：本計畫拍攝

圖 83 研討會會場外布置

資料來源：本計畫拍攝

圖 84 研討會工作人員

資料來源：本計畫拍攝

圖 85 研討會報到台配置

資料來源：本計畫拍攝

圖 86 研討會報到-1

資料來源：本計畫拍攝

圖 87 研討會報到-2

資料來源：本計畫拍攝

圖 88 研討會貴賓休息室一景

資料來源：本計畫拍攝

圖 89 研討會中午餐盒發放

資料來源：本計畫拍攝

圖 90 研討會開場配置

第二節 研討會內容摘要

一、長官致詞

（一）通傳會孫雅麗委員開場致詞

孫雅麗委員表示，今年為 5G 元年，也是國家發展通訊發展關鍵的一年。隨著 6 月底電信業者開始推動服務，以及 5G 行動裝置的接續問市，可望為產業創新科技的發展，帶來推波助瀾的動力；比方說促使高品質影音服務、自駕車、智慧城市、智慧製造、智慧醫療等創新應用相繼應運而生，不僅為社會經濟與交易市場帶來變革，更可望順勢實踐政府許下的「數位國家、智慧臺灣」願景。然而欲於通傳資料加值應用、法制整備之間求取平衡，必須從資安強化、個資保護、資料保護及資通安全強化四大防護重點著手建構可信任的基礎網路。著眼於此，今後通傳會將權衡產業發展、法規遵循等兩大主軸，持續與產業界溝通對話，理解業者需求，找出最具調適性的因應做法。

（二）資策會科技法律研究所王偉霖所長開場致詞

王偉霖所長指出，當今不論是自駕車、無人機還是無人船等偉大創新，都立基於通傳資料的運用，是以通傳資訊可謂數位匯流下的黑金。如何建構好的法制基礎，持續穩定地落實個人資料保護與隱私權維護，正是通傳事業永續發展的必要關鍵。因應通訊科技發展，各國

對於通訊網路、以及依附在通訊網路所建構的新型態產業格外重視，這些新興產業究竟會對個人隱私資料造成何等影響，備受關注。資策會科法所在通傳會的支持下舉辦本次研討會，希望藉由產官學各界專家的互動，為通傳事業的資料加值應用暨法制整備，激盪出具體可行的方案。

二、會議各場次重點內容

以下摘要研討會三場次重點內容以及與談分享（與談人簡歷、報告人簡報，詳參附錄 4 研討會手冊）。

（一）場次一：通傳產業資料應用與法制研析

本場次由資策會科法所顧振豪副所長主持，聚焦於 5G 匯流時代，因大數據應用技術的普及，資料的應用及共享討論度及重要性亦隨之水漲船高。然而以產業為切入點，如何於實務操作運用中，建立可信任之通傳網路，政府應思考如何運用規範的調整及設計，輔導業者及消費者在法遵成本與資料價值間取得平衡。

1. 報告主題：通傳產業資料應用與法制研析–資料經濟下個人資料的流通與應用

本場議題主講人資策會科法所孫鈺婷專案經理指出，隨著 2019 年金管會推動開放銀行、2020 年國發會推動數位服務個人化(MyData)，政府希冀透過引導個人資料的及時運用，推動台灣資料流通與應用進入新里程碑。惟在推動過程中，觀察到現行個人資料保護法未規範資料可攜權等法制不足之處，建議各領域主管機關於推動資料共享時可參酌國際經驗，或思考有無類似沙盒程序，達成實驗資料流動的機會。同時加強保護消費者權益、注重資料安全與隱私保護，發掘數位匯流下的通傳資訊的黑金，促進通傳產業永續發展。

孫經理進一步介紹近年來為眾人廣為討論的資料市集

(Data Marketplace)概念，在於如何轉換公開資訊(Open Data)為資料集，再透過資料集，成為應用程式介面(Application Programming Interface, API)提供各項資料服務之過程。透過政府與民間協力合作，共同提升資料價值、資料應用及資料處理方式，舉例而言，歐盟透過標準化的「開放應用程式介面」(Open API)確保流通資料不包含個人隱私，來達成如歐盟交通及大眾運輸數據資料的共享及串聯，創造更多新服務，亦可利用資料市集整理、保管各項資訊後轉化為資料銀行(Data Bank)，並視需求提供合作夥伴，或透過融資方式與新創公司合作，以分潤方式共享獲利，進而發揮資料轉換價值。

2. 第一場次與談分享

(1) 資料的加值運用

景翊科技股份有限公司陳奕廷總經理在資料銀行的概念下，進一步提出「資料理專」的概念，「資料理專」針對資料利用價值進行評估，並對資料內容與資料格式化標準化、格式化進行判斷。透過第三方審核機制，整合律師、道德專家、資安專家及系統專家組成審議委員會，排除個資等敏感資料，同時審核資料銀行運作及資料處理可能面臨之法遵相關議題。

(2) 資訊揭露及自律機制

國家發展委員會李世德參事分享，於 2013 年至 2015 年間，極端氣候的衝擊加上中古車車商與消費者間資訊不透明等因素，大量泡水車流入市場，產生如何權衡原車主資料保護及解決資訊不對等的問題，交通部會同消保處及民間汽車修理業公會業者向法務部請益的事例。

以取得維修紀錄等原車主之資料為例，應先徵求原

車主同意，或由下任車主提出查詢權後後始得要求提供，惟原車主提供資料情形多半被動，通常僅能要求中古商於資料去識別化後再行提供，實務操作上較模糊與困難。參考歐盟 2018 年正式實施 GDPR 後，於開放資料庫及資料可攜權的概念下，透過四方面角色，包含資料控管者、第三方服務者(Third-Party Provider, TPP)、個資當事人及 API 服務提供者，賦予個資當事人在固有的資料查詢權，進一步向資料控管者要求以一定可讀格式提供予個資當事人或第三方服務者，至於以何種規格執行，歐盟並未有明確規範，而是保留資料控管者及資料需求方預先討論。舉例來說，歐盟法案第二號支付服務指令(Payment Service Directive 2, PSD2)要求金融服務業以資料控管者角色釋出資料予第三方服務者時，應形成一定的規格標準規範。

觀察日本處理開放銀行(Open Banking)的做法，並未在日本個資法下規定資料可攜權，而是透過銀行法，要求銀行釋出客戶資料時須取得當事人同意；以及規範資料控管者與第三方服務者間，如何形成 API 等特殊規定方式，推動開放銀行運行。台灣可借鏡其他國家作法，以可攜權模式透過查詢權之行使，在當事人同意的前提下，以業者自律模式而非強制規範規格的方式，發揮資料的價值與應用。如金管會推動 Open Banking 的運行，由銀行端與第三方服務者以自律的方式訂定規格，並透過金管會輔導，找到合適的 API 服務業者進行資料轉換。

(3) 資料之相互連接性及共創資料所有權

意藍資訊股份有限公司楊立偉董事總經理分享產業經驗，通傳業者常礙於擔憂蒐集資料責任過重，而避免蒐集消費者資料。惟通訊產業因其特許行業性質，消

費者相對弱勢，因此若站在消費者角度，政府應對通傳產業業者間資料相互連接性，與第三方外部業者提供個資蒐集等服務，採較開放的態度。

在通傳產業中，共創資料之所有權因資料的共有性存在灰色地帶，如 Google 在蒐集、分析使用者軌跡資料時，該移動資訊乃使用者移動所產生，惟倘未有 Google 提供之設備及服務，亦無法產生該資料，因此建議共創資料應回到市場機制，向使用者充分揭露蒐集及利用範圍，設定當事人退出(Opt-out)機制，將是否繼續使用該服務的決定權交還使用者。

楊董事總經理進一步舉例電信資料，如基地台人數，可應用在房仲業者預估人流、店家選址等決策上；個人移動軌跡亦可運用於保險公司，如疫情間，判斷投保人移動紀錄及曾出入之場所以精算保費。然以上商業應用因仍處於模糊階段，該加值營業項目之商業應用或販售行為是否合法、費率為何等問題，建議主管機關給予較明確的規範。

(4) 資料加值服務之適法性及運用

東吳大學法律系余啟民副教授認為，台灣在 5G 的發展下，聯網互通發展最有潛力的產業，包含智慧金融、智慧醫療與智慧城市、交通通傳運用等資料加值服務應首重資料安全性，如國外許多大廠近來積極推動「資料零信任」(Zero trust)，意即 “Trust but Always Verify”，應隨時確認資料蒐集、分析及應用範圍。

智慧金融方面，以北市悠遊卡為例，獎勵民眾於報稅期間，以悠遊卡繳納地價稅可享有 7%回饋；在智慧醫療方面，台灣健保卡的利用率、普及率及可靠性高，因此在智慧金融及智慧醫療法制準備及連結上，余教授皆給予肯定；在智慧交通或在通傳產業方面，於首次訂

購時，業者通常要求消費者提供雙證件以供驗證，余教授認為應盡量使民眾於個資法上個資識別部分單一化、便捷化及安全化，增加民眾自主運作機制及誘因。

近年個資法重心移轉，在過去個資法重視的人格權保障，目前已逐漸轉向促進資料的合理利用，根據以往經驗，通傳產業常會遇到的障礙分別為去識別化，或於特定目的內或外的利用法律應另有規定或當事人同意等門檻。參考歐盟 GDPR 部分允許在當事人同意方面，設定當事人退出機制為例，建議主管機關與其要求法制上的作業，不如要求業者提出創新技術上的突破。

(5) 個資盤點之適法性

余教授亦指出，個資盤點為未來資料資產化的情況下之趨勢，其中最困難的部分為資料欄位的設計，因資料庫中，未來可運用於加值發展的資料最為重要，然而前端人員於欄位確認上，常未做適法性評估，以致法規準備及實務操作上存在很大的落差。企業僅願意做到形式合法，而不願做資料加值，以免觸碰法律邊際，余教授建議除了確認欄位，亦可同步製作表單標準程序及調整流程。至於制定類似沙盒程序方面，余教授認為因我國適用歐陸法系，實際運用上可能與英美法系國家成功經驗有所不同，且我國未若日韓國家有較上位制定類似沙盒程序之觀念，加上立法過程緩慢，可能拖緩創新及技術運用的腳步。

綜上所述，資料經濟仍首重資料安全，於第三方服務進入時，於合約訂定對消費者權益的保護應特別注意「消費者賦能」的概念，利用“Opt-out”機制，將資料運用的控制權還予消費者；另，適法性盤點的建立，可能因欄位設計上的欠缺，企業往往僅願做到形式合法，因而拖緩產業創新腳步；最後，余教授回應主講人提出類

似沙盒機制的建立，認為台灣因仍欠缺上位制定沙盒程序之配套法規，而持保留意見。

（二）場次二：通傳產業資料應用與法遵運作

本場次由達文西個資暨高科技法律事務所葉奇鑫所長主持。「通傳產業資料應用與法遵運作」議題主要討論通傳產業資料應用於實務處理上面臨的法遵議題，消費者在使用通訊傳播產業的過程中產生的個人資料，被業者作為商業利用的方式隨科技進步更加多元，如何創造個資價值並平衡目的外利用個人資料所產生之法遵風險，為本場研討會所著墨之主題。

1. 報告主題：通傳產業資料應用與法遵運作

本場主講人達文西個資暨高科技法律事務所王慕民合夥律師提醒，現行管理制度難以滿足創新應用的法遵性，常見實務操作兩大難題包含去識別化不在程序中，以及取得當事人同意部分缺乏操作性，因此強調業者須特別注意取得「有效的」去識別及「合法的」當事人同意。順應資料經濟崛起的浪潮，基於消費者保護的信賴基礎下，差異化的個人資料保護、隱私保護將成為未來業者競爭的亮點與利基。

2. 第二場次與談分享

(1) 資料運用的適法性

政治大學劉定基副教授認為，以通傳產業類別來討論資料運用的適法性，個資創新利用是否皆為目的外利用、解釋及界定履行契約範圍為討論關鍵。若資料的創新利用可以被解釋為履行契約的必要範圍為做目的內利用，服務契約即可作為利用個資之基礎，無須當事人額外同意或去識別化的程序。實務中資料利用價值常與去識別的程度呈反比，若能利用取得當事人同意作為其他目的外利用合法性基礎，可減少程序複雜性，並提供

消費者更多元的加值服務。

有鑑於現行台灣個資法所規定無法識別特定當事人的程度，無法律明確標準之要件，資料去識別化、匿名化及假名化的標準為何，在國際上亦無絕對標準，仍須按照個別案件情境，判斷是否落入個人資料範疇。以加總之統計資料為例，因已相當程度去識別化，因此在個人資料保護風險程度較低，事業主管機關應可給予較大空間；反之，若非加總之統計資料，應建立完善的個人資料風險評估機制，作相當程度的去識別程序，同時維持資料的可用性。故縱然個人資料風險評估機制在個資法上無直接相對應的明文規定，惟於個資法內有關安全維護義務規定可以看出，風險評估應納入安全維護一環思考，以達成使用資料目的及資料去識別化之間的平衡。

現行個資法仍有許多修正空間，如歐洲在個資的蒐集、處理、利用方面概括個人資料蒐集的合法事由，惟台灣因個資法欠缺上述利益權衡規定，以致業者需透過契約或當事人同意來蒐集個人資料，在發揮資料創新及資料價值上，現行法規較無利用彈性；同樣地，現行個資法針對目的外利用適用主體的限制，過於限縮政府機關或學術機構以外單位，合法享用目的外利用所帶來的價值。

(2) 由實務角度觀組織業務與法遵單位衝突的調和

有與談人指出，針對 5G 元年，有線電視及寬頻服務業者因應傳統收視用戶流失及剪線潮，逐年提高寬頻及加值服務比例，如機上盒服務於徵求用戶同意後，得蒐集、分析用戶的機上盒使用資訊，提供更優質的服務品質及更精確的廣告推播的議題。惟若要發展出具規模經濟的商業模式，以目前有線電視業者不若電信業者

「依裝置」蒐集使用者資訊，而是「依機上盒」蒐集家戶的匯總資訊的模式，將致行銷及推播服務不精確。目前主管機關以提出成立通傳產業資料庫的構想，以打破台灣有線電視收視戶長年反映「萬年頻道」的問題，期能透過蒐集收視行為建構未來民眾更優質的影、視、聽服務，並提供業者頻道安排的參考。

凱擘股份有限公司法務法規室林雅惠處長表示，相較於以往台灣電視台及廣告依賴極深的「AGB 尼爾森收視率」分析調查，「收視質」分析蒐集更深入的觀眾收視習慣，藉此了解其收視動機、興趣、評價或滿意程度，讓未來通傳產業的策略規劃具有更高的參考價值，因此林處長建議，除了收視率，收視指標應適時導入「收視質」，舉例而言，用戶可利用智慧錄影錄下喜愛節目，或是利用機上盒回覆問卷，使業者得以分析用戶觀看時間、次數或習慣等資訊。

遠傳電信法務法規暨採購群李和音資深副總經理，接續以智慧音箱蒐集台灣用戶聲紋資料，並轉換進資料庫為例，在未來萬物相連的物聯網時代，若當事人嗣後撤銷同意，在多角化經營及異業經營的趨勢下，資料於資料集中流動實務上難以拆分。又各項應用服務、不同單位所蒐集之資料，是否皆被認定為個資，因為台灣目前未有單一主管機關負責，不同主管機關的認定可能不同，徒增企業經營風險之不確定性。

綜整通傳產業業者的回應，主講人整理歸納去識別化制度未在法規範圍內，以及當事人同意缺乏操作性等兩大議題，形成兩項建議。首先，何謂「有效的」去識別化，我國目前未有明確規範，仍有待主管機關提供如何達成有效去識別化的指引；另，何謂「合法的」當事人同意，實務操作中，若無法取得當事人對各項服務一致同意，實難精確蒐集用戶收視行為，提供完整的加值

服務。

與談人表示，業者期待主管機關更明確界定當事人同意範圍，或提出更便利取得用戶同意的執行模式。並呼籲主管機關輔導數位轉型的過程中，在目前法規尚未明確規範的情況下，給予新服務（特別是破壞式創新服務）更低度的管制及更高度的彈性。

此外，亦有與談人指出，個資法之修法並非一蹴可幾，可參歐盟「利益權衡」的概念，或以函釋取代修法的做法，如 2013 年金管會函釋（金管銀合字第 10230001141 號），提出在金融控股公司規定建置子公司業務及客戶資料庫、管理集團風險的情況下，得免向當事人為告知及取得書面同意的義務。在集團及跨部門行銷應用方面，業者期待主管機關參考上述函釋作法，透過函釋提供業者集團內之個資使用的情形，更為便利、彈性，達成創新與法規的雙贏，同時降低企業經營風險及營運不確定性。

(3) 通傳資料風險管理

在討論到資料風險管理部分，有與談人提醒，資安與個資的概念易混淆。二者雖具一定程度的相關性，然而許多廠商往往偏重一方，如業者僅作資安檢測，卻未針對內部資料偵測錯誤點。然而個資系統的建立應與資安相輔相成，隨著法規環境的變化，需要持續調整及強化。

資策會科法所林冠宇組長更以實際輔導國內廠商為例，指出業者在實務操作上最常遭遇的困難包含「去識別化」後資料價值降低、「當事人同意」濫用的情形、委外監督的成本效益權衡等議題。因我國企業常見集團式的經營模式，過去可能為了業務推展的便利性，其所蒐集的資料在不同單位間傳輸、流轉，未作妥適的資料

風險管理。惟風險的識別及控管，係個資管理重要的一環，需要企業識別不同風險後，按集團資源成本分配，透過階段性處理、識別，優先處理高風險部門之風險，建立滾動式的個資管理制度。

（三）場次三：通傳資料應用與疫情防治議題研析

本場次由財團法人電信技術中心陳人傑主任主持。第三場「通傳資料應用與疫情防制議題研析」議題，透過通訊資訊應用與疫情防治議題，研析 COVID-19 減災及調適等面向，探討疫情中「科技防疫」、「在家工作」所引發的個資隱私保護疑慮，在防疫的同時，善用科技確保個人資料隱私安全。

1. 報告主題：通傳資料應用與疫情防制議題研析

COVID-19 全球大流行下的科技減災與調適

資策會王德瀛專案經理為本場主講人，分享在疫情下如何運用科技達成減災與調適的看法。針對減災部份，王經理認為可透過手機定位等資訊，「以資料的流通追蹤人的流動」；調適部份，他強調 “Low Touch Economy”，「以資料的流動來取代人的流動」，透過流程、資料與資訊、互動溝通的數位化，迎向「低接觸經濟」。最後提出，面對防疫下半場，台灣國家隊應思考科技防疫的合理界線，重新構思數位化下流程及組織的安排規劃。

2. 第三場次與談分享

(1) 追蹤資料應符合比例原則

中原大學江耀國教授談到政府對不同對象採用之追蹤技術。第一，依照追蹤對象的不同，採用的追蹤方式應合乎比例原則，如依照追蹤對象區分一般人民適用「低」度追蹤、隔離者適用「中」度追蹤、確診者適用「高」度追蹤；第二，追蹤方式定位與否，如德國

“Corona-Warn-App”採非定位追蹤，不蒐集位置資訊，相反地，中國政府採用的「健康碼」計畫則為定位追蹤，在中國數百個城市裡蒐集個人包括定位數據等資訊；最後，追蹤結果存放位置的不同，分為集中式資料庫或分散式資料庫，前者將蒐集之資料存放於國家研究機構所建立的集中式資料庫，後者如 Apple 及 Google 等科技公司，將追蹤資訊存入個人手機而不傳入中央伺服器，且 14 天後自動消失。綜上，依照追蹤對象不同、追蹤方式定位與否、追蹤結果分散式或集中式儲存方式的不同，產生 12 種象限(3x2x2)矩陣。建議政府預先界定傳染性疾病，依照嚴重程度落入何種象限中，以強化政府防疫手段的正當性。此外，蒐集資料保存期間亦可作為另一個面向的思考，資料的即時性與資料價值呈正相關，以防疫追蹤軌跡資訊為例，越近期的位置與接觸史資訊越為重要，隨著時間的推演資訊重要程度降低。故資料保存期間亦可作為政府對於資料隱私與健康權平衡的參考。

(2) 我國通傳資料防疫措施

整理與談人對本場主題，政府「以資料流動追蹤人的流動」概念的回應。有與談人表示，針對疫情，我國政府已推動電子圍籬、類細胞簡訊等措施，若該資料得以追蹤某特定人，將符合個資法所界定「具識別性」的資料。即便在處理及利用的過程已作去識別化的程序，亦未完全排除再識別的可能性，故仍可能被認定為個人資料，而觸及個資法蒐集、處理、利用等面向，或觸及其他如傳染疾病防治法等特別條例的相關規定。雖然政府在蒐集上述資訊，乃基於高度公益目的蒐集個資執行防疫，並無不當。惟政府針對當事人的個人資料應做比例性應用，並留意是否符合個資法第 5 條：「個人資料

之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯」的規定。

文化大學李寧修教授表示，因目前台灣疫情處於較緩和階段，已蒐集的資料於國家手中作何運用，政府未有明確說明。如已蒐集的資料除做防疫使用功能外，是否被拿來作其他用途利用，或與其他健保卡、悠遊卡等資訊作結合比對。因此，李教授建議，政府應就已蒐集的個資說明是否有防疫目的外的其他利用，以弭平人民因不信任所生之疑慮。如說明政府欲取得何種資料、該資料保存期限及資料使用足跡，並紀錄、告知、開放查詢和蒐集民眾個資歷史，應可有效降低民眾的不信任感。

李教授進一步指出，我國政府現行防疫蒐集、處理及利用民眾個資方式，以傳染病防治法為例，新興科技追蹤技術尚未加入考量。檢討目前傳染病防治法現行措施，較多為針對人身自由的限制，有關新興科技發展的思維仍有待補充。而個資法是否適合作為我國政府採取防疫措施，蒐集、處理及利用個資的依據，李教授持否定看法，因個資法主要規範一般性資料的蒐集、處理、利用，而非針對特殊傳染疾病等特殊類型資料作規範；另外，李教授也認為以特別條例方式作為法律依據亦不適當，如何謂必要措施、可蒐集個資範圍、如何蒐集保存、可否作為目的外利用等面向，無法由特別條例明顯看出，因而產生明確性原則之疑慮。

中華電信法務處鍾國強副總指出，在防疫下半場的整備上，應作法規盤點並加入新興科技的思考，針對目前法規可能存在的不確定法律概念，或無法完全涵蓋的議題，有再發展的空間；另在法規運用上，存在一個監督機關以確保法律在個人資料保護上是否足夠，是相當

重要的一環，如目前國發會僅針對法律作解釋，對於個案的運用如何定奪，仍要回到各機關作核定，因此建議針對個資監管，應有一專責監督機關。鍾副總更進一步以電信業者角度，提出在我國目前透過科技防疫有成、台灣疫情相對穩定的時機，應將個資保護相關議題在法制面完整化，以消弭業者不確定性，並在政府防疫的同時兼具法律明確性。

(3) 後疫情時代之展望

理律法律事務所曾更瑩合夥律師分享，在後疫情時代，其處理疫情期間與個資議題相關的執業經驗。因個資法為概括規定，因此針對具體個案須參酌各項具體事實所適用的法律，實務上常見問題為公司於疫情期間，是否可合法蒐集員工確診資料，以利調整員工上班地點及人力的安排。確診資料符合個資法第 6 條規定，有關病歷、醫療之敏感性資料，因此若無同條之例外規定，不得任意蒐集。可見我國於法律規範上，針對雇主是否可以蒐集、處理、利用確診資料的空間不大。衛福部因此提供解套作法，於公司入口篩選員工體溫異常者，避免觸碰個資法第 6 條的問題。就上述問題，曾律師建議，民眾對於科技蒐集個資的疑慮，可透過修法或函釋處理；另外，政府透明化的問題，如個資法第 8 條及第 9 條給予公務機關及非公務機關免除告知義務的例外事項，隱私權的保護與政府利用科技防疫方法的調和，應更透明及明確。

最後，資策會科法所宋佩珊副主任回應主講人「調適」及「減災」兩方面主題，分享疫情帶來的危機與轉機。「調適」方面，運用科技方式，優化流程達成數位轉型的提升；「減災」部分，面對隱私權與科技濫用的風險，應特別留意對於基本權利的影響。因隱私權為流動

性概念，新興追蹤科技應區分為「前」、「中」、「後」三階段，前段如同 NCC 孫雅麗委員強調的”Privacy Protection by Design”，在一開始設計時，鑲嵌隱私保護概念以降低侵害隱私風險；中段運用部分應符合比例原則，如隨著感染人數、傳染率、致死率增高，得重新檢視個人資料使用的範圍及方向；後段部分，針對已蒐集資料的保存，及防疫資料蒐集機制是否退場，應透過專業計算或浮動性思考作後疫情時代相關調整。

三、研討會花絮

資料來源：本計畫拍攝

圖 91 研討會大合照

資料來源：本計畫拍攝

圖 92 研討會 NCC 孫委員開場致詞

資料來源：本計畫拍攝

圖 93 研討會科法所王所長開場致詞

資料來源：本計畫拍攝

圖 94 研討會第一場次發表

資料來源：本計畫拍攝

圖 95 研討會第一場次與談

資料來源：本計畫拍攝

圖 96 研討會第一場次 NCC 鄧委員簡報與談

資料來源：本計畫拍攝

圖 97 研討會與會貴賓

資料來源：本計畫拍攝

圖 98 研討會第二場次發表

資料來源：本計畫拍攝

圖 99 研討會第二場次郭教授簡報與談

資料來源：本計畫拍攝

圖 100 研討會第二場次與談

資料來源：本計畫拍攝

圖 101 研討會第三場次發表

資料來源：本計畫拍攝

圖 102 研討會第三場次 NCC 孫委員簡報與談

資料來源：本計畫拍攝

圖 103 研討會第三場次與談

資料來源：本計畫拍攝

圖 104 研討會現場-1

資料來源：本計畫拍攝

圖 105 研討會現場-2

資料來源：本計畫拍攝

圖 106 研討會現場-3

第八章 國際個資保護管理及資料加值創新應用發展趨勢活動報告

近年來，由於技術的進步，資料的利用價值越發受到看重，而與此同時，資料應用所引發的個人隱私疑慮也日漸升高。如何在個人隱私保護及資料的加值創新應用間取得合理的平衡，成為國際間隱私專業社群相當重視的議題，並展開諸多嘗試。舉例而言，近年來強調以當事人賦權為核心的「我的資料」(my data)概念在許多國家正積極推展，希望以當事人持續性的知情及參與，使資料能更充分的發揮價值；此外，自歐盟 GDPR 施行以來，已有許多國家針對個人資料保護法制展開翻新工作。整體而言，近年來國際社會對於隱私保護、資料合理利用、充分發揮資料價值等議題之討論，有越來越升溫之趨勢。

為有效掌握國際間重要之議題討論進度，提供主管機關參酌，本研究擬挑選國際知名組織所舉辦有關個資保護管理機制及資料加值創新應用之研討會，針對目前國際主要討論之議題進行廣泛之蒐集，並據以彙整為分析報告，提供主管機關參考。本工作項目原為「蒐集與研析 109 年度 2 則以上國際知名組織之個資保護管理機制及資料

加值創新應用等議題發展趨勢活動報告」，於服務建議書所規劃 2 場（2 人次）國際發展趨勢活動部分，因受新冠肺炎疫情影響，相關活動已取消或改採線上會議方式進行，為不影響該工作項目之實行，並蒐集更多元的國際發展趨勢之研析資料，因此變更規劃改為參與 3 場（4 人次）之國際發展趨勢活動線上會議如下表。

表 14 參與國際發展趨勢活動線上會議分工表

會議名稱	會議日期	參與人員
Big Data and Competition Law 2020	2020/10/20（二）	資策會科法所 許嘉芳 法律研究員
Privacy+Security Forum Fall Academy	2020/10/22（四） -2020/10/23（五）	資策會科法所 許嘉芳、周芷瑄 法律研究員
Big Data: Consolidating the EU Legal Framework in the Digital Economy	2020/10/26（一） -2020/10/27（二）	資策會科法所 孫鈺婷 專案經理

資料來源：本計畫製作

第一節 大數據與競爭法 2020 線上研討會

一、研討會資訊

表 15「大數據與競爭法 2020」研討會資訊

名稱	大數據與競爭法 2020 (Big Data and Competition Law 2020)
時間	2020 年 10 月 20 日（二）
地點	線上
出席人員	許嘉芳

資料來源：本計畫製作

（一）整體說明

會議主題為「大數據與競爭法 2020」，議題包含歐盟、美、澳等各國競爭監管機關如何實施監管的全球觀點，如新競爭法提案、數位服務法等；以及業界實務看法，如 Facebook、電腦暨通訊產業協會(CCIA)等代表，分享資料應用、GDPR 跨國公司法遵議題等，還有資料保護的要求與競爭法間關係、GDPR 對競爭法調查的影響、非個人資料的所有權等。

（二）議程資訊

表 16「大數據與競爭法 2020」議程資訊

2020 年 10 月 20 日	
時間	主題
09:50 - 10:20	(Regulating the Digital Sphere) **「數位服務法」配套措施：數位平台是否需要事前監管？** The Digital Services Act Package: Do Digital Platforms Need Ex Ante Regulation?
10:20 - 11:05	(Regulating the Digital Sphere) **新競爭法工具提案** Proposals for a New Competition Law Tool
11:25 - 12:15	(Regulating the Digital Sphere) **全球發展回顧** Review of Global Developments
12:15 - 13:10	(Regulating the Digital Sphere) **反托拉斯適合 21 世紀嗎？** Is Antitrust Fit for 21st Century?
14:10 - 14:50	(Merger Control) **大數據和合併控制：公司防禦失敗和殺手級收購**

2020 年 10 月 20 日	
時間	主題
	Big Data and Merger Control: Failing Firm Defence and Killer Acquisitions
14:50 - 15:20	(Merger Control) **資料驅動市場中的市場定義** Market Definition in Data Driven Markets
15:20 - 16:00	(Horizontal Guidelines) **橫向合作準則：資料池、資料共享與資訊交換** Horizontal Cooperation Guidelines: Data Pooling, Data Sharing and Information Exchange
16:20 - 17:00	(Horizontal Guidelines) **水平/垂直二分法和雙重分配** Horizontal/ Vertical Dichotomy and Dual Distribution
17:00 - 17:40	(Data Protection & Competition Law) **資料保護與競爭法之互動** The Interplay Between Data Protection and Competition Law

資料來源：本計畫編譯

二、場次重要摘要

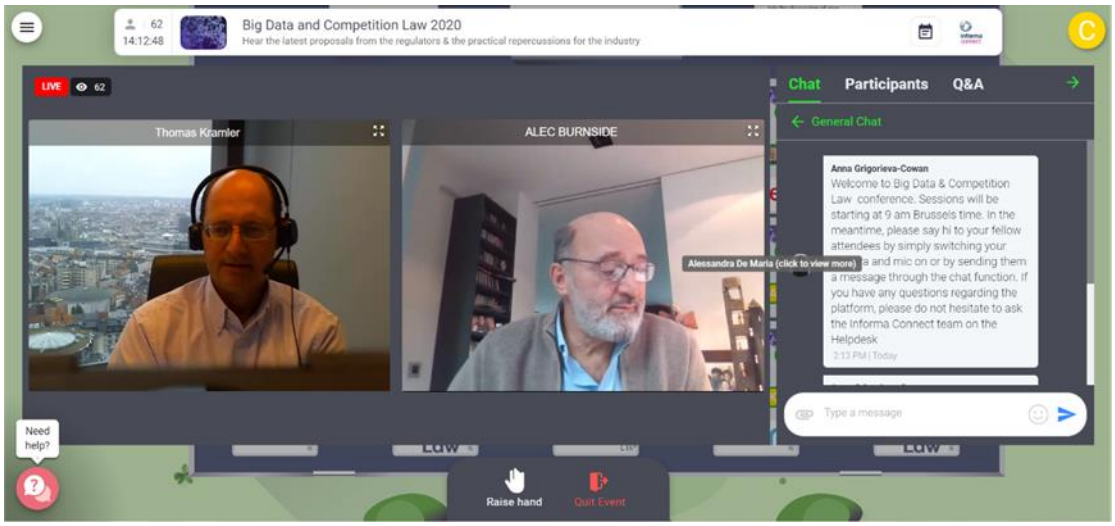
（一）「數位服務法」配套措施：數位平台是否需要事前監管？

本場次由 Thomas Kramler(Head of Unit, Antitrust: E-commerce and the Data Economy, DG Competition at European Commission)進行分享，從數位服務法的角度討論數位平台未來是否需要進行事前監管。

目前線上服務遇到的問題在於競爭性、公平性及進入市場的可能性，當線上平台業者大量資料串連後，即能夠透過自己平台的優勢來

改善或開發新服務。因此，根據數位服務法(The Digital Services Act)初稿內容可知，未來大型科技公司需與規模較小的競爭對手共享其龐大的客戶資料，使其他競爭者能夠近用這些資料。

因此，數位服務法希望透過訂立明確的規則，以建立數位服務的提供者的權利義務，並監督數位平台合作系統能夠有效地執行，以解決其使用者可能遇到的風險，為其提供適當的保護。再者，數位服務法提出事前監管的原則，以確保公平性和進入市場的競爭可能性。



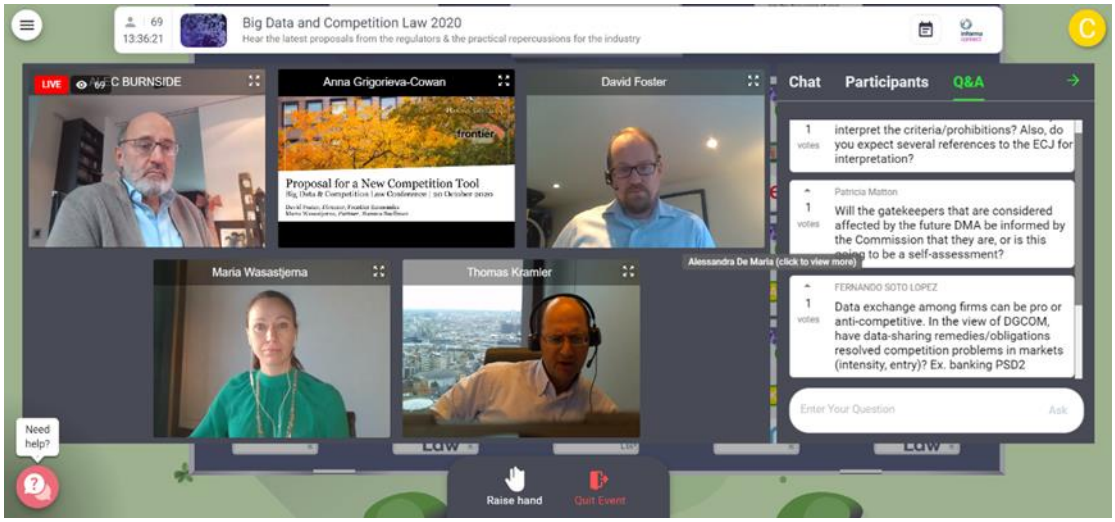
資料來源：本計畫拍攝

圖 107「數位服務法」配套措施：數位平台是否需要事前監管？」場次截圖

（二）新競爭法工具提案

本場次由 David Forster(Director at Frontier Economics)和 Maria Wasastjerna(Partner at Hannes Snellman)分享，競爭法在資料市場上存在的問題，以及數位市場是否存在結構性問題。

資料作為數位市場中的一種交易形式，資料的交易在本質上是困難的。因為資料本身難以定價，同時也難以確定資料在進行交互作用後，未來能夠創造哪些價值。故講者認為，數位平台以「免費」提供服務的方式換取個人資料，並非一公平的行為，因為本質上數位平台擴大了自身的市場力量，卻同時可能損害消費者「無形」的權利。



資料來源：本計畫拍攝

圖 108「新競爭法工具提案」場次截圖

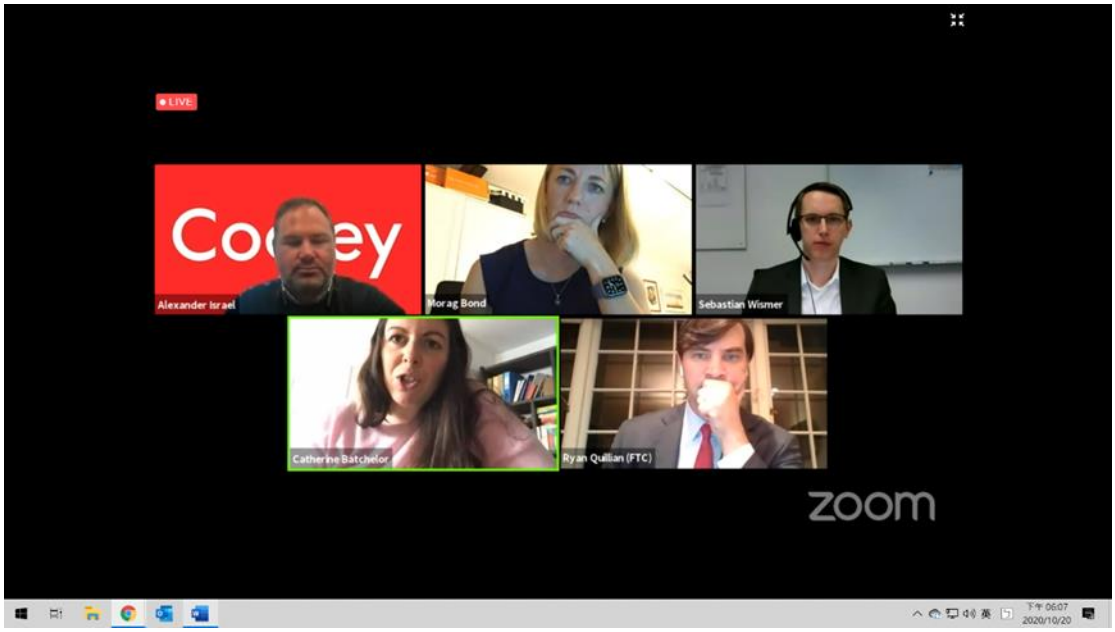
（三）全球發展回顧

本場次由 Alexander Israel(Partner at Cooley)、Ryan Quillian(Deputy Assistant Director, Technology Enforcement Division, Bureau of Competition at Federal Trade Commission)、Morag Bond(Joint General Manager, Digital Platform Branch at Australian Competition & Consumer Commission) 、 Sebastian Wismer(Head of Digital Policy Unit at Bundeskartellamt)，和 Catherine Batchelor(Director, Digital Taskforce at Competition and Markets Authority)進行對談，討論德國競爭法之於歐洲的意義。

數位平台對於競爭法上產生許多新的問題，故德國和歐盟對於大型數位媒體平台的立場轉為對濫用行為應進行監管。從競爭政策角度而言，數位平台透過不同平台彼此交互的作用，高度集中提供線上內容或搜尋檢索資料的資料庫，資料驅動的經營模式在網路中獲得市場支配力，導致與需要競爭的商業模式有所衝突。平台規模對使用者雖有正面影響，卻可能造成因為競爭減少而生負面效果。

講者認為，大型數位平台可能引發的問題有兩個面向，一是可能造成市場永久性的傾斜，使其他平台不再具有競爭力；二是大型數位平台可以利用其市場力量進入其他市場，創建「完美生態系統」。因此，德國於 2020 年 1 月發布競爭法(German Competition Act)修法草

案，修法重點在於重新評估主導地位的市場支配能力、新的濫用市場支配理論，及執行能力。其中，對市場支配能力的判斷已擴張到包含資料在內的評估，不僅限於相關市場。



資料來源：本計畫拍攝

圖 109「全球發展回顧」場次截圖

（四）反托拉斯適合 21 世紀嗎？

本場次由 Steve Thomas(General Counsel at Kelkoo)、Caroline Eggert Frydenberg(Head of Competition Law at Nets Denmark A/S)、Marianela Lopez-Galdos(Global Competition Counsel at Computer & Communications Industry Association)、Ajinkya M Tulpule(Senior Legal Counsel at Ferrero)、Raegan Macdonald(Head of EU Public Policy at Mozilla)，和 Jantira Raftery(Lead Competition Counsel at Facebook)，討論如何在數位環境下進行反托拉斯及事前監管。

2020 年 6 月歐盟執委會(European Commission)對於市場定義進行公開諮詢，認為競爭規則應該保持彈性，以因應數位化的世界。市場定義作為競爭法評估的第一步，講者認為，若將市場比喻成產品，即表示除了應接受調查產品的滿意度外，還應該一併檢查其他產品中是否有其他合適的替代品。另外，對於市場範圍也不再有地理上的限制，市場範圍可以擴及全球。

講者認為，目前美國對於競爭法的相關法規與歐盟相比較弱。對於如何監管及平衡市場是一種經濟手段，在數位經濟市場仍在發展的情況下來看，應該謹慎思考數位環境與傳統上競爭法的差異，以避免扼殺仍在發展中的數位環境商業和經濟模式。

資料來源：本計畫拍攝

圖 110「反托拉斯適合 21 世紀嗎？」場次截圖

（五）大數據和合併控制：公司防禦失敗和殺手級收購

本場次由 Martin d'Halluin(Senior Vice President, Global Competition Law and Policy Counsel at News Corp)、Norbert Maier(Managing Economist at Copenhagen Economics)及 Nelson Jung(Partner at Clifford Chance)討論從美國、英國及澳洲的角度來看競爭管理機構如何處理全球殺手級合併案。

首先說明 2012 年 Facebook 收購 Instagram 的案例，認為 Facebook 的收購目的在於扼殺潛在的競爭對手。第二個案例說明 Google 收購 Fitbit，Google 承諾十年內不會使用 Fitbit 蒐集到的資料進行個人化廣告投放。歐盟於 2020 年 8 月展開為期四個月的調查，以瞭解這項收購案是否對未來造成競爭市場傾斜。

講者認為 Google-Fitbit 收購案將使 Google 未來能夠近用大量新的資料集，其中有近 3000 萬人的生物統計資料，包括使用者的睡眠方式、心律、健身及運動狀況。爭點在於，Google 若未來能夠近用這些生物統計資料，可能與 Google 原有的資料集（如搜尋引擎、廣告、

Android 系統、Gmail、Youtube 或 Google Map 等）進行交互使用，對使用者的健康狀況作出干擾性的判斷，並且可能導致在整個數位服務範圍佔有更強勢的領導地位。講者認為，這意味著民眾為來將無法控制自己的資料使用方式或避免 Google 的廣告投放。

資料來源：本計畫拍攝

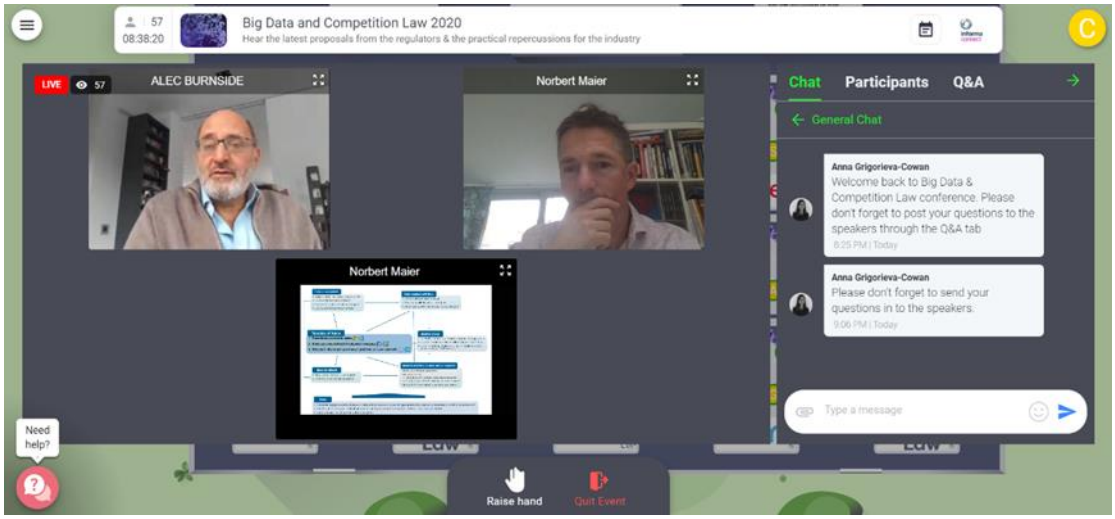
圖 111「數據和合併控制：公司防禦失敗和殺手級收購」場次截圖

（六）資料驅動市場中的市場定義

本場次由 Norbert Maier(Managing Economist at Copenhagen Economics)說明如何在資料驅動市場中定義市場。

在資料可用性增加及人工智慧技術進步的推動下，生活數位化不斷發展。所謂資料驅動市場是指由蒐集到的大數據進行分析與預測，進而產出洞察與策略，其中必須要先了解目前已擁有哪些資料、未來可以取得哪些資料，以及如何歸納、分析及應用蒐集到的資料，才能更有效地使用資料。

講者認為，資料共享機制也可用於競爭，因為資料驅動市場中，資料共享能夠加強創新能力，透過資料共享即可以減少資料流失。因此，當數位平台近用某些特定資料時（如消費者偏好），其他企業為了競爭這些資料，可能也會盡可能地完整此類資料，使得平台共享相關資料在合理條件下達到資料驅動市場的目的。



資料來源：本計畫拍攝

圖 112「資料驅動市場中的市場定義」場次截圖

（七）橫向合作準則：資料池、資料共享與資訊交換

本場次邀請 Ian Rose(Vice-President, Compliance at Volvo Trucks)、Grania Holzwarth(Legal Counsel at Deutsche Telekom)、Gareth Shier(Senior Consultant at Oxera Consulting LLP)，及 Sascha Schubert(Partner at Freshfields Bruckhaus Deringer LLP)討論資料共享在競爭法上的意義。

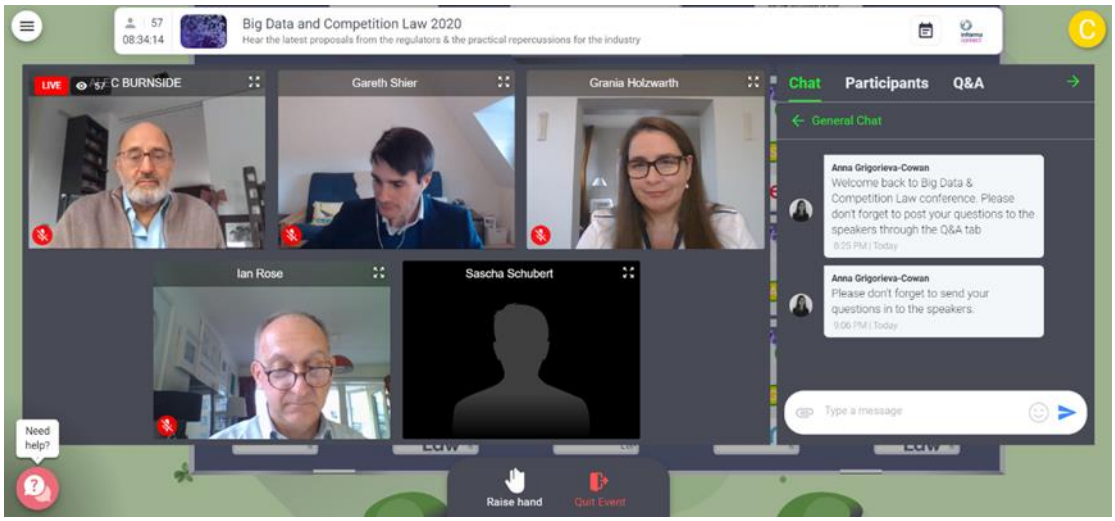
競爭者共同努力的情況可能會引起全球競爭或反托拉斯法下的問題，競爭者之間的協議可能影響價格、客戶、產量或品質。目前社會上也開始打擊資料共享的「漂綠」(Greenwash)[28]，意即僅以資料共享的名義掩蓋行使資料壟斷之實。

講者以車聯網舉例說明資料交換在競爭法上的問題。智慧汽車從車輛維修、保養、汽車保險，或是停車收費網路，串聯蒐集大量資料以進行多面化的平台服務。競爭主管機關認為這可能帶來市場支配力，使得資料交換帶來競爭法上的風險。

講者認為，在資料驅動的狀態下，應該保有更多的競爭空間，例如企業獨立決定其行業目標或標準，以選擇該結果會使何人受益與合時受益。另外，應確保資料交換或共享符合法律依據，以避免第三方

[28] 所謂「漂綠」是指公司、政府或是組織以某些行為或行動宣示自身對環境保護的付出但實際上卻是反其道而行。

競爭。



資料來源：本計畫拍攝

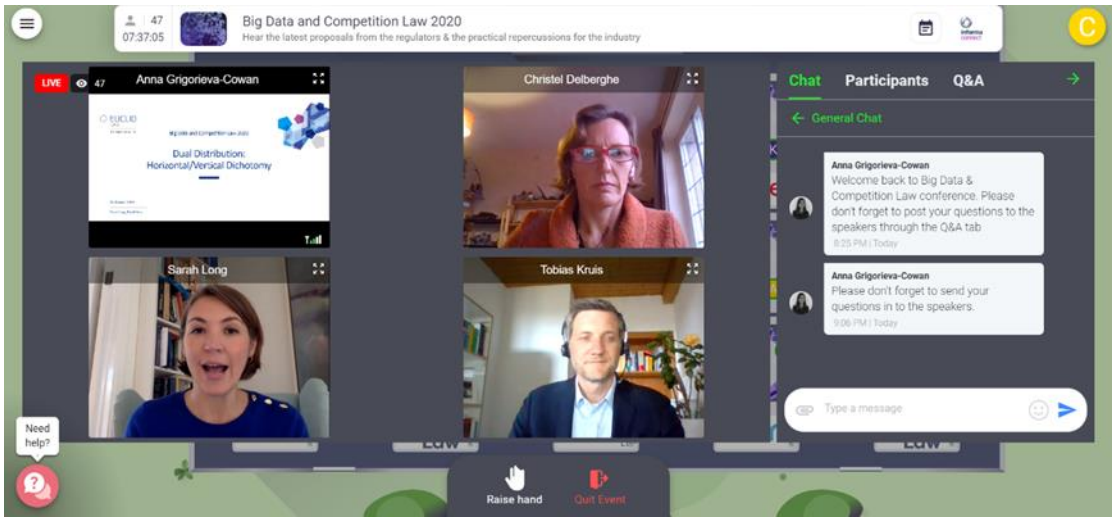
圖 113「橫向合作準則：資料池、資料共享與資訊交換」場次截圖

（八）水平/垂直二分法和雙重分配

本場次由 Tobias Kruis(Senior Counsel - Competition Law at Tech Data)、Christel Delberghe(Director, Competitiveness and Commercial Relations at EuroCommerce)、Sarah Long(Partner at Euclid Law)主講，以 Amazon 為例，說明企業競爭的垂直關係及水平關係。

當企業存在商業化過程的不同層級時（如供應商和經銷商），應被認為是垂直關係；當企業具有可替代商品或服務，即具有潛在競爭關係時，屬於橫向關係；雙重分配模式則同時涉及與經銷商的垂直關係橫向關係，這種混和模式可能會為競爭法上評估是垂直還是橫向關係帶來挑戰。

Amazon 作為第三方供應市場，同時也是出售商品的賣家，此種混合模式可能使 Amazon 在作為第三方市場角色時，可以利用自己平台上的其他資料，導致在競爭上形成壟斷市場。講者認為，若是資料交換的資料具有敏感性，例如商品價格、折扣或是客戶名稱，可能使 Amazon 可以不斷地加強其搜索功能和演算法，導致濫用支配地位，進而制訂掠奪性定價。



資料來源：本計畫拍攝

圖 114「水平/垂直二分法和雙重分配」場次截圖

（九）資料保護與競爭法之互動

本場次邀請 Patrick Van Eecke(Partner at Cooley)、Agustín Reyna(Director, Legal and Economic Affairs at BEUC)、Linda NiChualladh(Head of Privacy (Legal) EMEA and Assistant General Counsel at Citi)，和 Thomas Graf(Partner at Cleary Gottlieb Steen & Hamilton LLP)分享資料保護和競爭法之間是否可以進行調和。

目前，數位經濟快速發展，巨大的資料蒐集規模與市場為人民帶來便利線上數位平台，同時也有許多「市場失靈」的案例，例如平台的資料蒐集時常缺乏使用者的知情同意，以及不透明的隱私政策可能導致無法符合使用者的隱私偏好。

講者認為，資料經濟可能影響競爭法的執行，因為數位平台的定型化契約服務條款時常對使用者增加使用成本。因此，競爭的目的在於為消費者的各項利益（包含隱私權利）及經濟市場中謀求最大的福利。

資料來源：本計畫拍攝

圖 115「資料保護與競爭法之互動」場次截圖

第二節 隱私+安全秋季線上論壇

一、研討會資訊

表 17「隱私+安全秋季論壇」研討會資訊

名稱	隱私+安全秋季論壇(Privacy+Security Forum Fall Academy)
時間	2020 年 10 月 22 日至 10 月 23 日
地點	線上
出席人員	周芷瑄、許嘉芳

資料來源：本計畫製作

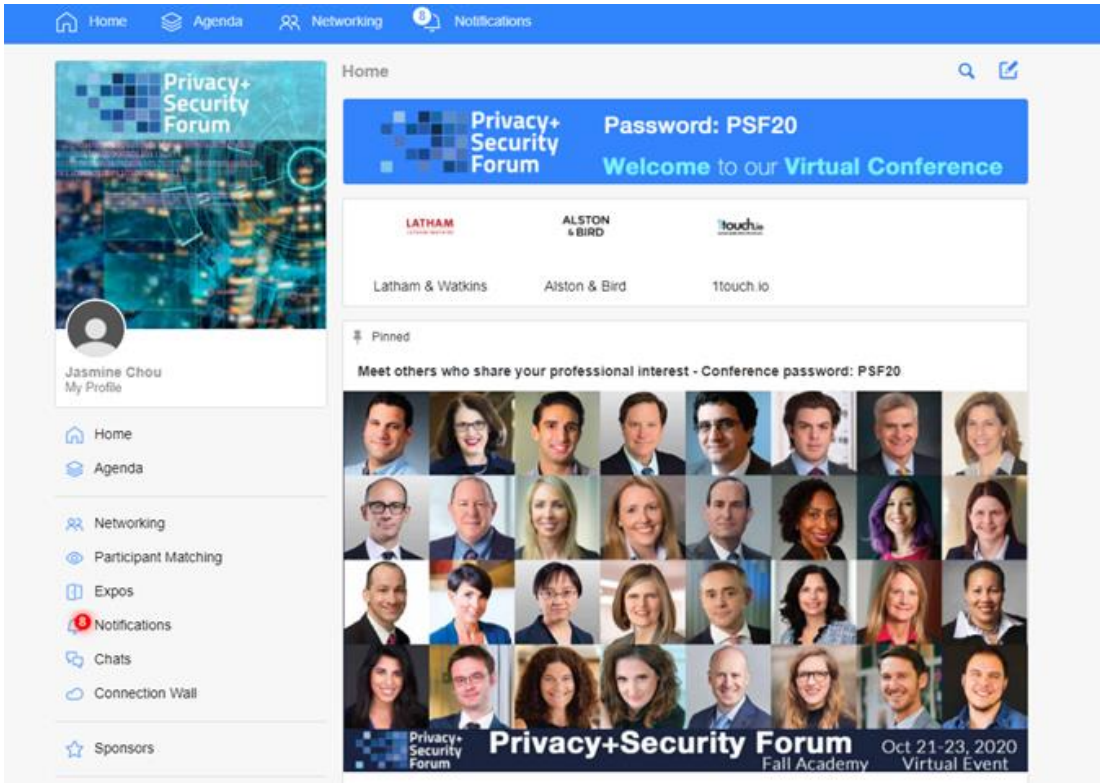
（一）整體說明

The Privacy + Security Academy 成立於 2014 年，創辦人為國際隱私法專家 Daniel Solove(John Marshall Harlan Research Professor at George Washington University Law School)和 Paul Schwartz(Jefferson E. Peyser Professor at University of California Berkeley School of Law)。兩位創辦人每一年於美國華盛頓特區(Washington DC)籌備舉行 2 場研討會，今年受 COVID-19 疫情影響改由線上舉辦，依然吸引世界各地

隱私界的權威前往參與，包括律師、資料隱私委員長、學界教授、科技工程師、智庫研究員、政策制定者等。

本次 2020 年度「隱私+安全秋季論壇」(Virtual Fall Academy 2020 Privacy + Security Forum)由 Privacy + Security Academy 舉辦，於兩天議程中與線上參與者分享近期國際隱私法、各國隱私法趨勢及新興法規，集結隱私業界專業人士提供實務經驗及知識分享，更加證明隱私議題日重，後疫情時代各國將更重視隱私及資料安全。

會議主題為「隱私+安全秋季論壇」，議題包含大數據、一般隱私、消費者隱私（如美國加州消費者隱私保護法探討）、健康隱私（如聯邦健康資料隱私立法、COVID-19 防疫追蹤技術隱私風險等）、隱私保護管理制度、國際隱私與相關案例等，不僅是隱私保護，還有與資料安全相關之議題探討。



資料來源：本計畫拍攝

圖 116「隱私+安全秋季論壇」截圖

（二）議程資訊

表 18「隱私+安全秋季論壇」議程資訊

2020 年 10 月 22 日		
時間	主題	參加人
10:00–11:00	**您準備好應對全球性事件了嗎？** Are you ready for a Global Incident?	
	美國和德國在 Covid-19 中之隱私和公民自由取捨 Covid-19, Privacy and Civil Liberties in the U.S. and Germany	許嘉芳
	歐洲實施 GDPR 之四個主要國家：愛爾蘭、德國、義大利和英國 GDPR Enforcement Across Four Key European Countries: Ireland, Germany, Italy and the UK	周芷瑄
	法國、德國和英國之隱私權發展 Privacy Developments in France, Germany, and the UK	
	IT 系統整合及隱私 Privacy Integrations with IT	
	數位化轉型時代：在日新月異的環境中構建隱私和安全實踐 The Era of Digital Transformation: Building A Privacy and Security Practice in the Ever-Changing Landscape	
11:30 – 12:30	**歐盟法院案例更新** CJEU Caselaw Update	許嘉芳
	數位醫療隱私：OCR 和 FTC 觀點 Digital Health Privacy: OCR and FTC Perspectives	周芷瑄

2020 年 10 月 22 日		
時間	主題	參加人
	Schrems 案後解決方案–如何在短期和長期內解決監視問題 Post-Schrems Solutions – How Can the Surveillance Problem be addressed in the short and long-term	
	各品牌間之隱私和透明度差異 Privacy and Transparency as a Brand Differentiator	
	在 Uber 之後－負責任的揭露要求及漏洞獎金計劃 Taming the Wild West – Responsible Disclosure and Bug Bounty Interactions after Uber	
13:00- 14:00	**專家與談：──在隱私權之前：人工智慧、演算法和新技術** Keynote: Tales from the Front Lines of Privacy: AI, Algorithms, and New Technologies	
14:00- 15:00	**數位化未來：使用隱私計畫引領創新** Digitalization for Tomorrow: Using your Privacy Program to Lead on Innovation	
	聯邦健康資料隱私立法：超越 HIPAA Federal Health Data Privacy Legislation: Beyond HIPAA	許嘉芳
	全球隱私設計 Global Privacy by Design	
	將影響企業營運的新隱私法規－LGPD(巴西)、APPI 修正案（日本）和 CPRA（加州） New Privacy Laws that Impact Your Operations – the LGPD (Brazil), APPI Amendments (Japan), and the CPRA (California)	周芷瑄

2020 年 10 月 22 日		
時間	主題	參加人
	州政府希望在聯邦隱私法中看到什麼 What State AGs Want to See in a Federal Privacy Law	
15:30-16:30	**巨量資料：隱私法對巨量資料分析的影響** Big Data: Impact of Privacy Laws on Big Data Analytics	
	規範新科技的政策考慮 Policy considerations for regulating new technologies	許嘉芳
	Schrems II：管理跨境資料風險之實際方法 Schrems II: Practical Approaches to Manage Cross Border Data Flow Risks	周芷瑄
	解決全球疫情大流行期間有關資料外洩的訴訟 Settling Data Breach Class Actions During A Global Pandemic	
	CCPA 作為行動目標 The CCPA as Moving Target	

2020 年 10 月 23 日		
時間	主題	參加人
10:00–11:00	**中國在全球網路安全和隱私中的作用** China's Role in Global Cybersecurity and Privacy	許嘉芳
	資料稽核和數位解碼 Data Audits and Unscrambling the Digital Eggs	
	2021 年聯邦和州的隱私立法 Federal and State Privacy Legislation for 2021	周芷瑄
	金融和保險業中資料安全法規──以美國和瑞士	

2020 年 10 月 23 日		
時間	主題	參加人
	為例 Information Security Regulation in the Financial and Insurance Industries – U.S. and Swiss Laws	
11:30 –12:30	**CCPA 和其他網路安全訴訟** CCPA and Other Cybersecurity Litigation	
	接觸者追蹤技術：公共衛生利益與隱私風險之間的平衡在哪裡？ Contact Tracing Technologies: Where is the Balance of Public Health Benefits vs. Privacy Risks?	周芷瑄
	資料與民主：數位隱私、基本權和權力影響的相互關係 Data and Democracy: The Intersection between Digital Privacy, Civil Rights, and Influence Operations	許嘉芳
	CPRA 對數位廣告的影響 Impact of CPRA on Digital Advertising	
	勒索病毒──駭客攻擊與法律風險之變化 Ransomware – Changes in Attacks and Changes in Legal Exposure	
13:00- 14:00	**專家與談：Helen Dixon** Keynote: Helen Dixon	
	CCPA 執行動向 CCPA: What's Being Enforced (and What's Not)	周芷瑄
	公司董事的網路安全維護職責 Corporate Directors' Duty of Cybersecurity Care	
	處理 DSAR Dealing with DSARs	許嘉芳

2020 年 10 月 23 日		
時間	主題	參加人
	國家隱私法和受規範的部門 National Privacy Law and the Regulated Sectors	
	適應日新月異的 TCPA 合規性 Navigating the Ever-Changing Landscape for TCPA Compliance	
15:30-16:30	**雞尾酒論壇：透過設計實現安全性和隱私性** A Conversation with Cocktails: Operationalizing Security & Privacy by Design	周芷瑄
	最新的全球廣告定位和分析追蹤規則 An Update on the Regulation of Tracking for Ad Targeting and Analysis Around the World	許嘉芳
	從隱私政策到隱私行動 From Privacy Policy to Privacy Ops	

資料來源：本計畫編譯

二、場次重要摘要

（一）歐洲實施 GDPR 之四個主要國家：愛爾蘭、德國、義大利和英國

本場邀請 Colin Rooney(Partner of Arthru Cox)、Rohan Massey(Partner of Ropes & Gray)、Vera Jungkind(Partner of Hengeler Mueller)和 Laura Liguori(Partner of Portolano Cavallo)四位來自愛爾蘭、英國、德國及義大利合夥律師與談，分享各國 GDPR 實務執行之體制與狀況(GDPR enforcement)。

四位律師表示愛爾蘭、英國、德國及義大利在執行 GDPR 之體制及方式相似，皆以投訴方式(complaint based approach)展開資料保護執委會(data protection commission)調查程序，投訴方式分為兩種：投訴者自行遞交投訴文件或資料保護執委會自行對某業者展開調查。

愛爾蘭同英國為英美法系(common law system)，在英美法系國家中，監理機關(regulator)職權必須與法院職權平衡。各國資料保護法雖賦予監理機關龐大權力(legislative powers)以執行資料保護之法定職責，惟法院保有詮釋法律之權力(judicial interpretation)隨時監督及糾正監理機關執行職責，避免權力濫用。法院並不是只有在監理機關完成調查後才能行使監督，法院對監理機關之監督權任何時候都存在、任何時候得透過訴訟啟動監督權。

各位專家一致認為，歐盟需要一套全歐盟國家能共同執行的(common)、簡單的(comprehensive)GDPR 執行標準和方式，希望歐盟資料保護委員會(European Data Protection Board, EDPB)能承擔此業務，更希望 EDPB 之後能頒布主題性的資料保護指引，特別是針對人工智慧或生物識別技術（biometrics）。

資料來源：本計畫拍攝

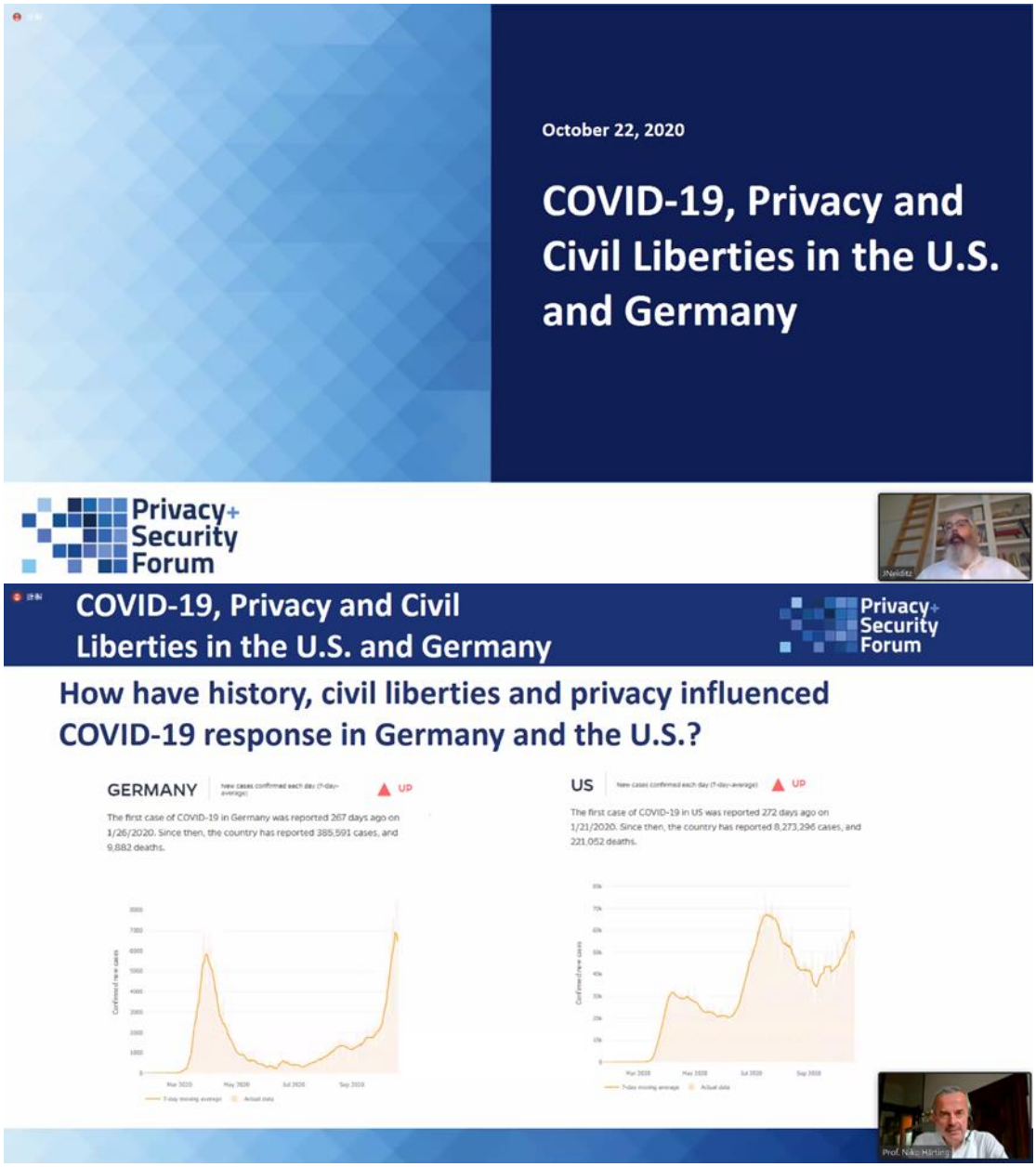
圖 117「歐洲實施 GDPR 之四個主要國家」場次截圖

（二）美國和德國在 Covid-19 中之隱私和公民自由取捨

由於 Covid-19 大流行讓全世界都開始重新思考公民自由與隱私之間的關係，而美國和德國在資料保護規則、公共衛生系統、政府、社會文化，和歷史發展都大相逕庭，故本場次邀請 Niko Härting(Partner, HÄRTING Rechtsanwälte) 、 Yendelela Neely Holston(Partner and Chief Diversity & Inclusion Officer, Kilpatrick Townsend & Stockton)和 Jon Neiditz(Partner, Kilpatrick Townsend & Stockton)分享美國與德國在與病毒鬥爭的過程中，對於人與人之間的社交距離，以及人與政府之間的關係如何變化。這些變化對於未來在隱私權和資料保護之間將造成什麼樣的後果。

本場次首先介紹美國與德國隱私權的歷史發展。美國憲法中雖然沒有明確提及隱私權，但隱私權最早出現的時間可以追溯到 1890 年，由 Samuel Warren 和 Louis Brandeis 在「哈佛法學評論」所提出的「The Right to Privacy」一文。而相較於美國把隱私權認為是一種不受干擾的權利，德國的隱私權強調的是人格的自由發展性，是人格完整不可或缺之要件。

再從 2020 年 5 月發生的佛洛伊德案件說明新興科技對於隱私的侵犯及不公平性，認為新興科技造成民眾無時無刻都在被記錄及分享，這些影響人民自由的問題都應該被視為隱私問題。然而，講者認為，美國在 COVID-19 大流行期間，隱私幾乎蕩然無存。在疫苗出現之前，面對疫情最好的方法是保持社交距離及戴口罩，惟戴口罩彷彿成為一種政治選擇，將個人資料及被認為是敏感的健康資料掛勾。因此，講者認為，應該從更廣泛的面向去考慮個人隱私以及合理的隱私期待範圍。



資料來源：本計畫拍攝

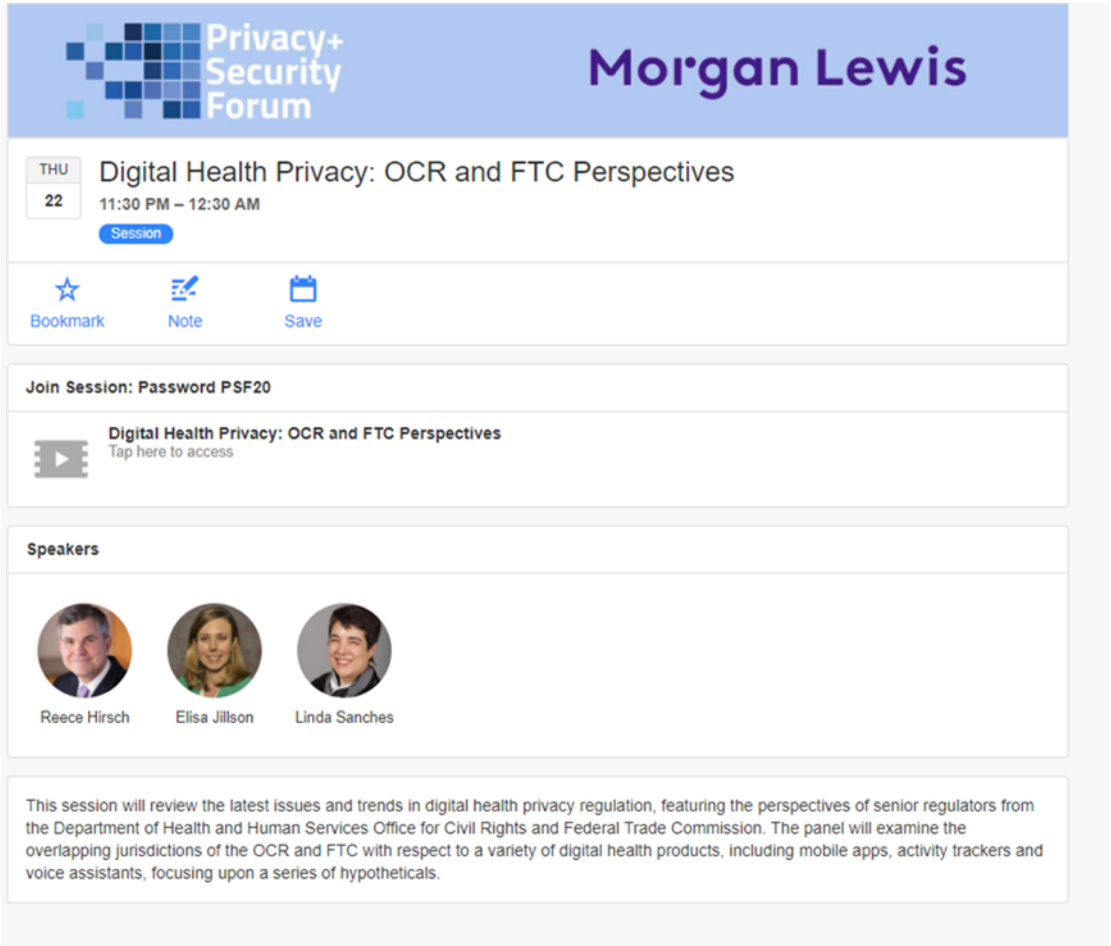
圖 118「美國和德國在 COVID-19 中之隱私和公民自由取捨」場次截圖

（三）數位醫療隱私：OCR 和 FTC 觀點 Digital Health Privacy: OCR and FTC Perspectives

本場邀請 Reese Hirsch(Co-head of Privacy & Cybersecurity Practice of Morgan Lewis)、Eilsa Jillson(Attorney of Federal Trade Commission)和 Linda Sanches(Senior Advisor of Office for Civil Rights)討論數位化時代醫療資料隱私法遵主題。

美國規範醫療資料隱私之聯邦法係「健康保險可攜性及責任法」(The Health Insurance Portability & Accountability Act, HIPAA)和聯邦交易委員會法(Federal Trade Commission Act, FTC Act)第五條「不公平或或欺罔之行為慣性」(unfair or deceptive acts and practices)。HIPAA 主管機關係民權辦公室(Office for Civil Rights)；FTC Act 主管機關係聯邦貿易委員會。FTC 管轄權(jurisdiction)非常廣，管轄任何傷害消費者之行為。原則上，HIPAA 管轄權外的機關落入 FTC 管轄權。HIPPA 明確於法條中列出醫療資料隱私保護的規定，反之，FTC Act 未明確於法條中列出醫療資料隱私保護的規定，相關規定存在於判例中。

HIPPA 中較為複雜及困難的概念為商業伙伴(business associates)。商業伙伴雖不是 HIPAA 直接規範的受規範機關(covered entities)，HIPAA 針對商業伙伴有特定的隱私保護規範。通常機關在審視是否屬於商業伙伴時，爭點往往為「機關是否代表受規範機關行事」(whether a person or entity is acting on behalf of a covered entity)。當前最新的議題為，消費者下載醫療 APP 去追蹤控管其慢性病，使用醫療 APP 時必定會蒐集、處理、利用、傳輸消費者的醫療資料，這時醫療 APP 的開發公司是否是商業夥伴？三位專家認為應特別注意金錢流向及醫療資訊流向來斷定此問題。



資料來源：本計畫拍攝

圖 119「數位醫療隱私」場次截圖

（四）歐盟法院案例更新

本場次邀請 Daniel P. Cooper(Partner, Covington)、Joe Jones(Head of International Data Transfer Regime, UK Dept. for Digital, Culture, Media & Sport)、Caroline Wilson Palow(Legal Director & General Counsel Privacy International)和 Herke Kranenborg(Member Legal Service, European Commission)分享兩個近期歐盟法院作出的判決，以說明歐盟法院在面對 GDPR 時的一些關鍵原則。

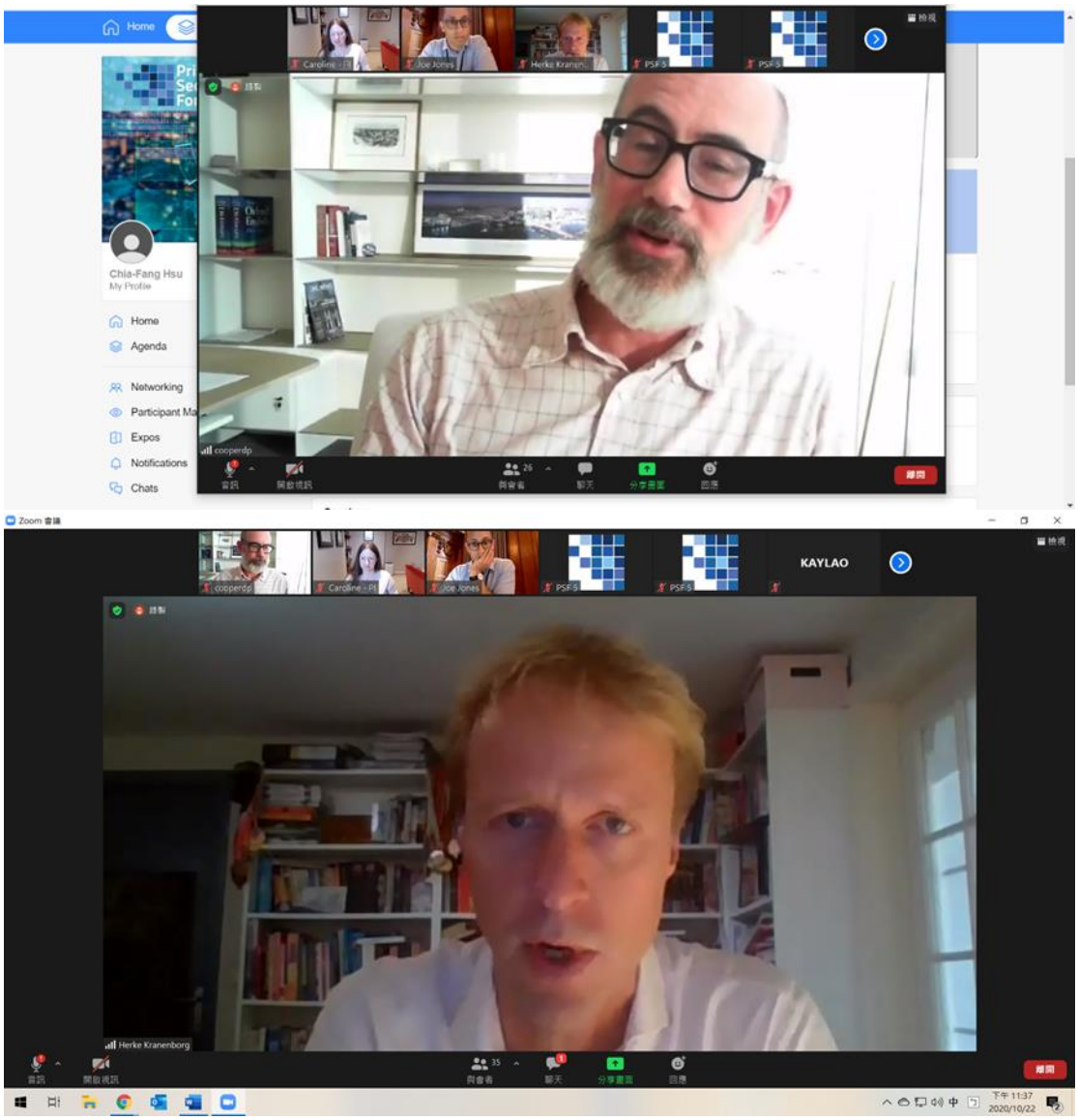
1. Schrems II

歐盟法院在 2020 年 7 月 16 日廢除歐盟與美國之間的隱私盾資料保護傳輸協議。原告 Schrems 認為，Facebook 把使用者的部分或全部資料從歐洲總部（愛爾蘭）傳回美國處理，但美國的法令並未提供足夠的隱私保護，因此要求禁止資料的轉移。法院認為，

美國法令對於公家機關存取歐洲民眾資料的保護有限，並不符合歐盟要求移轉資料的第三方。若欲將歐盟之個人資料移轉的第三國，對於資料保護水平必須具備與歐盟隱私法令(GDPR)同等級保護的規定，因而認定隱私盾協議是無效的。

2. 歐盟法院禁止政府大規模蒐集人民通訊資料

英國在 2016 年通過調查權力法案，整合執法機關和情報單位資料蒐集的相關權利，以授權通信監察書及監督的方式，要求業者保留網路連結紀錄以提供執法單位識別網路使用者。因此，隱私倡議團體 Privacy International 在 2017 年提出訴訟，要求歐盟法院針對英國、比利時和法國政府透過立法，允許情報機關要求電信業者大規模蒐集民眾通訊資料的行為是否違憲進行審理。歐盟法院於 2020 年 10 月 6 日作出裁定，禁止政府僅以打擊一般犯罪或確保國家安全為由，要求電子通訊服務供應商對民眾流量資料及地點資料進行大規模、無差別的傳輸的立法。



資料來源：本計畫拍攝

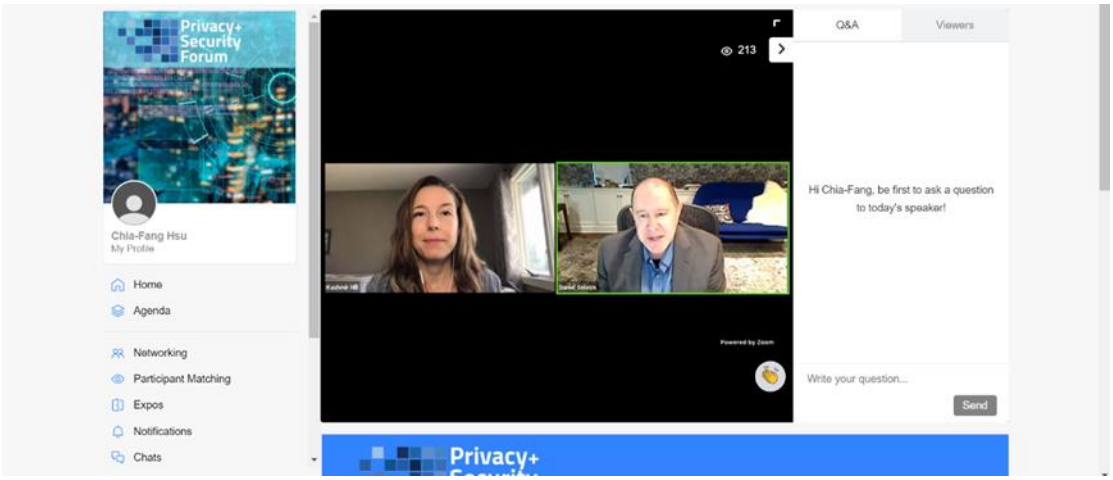
圖 120「歐盟法院案例更新」場次截圖

（五）專家與談：在隱私權之前：人工智慧、演算法和新技術

本主題演講由 Kashmir Hill 主講，分享對隱私發展的看法以及科技對於日常生活和自由的影響。

講者分享 Airbnb 的商業模式，Airbnb 的隱私條款長達一百頁卻沒有人會認真閱讀裡面的內容。講者認為 Airbnb 蒐集訂房資料並分析的行為可以取得許多個人資料，使用者卻沒有意識到這件事情。人們對於演算法如何進行資料處理分析並改變自己的生活一無所知，講者認為，並非要阻止企業取得個人資料，而是應該把隱私和科技擺

在同一地位進行思考，讓民眾更了解如何保護自己的隱私。



資料來源：本計畫拍攝

圖 121「專家與談」場次截圖

（六）將影響企業營運的新隱私法規－LGPD（巴西）、APPI 修正案（日本）和 CPRA（加州）

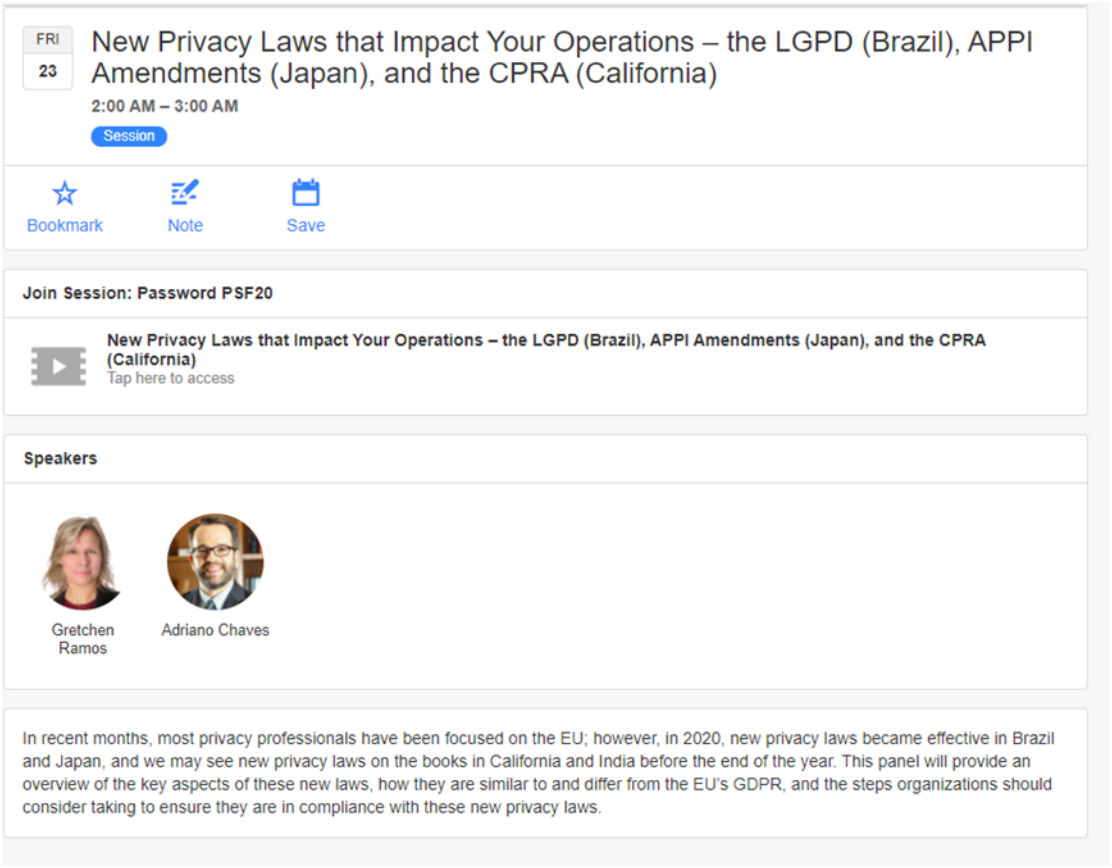
本場邀請 Gretchen Ramos(Co-Chair of GlobalData)及 Adriano Chaves(Partner of CGM)介紹巴西一般個人資料保護法(Lei Geral de Proteção de Dados, LGPD)、日本個人資訊保護法(the Act on the Protection of Personal Information, APPI)、加州隱私權利法(California Privacy Rights Act, CPRA)。

巴西的 LGPD 係依 GDPR 草擬，被譽南美 GDPR。巴西 LGPD 於 2020 年 9 月 18 日正式實施，行政罰鍰於 2021 年 8 月 1 日正式實施，提供民間企業緩衝期。雖「從設計包含隱私」(Privacy by Design)並未明文規定於 LGPD 中，卻是 LGPD 的核心精神。GDPR 並未規定每一個公司需要有隱私保護長(Data Protection Officer, DPO)，惟 LGPD 規定每一間公司應有 DPO，DPO 可以是個人(individual)或機關(entity)，可以是內部或外部。目前，雖未明文規定，絕大多數公司會聘請律師作為外部 DPO。

日本 APPI 修法後於 2022 正式實施，國際上仍認為與 GDPR 相比，本次修法後的罰款依然較低。

會議時，Ramos 認為 2020 年 11 月 3 日公投應會通過，藉此，加

州效力最強的隱私法 CPRA 將於 2023 年 1 月 1 日 正式實施。CPRA 廢除加州消費者隱私法(California Consumer Privacy Act, CCPA)所賦予的 30 天修復區間(30 day cure period)，違規者將不再有 30 天得修復違反 CPRA 之條款，如違規得立即負法律責任。



資料來源：本計畫拍攝

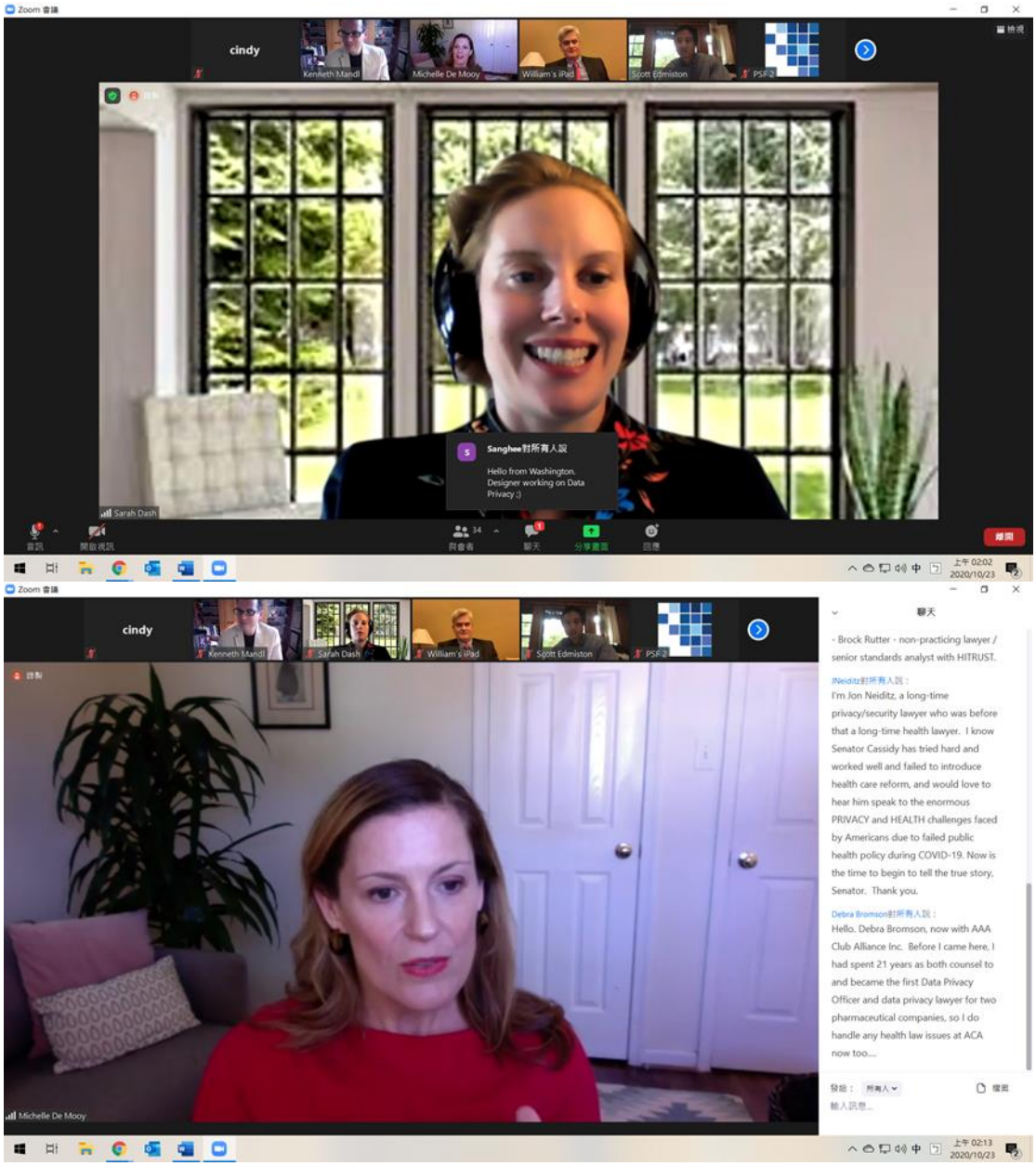
圖 122「將影響企業營運的新隱私法規」場次截圖

（七）聯邦健康資料隱私立法：超越 HIPAA

本場次邀請 Senator Bill Cassidy(M.D., U.S. Senator, Louisiana)、Dr. Kenneth Mandl(Director, Computational Health Informatics Program, Boston Children's Hospital & Donald A.B. Lindberg Professor, Harvard Medical School)、Sarah Dash(President & CEO, Alliance for Health Policy)以及 Michelle De Mooy(Principal, De Mooy Consulting)，說明「健康保險可攜性及責任法」(The Health Insurance Portability and Accountability Act, HIPAA)中未提到的健康資料種類，包括可穿戴式裝置中的健康資料、對電子健康紀錄的 API 訪問，以及消費者的基因檢測及健康碼等。

講者認為，雖然健康大數據有助於醫療及治療方法的研究，惟健康資料具有敏感性，資料主體通常不了解該病歷資料蒐集的內容範圍及其所創造的利益。如果穿戴式裝置能夠蒐集並下載分析資料主體之健康資料，將可能造成侵犯個人隱私的風險。對於個別病患受到的醫療治療利益，與整體資料主體的隱私外洩風險，二者是無法衡量的。

目前資料經濟的市場快速發展，在資料蒐集成本降低的同時，隱私成本就會上升。科技創新應該要取得使用者的信賴，並將隱私權及其他基本人權放在同一地位進行思考，使得任何族群的人都可以公平地使用該科技技術。因此，COVID-19 大流行即提供科技與隱私衡平的一個很好的測試機會，以在未來建立更適當的資料保護機制。



資料來源：本計畫拍攝

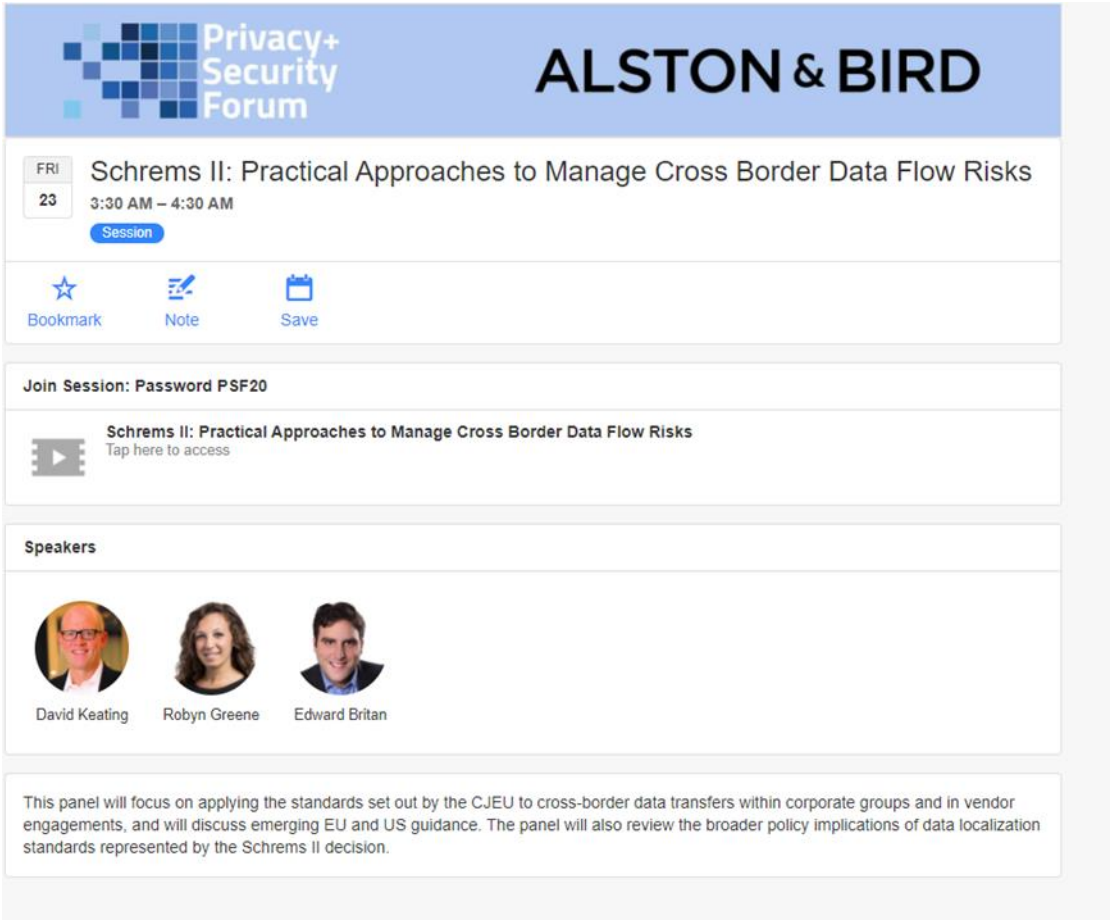
圖 123「聯邦健康資料隱私立法：超越 HIPAA」場次截圖

（八）Schrems II：管理跨境資料風險之實際方法

本場邀請 David Keating(Partner of Alston & Bird)、Robyn Greene(Privacy Policy Manager of Facebook)和 Edward Britan(Senior Director & Policy Counsel for Privacy & AI of Microsoft)討論既 Schrems II 一案判決歐盟美國隱私盾無效後應如何在實務上管理跨境資料傳輸之風險。

Schrems II 判決歐盟美國隱私盾無效，標準契約條款(SCCs)持續有效惟應落實額外措施(supplementary measures)。Keating 表示，額外措施之法律意涵及確切應做到之哪些事項，待歐盟資料保護委員會發表指引，並希望能將額外措施清楚明文訂之。Britan 表示，Schrems II 判決後美國與歐盟正積極討論制定新的歐盟美國隱私盾，目前進度並未因美國總統大選受延宕。

Green 認為現代的企業勢必需要跨境傳輸個人資料，因此 Schrems II 判決不單只影響 Facebook，亦會影響整個科技產業。Schrems II 判決雖然是隱私保護的勝利，然而在倡議隱私保護的同時已侵犯、犧牲人民的其他基本人權—經濟權(economic rights)、資訊自由權(right to freedom of information)等，尤其現代人往往透過網路行使這些權利。Facebook 認為，Schrems II 所產生的影響唯有政府能解決並期盼之。



資料來源：本計畫拍攝

圖 124「Schrems II：管理跨境資料風險之實際方法」場次截圖

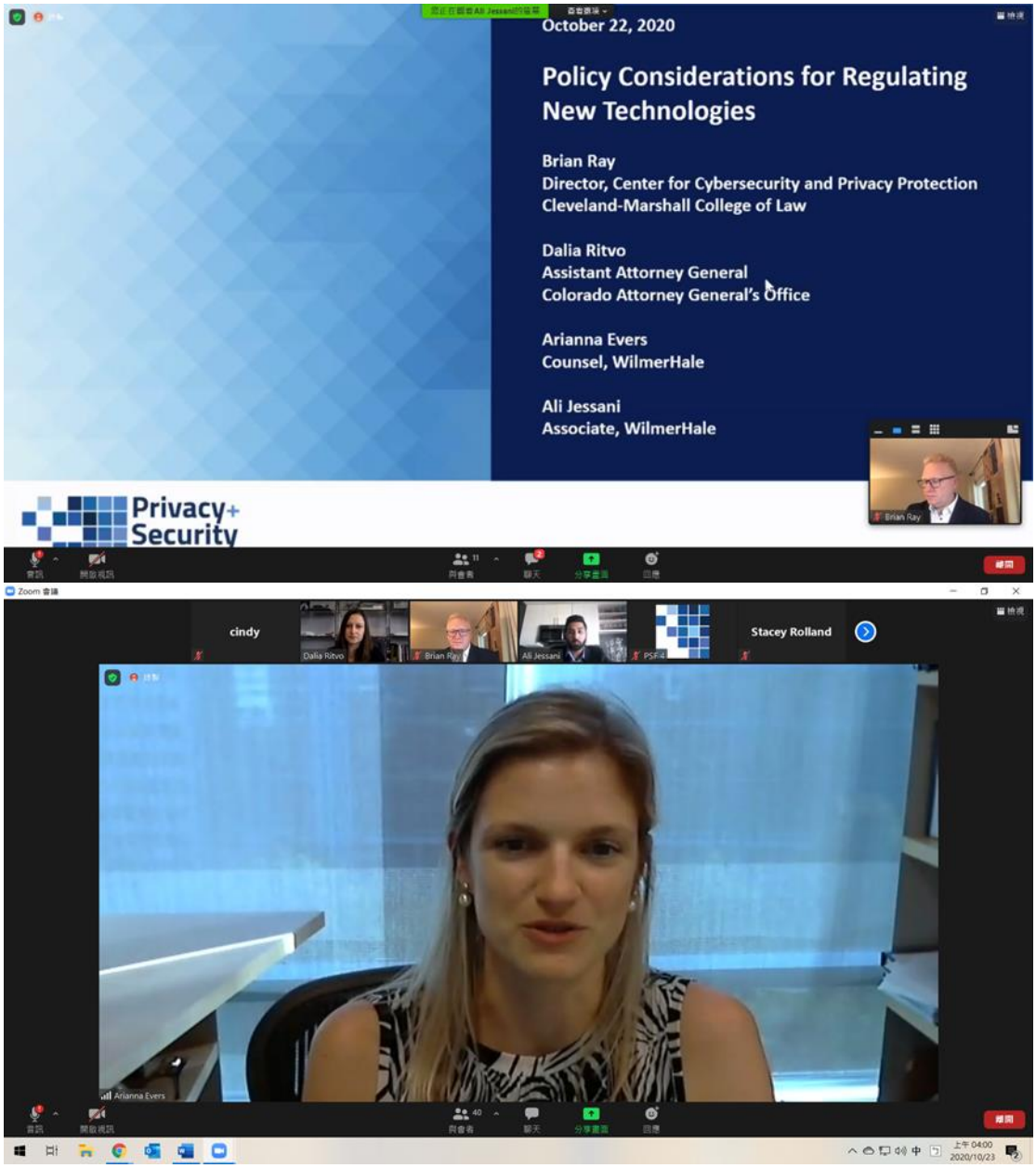
（九）規範新科技的政策考慮

本場次由 Arianna Evers(Partner, WilmerHale)、Ali Jessani(Privacy & Cybersecurity Group, WilmerHale)、Brian E. Ray(Director, Center for Cybersecurity and Privacy Protection)和 Dalia Ritvo(Assistant Attorney General, Colorado Attorney General's Office)討論目前的生物辨識隱私法和研議中的聯邦立法，說明在實施和執行這些法律時會出現的一些政策問題。

美國目前並未有針對生物辨識的聯邦法律，僅在伊利諾州、華盛頓州和德州有生物辨識隱私法，其中最具代表性的是伊利諾州的「生物辨識資料隱私法」(Biometric Information Privacy Act, BIPA)。BIPA 要求在蒐集和公開生物辨識資料之前須取得資料主體之書面同意、禁止從生物辨識技術中獲利，並要求企業需有合理的注意標準

(reasonable standard of care)以保護生物辨識資料。2020 年 8 月，參議員 Bernie Sanders 和 Jeff Merkley 提議參考 BIPA，提出「國家生物辨識資料隱私法案」(National Biometric Information Privacy Act, NBIPA)。限制企業未經書面同意即蒐集、處理、利用，甚至交易個人生物辨識資料的能力，並須向資料主體揭露其所蒐集之個人資料。

講者認為，若是企業以商業目的蒐集個人生物辨識資料，該資料庫之後卻出售給政府，作為如犯罪資料庫等具有「重大公益目的」使用，恐仍產生道德上即憲法上之質疑。技術使用並不是非黑即白，應該確保在技術準確性和是否存有偏見方面，人類仍然保有自由裁量權。在科技使用的監管上，應思考在什麼樣科技應用的程度上須要進行立法，而非僅闡述類似具體標準的政策。



資料來源：本計畫拍攝

圖 125「規範新科技的政策考慮」場次截圖

（十）2021 年聯邦和州的隱私立法

本場邀請 Tim Tobin(Partner of Hogan Lovells)、Jared Bomberg (Senior Counsel of US Senate Committee of Commerce, Science and Transportation)、Olivia Trusty(Policy Director of US Senate Committee of Commerce, Science and Transportation)，和 Bret Cohen(Partner of Hogan Lovells)主要討論目前美國兩黨分別提出的聯邦隱私法草案。Trusty 係共和黨代表(Republican)、Bomberg 係民主黨代表(Democrat)。

近幾年國際社會越來越重視隱私法的重要性，各國積極修國內隱私法，2020 年起，美國國內不斷有聲浪呼籲應有一部聯邦隱私法，目前美國並沒有一部統一的聯邦隱私法，聯邦隱私法係以分散的部門法條(sectoral laws)形式存在，例如，醫療資料的個資保護屬「健康保險可攜性及責任法」(The Health Insurance Portability & Accountability Act, HIPAA)規範。

共和黨提交之聯邦隱私草案係安全資料法(Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, SAFE DATA Act)。本法立法理由及目的為：保障消費者既有的隱私權利(privacy rights for consumers)、鞏固法規明確性(regulatory certainty)、提供企業清楚及實用的規則因現有的聯邦隱私法複雜和多處相互矛盾。本法包含資料安全及資料最小化要件，並賦予聯邦交易委員會(Federal Trade Commission, FTC)裁罰民事罰鍰(civil penalty)之權力。

民主黨提交之聯邦隱私草案係消費者網路隱私權利法(Consumer Online Privacy Rights Act, COPRA)。本法所賦予的消費者權利(consumer rights)與 GDPR 相似，惟 COPRA 係一部典型美國法律承襲美國隱私法歷史，並非依 GDPR 撰擬。COPRA 賦予消費者訴訟權(private right of action)，立法目的強調 COPRA 執行效力，認為一部有意義的法律應有高執行效力。

資料來源：本計畫拍攝

圖 126「2021 年聯邦和州的隱私立法場」次截圖

（十一） 中國在全球網路安全和隱私中的作用

本場次邀請 Yan Luo(Partner, Covington)、Ashden Fein(Partner, Covington)和 Samm Sacks(Senior Fellow at Yale Law School Paul Tsai China Center & Cyber Policy Fellow, New America)討論中國對於全球網路安全和隱私的影響。

中國於 2017 年 6 月通過「網絡安全法」，並於 2020 年 7 月及 10 月分別提出「數據安全法」草案及「個人信息保護法」草案，預計明年通過施行。本場次分別介紹中國這三項法律的內涵，並討論這三項法律對於全球網路安全和資料隱私可能造成的影響。

「網絡安全法」是中國第一部關於全面規範網路空間安全權的基礎法律，規定任何個人和組織不得竊取或者以其他非法方式獲取個人資料，不得非法出售或者非法向他人提供個人資料；「數據安全法」

要求外國企業若要在中國境內營運，將得依法調查其資料，若被認定為危害中國國家安全、公共利益或者公民、組織合法權益的資料活動，將被追究相關責任；「個人信息保護法」要求關鍵基礎設施的營運者和處理大量個資的處理者，須將資料儲存在境內，也對資料跨境傳輸做一般性的限制，意即除了個資保護，還多了「國安」以及「貿易競爭」的考量。

講者認為，美國正透過外資投資委員會(Committee on Foreign Investment in the United States)或是其他工具限制中國對美國民眾資料的近用，而歐洲陷入中美科技冷戰的中間。「數據安全法」中對於域外效力的規定反映出對美國「雲端法」(CLOUD Act，全名為「釐清境外合法利用資料法」(Clarifying Lawful Overseas Use of Data Act))和 GDPR 的態度。因此，中國目前的資料治理政策是由於資料主權的衝突而引發的全球連鎖反映。

資料來源：本計畫拍攝

圖 127「中國在全球網路安全和隱私中的作用」場次截圖

（十二） 接觸者追蹤技術：公共衛生利益與隱私風險之間的平衡在哪裡？

本場邀請 Joseph Ali(Associate Director of Johns Hopkins Berman Institute of Bioethics)、Brian Hutler(Hecht-Levi Fellow of Johns Hopkins Berman Institute of Bioethics)、Deven McGraw(Chief Regulatory Officer of Ciitizen)和 Nancy Perkins(Counsel of Arnold & Porter)討論對抗 COVID-19 疫情下研發的接觸者追蹤技術所產生之隱私風險以及該如何與公共利益達成平衡。

接觸者追蹤技術(contact tracing technologies)的研發以公共衛生利益為目的，惟牽涉民眾個人資料的分享，對隱私產生莫大風險。全球使用接觸者追蹤技術的國家有：俄羅斯、中國、南韓、日本、印度、澳洲、紐西蘭、大多數歐洲國家、加拿大、美國、巴西等。挪威禁止使用接觸者追蹤技術。接觸者追蹤技術分為三種：以隱私保護為核心、以公共利益為核心、以兩者共同為核心。

Google 和 Apple 研發的接觸者追蹤技術係以隱私保護為核心，每位使用者手機中有一組不可識別的雜湊數值，為達防疫目的被交換、傳輸、分享，惟個人身分無法識別，資料不會儲存於 Google 和 Apple 的資料庫中。

南韓使用的接觸者追蹤技術係以公共利益為核心，確診者的位置、過去幾天的行蹤被電話公司蒐集後，政府至電話公司擷取這些資料判定接觸者，政府亦可至銀行取得確診者信用卡交易資料判定接觸者，產生隱私保護疑慮。

專家們表示，文化係影響各國應使用何種接觸者追蹤技術的重要因素，亞洲國家較注重公共利益因此其接觸者追蹤技術以公共利益為核心，反之，西方國家較注重隱私保護因此其接觸者追蹤技術以隱私保護為核心。然而，使用任何接觸者追蹤技術前都必須思考該如何在隱私保護和公共利益間取得平衡。

資料來源：本計畫拍攝

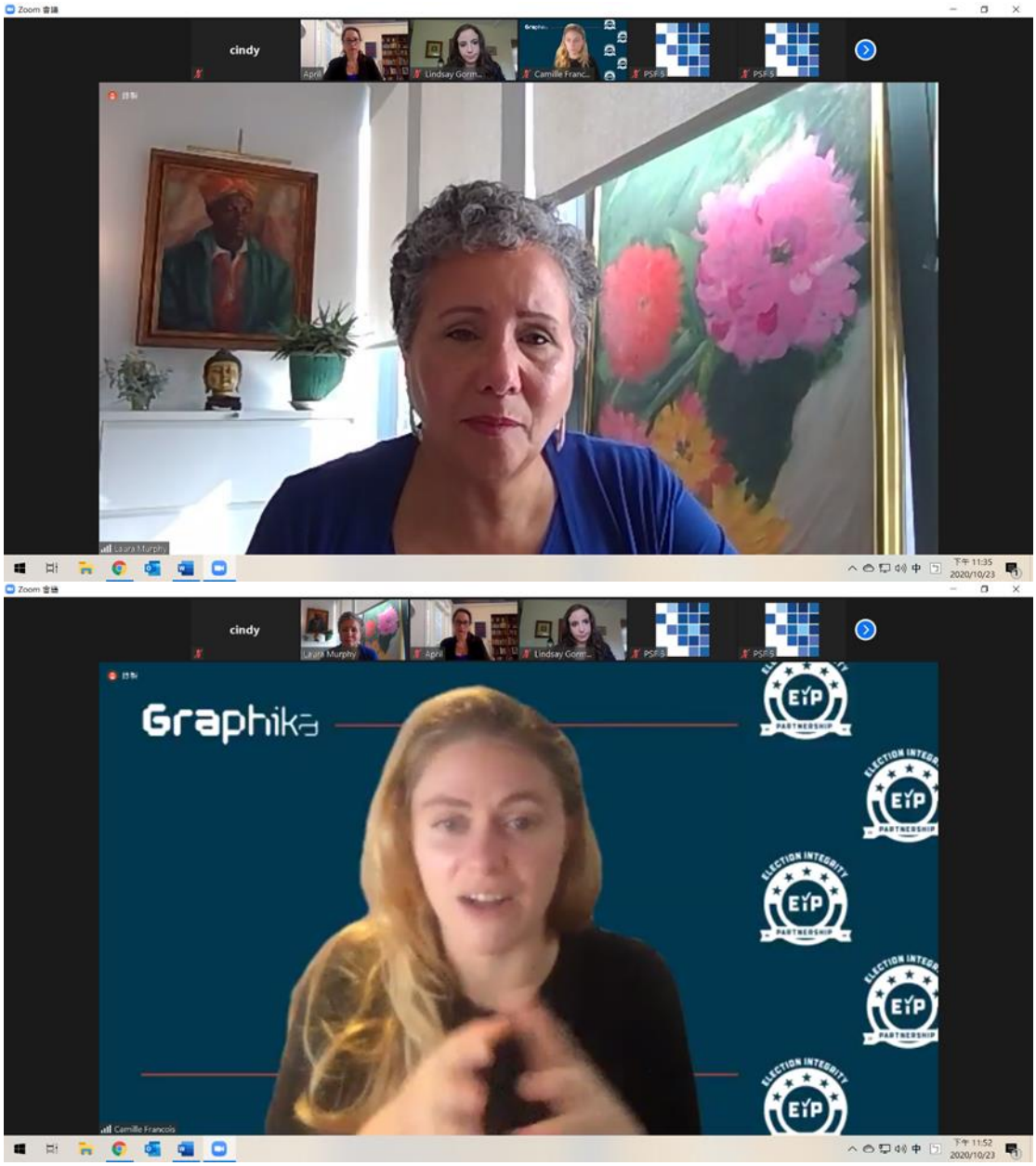
圖 128「接觸者追蹤技術」場次截圖

（十三） 資料與民主：數位隱私、基本權和權力影響的相互關係

隨著 2020 年美國大選即將到來，有關於假新聞的影響力將可能影響大選的結果，故本場次邀請 April Falcon Doss(Partner, Cybersecurity & Privacy Practice Chair, Saul Ewing Arnstein & Lehr)、Laura Murphy(former ACLU legislative director and lead auditor of Facebook civil rights audit)、Camille Francois(Chief Innovation Officer, Graphika)和 Lindsay Gorman(Emerging Technologies Fellow, Alliance for Securing Democracy)討論技術、政策和法律三者的關係，了解社群媒體平台如何使用個人資料，例如將資料貨幣化、演算法的影響，以及付費廣告的作用，是如何影響目前的政治環境。

講者認為，美國沒有針對消費者資料隱私的明確法律規定，幾乎無論大型的社群媒體平台或小型的 APP 開發商，其蒐集、保存、使用、共享、出售或交叉使用個人資料都不受約束，僅要求向使用者提供資料使用的隱私聲明。然而，隨著科技產品使用日益複雜，隱私聲明通知和同意的形式已受到難以理解和冗長的因素侵蝕，消費者也無權向企業談判到不同或更好的隱私條款。尤其是已有研究顯示出對資料追蹤、蒐集、分析和開發的速度往往比消費者意識到的速度還快。

資料的使用可能是針對普通目的（如個人化廣告），當沒有如第四增補條款的保護措施限制私人企業蒐集資料，對於個人隱私受侵犯時可能沒有適當的法律保護。更可能作為政治廣告，進而影響公眾輿論的政治觀點，影響民主的價值。



資料來源：本計畫拍攝

圖 129「資料與民主」場次截圖

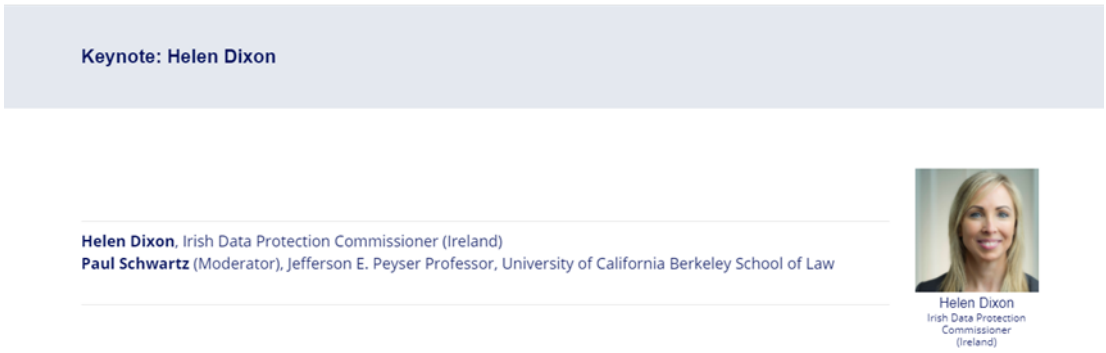
（十四） 專家與談：Helen Dixon

本場主持人 Paul Schwartz(Professor at UC Berkeley School of Law)邀請到愛爾蘭隱私保護長 Helen Dixon(Commissioner for Data Protection of Ireland)與談，分享隱私保護經驗。

愛爾蘭隱私保護委員會(Data Protection Commission of Ireland)近年頻登國際版面，除了將美國歐盟隱私盾議題帶到歐盟法院，眾多科技公司亦選擇將公司歐盟總部設在愛爾蘭。目前在愛爾蘭國內法院中，愛爾蘭隱私保護委員會身上總共有約 40 起訴訟案件，全為應答人(respondent)，愛爾蘭隱私保護委員會每天都受檢視，Dixon 表示這是好事。Dixon 表示 GDPR 法遵之執行最困難之處必然出於其規範範圍太廣，隱私委員會必須接觸各機關、政府部門、民間企業、個人，業務量龐大且複雜。其中，個人申訴案件(individual complaints)人力成本最高，每件個案必須依其情境狀況獨立審查(case by case basis)。

Dixon 表示現階段歐洲國家似乎認為 GDPR 執行的唯一方法為裁罰(fines)，他擔心之後歐洲國家會吹起罰鍰拉鋸戰，相互比較哪國判定較高罰鍰。

未來，Dixon 鼓勵歐盟國家開始多於國內法院提起 GDPR 訴訟案件，越多訴訟可使法官開始針對 GDPR 進行釋法、釐清爭點、給予實務建議，有助各國落實 GDPR 法遵，畢竟法律是透過訴訟而形成、釐清。同時，Dixon 認為雖歐盟國家持續積極整併歐盟隱私法，欲制定一套單屬歐盟的隱私法(harmonization of EU data privacy law)卻極為困難，因各國法律文化、語言差異甚大。



資料來源：本計畫拍攝

圖 130「專家與談：Helen Dixon」場次截圖

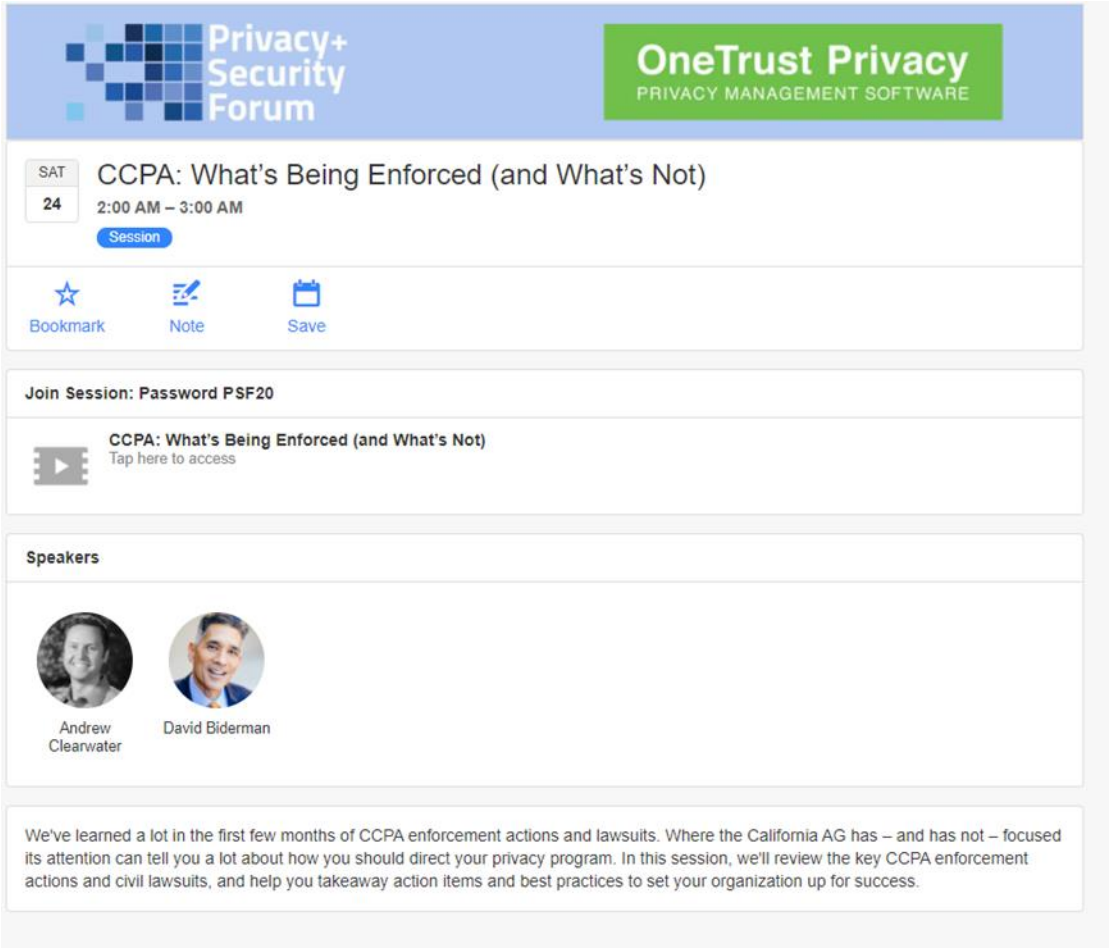
（十五） CCPA 執行動向

本場邀請 Andrew Clearwater(CPO of OneTrust)和 David Biderman(Partner of Perkins Coie)概述加州消費者隱私法(CCPA)以及 CCPA 之未來動向。

CCPA 賦予加州消費者新的隱私權，包括調取資料權(right to request information)、刪除權(right of deletion)、退出權(right to Opt-Out)、反歧視權(right to non-discrimination)，退出權要求網站上應有不販賣消費者個資的連結(Do Not Sell)。專家們目前認為加州消費者並不清楚自己擁有這些權利，權利推廣應是未來首要之事。

如違反 CCPA，加州司法部長(Attorney General of California)以及加州消費者有權起訴(Private Right of Action)。

Biderman 表示以自身作為集體訴訟(Class Action)律師的經驗，未來加州司法部長趨向於起訴累犯或重大違反事件，因重視企業是否盡力進到法遵義務，而大型公司則趨向於和解。



資料來源：本計畫拍攝

圖 131「CCPA 執行動向」場次截圖

（十六） 處理 DSAR

為符合 GDPR 及 CCPA 中對於個人隱私日漸嚴格的保護，本場次邀請 Heather Federman(VP of Privacy & Policy, BigID)、Rachel Glasser(Chief Privacy Officer, Wunderman Thompson) 和 Heather Sussman(Partner, Orrick)討論資料主體在未來可能會遇到的「資料權利」問題，並說明企業在面對這些問題時應如何解決這些潛在的障礙。以資料主體近用請求權(Data Subject Access Requests, DSAR)的方式符合資料合規性，並建立資料主體的信任。

所謂 DSAR 是指資料主體有權近用已蒐集到的有關他的個人資料，並有權在合理的時間內輕易地行使該權利，以了解並驗證資料處理的合法性。資料主體可以要求近用的資料包括確認及近用正在處理的個人資料、資料處理者處理資料的法源依據、資料儲存的時間、如何取得個人資料的相關資訊、自動化決策和分析的任何相關資訊，以及知悉共享該資料的第三方。雖然目前沒有 DSAR 的正式流程規定，但其申請大致有以下步驟：驗證申請者身分、確認申請者想了解的資料為何、查找該資料、蒐集並打包資料、向資料主體說明其權利、將蒐集到的資料回覆給資料主體。

講者認為，DSAR 遇到的挑戰在於，目前資料集的成長非常快速，卻很少有企業關注資料治理及資料管理，導致資料無所不在卻沒有進行有效的盤點。因此，資料請求所花費的成本將是一個很大的障礙。

資料來源：本計畫拍攝

圖 132「處理 DSAR」場次截圖

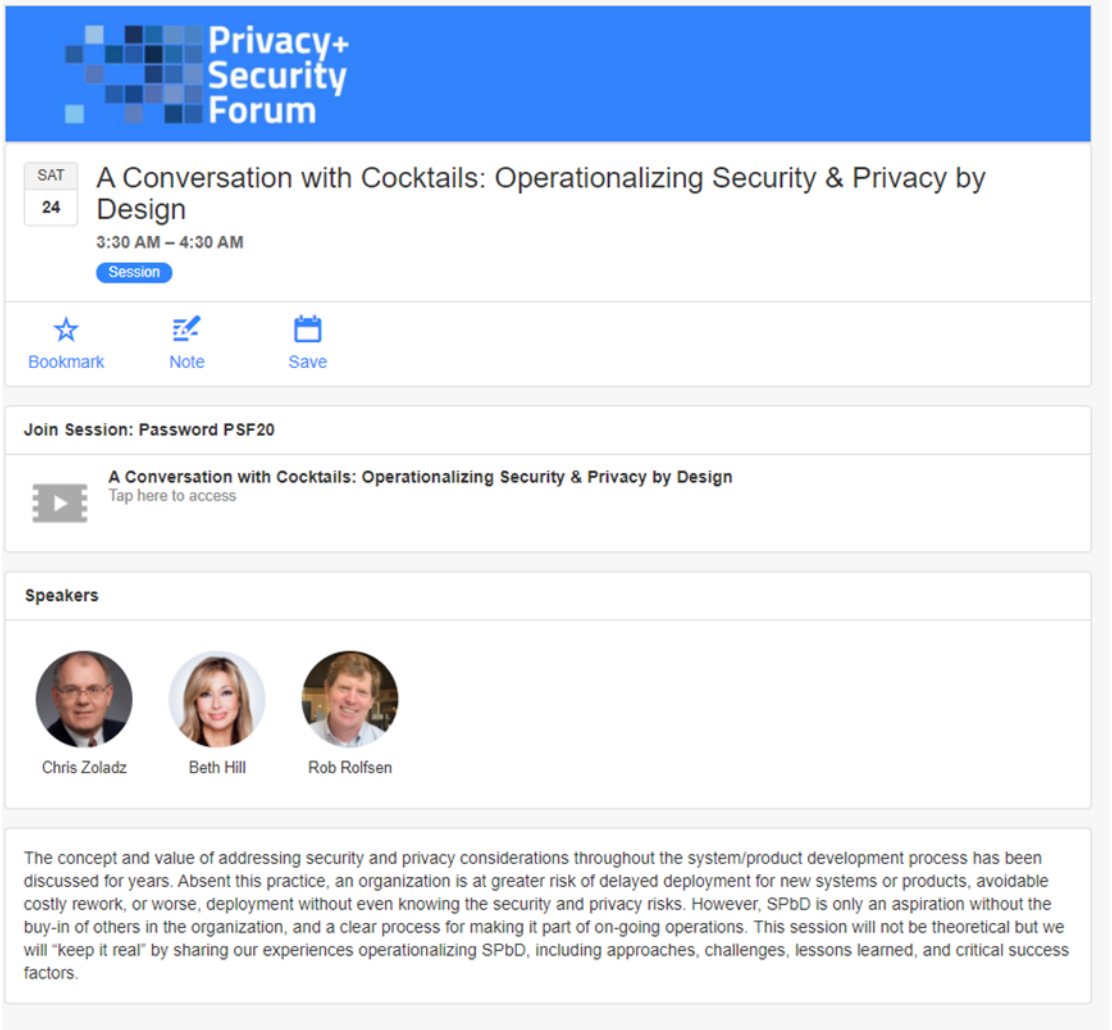
（十七） 雞尾酒論壇：透過設計實現安全性和隱私性

本場邀請 Chris Zoladz(Founder of Navigate)、Beth Hill(General Counsel & Chief Compliance Officer of FordDirect)和 Rob Rolfsen(Chief Privacy Officer of Asurion)討論各公司實務上如何落實「從設計包含隱私」(Privacy by Design)原則。

專家們一致認為公司實踐「從設計包含隱私」原則最重要的關鍵係應花時間跟員工解釋其重要性，依他們的經驗這大幅提升員工做好

隱私保護的意願。另，「從設計包含隱私」原則之落實係企業永恆經營之項目，因此公司在選擇哪些員工應做隱私保護業務時，建議以自願的方式挑選對隱私議題有熱忱的同仁。

制度的建置，從無到有往往需要幾個月的時間，更重要的是找到支持及重視隱私保護制度的高階主管，公司內部隱私保護規範需要領導者全力支持才能落實，尤其是人力與財務層面。專家們分享，各自公司都有因隱私保護做的不夠周全而推遲產品上市時間的經驗，惟他們認為花時間將隱私保護做得完整以利公司長遠發展，增進產品品質，進而增加收益。



資料來源：本計畫拍攝

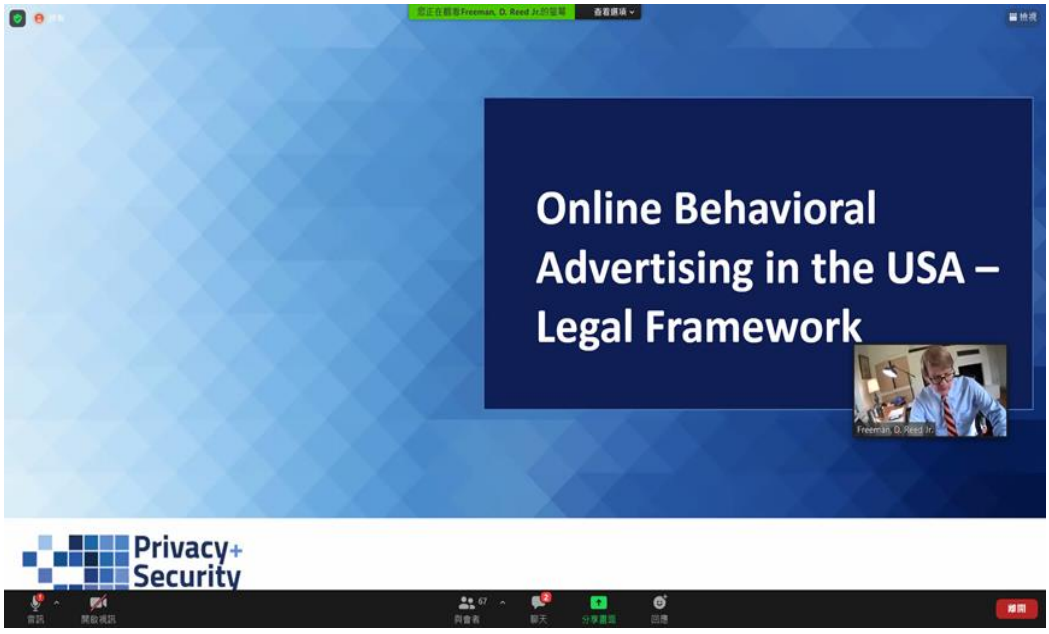
圖 133「雞尾酒論壇」場次截圖

（十八） 最新的全球廣告定位和分析追蹤規則

本場會議主要邀請 Reed Freeman(Partner, Venable)、Chelsea Reckell(Privacy Law Group, Venable)和 Brandy Walsh(Attorney, Privacy Compliance, Acxiom Corporation)討論各種追蹤技術、社群媒體及 IoT 設備目前全球的法規概況。

藉由說明 CCPA 及加州隱私權法(California Privacy Rights Act, CPRA)的差異，討論美國目前在商業上對於隱私的保護規範。CPRA 在 2020 年 11 月 3 日通過，將在 2023 年 1 月 1 日正式生效。CPRA 是 CCPA 的附錄，旨在加強加州民眾的權利，限制關於使用個人資料的商業法規，建立新的保護規則。

CPRA 建立加州消費者隱私保護局(Consumer Privacy Protection Agency, CPPA)，作為 CPRA 和 CCPA 資料隱私制度的主要執行者和主管機關，並且建立敏感個人資料類別進行單獨監管。另外，CPRA 修改退出權利，並規定負責任的第三方應如何使用、共享或出售個人資料。



資料來源：本計畫拍攝

圖 134「最新的全球廣告定位和分析追蹤規則」場次截圖

第三節 大數據：鞏固數位經濟中的歐盟法律框架線上研討會

歐盟執委會於 2020 年 2 月提出歐洲資料戰略(European Data Strategy)，該戰略所提出之資料共享政策與法制調適框架，期能建構資料單一市場(single market for data)，資料在歐盟內與跨域流通並使所有人受益、遵守個資保護、消費者保護與競爭法等歐盟相關規範，以及資料近用和使用的規定，應平等實用且明確，並以之建立資料治理機制。

因此為能掌握歐盟法律框架，關注於資料治理、近用與再利用方面所面臨之法律挑戰，如對於歐盟 2021 年資料法案之期望、公私資料如何共享、如何處理混合資料集、使用資料破壞性技術之責任、如何鼓勵建立公平透明之線上資料近用平台等，以作為我國發展資料經濟參考依據。

一、研討會資訊

表 19「大數據：鞏固數位經濟中的歐盟法律框架」研討會資訊

名稱	大數據：鞏固數位經濟中的歐盟法律框架(Big Data: Consolidating the EU Legal Framework in the Digital Economy)
時間	2020 年 10 月 26 日（一）至 2020 年 10 月 27 日（二）
地點	線上
出席人員	孫鈺婷

資料來源：本計畫製作

（一）整體說明

會議主題為「大數據：鞏固數位經濟中的歐盟法律框架」，將探討歐盟法律框架及其可能漏洞，並討論如何使該框架因應歐洲數位經濟發展，議題包含歐洲資料戰略、歐盟有關公私部門資料共享的提案、大數據和資料自由流通、資料所有權、互操作性、可用性等。

（二）議程資訊

表 20「大數據：鞏固數位經濟中的歐盟法律框架」議程資訊

2020 年 10 月 26 日	
時間	主題
14:00-15:00	14:00 Opening of the conference 開場 主持人：Florence Hartmann-Vareilles I. EU INITIATIVES ON BIG DATA 歐盟大數據倡議 主持人: Florence Hartmann-Vareilles 14:15 A European strategy for data 歐洲資料戰略 講者：Gail Kent 14:45 Discussion 討論
15:00-15:45	15:00 B2B data-exchange and trusted B2B data-sharing B2B 資料交換和受信任的 B2B 資料共享 • Guidance on “Sharing private sector data in the European data economy” 關於「在歐洲資料經濟中共享私部門資料」指引 • Principles to govern B2B data -sharing agreements 管理 B2B 資料共享協議的原則 • Legal challenges encountered by private companies trying to share data 公司共享資料可能遇到的法律挑戰 • The “Platform-to-Business” Regulation 「平台與業者關係」法規 講者：Alain Strowel 15:30 Discussion 討論 15:45 Break 休息
16:15-17:45	16:15 Round table discussion: Fostering access and use

2020 年 10 月 26 日	
時間	主題
	of data 圓桌會議討論：促進資料的近用和使用 主持人：Alain Strowel • Recommendations of the High-Level Expert Group on B2G Data-Sharing B2G 資料共享高級專家組的建議 • What kind of incentives should be created? 應該制定何種激勵措施？ • Contractual aspects of data sharing and other related issues data 資料共享契約方面相關議題 • Data collection and data concentration 資料蒐集和資料集中 • Towards a EU legislative framework for a governance of European data spaces 建立歐盟管理歐洲資料空間的立法框架 講者：Alberto Alemanno, Cornelia Kutterer, Malte Beyer-Katzenberger 17:15 Discussion 討論 17:45 End of first conference day 結束

2020 年 10 月 27 日	
時間	主題
09:15-10:45	主持人：Herbert Zech 09:15 Free flow of data and big data 資料和大數據的自由流通 • Overview of the EU Regulation 歐盟法規概述 • Consistency with the EU cybersecurity package 歐盟網路安全計畫的一致性 • Practical guidance on how to process mixed datasets 關於如何處理混合資料集的實用指引 • Cloud and data portability 雲和資料可攜性 講者：Christoph Werkmeister 09:45 Discussion 討論
	10:00 Legislative and non-legislative measures to encourage 鼓勵採用開放資料的立法和非立法措施 • the uptake of open data 開放資料的接受率 • Challenges in the implementation of the PSI Directive 實施 PSI 指令面臨的挑戰 • Non-legislative initiatives in the pipeline 正在進行的非立法舉措 • The EU Open Data Portal 歐盟開放資料網站 講者：Jiri Pilar 10:30 Discussion 討論 10:45 Break 休息
11:15-12:00	III. ARTIFICIAL INTELLIGENCE AND BIG DATA 人工智慧與大數據 主持人：Florence Hartmann-Vareilles

2020 年 10 月 27 日	
時間	主題
	11:15 Liability for disruptive technologies using data: is an EU legal intervention needed? 破壞性技術對資料使用的責任：是否需要歐盟法律干預？ • Recommendations of the European Commission's Expert Group on Liability for Emerging Digital Technologies 歐盟執委會新興數位科技責任專家組的建議 • Open questions on data ownership, interoperability, (re-)usability, access to data, and liability 有關資料所有權、互操作性，可用性（再利用）、資料近用與責任的未解決問題 • Decisions of autonomous digital systems: are regulations on responsibility and liability advisable? autonomous 自主數位系統的決策：關於責任和義務的法規之適當性 講者：Herbert Zech 11:45 Discussion 討論 12:00 Break 休息
13:15-14:45	13:15 Round table: What kind of legal framework for using the potential of AI and Big Data? 圓桌會議：人工智慧和大數據潛力的法律框架 • Cloud computer, public-private partnership, open sources and other cooperation tools 雲端運算、公私伙伴關係、開源和其他合作工具 • Horizontal or sectoral approach?橫向或部門方法？ 講者：Agustin Reyna, Cornelia Kutterer 14:15 Discussion 討論

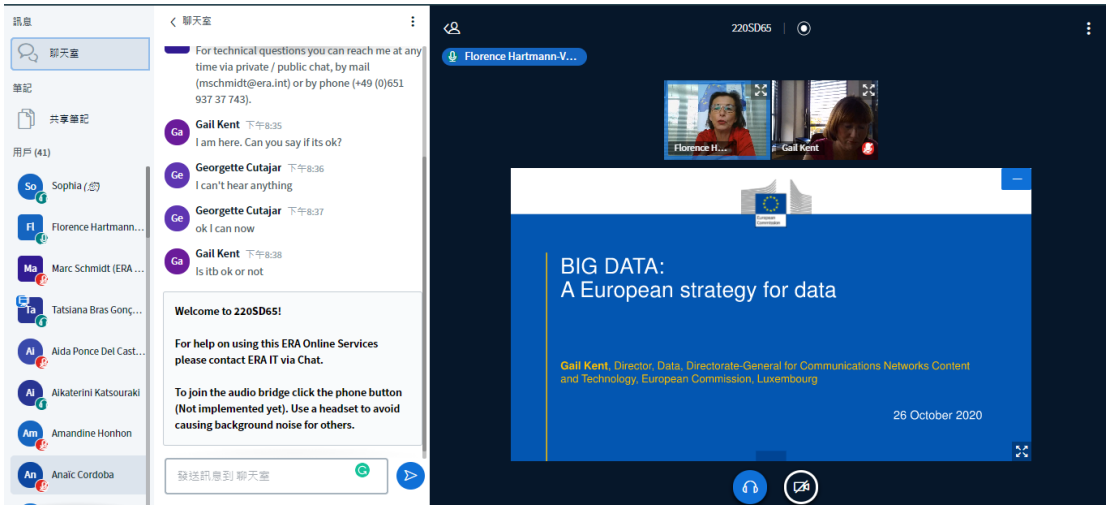
2020 年 10 月 27 日	
時間	主題
	14:45 Break 休息
15:15-16:15	IV. ACCESS TO DATA, DATA SHARING AND ONLINE PLATFORMS 資料近用、共享和線上平台 15:15 How to encourage a fair system of access to data of online platforms? 如何鼓勵建立公平的線上平台資料近用系統？ • Overview of the Regulation on fairness and transparency of online intermediaries 線上中介機構的公平和透明性法規概述 • The future Digital Services Act 未來的「數位服務法」 • Fostering access to data via competition law 透過競爭法促進對資料的近用 講者：Miranda Cole, Paola Colombo 16:00 Discussion 討論 16:15 End of conference 會議結束

資料來源：本計畫製作

二、場次重要摘要

（一）歐洲資料戰略

本場次主持人為 Florence Hartmann-Vareilles，邀請歐盟執委會資通訊網路暨科技總署(DG CONNECT)資料總監 Gail Kent 說明歐洲資料戰略作為研討會開場。講者簡要說明關於歐洲資料戰略之相關重點，並說明後續相關資料應用法律框架之規劃，其中參與者相當有興趣莫過於預計於 2021 年提出之「資料法」(Data Act)的規劃，但他說明目前仍需要先進行法規影響評估，而參與者也對此提出許多問題，如該法將如何激勵大型企業共享工業資料集；資料的近用與所有權差別為何，若無資料所有權，資料功能市場將如何發展；該是否會為資料庫權利創造新的例外；資料如何共享，如何設計共享機制、標準等。還有關於 B2B、B2G 等領域資料共享，特定領域之資料空間(Data space)規畫等。



資料來源：本計畫拍攝

圖 135「歐洲資料戰略」場次截圖

（二）B2B 資料交換和受信任的 B2B 資料共享

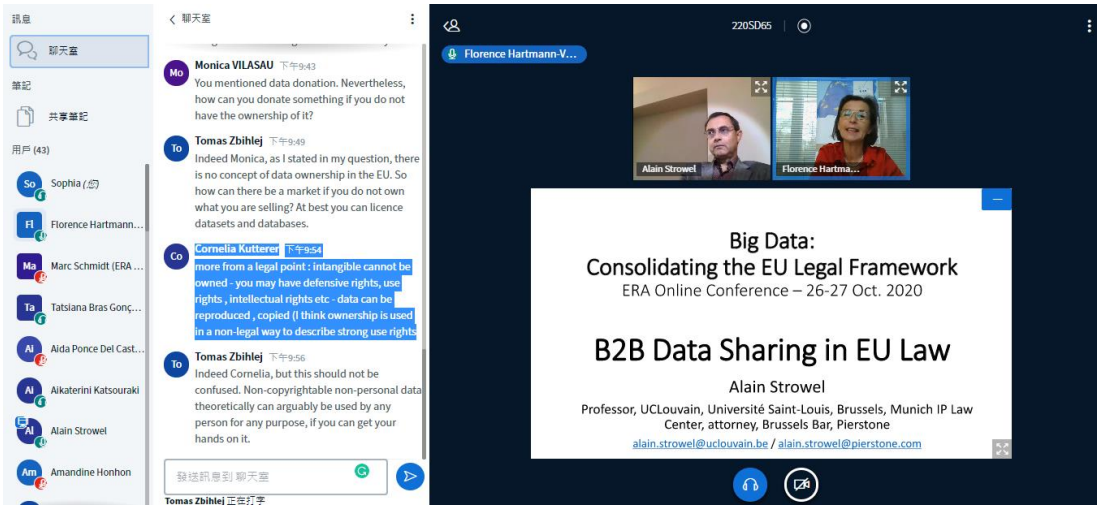
本場次主持人為 Florence Hartmann-Vareilles，邀請 UCLouvain 教授同時也是律師的 PierstoneAlain Strowel 報告關於「B2B 資料交換和受信任的 B2B 資料共享」議題。報告包含歐洲資料經濟中共享私部門資料之指引、管理 B2B 資料共享協議的原則，平台與業者間關係之相關規範，以及公司共享資料可能遇到的法律挑戰。

講者首先定義並說明大數據為大量動態、變化的數據，可以輕鬆地在 ICT 網路中進行合併、共享和近用，進行資料分析，應對豐富資料的情況。接續就資料共享的範圍討論，包含資料類型如非個人資料與個人資料，機密與公開資料，還有在不同組織單位間，如 B2B、B2C、B2G、P2B 等，還有關於歐盟內外部的資料共享、近用、再利用等。針對上述內容，整理相對應法規，如 GDPR、FFDR 2018、Open Data Directive 2019、Trade secret directive 2016 等。

至於如何處理混合資料集，講者提到關於 FFDR 的 2019 年指引中，因物聯網、人工智慧技術，混合資料集代表資料經濟中的大多數資料集，因此原則上如果資料可以合理連接到特定個人時，依據 GDPR 應使用基於風險模式來重新識別。

講者提到影響資料共享的資料特徵，原則上不具競爭性，資料消耗不可競爭，且從理論上來說，資料蒐集亦是如此，因為各方皆得以蒐集相同的資料，除非是僅有唯一來源或競爭對手，但是資料具排他性，排除第三方的可能性，即為資料佔用，從而限制資料共享。

講者認為資料共享需要試驗和投資，值得關注模式如英國的開放銀行，透過開發通用和開放的 API，以近用客戶的帳戶資訊並共享交易資料；還有實驗和開發專用的雲端，以實踐資料共享，在不同的資料空間，透過標準和特定的資料管理規則（如互操作性、安全性），並針對某些資料集開放，在共享目標和機密性間尋求平衡。



資料來源：本計畫拍攝

圖 136「B2B 資料交換和受信任的 B2B 資料共享」場次截圖

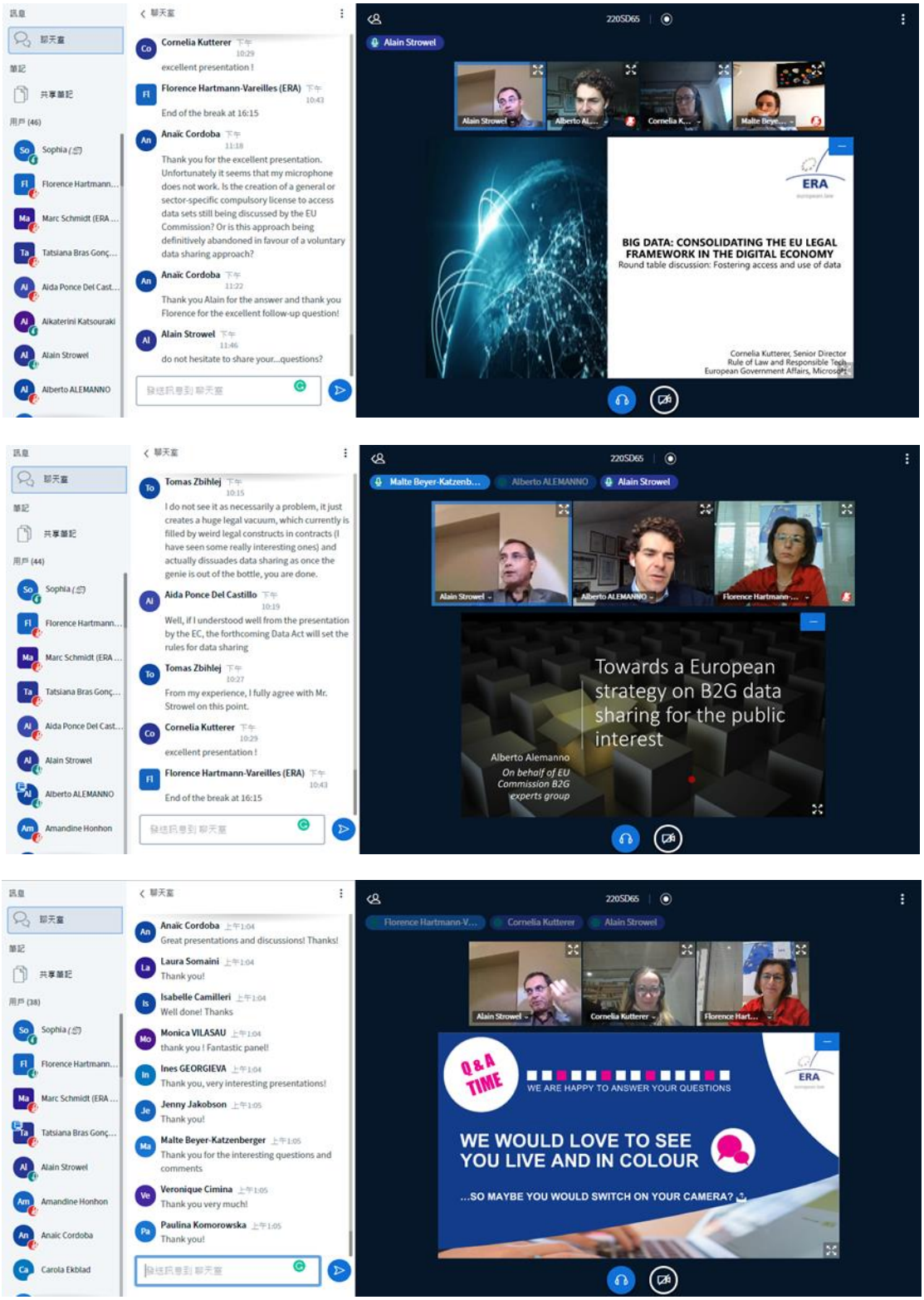
（三）圓桌會議：促進資料的近用和使用

本場次主持人為 Alain Strowel，邀請 Alberto Alemanno、Cornelia Kutterer，與 Malte Beyer-Katzenberger 與談關於「促進資料的近用和使用」議題，包含 B2G 資料共享高級專家組的建議、應制定何種激勵措施、資料共享契約方面相關議題、資料蒐集和資料集中，以及建立歐盟管理歐洲資料空間的立法框架等。

講者 Cornelia Kutterer 為 Microsoft 微軟歐洲法律事務及技術高級總監，他提到可信賴的資料協作的五項原則，分別為「開放」(Open)，致力於重要社會問題相關的資料儘可能開放；「可用」(Usable)，將投資於建立新技術和工具、治理機制與政策；「賦權」(Empowering)，協助組織根據其選擇從其資料中產生價值，並培養其 AI 人才以有效和獨立地使用資料；「安全」(Secure)，採用安全控制措施來確保資料協作；「隱私」(Private)，協助組織在涉及個人身份資料的共享協作中保護個人隱私。此外，他還提及「開放資料運動：探索開放資料的力量」，預計於 2022 年就 20 個進行資料協作，由 Microsoft 和倫敦資料委員會(London Data Commission)支持的艾倫·圖靈研究所(Alan Turing Institute)與大倫敦管理局(the Greater London Authority)合作，展示資料共享的價值，以幫助支持倫敦因應 COVID-19；還有與歐洲醫院聯盟合作針對癌症研究、氣候變遷、教育等議題。

另一講者為歐盟執委會 DG CONNECT 的 Malte Beyer-Katzenberger，從歐洲資料戰略切入，提到資料可以改變經濟發展，且對於 AI 至關重要；且個人和非個人資料可以成為新產品和服務創新的來源，同時可以應對社會挑戰，例如氣候變化、健康、交通等，資料可以成就我們的生活和工作。此外關於充分利用資料在經濟中的潛力，如再利用概念，亦即資料共享、資料交易、資料貨幣化，以及對於資料共享的信任，使各方自主決定資料應用，確保技術和法律促進資料的價值，並應遵循 GDPR。最後他提到歐盟將針對資料相關立法規劃，如資料治理之立法，針對資料共享中介、資料利他主義，如何更好地利用敏感的公部門資料；以及將於 2021 年初提出的高價值公部門資料立法(High value public sector data legislation)，作為提供具有特別高價值的公部門資料，如地理、天氣、統計資料等，還有透過機器可讀格式並以 API 免費取得的資料，最後則是預計於 2021 年末提出之資料法(Data Act)。

另一講者 Alberto Alemanno 代表歐盟委員會 B2G 專家小組，說明該小組任務有三，分別為評估 B2G 資料共享的法律、經濟和技術障礙，其次為就促進公共利益目的之 B2G 資料共享的建議，最後則為向執委會建議如何進一步訂定 B2G 資料共享政策。他認為共享範圍僅適用於私人公司和民間組織已蒐集的資料，用於內部業務目的或用於開發未來產品或服務的資料，在歐盟的資料提供者，從歐盟公民蒐集之資料，公部門不會控制私部門的資料，因為資料為有價值的非競爭性和基礎設施，因此企業將繼續在現有或未來的 B2B 資料市場中利用相同的資料獲利。最後他認為歐盟執委會和成員國應將資料視為歐洲未來的重要公共基礎設施，並採取措施促進公益使用私人擁有的資料，公私部門應充分合作，以確保基於公益目的能夠更多樣化和常規地使用資料。



資料來源：本計畫拍攝

圖 137「圓桌會議：促進資料的近用和使用」場次截圖

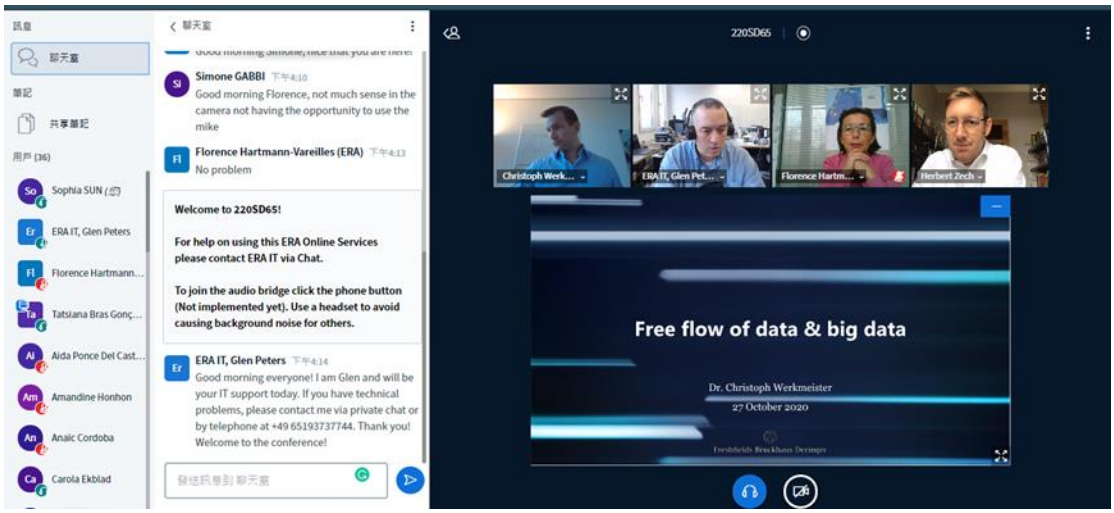
（四）資料和大數據的自由流通

本場次主持人為 Herbert Zech，邀請 Düsseldorf 資料與技術首席研究員 Christoph Werkmeister 博士報告關於「促進資料的近用和使用」議題，包含歐盟非個人資料流通之法規概述、歐盟網路安全計畫的一致性、關於如何處理混合資料集的實用指引與雲端和資料可攜性等。

他首先說明歐盟非個人資料流通規則(Free flow of non personal data Regulation (EU) 2018/1807)，透過禁止資料在本地化要求、資料可攜性行為準則、資料可用性，達成資料自由流通目的，並整理對應條文如第 1、2 與 4 至 5 條，並舉德國為例於資料在地化法律的影響。

接續說明處理混合資料集，亦即涉及個資與非個資資料集，非個人資料流通規則僅適用非個人部分，當個人和非個人部分密不可分(nextricably linked)時，則應適用 GDPR。至於如何判斷密不可分，若分割二者是不可能的、經濟不效率、技術上不可行，則為密不可分，應個案具體判斷。講者接續就歐盟新的資安戰略與資安相關法規說明，如 NIS 指令、GDPR、ePrivacy 指令是否由電子隱私法規(ePR)取代、資安法(Cybersecurity Act)該法之下的認證框架。

最後講者盤點與雲端和資料可攜性議題，為促進歐洲單一的雲服務市場，應關注如數位單一市場政策、GDPR 和非個人資料的自由流通、資料可攜性行為準則、資安認證、雲端資料保護的行為準則、標準化雲服務協議(SLA)、歐洲金融機構 SC、歐盟資料流通、歐洲的資料基礎架構等，此外歐洲法院關於 Schrems II 判決仍可能造成深遠的不確定性。



資料來源：本計畫拍攝

圖 138「資料和大數據的自由流通」場次截圖

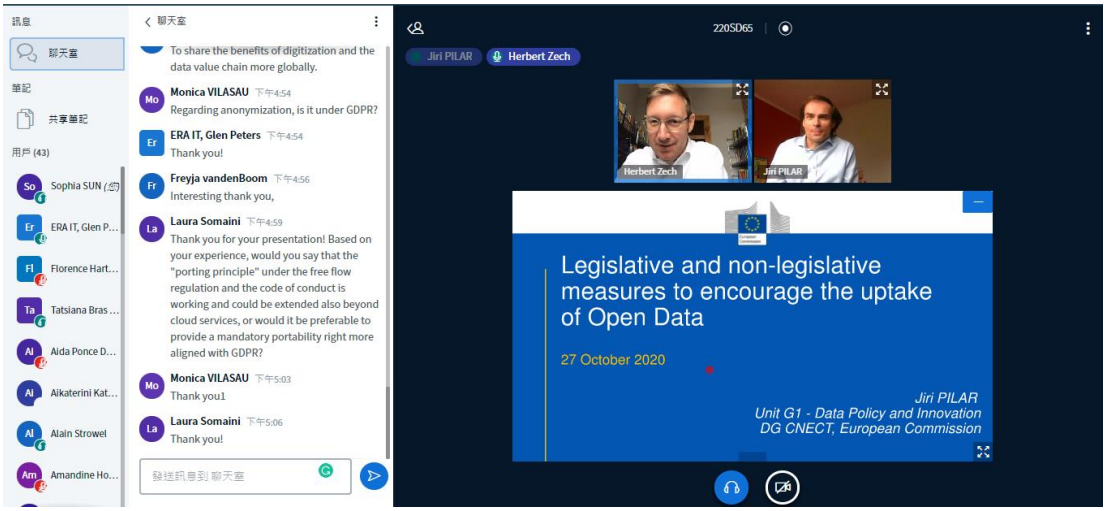
（五）鼓勵採用開放資料的立法和非立法措施

本場次主持人為 Herbert Zech，邀請歐盟執委會 DG CONNECT 資料政策與創新工作組的 Jiri Pilar 報告關於「鼓勵採用開放資料的立法和非立法措施」議題，包含開放資料的接受率、實施 PSI 指令面臨的挑戰、正在進行的非立法舉措，以及歐盟開放資料網站等。

講者一開始說明關於歐洲資料戰略願景、具體措施，接續針對開放資料議題討論，其中關於開放資料立法迄今觀察到的主要挑戰，包含收費問題、專有或準專有協議以進行再利用，符合個人資料保護規則疑義等。此外戰略中提到關於高價值資料集(High value datasets)新概念，法案中列出的資料集將透過 API 以機器可讀格式免費提供，並且可以大量下載，例外為免費提供的要求不適用於公共事業當存在競爭扭曲的風險時，且若對其預算有重大影響，則免費提供時間最多可能為 2 年。高價值資料集的主題類別，包含如地理空間、地球觀測和環境、氣象、統計、公司和公司所有權、流動性等，於 2021 年將在附件列出的 6 個主題類別中定義特定的高價值資料集的列表。

至於促進開放資料的非立法活動，講者提到開放資料數位基礎結構為歐洲資料入口網站(European Data Portal)、歐盟開放資料入口網站(EU Open Data)，與連接歐洲設施(Connecting Europe Facility, CEF)，而數位歐洲計畫(Digital Europe Programme, DEP)的具體目標加強歐

洲的核心 AI 能力，包括資料資源，特別關注特定資料集可互操作，並適合 AI 應用，相關活動如度用(curation)、語意標示(Semantic annotation)、統一元資料(harmonisationof metadata)、促進機器可讀格式，以及 API 的可近用性等。



資料來源：本計畫拍攝

圖 139「鼓勵採用開放資料的立法和非立法措施」場次截圖

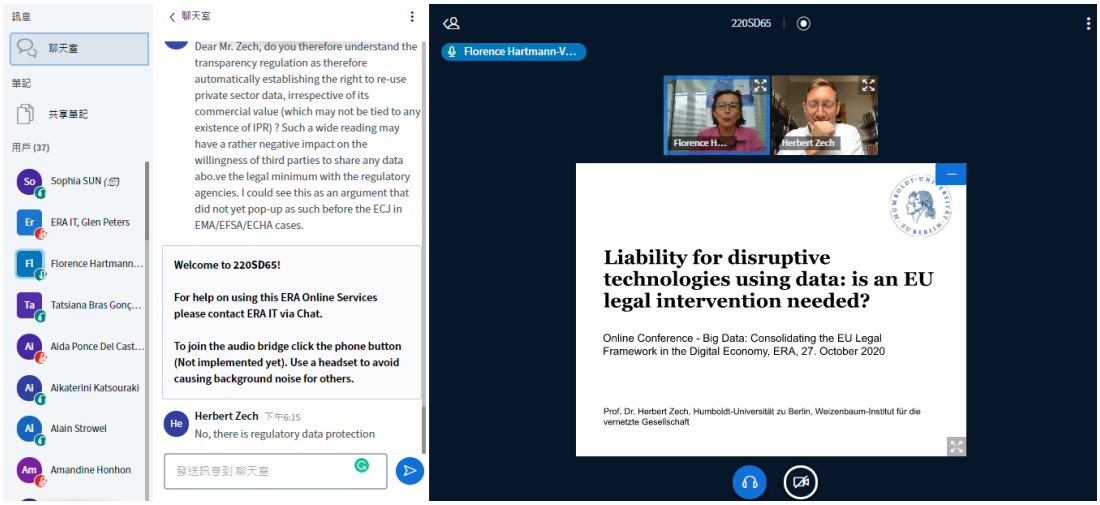
（六）破壞性技術對資料使用的責任：是否需要歐盟法律干預？

本場次主持人為 Florence Hartmann-Vareilles，邀請柏林洪堡大學 Herbert Zech 教授與談關於「促進資料的近用和使用」議題，包含歐盟執委會新興數位科技責任專家組的建議、有關資料所有權、互操作性，可用性（再利用）、資料近用與責任的未解決問題，以及自主數位系統的決策：關於責任和義務的法規之適當性等。

講者報告針對技術應用對於資料的責任分為以下 5 點討論，分別為現行法規、技術背景、現有責任制度、功能，究竟誰應該承擔責任，以及智慧財產權相關議題。人工智慧責任當前的辯論，講者提到得參考如執委會 2020 年人工智慧白皮書，還有歐洲議會於 2017 年 2 月關於機器人技術規則的建議，以及關於資料所有權、互操作性、再利用資料以及責任等新興問題的研究報告。

至於數位系統機器人連接自主性（機器學習）之技術背景，參考人工智慧、物聯網和機器人技術的安全和責任影響報告，關於連接性和開放性、自治性、心理健康風險、資料依賴性、不透明性、產品和

系統的複雜性，以及複雜的價值鏈等議題都需考量。而目前責任制度，包含過失（違反職責、因果關係判斷）、產品賠償責任、嚴格賠償責任（生產者、經營者），與代理商的賠償責任等。其中關於產品責任，參考責任與新技術專家組的報告，軟體為產品，包括學習引起的缺陷、危害增加的嚴格責任、記錄功能，舉證責任之可逆。至於誰應該承擔責任，從風險控制角度，判斷風險歸因，思考涉及利害關係人包含工程師、資料提供者、培訓人員、操作人員與使用者等。最後是責任和智慧財產權，思考風險和機會分配，使用技術的資料外部性，以及透明性義務。



資料來源：本計畫拍攝

圖 140「破壞性技術對資料使用的責任：是否需要歐盟法律干預？」場次截圖

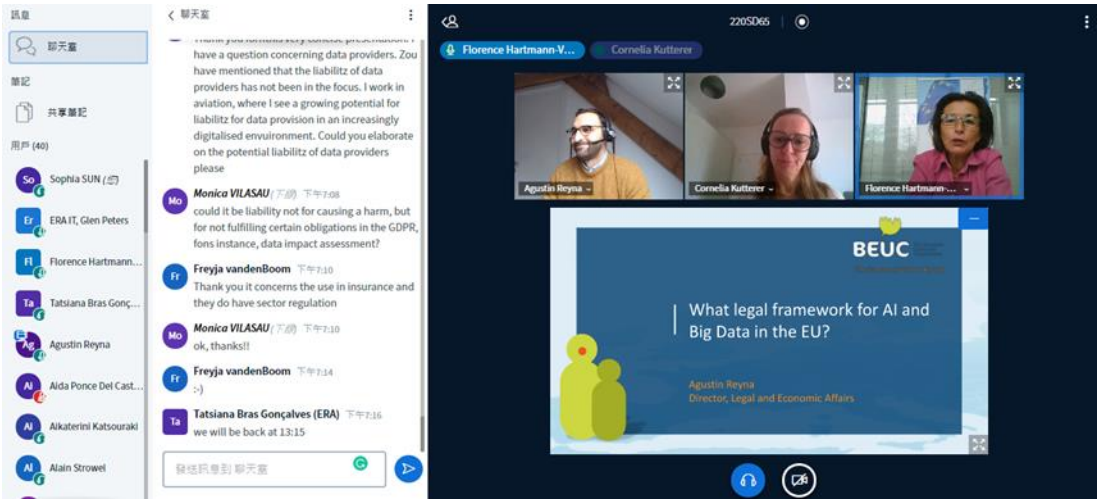
（七）圓桌會議：人工智慧和大數據潛力的法律框架

本場次主持人為 Florence Hartmann-Vareilles，邀請 Agustin Reyna, Cornelia Kutterer 與談關於「人工智慧和大數據潛力的法律框架」議題，包含雲端運算、公私伙伴關係、開源和其他合作工具，與橫向或部門方法等。

講者 Agustin Reyna 為 BEUC 法律和經濟事務總監分享「歐盟針對 AI 和大資料的法律框架」，首先說明歐盟對資料經濟與社會的願景源於歐洲的價值觀和基本權利，並堅信以人為本，歐盟可以引領開發和使用人工智慧造福所有人。接著說明建立消費者信任的 AI 法律框

架包含透明、安全、監督、公平與非歧視。其一針對透明，業者必須對其業務模型和使用界面保持透明，並根據風險級別，建立問責措施，應包括針對用戶的 ADM 影響評估、強制性標準來實現設計透明(transparency by design)；其次為安全，應更新的數位商品責任框架(PLD)、一般產品安全指令(General Product Safety Directive, GPSD)的現代化；其三，ADM 技術原則上應受到獨立控制和監督，對高風險 AI 產品進行事前審查、上市後階段應持續合規(continued conformity)；最後公平與非歧視，公平設計(Fairness by design)演算法決策以公平負責的方式進行，不歧視則是消費者應受到保護，免受非法歧視和不公平分化，包括經濟歧視。最後講者也盤點目前相關政策，包含人工智慧白皮書的後續行動、數位服務法、AI 高風險責任規則、PLD、資料法、資料空間的監管措施資料庫指令等。

另一講者 Cornelia Kutterer 歐洲政府事務法治與技術公司法律事務(CELA)高級總監分享「大數據：鞏固數位經濟中的歐盟法律框架」，首先分享 Microsoft 的 CEO Satya Nadella 對於 AI 說明，它不僅僅是一項技術，它可能是人類創造的世界上最基本的技術之一，至於為何要有負責任 AI，講者引用 Brad Smith 微軟總裁「該工具越強大，它所帶來的利益或損害就越大，技術創新不會減慢，管理它的工作需要加快」來說明。接著，講者提到原則，應包含公平性、問責制、透明、包容性、可信賴性、隱私與安全性等，並舉例說明如何實際執行，如以人為本 AI 準則、對話式 AI 準則、包容性設計準則、AI 公平性檢查表、資料集表格，透過了解、保護、控制工具來執行，最後則是治理，包含 RAI 委員會與相關成員與 AI 手冊制定。



資料來源：本計畫拍攝

圖 141「圓桌會議：人工智慧和大數據潛力的法律框架」場次截圖

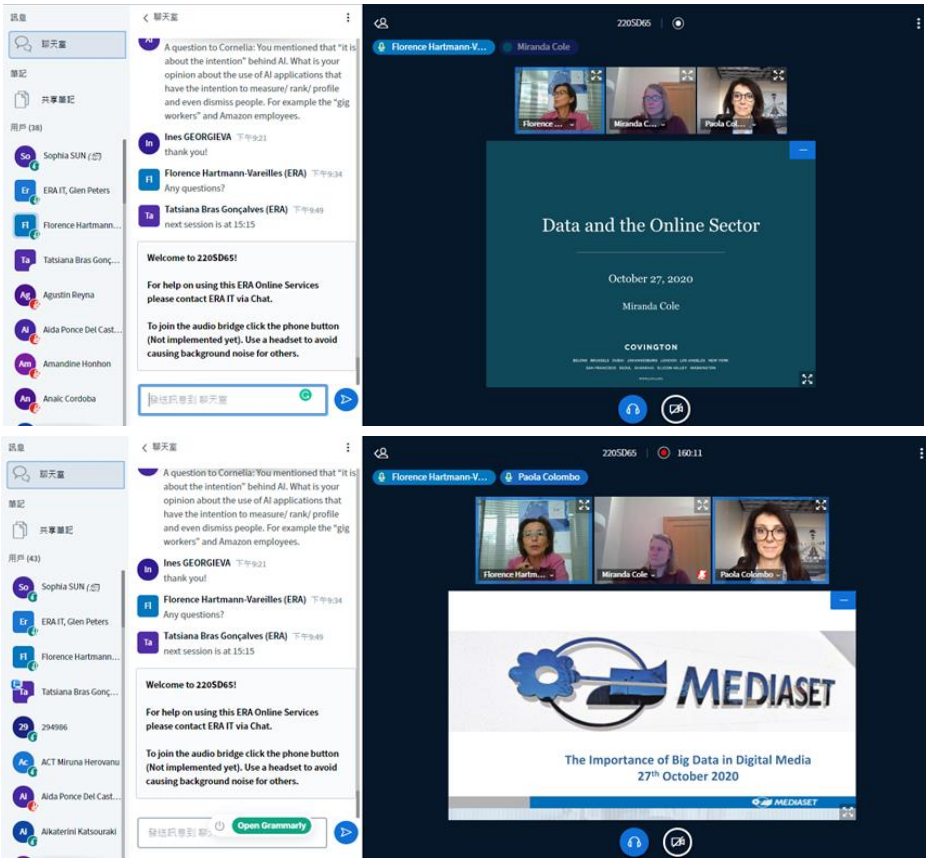
（八）如何鼓勵建立公平的線上平台資料近用系統？

本場次主持人為 Florence Hartmann-Vareilles，邀請 Miranda Cole, Paola Colombo 與談關於「如何鼓勵建立公平的線上平台資料近用系統」議題，包含線上中介機構的公平和透明性法規概述、數位服務法與透過競爭法促進對資料的近用等。

講者 Miranda Cole 為 Covington 事務所的合夥人，分享「資料與線上領域」，分別針對資料及其用途、競爭法分析框架、監管說明。首先，說明何謂大數據，不僅是個人資料，還有匯總和匿名資料集，於許多產業中廣泛應用。接著，講者就競爭法和資料說明，資料大多數情況是輸入，消費者可以直接提供資料，或服務提供者可以透過觀察行為來蒐集資料，資料可以用於多邊市場，以使服務貨幣化。至於競爭法分析框架著眼於資料蒐集和用作輸入，評估資料類型（需要近用之特定資料或規模效應的潛在問題），而資料是否具有排他性，考量資料具有可重複性，如許多消費者生成的資料是可複製的，還需要思考資料對於在市場中競爭重要的程度、資料的收益、資料過時的速度等。監管方面，分別從相關政策、線上中介的公平和透明相關規範說明，如中介服務、搜尋引擎與業務用途之間的關係的透明度、公平性，以及條款於通知更改限制等。最後講者提到潛在數位服務/市場法相關中議題，如資料實踐是政策辯論中的核心問題，包括業務近用資

料、合併來自多個來源的資料與資料可攜性（互操作性）等。

另一講者為 Mediaset 電視公司的 Paola Colombo，分享「大數據對數位媒體的重要性」，首先，講者提到兩個水平面向，其一為資料蒐集的水平，包含搜尋、社群媒體、推薦系統、家用設備，其二為資料貨幣化的水平，包含技術平台、測量、銷售、業務成果等，並分享該公司現況。他認為媒體擁有者與和發布者未來趨勢是漸進式用戶去中介化(Progressive user disintermediation)，將有個人化節目表、廣告等，且數位媒體的增長速度已超過所有其他媒體，並分享未來媒體關於行銷發展趨勢，而資料至關重要，因此必須掌控資料，關注議題如消費者資料和 GDPR，活動資料、內容資料、控制廣告投資、透明且經過驗證的衡量標準、演算法機器學習等。



資料來源：本計畫拍攝

圖 142「如何鼓勵建立公平的線上平台資料近用系統？」場次截圖

第九章 國際資料經濟與個資保護趨勢動態資訊與研究調查摘譯

第一節 趨勢動態資訊

研究團隊於計畫執行期間，亦隨時觀測國際資料經濟與個資保護趨勢動態，總共蒐集 16 篇。

期中報告共 10 篇與本研究議題相關性較高之國際資訊，歸納出三項資料經濟與個資保護重要議題：

1. **新冠疫情防治需求下的科技應用與隱私保護**：觀察疫情發展對於資料經濟與個資保護之影響，亦顯示各國在科技防疫下對於個資保護的重視。
2. **社群媒體於數位時代之個資保護與產業競爭態勢**：網路社群平台藉由資料的收集與分析形成強大的市場力量，各國亦由個資保護與市場競爭兩方向加以探討管制。
3. **國際隱私與資料流通政策發展**：追蹤國際個資保護與資料流通的重大政策發展，包含臉部辨識技術的探討、歐盟雲端政策與資料流通，以及歐盟與美國間隱私盾協議被判決無效的發展。

對於以上議題，分別收集之國際動態資訊於下詳述。

表 21 2020 年 4 月至 8 月趨勢動態資訊彙整

重要議題	國際動態資訊
新冠疫情防治需求下的科技應用與隱私保護	1. 歐盟發佈自願性符合隱私保護規範的追蹤 Apps 設計指南 2. ETSI 成立新的產業準小組制定 COVID-19 接觸追蹤應用的安全標準架構
社群媒體於數位時代之個資保護與產業競爭態勢	3. 美國聯邦貿易委員會與 Facebook 就隱私洩漏與保護措施不足的案件達成行政和解 4. 美國立法禁止政府設備使用抖音（TikTok） 5. Facebook 發佈新的照片傳輸工具以解決美國競爭法的問題
國際隱私與資料流通政策發展	6. 美國大型科技企業因隱私爭議暫停提供執法機關臉部辨識技術

重要議題	國際動態資訊
	7. 英國法院裁定警察機關使用臉部辨識技術違反隱私法 8. 英國使用演算法決定 A 級考試成績衍生之爭議 9. 法國與德國聯合推動 GAIA-X 歐洲資料基礎架構 10. 歐盟法院裁定歐盟與美國間的隱私盾保護協議無效

資料來源：本計畫製作

一、 新冠疫情防治需求下的科技應用與隱私保護

2020 年適逢 COVID-19 之影響下，全球不論食衣住行育樂均產生巨變，而在科技與精銳技術邁進下，為了阻擋疫情肆虐，科技防疫則成為國際各國重要執行手段之一，尤其各項多元應用不僅協助政府知曉感染情況，亦能減緩疫情擴散之機會。但在科技防疫背後，則是藉由資料蒐集之處理與利用，始能達到一定成效；然而，防疫之重要性與民眾隱私權均不可偏廢，兩者應如何調適，將由以下兩則趨勢說明。

（一）歐盟發佈自願性符合隱私保護規範的追蹤 Apps 設計指南

隨著新型冠狀病毒（COVID-19）疫情的演進，各國逐漸採用接觸追蹤程式（contact tracing Apps）以辨識及阻擋疫情的擴散。為了協助歐盟各會員國醫療主管機關，透過追蹤 Apps 控制疫情的擴散，並確保 Apps 的設計符合歐盟一般資料保護規則（General Data Protection Regulation, GDPR），維護歐洲民眾的個人隱私，歐盟發佈了有關此類追蹤預警 Apps 的設計指南，規定了各會員國提供使用此類追蹤 Apps 的基本要求。

這些要求包括：

- 運作應完全符合歐盟資料保護和隱私規則。
- 提供與使用應與各國公衛或醫療主管機關協調與許可。
- 應讓民眾自願安裝或自行選擇移除。
- 應利用最新隱私強化保護技術，避免追蹤民眾的位置。
- 應以去識別化資料為基礎，提醒與感染者接近的民眾接受檢測或自我隔離，而不透露感染者的身份。

- 在歐盟境內的使用應具有互通性，使民眾即使跨境也能繼續得到保護。
- 應以公認的流行病學指導為基礎，具備網路安全性和容易取得，並能有效發揮功能。

其他如美國的 Apple 與 Google 亦使用以藍芽為基礎的 Apps，保持去識別化且不包含使用者位置資訊；南韓則透過提供被感染者足跡的地圖，使一般民眾可避開危險地點；新加坡則使用提供自願下載、以藍芽為基礎的追蹤 Apps，當使用者註冊時，Apps 會蒐集手機號碼和發給隨機匿名 ID，並且不蒐集任何位置資訊，Apps 會通知與受感染者非常接近的人；以色列則透過 HaMagen 系統，蒐集個人手機位置資訊，並與確診者位置比對後，公布確診者的足跡。

面對新型冠狀病毒的擴散，新興通訊技術提供了相當多應變與協助，但也同時讓隱私保護的問題浮現，若不加以注意，新的隱私威脅可能會從危機中浮現出來，各國在努力以新科技防堵疫情的同時，也仍將繼續討論如何更完善保護民眾的隱私權利，不因疫情而受到過度侵害。

（二）ETSI 成立新的產業準小組制定 COVID-19 接觸追蹤應用的安全標準架構

歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）於 5 月 26 日公佈 eHealth 白皮書（ETSI White Paper No. 33 The role of SDOs in developing standards for ICT to mitigate the impact of a pandemic），闡述 ETSI eHealth 計畫關於制訂 ICT 標準、減輕新型冠狀病毒（COVID-19）流行上的作用，以及各標準制定組織（Standards Developing Organizations, SDOs）所扮演的角色。eHealth 的實現相當仰賴 ICT 技術，但也需克服隨之而來的社會性（sociality）、可靠性（reliability）和互操作性（interoperability）的障礙，因此，在設計相關技術標準時，應充分設想該項技術於 eHealth 應用時的安全隱私需求，落實「設計時納入安全（security by design）」以及「設計時納入隱私（privacy by design）」。有鑑於 COVID-19 對全球嚴重性影

響，ETSI 藉由白皮書對各標準組織及成員進行「戰備呼籲（call to arms）」，期望能確保下一次病毒大流行到來時，國際社會可以更快更穩定的協調 ICT 技術與供應鏈。

在白皮書中特別提及「接觸追蹤」（proximity tracing）是一種 ICT 技術概念，用以瞭解 COVID-19 的傳播途徑，並分析民眾感染的風險，進而抑制病毒傳播。歐盟執委會於 4 月公布接觸追蹤 APP 的規範建議，而 ETSI 則於 5 月 12 日設立新的產業標準小組（Industry Specification Group, ISG）」—「歐洲隱私保護及大流行保護」（Europe For Privacy-Preserving Pandemic Protection, E4P）（合併簡稱 ISG E4P），ISG E4P 小組的任務，除了考量歐盟執委會的規範與一般資料保護規則（General Data Protection Regulation, GDPR）外，也將發揮 ETSI 在網路安全、eHealth 和緊急通訊等領域的專業知識，協助歐盟會員國對抗 COVID-19。

ISG E4P 小組制訂的標準架構，可為各國程式開發者提供一致性的技術規範，在資料處理、傳輸、分析，網路系統等技術面達成相容性與互操作性，並藉由 ETSI 安全隱私技術的專業背景，贏得民眾信任。ISG E4P 未來將制訂技術文件，主要內含接觸追蹤系統的應用程式介面（Application Programming Interface, API）定義，資訊安全的技術標準，並符合 GDPR 的資訊保護要求。

二、 社群媒體於數位時代之個資保護與產業競爭態勢

社群媒體近年內之發展已從分享生活為目的之性質，轉變為多樣化資訊的重要推播媒介，其影響力可說無遠弗屆。尤其在全球用戶日益劇增下，蒐集用戶資料進行分析，並推送個人化資訊與廣告亦為各平臺業者之日常。因此社群媒體早已成為掌握個人資料的巨型業者，並引發諸多隱私爭議，甚至造成壟斷市場之嫌。在此情形下，保障用戶隱私權益則成為各國政府主要目標，由以下三則趨勢說明。

（一）美國聯邦貿易委員會與 Facebook 就隱私洩漏與保護措施不

足的案件達成行政和解

為了確保 Facebook 在使用消費者資料前必須通知並徵得同意，美國聯邦貿易委員會（Federal Trade Commission, FTC）早於 2012 年便與 Facebook 達成行政和解，Facebook 需持續維護全面的隱私保護計畫並每兩年接受稽核。然而 2018 年劍橋分析公司（Cambridge Analytica Ltd）被控告洩露消費者資訊，而 Facebook 因未能為在劍橋分析資料洩露案有效保護其用戶資料，且對於用戶資料之利用有違反 Facebook 與 FTC 的 2012 年和解協議之虞，FTC 因此再度展開對 Facebook 的調查。

2019 年，FTC 基於 Facebook 反覆侵害消費者隱私，違反 2012 年行政和解條款，對 Facebook 處以 50 億美元罰款，並要求 Facebook 必須由董事會成立獨立隱私委員會，並指定專責法令遵循人員（compliance officers），負責制訂 Facebook 的隱私保護計畫，上述專責法遵人員僅能由董事會或隱私委員會任免。FTC 藉由此項要求，由公司治理的層面強化對於 Facebook 的外部監督，並由第三方評估 Facebook 隱私計畫的有效性。

作為 Facebook 強制性隱私計畫（涵蓋 WhatsApp 和 Instagram）的一部分，Facebook 必須在推出新的或修改產品或服務前，對其進行隱私審查，並記錄有關用戶隱私的決定。該命令還要求 Facebook 需加強對第三方應用程式的監督；明確告知使用者有關臉部辨識技術的使用；實施全面的資訊安全維護計畫等。

2020 年 4 月美國哥倫比亞特區地方法院批准了 FTC 與 Facebook 就上述事項達成行政和解協議，該和解協議將督促 Facebook 在開發技術與服務的每個階段都必須考慮隱私保護，並將責任層級提升至管理階層，以提供更大的透明度和問責制。

（二）美國立法禁止政府設備使用抖音（TikTok）

以北京為總部的「字節跳動（Byte Dance）」，於 2012 年推出社群應用「抖音（TikTok）」，目前已成為時下最流行影音短片共享 app，其受歡迎的程度甚至超越 Netflix、YouTube、Twitter、Instagram 等社

群應用 app。然而，抖音的兩大特性，卻使其在全球市場遭遇諸多的挑戰。

首先，抖音的使用者大多數為未成年人，因此被質疑是否不當蒐集未成年人的個人資料，而受到全球隱私主管機關的關注。如 2020 年 7 月 15 日韓國通訊傳播委員會（Korea Communications Commission，KCC）表示，因抖音未經父母同意蒐集 14 歲以下兒童的個資，違反韓國電信法，且未正確告知使用者其所蒐集個資將傳輸至美國或新加坡，KCC 因此對抖音處以 1.86 億韓元罰款。同時，美國聯邦貿易委員會（Federal Trade Commission, FTC）也因民間團體指控，抖音未能履行 FTC 與 Byte Dance 於 2019 年達成之有關保護兒童隱私的行政和解協議（consent agreement），而再度對抖音展開調查。另一方面，國際上長期存有對中國企業可能將資料回傳中國的疑慮，印度政府於 6 月即以「國安與國民隱私風險」為由禁止抖音在印度上架。

美國眾議院於 7 月 21 日通過的「國防授權法」（National Defense Authorization Act, NDAA）中，以附加修正案禁止美國聯邦政府人員，在政府設備上使用抖音；同時，參議院也同步提出「禁止抖音用於政府設備法」（No TikTok on Government Devices Act）草案。該草案規範，除網路安全研究、調查、執法或情報活動外，美國政府人員（含公務員、官員、議員等），均不得在美國政府機構的任何設備上，下載或使用由 Byte Dance 公司或其子公司開發的任何應用程式。

抖音為中國企業推出的 app，但其為取得國際信任，將抖音區分為國際版與中國版，並宣稱「兩個版本的平台彼此獨立」。抖音國際版的主要經營方針由美國團隊主導，不受中國官方或任何政府指示審查內容。然而，在國際政經局勢的演變之下，想兼顧兩個差異頗大的市場，顯然非常困難。

（三）Facebook 發佈新的照片傳輸工具以解決美國競爭法的問題

網路社群平台 Facebook 在數位服務市場上佔有率極高，且頻繁發生使用者個人隱私保護的爭議，分別導致其於美國與歐盟受到個人資

料保護法與競爭法相關主管機關的關注。在資料經濟的發展下，如何確保個人資料安全的同時，提升資料流通性，在法律面做出清晰地規範，一直是個人隱私保護與經濟發展的重要議題。對此，歐盟「一般資料保護規則（General Data Protection Regulation, GDPR）中，即制訂了「資料可攜權」（Right to data portability）的規範，要求業者必須提供消費者可隨時自由的在數位平台間轉移個人資料的措施，以提升消費者資料控制權，自行掌控資料的利用與流向。

Facebook 近期推出了照片傳輸工具（photo transfer tool），允許美國和加拿大的用戶將照片和影片傳輸至另一個影像儲存服務平台（例如 Google Photos）上，未來也將擴張至其他儲存雲端平台，或類似服務型態的數位平台上。此舉可說是部分實現了資料可攜權，而 Facebook 也表示，希望最終開放消費者以安全隱私的方式將如聯絡人、好友名單等資料也能轉移到其他數位平台上。

資料可攜權，除了歐盟 GDPR 外，美國「加州消費者保護法（California Consumer Privacy Act, CCPA）」中，對於個人資料權利也有類似規範，以確保消費者不受數位平台的技術鎖定（lock-in）影響。

當消費者對個人資料擁有更大的控制權，並能更自由的選擇數位平台時，數位服務市場的競爭程度將能有所提升。美國與歐盟近來均針對數位平台的資料掌控程度，以及市場地位，展開競爭法上的討論，其中對於如何促進資料流通，以增進市場競爭，以及對於資料開放與資料可攜權的落實與效益，亦成為關注與討論的焦點。

Facebook 此次的作為，也可說是因應美國與歐盟對其市場競爭行為的調查，回應關於不當使用市場力量的指控，未來也需持續關注隱私保護與市場競爭間的互動。

三、 國際隱私政策與資料流通政策發展

資料在 21 世紀已成為最有價值的資源，舉凡世界諸國均利用資料促進國家整體發展，畢竟掌握巨量資料者將可在壁壘分明之國際市場獲得先機；然而資料應如何處理、利用，並且在資料流通與隱私保護間取得衡平，使社會與市場更為蓬勃發展，則成為各國推動政策之

軸心理念，以下由五則趨勢介紹國際間目前政策動態。

（一）美國大型科技企業因隱私爭議暫停提供執法機關臉部辨識技術

有鑑於近期臉部辨識技術在執法用途上，造成種族歧視及隱私侵害的爭議，美國大型科技企業包括 IBM、亞馬遜（Amazon）及微軟（Microsoft），先後宣布暫停發展或暫不提供執法機關使用臉部辨識技術。

長期以來，臉部辨識技術飽受人權和隱私倡議者的批評，例如其準確性、種族特徵和大規模監視等問題。IBM 執行長 Arvind Krishna 首先宣布，該公司將放棄該類技術的研發及提供，並指出執法機關在使用臉部辨識技術時，可能相當程度侵害基本人權和自由，呼籲其他同業重視此一問題。

而後，亞馬遜在其官方 blog 中宣布，將暫停提供警方使用亞馬遜開發的臉部辨識軟體 Rekognition 一年。亞馬遜指出，政府應制定更嚴格的法規來管理該類技術，以合乎倫理的使用（ethical use），避免對於人權及隱私的侵害；而亞馬遜將允許防止兒童性侵害的非營利組織 Thorn、國際失踪與受虐兒童援助中心（International Center for Missing and Exploited Children）以及研究以大數據打擊犯罪的 Marinus Analytics 公司等，繼續使用 Rekognition 軟體，於幫助營救人口販運受害者，協助失踪兒童與家人團聚等公益用途。

隨後，微軟總裁 Brad Smith 亦宣布，將拒絕向美國警方出售臉部辨識技術，直到政府對該技術進行監管，並制訂適當的聯邦規範。微軟建議政府應解決三個問題：首先，臉部辨識技術增加不當執法的風險，因其結果可能帶有偏見，違反了禁止歧視的規範；其次，該類技術的廣泛使用可能導致對民眾隱私的嚴重侵犯；最後，政府使用該類技術進行大規模監視，有侵害民主自由之虞。

而在立法方面，美國參議員 Edward J. Markey、Jeff Merkley、Pramila Jayapal 與 Ayanna Pressley 等人宣布推動「暫緩使用臉部辨識和生物辨識技術法（The Facial Recognition and Biometric Technology

Moratorium Act）」，限制聯邦政府使用臉部辨識，以及其他類型的生物辨識技術，例如語音等，除非經國會立法許可使用。此外，對於自願停止使用臉部及生物辨識技術的各州及地方政府，提供聯邦資金補助；並限制聯邦不得補助生物辨識監視系統；鼓勵各州及地方政府，制訂有關使用臉部及生物辨識技術的規範。

由於臉部辨識技術存在系統性的誤差，對有色人種的誤判率較高，形成顯著的種族偏見問題，尤其是作為執法工具時，將造成相當大的爭議，因而制訂明確的規範，確保相關技術不被濫用，保障人權及隱私，已成為當前不可忽視的重要議題。

（二）英國法院裁定警察機關使用臉部辨識技術違反隱私法

在大數據與人工智慧的發展下，各種自動化圖像識別技術被應用於各領域，該技術使用雖降低人為出錯的機率，但因其對於資料的快速與大量的處理，也引發對於個人隱私侵害的疑慮。

英國南威爾斯警方（South Wales Police, SWP）於 2017 年開始嘗試使用自動臉部識別技術（Automated Facial Recognition technology, AFR），協助執行部份勤務。自 2017 年 5 月至 2019 年 4 月間，在威爾斯的各種公共活動中，約使用了 50 次 AFR 的即時定位比對功能（AFR Locate）。警方利用 AFR 比對約 400 至 800 人之監視清單（watch lists），清單中包括通緝犯、逃離羈押的嫌犯、特別的弱勢族群，或是基於特定情報而受到關注的對象。AFR 會即時將清單內與活動中的民眾臉部資訊進行比對，如果沒有與清單中的任何一個對象匹配，則民眾的臉部圖像會立即被刪除。

公民運動者 Edward Bridges 於 2019 年 5 月向卡地夫（Cardiff）地方法院（Division Court）提出申訴，認為警方處理敏感個人資料之法律授權不足，對人權保護恐造成侵害。此外，自動化身份辨識可能產生的誤差風險，也是一個必須被考量的因素。該案件因屬行政訴訟，而移轉至英格蘭與威爾斯高等法院（High Court of Justice）之皇座法庭（Queen’s Bench Division）審理。於 2019 年 9 月，高等法院駁回 Edward Bridges 對於 SWP 使用 AFR 的申訴，高等法院認為使用 AFR

是實現警察法定義務所必要且適當的。因此 Edward Bridges 持續向上訴法院（Courtt of Appeal）提出申訴。

2020 年 8 月 11 日，上訴法院認為警方使用 AFR 違法且侵害人權，且 SWP 使用 AFR 的規範與政策不夠明確，給予警方過多的裁量權。同時，SWP 也並未採取合理措施，以確認 AFR 是否包含基於種族或性別的偏見。值得注意的是，上訴法院認為警方基於比例原則判斷，若對於個人權益影響較小，但有利於公共利益，則 AFR 的使用是合理的。亦即 AFR 並非當然違法，而是應基於嚴格的程序規範，並遵守公平原則之下，警方始得合理的使用 AFR，以增進公共利益。

（三）英國使用演算法決定 A 級考試成績衍生之爭議

由於新型冠狀病毒（COVID-19）危機仍未解除，英國取消 A 級（A-Level）考試，改以學校老師預測的成績以及學生在學表現為基礎，透過演算法決定本年度學生的 A 級成績。

A Level 是英格蘭、威爾斯、北愛爾蘭和英國其他地區的青少年的學校課程，學生選擇三到四門的課程修習，透過繳交作業及參加最終考試的方式，作為最後大學入學資格依據。特定的大學課程可能要求特定學科成績，因此學生選修的課程與考試成績，影響是否能進入特定大學。今年由於 COVID-19 流行，取消 A-Level 考試，故英國政府決定透過演算法，預測學生 A-Level 之分數。

為使所有學校的老師判斷標準具有一致性，並確保結果與歷年表現相當，英國負責規範學歷與考試事項的主管機關資格和考試管理辦公室（Office of Qualifications and Examinations Regulation, Ofqual），開發一套標準化模型以預測各學科的成績，並根據學校的歷史成績分佈和學生歷年的成績表現，預測本年度預定參與 A-Level 學生的成績。亦即，本年度 A-Level 並非學生準備兩年的直接考試結果，而是演算法計算的結果。

Ofqual 表示，演算法旨在調節（moderate）英國的成績授予過程，防止不同地區、學校、老師給學生打分數主觀上不一致的狀況。然而，該演算法因結果疑似對弱勢學生不公平而遭受抨擊。論者表示，該演

算法有利於規模較小的學校，而因為私立學校的班級規模通常較小，故有擴大私立學校優勢之虞，不利於班級規模較大的公立學校。從而，在公立學校中表現優異的學生，可能因此獲得遠低於預期的 A-Level 成績，失去進入大學的機會；而私校學生的成績則可能大幅提高。此外，私校學生通常社經地位較為優勢，該演算法恐加劇公私校間的落差。由於前述的爭議，英國政府決定取消演算法預測的成績，改為由老師預測的成績作為依據，並協調各大學進行增額錄取，以確保本年度學生的權益。

歐盟於一般資料保護規則（General Data Protection Regulation, GDPR）第 22 條第一項規定，資料主體有權不接受僅基於自動化處理（automated processing），包括剖析（profiling）的決定，且該處理是會對當事人產生法律效力，或產生類似的重大影響。本次英國在 A-Level 成績的爭議上，透過參考老師及學校的意見，避免僅依據自動化處理機制，做出對個人有重大影響的決定，且可能帶來負面和不公平後果，因此演算法所預測的僅為學科成績，尚不等於大學的入學決定，並未完全違反 GDPR 第 22 條第一項的規範。

（四）法國與德國聯合推動 GAIA-X 歐洲資料基礎架構

手機與民眾生活緊密結合，無論是購物、娛樂、追劇、運動等網路活動，均可能伴隨大量資料蒐集、應用，當消費需求或市場資訊被加以連結分析後，其所產生的巨大經濟價值，促成數位經濟發展。許多大型數位服務平臺，如 Google、Facebook、Amazon 等，便是運用其資料蒐集與分析技術上的優勢，在數位時代中領先群倫。

歐盟為強化其數位經濟實力，於 2020 年 2 月宣布「歐洲資料策略」（A European strategy for data），提出以雲端為基礎、建立歐洲共同資料空間（common European data space），使境內各機構能共享資料，進而促進數位經濟發展。在資料利用上，必須遵守一般資料保護規則（General Data Protection Regulation，GDPR），例如須確保資料安全性和資料控制權，並保護個人隱私與機密。而在資料交換上，則須於技術上確保資料的安全與互通。這意味著，歐盟的資料平臺不僅

必須遵守隱私法規，也必須遵守開放的技術標準。

考量規範與技術兩方面的需求，德國聯邦經濟事務和能源部（BMWi）部長 Peter Altmaier，和法國經濟和財政部（MINEFI）部長 Bruno Le Maire，共同於 2020 年 6 月 4 日宣布啟動 GAIA-X 計畫，打造歐洲資料基礎架構（Data Infrastructure for Europe）。GAIA-X 計畫目的在於建立歐盟的雲端資料基礎架構，結合歐盟數位單一市場政策，形塑歐洲的數位未來，透過促進歐洲在科學、經濟、政治、金融、醫療和社會等許多領域的資料共享互通，打造歐盟數位轉型基礎。

在雲端服務市場已存在 Amazon、Google 與微軟等巨頭的情形下，GAIA-X 並非重新建立一個競爭性的雲端服務，而是以「歐洲價值」為核心，打造一個可信賴（trustworthy）、安全（secure）和透明（transparent）的資料基礎架構，以確保資料可用性（data availability）。GAIA-X 將建立相關技術規範，以整合不同的雲端服務業者（cloud service provider, CSP）、網路接取與互連服務業者、高性能運算（high performance computing, HPC），以及不同產業的雲端和邊緣系統（edge system）。

GAIA-X 架構在優勢上，首先是確保使用者的資料主權（data sovereignty），使用者可自行決定資料分類、儲存位置、利用的對象與目的。為了使資料自由流通，在不同的網路、系統、平臺與應用服務之間，應確保資料可攜性（data portability），及資料互通性（interoperability）；並支援開放原始碼（open source）以及資料開放（open data）等要求，以建立歐盟的資料經濟生態系。

目前共有來自 7 個歐洲國家、約 22 家業者規劃參與 GAIA-X，同時 GAIA-X 也正與歐盟執委會持續交流，希望得到更多歐盟會員國的支持，成為一個泛歐的資料基礎架構，進而呼應歐盟數位轉型政策，強化歐盟數位時代的競爭力。

（五）歐盟法院裁定歐盟與美國間的隱私盾保護協議無效

個人資料的跨境傳輸是許多美國跨國企業的命脈，這些跨國企業從位於美國的總部集中管理全球員工的職位、薪資與福利，也管理員

工使用企業網路系統的權限，倘若不允許個人資料跨境傳輸，則跨國企業的運作或管理上，均會遭遇相當大的困難。在歐盟嚴格的個人資料保護法規下，美國跨國企業長期仰賴特殊的隱私保護協議進行資料跨境傳輸。

在早期，美國與歐盟間建立了安全港協議（Safe Harbor），跨國企業遵守安全港協議，承諾保障個人隱私安全，便得進行跨境傳輸個人資料；然而於 2013 年，愛爾蘭高等法院因處理奧地利公民 Schrems 與 Facebook 間，關於 Facebook 將歐盟公民個人資料傳輸至美國一事之訴訟，而請求歐盟法院確認安全港協議之效力；2015 年 10 月 6 日，歐盟法院認定安全港協議無效。而後，美國與歐盟就新的隱私保護架構展開談判，歐盟於 2016 年 7 月 12 日通過了新的 2016/1250 號決定（Commission Implementing Decision (EU) 2016/1250），即隱私盾協議（EU-U.S. Privacy Shield）。

在同一時間過程中，前述 Schrems 訴訟也尚未結束。Facebook 主張依據歐盟執委會 2010/87 號決定（Commission Decision 2010/87/EU）內的「標準契約條款」（Standard Contractual Clauses, SCC），跨境傳輸歐盟個人資料到美國。SCC 是基於企業與使用者之間合意的標準化契約條款，用以確保個人資料符合歐盟個資保護規範，進而傳輸至第三方國家。Schrems 於 2015 年 12 月 1 日修改訴訟主張，認為不能以 SCC 作為主張個人資料跨境傳輸的正當性。愛爾蘭高等法院於 2018 年 5 月 4 日將本案提交至歐盟法院，確認 SCC 和隱私盾協議的有效性。

歐盟法院於 2020 年 7 月 16 日判決隱私盾協議無效，SCC 仍保持有效。歐盟法院認為，首先，美國有關情報監控的規範，在實施個人資料監控時，不符合比例原則以及必要性原則；其次，雖然依據隱私盾協議，美國政府實施個人資料監控時，必須遵守其要求，但並未賦予資料主體於權益受侵害時，可提起訴訟保障自身權益的訴訟權保障。故基於上述理由，隱私盾協議不符合歐盟隱私規範要求，故判決隱私盾協議無效。

此一裁決對美國的網路企業帶來巨大挑戰，這些企業可能必須被

迫改變其個人資料處理策略，美國企業需要了解他們如何受到美國相關監控法律的約束，以及他們的資料保護是否符合歐盟要求。長遠來看，可能必須考慮將涉及歐盟的部份業務移出美國，或等待美國與歐盟重新制定新的協議。

四、 分析與小結

整體而言，由前述 10 篇國際趨勢觀測報導加以觀察，最核心的概念是在於科技的運用對於各種類型個資的影響，包含有疫情、網路社群平台，以及臉部辨識。而這些議題逐漸變得非常重要，則是透過人工智慧（AI）或是特定的演算法的應用，可快速而大量的處理個人資料，從而若技術使用不當時，便可能對個資保護產生非常大的侵害，不單是處理敏感的個人健康資料的問題，甚至產生種族歧視的問題。

而另一個層面的概念，則是因為個人資料使用於商業用途，使社群平台獲得巨大的市場利益，甚或影響到國家之間的經濟競爭，例如歐盟的雲端政策重視在個資保護與資料互通上，以促進市場競爭；美國則因近年與中國大陸的經濟競爭，所以封鎖了社群軟體 TikTok，這也顯示出數位經濟已成為主要國家之間的新經濟戰場。而實際上，最具重大影響的議題，即歐盟與美國間隱私盾協議被判決無效的事件，也可以看成是美國與歐盟在數位經濟上的再一次交鋒。

最後一個有趣的觀察點，則是 Facebook 所涉及議題之廣，也無怪乎其身為最大的社群平台，無論在美國或歐盟，都是諸多爭議的焦點，而其對於個人資料的處理與應用，在美國與歐盟都分別受到個資主管機關以及競爭主管機關的關注；由此亦可推論，資料利用對於數位經濟發展佔據非常關鍵的角色，依當下觀察，其受到的關注將持續有增無減。

期末報告則是持續觀測並蒐集共 6 篇與本研究議題相關性較高之國際資訊，並歸納為兩項資料經濟與個資保護重要議題：

1. 數位經濟與防疫發展下的線上服務安全與隱私保護：期末報告觀察數位經濟與新冠疫情發展下，各國政府對於線上服務可能引發的隱私與個資保護議題，包括美國對於線上視訊會

議軟體服務的規管、英國對於線上服務的兒少線上安全與隱私保護規管的發展動態，以及歐盟議會為維護民眾線上安全與個資保護權益、健全線上環境發展，對於未來數位服務市場與人工智慧規範所提出之規範政策倡議。

2. 國際個資保護與資料治理政策發展：期末報告持續觀測國際個資保護與資料治理的重大政策發展，包括美國參議院近來提出的安全資料法案、英國為能取得 GDPR 適足性認定所進行相關個資法制與制度整備發展，以及歐盟執委會近來提出的資料治理法草案。

對於以上議題，分別收集之國際動態資訊於下詳述。

表 22 2020 年 9 月至 11 月趨勢動態資訊彙整

重要議題	國際動態資訊
數位經濟與防疫發展下的線上服務安全與隱私保護	1. 美國 FTC 透過行政和解令要求 Zoom 強化隱私安全保護 2. 英國 ICO 發布適齡線上服務設計規範以保護兒童隱私 3. 歐洲議會提出有關數位平臺及人工智慧管制的立法倡議
國際個資保護與資料治理政策發展	4. 美國參議院提出安全資料法草案 5. 英國發布脫歐過渡期後的個人資料保護措施 6. 歐盟提出新的資料治理規範

資料來源：本計畫製作

一、數位經濟與防疫發展下的線上服務與隱私保護

在全球 COVID-19 疫情持續嚴峻的發展情勢下，加速了全球數位經濟的發展，而各式線上服務的蓬勃發展，於各國引起許多隱私與安全相關議題。本研究蒐集有關線上視訊的隱私安全、一般民眾甚至是兒少線上環境安全與隱私保護等議題，亦觀察到各國政府以保護線上環境的隱私與安全為目標，除陸續透過行政規管措施外，並探討相關法制之研擬，以因應防制相關問題。上述議題由以下三則趨勢進行說明。

（一）美國 FTC 透過行政和解令要求 Zoom 強化隱私安全保護[29]

受到新冠病毒(COVID-19)疫情影響，居家遠距辦公的需求高速攀升，全球各大企業紛紛透過遠距會議軟體，應對防疫時期的會議需求。其中快速席捲市場的視訊會議平台 Zoom(Zoom Video Communications, Inc.)，其用戶數從 2019 年 12 月的 1000 萬飆升至 2020 年 4 月的 3 億，成為疫情期間不可或缺的線上服務。然而其標榜的易用性與方便性，卻面臨隱私保護和資料安全的爭議與挑戰。

電子隱私資訊中心(Electronic Privacy Information Center, EPIC)於 2019 年 7 月，向美國聯邦貿易委員會(Federal Trade Commission, FTC)投訴，要求調查 Zoom 網路安全及隱私保護風險。EPIC 指出，Zoom 軟體存在諸多安全漏洞，使用戶可能受到隱私安全的侵害及網路駭客攻擊。Zoom 則宣稱其將消費者隱私和安全放在首位，並致力於保護用戶的通訊安全，例如強調其通訊過程中使用「端對端 AES 256 位元加密」(end-to-end AES 256-bit encryption)；或在會議結束後，會立即將內容儲存於加密的安全雲端空間等。

歷經一年多的調查後，FTC 指出 Zoom 實際並未完全達成其所宣稱之安全性，大多數 Zoom 會議並無端對端加密，或加密等級並未達到 256 位元，以及其所宣稱的雲端加密儲存機制，實際上卻出現未加密的狀態等。同時，Zoom 雖然宣稱已不斷改善及加強產品安全性，實際上卻未能快速且及時的修補資安漏洞，以降低用戶的安全風險，進而導致侵害消費者權益。

有鑑於上述情況，FTC 認為 Zoom 對於隱私安全保護的不足，構成欺詐消費者行為，於 2020 年 11 月 9 日宣布與 Zoom 的行政和解協議(agreement containing consent order)，要求 Zoom 必須對其資訊安全程序進行徹底的改進，確保公司履行其對用戶的隱私和安全性承諾，並禁止該公司對外不當地宣傳錯誤資訊。

---

[29] FTC Requires Zoom to Enhance its Security Practices as Part of Settlement, FTC, https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement; FTC orders Zoom to tighten data security practices, Iapp, https://iapp.org/news/a/ftc-orders-zoom-to-tighten-privacy-infosecurity-practices/ (last visited Dec.7, 2020).

具體來說，Zoom 需制定一個全面的資訊安全計畫，從軟體開發階段即建立安全管理流程，以確保軟體開發及後續發布的安全性。Zoom 還需對所有員工進行定期安全培訓，對軟體開發相關人員和工程師進行更專業的訓練。Zoom 還需於未來的 20 年內，每 2 年由合格的第三方進行獨立的安全稽核與評估，並提交報告予 FTC。若 Zoom 未遵守與 FTC 的行政和解協議，FTC 將施與更嚴厲的經濟上處罰。

（二）英國 ICO 發布適齡線上服務設計規範以保護兒童隱私[30]

資料是數位服務的運作核心，無論是成年人或兒童，從打開應用程式、玩遊戲或存取網站內容的那一刻起，各式各樣的資料就開始被蒐集，提供服務或內容的業者可以得知誰在使用該服務、如何使用、使用頻率、使用什麼類型的裝置等。業者透過分析這些資料，提供個人化的誘因，吸引民眾花費更多時間使用服務，增進與使用者的互動，提供量身訂製的服務，推播個人化的廣告。然而，對於兒童而言，當前的網路環境可能不適於其安全地學習、探索。

有鑑於此，英國資訊專員辦公室(Information Commissioner's Office, ICO)於 2020 年 8 月 12 日，依據 2018 年資料保護法(Data Protection Act 2018)第 125(1)(b)條，發布了「適齡線上服務設計規則」(Age Appropriate Design Code)，該規則於 2020 年 9 月 2 日生效，過渡期為 12 個月，亦即受規範之企業或組織，應在 2021 年 9 月 2 日之前完成規則之要求。

ICO 表示，制定此規則的目的，在於保護與協助兒童面對數位世界中的事物，落實英國資料保護法對於兒童網路保護的要求。該規則基於一般資料保護規則(General Data Protection Regulation, GDPR)的基礎，要求兒童所使用的資訊社會服務(Information Society Services, ISS)，包含各種社群媒體與遊戲等，在設計和開發兒童使用的網站服務、應用程式、遊戲、聯網玩具(connected toys)時，應該充分考量保

[30] ICO's Children's Code will help protect children online, ICO, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/09/ico-s-children-s-code-will-help-protect-children-online/;Age appropriate design: a code of practice for online services, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/ (last visited Dec.7, 2020).

護兒童的最大利益。

該規則為線上服務和產品的設計人員提供了 15 條彈性標準，闡述應如何遵守英國資料保護法，要求數位服務業者在兒童下載新應用程式、遊戲或存取網站時，預設自動提供高度的資料保護設定，以確保兒童的最大利益，安全的在網路上進行探索與學習。網站或應用程式應僅蒐集、保留最少量的個人資料，有關兒童的資料不應共享，在預設情形下，不可蒐集兒童位置資訊，也不應誘使兒童自行降低或關閉其個人隱私的設定。

在未來 1 年的過渡期內，ICO 將協助數位服務業者符合該規則的要求，並與網路創新服務業者持續溝通，改進相關資料保護規範，以妥善保障兒童個人資料安全，並促進數位經濟發展。

（三）歐洲議會提出有關數位平臺及人工智慧管制的立法倡議[31]

在數位經濟的趨勢下，歐洲議會分別針對數位服務市場，包含數位平臺和數位市集(marketplaces)的管制，以及人工智慧(Artificial Intelligence, AI)的道德、責任與智慧財產權(ethics, liability and intellectual property rights)法制，提出未來立法建議，以促進創新、道德標準和對技術的信任。

針對數位平臺管制，歐洲議會(European Parliament)通過二項立法倡議(legislative initiative)，呼籲歐盟委員會(Commission)應在預計於 2020 年 12 月提出的「數位服務法」(Digital Services Act, DSA)草案中，解決數位環境存在的不當內容問題，以提供消費者更安全的網路環境。

在資料利用的部份，則是降低消費者對於演算法的依賴，歐洲議會希望消費者對於其在網路上觀看的內容，能有更多的控制權，降低業者內容管理的影響，減少消費者對演算法的依賴。具目標性(targeted)的廣告必須受到更嚴格的監管，以減少依據個人資料分析的

[31] Parliament leads the way on first set of EU rules for Artificial Intelligence, European Parliament, https://www.europarl.europa.eu/news/en/press-room/20201016IPR89544/parliament-leads-the-way-on-first-set-of-eu-rules-for-artificial-intelligence; Digital: The EU must set the standards for regulating online platforms, say MEPs, European Parliament, https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps (last visited Dec.7, 2020).

推播廣告。

而在人工智慧(AI)部份，就道德、責任與智慧財產權方面提出建議。首要建立在開發 AI 時（包括軟體、演算法與資料分析）需遵守的道德原則和法律義務；其次，在責任方面，要求建立清晰的的民事責任架構，為企業提供法律確定性來刺激創新，並增強民眾對 AI 技術的信任；最後，區分 AI 輔助人類創造(AI-assisted human creations)和 AI 自行創造(AI-generated creations)非常重要，將影響智慧財產的認定與歸屬。

數位平臺與人工智慧是數位經濟下，資料運用的主要角色與技術，其發展對於民眾的生活影響也越來越深入。對於個人資料與個人權利保護相當重視的歐盟，也已逐漸進入法制的討論，歐盟數位服務法的立法，以及人工智慧法制的發展，對於全球數位經濟將有非常大的影響，後續發展亦須持續關注。

二、國際個資保護與資料治理政策發展

數位化及網路化型塑出資訊社會的風貌，也驅動資料經濟發展，資料成為 21 世紀最有價值的資源，全球各國均利用資料促進國家整體發展，畢竟掌握巨量資料者將可在國際數位市場搶得先機；然而資料應如何處理、利用，並且在資料流通與隱私保護間取得衡平，使社會與市場更為蓬勃發展，則成為各國推動政策之軸心理念。本研究由以下三則趨勢介紹國際間目前資料治理相關政策動態。

（一）美國參議院提出安全資料法草案[32]

在保障個人資料隱私的法制上，美國並未如歐盟制定獨立的個人資料保護規範，而是散見於不同產業規範，如有關金融或健康法規，或是各州自行制定。由於不同產業的個資保護規範未必一致，部份產業甚至沒有個資保護之規定；而美國也並非每一州均有制定個資法

[32] Consolidating US privacy legislation: The SAFE DATA Act, Iapp, https://iapp.org/news/a/consolidating-u-s-privacy-legislation-the-safe-data-act/; S.4626 - SAFE DATA Act, Congress, https://www.congress.gov/bill/116th-congress/senate-bill/4626. See also the Committee on Commerce, Science, and Transportation, https://www.commerce.senate.gov/services/files/BD190421-F67C-4E37-A25E-5D522B1053C7 (last visited Dec.7, 2020).

規，因此產生個人隱私保護不足的疑慮。有鑑於此，美國參議院商業、科學和運輸委員會主席、參議員 Roger Wicker 與數名同黨參議員共同提出「制定確保美國資料存取、透明度和責任的架構法」草案（Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act，依其字首簡寫為 SAFE DATA Act，故簡稱為「安全資料法」）。追溯其立法形成之過程，「安全資料法」可說是由早先提出的三個法案中所包含的資料隱私保護措施整合而成，包括「美國消費者資料保護法」(U.S. Consumer Data Protection Act)、「資訊篩選器透明法」(Filter Bubble Transparency Act)、「降低線上使用者詐騙經驗法」(Deceptive Experiences To Online Users Reduction Act)。故而，「安全資料法」為參議院共和黨迄今提出最完整的隱私保護法案，也可說是綜合了美國聯邦隱私立法的最新發展。

「安全資料法」基本規定包括要求企業在處理或傳輸個人敏感資料之前，須獲得明確的同意，企業須公開個資保護政策，實施合理的資料安全措施，並且不得因消費者不同意個資蒐集，而拒絕提供商品或服務。該法案也保障消費者存取、更正、刪除和可攜資料的權利；並要求企業應該盡可能減少資料蒐集，需有專人維護個人隱私與資料安全，並進行年度隱私影響評估等。

由於「安全資料法」整合了其他法案的內容，因此也將數位平臺的演算法、排名機制的透明度納入，要求數位平臺必須讓使用者知悉是否受到演算法的影響；另一部份則包含限制網路上相關的不公平和詐欺行為，例如偽裝成心理測驗或研究的詐騙內容，或是在網站界面上設計容易使消費者誤觸的按鈕，以達到詐取消費者同意，進而蒐集個人資料的行為。

總體而言，「安全資料法」納入了當代個資保護最重要的數位平臺行為規範，也可說是集數年來美國個資保護立法討論的大成；雖然依據美國的法律制定過程以及當前的政治生態，「安全資料法」的立法未必一帆風順，但因其內容之完整度，相關後續發展值得持續追蹤。

（二）英國發布脫歐過渡期後的個人資料保護措施[33]

在英國決定脫離歐盟時，也同時與歐盟執委會就英國與歐盟未來各層面的關係展開談判，其中關於個人資料保護方面，是透過尋求歐盟執委會的資料保護適足性認定(adequacy decision)，以使英國在脫離歐盟的過渡期於 2020 年 12 月 31 日結束後，仍能維持從歐盟到英國的個人資料自由流通。

適足性認定的程序，規範於歐盟「一般資料保護規則」(General Data Protection Regulation, GDPR)第 45 條，以評估申請人（非歐盟成員國）提供的資料保護的充份程度，歐盟委員會必須考慮的一系列因素，包括法制、對人權和自由的尊重，以及個資保護相關法律規範狀況；其次則是一個或多個獨立監管機構存在，並能有效運作；最後則是該國已參與有關個人資料保護的國際組織或已簽署的國際公約。因此，歐盟執委會必須評估英國是否設有有效且運作正常的獨立個資監管機構，負責確保和強制遵守英國個人資料保護相關規範，確認英國個資保護水準與歐盟保持一致。

由於英國政府取得適足性認定的時程有所延遲，因此發布了有關脫歐過渡期結束後，國內各公私組織應如何處理個資保護和資料傳輸的指南。而 2020 年 7 月 16 日歐盟法院撤銷了歐盟與美國間的隱私盾協議(privacy shield)，不僅表明了歐盟個資不可任意傳輸至美國，英國政府也認為，歐盟「標準合約條款」(Standard Contractual Clauses, SCCs)後續將成為個人資料國際傳輸的合法方式。

因此，在過渡期結束之前，若英國尚未獲得適足性認定，英國企業將如何合法的資料傳輸，以及歐盟 GDPR 將如何於 2021 年 1 月 1 日後適用，該指南說明得要求企業透過 SCC 條款建立替代的傳輸機制，以確保個人資料可以從歐盟合法地傳輸至英國。

當前，歐盟對英國的適足性認定正在進行中，若順利通過，則企業無需採取進一步行動。然而若不如預期，英國資訊專員辦公室

[33] Using personal data in your business or other organisation from 1 January 2021, GOV.UK, https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period; Clock ticks on Brexit adequacy decision, Iapp, https://iapp.org/news/a/clock-ticks-on-brexit-adequacy-decision/ (last visited Dec.7, 2020).

(Information Commissioner's Office, ICO)亦會持續協助英國企業合法傳輸資料，或是建立適當的 SCC 協議。

除此之外，在通過歐盟適足性認定的 12 個國家中，有 11 個國家將與英國保持不受限制的個人資料傳輸。

（三）歐盟提出新的資料治理規範[34]

數位經濟的趨勢下，資料使用的社會與經濟潛力相當巨大，有助於創新技術、產品和服務的開發、提高生產效率與公共利益。例如，在醫療健康領域，資料利用有助於提供更好的醫療品質，在罕見或慢性疾病方面提供精準醫療。為了實現此一巨大潛力，歐盟認為必須促進更多的資料利用，增進資料共享的信任(shared with confidence)，並且在技術上使資料易於再利用(reuse)。

歐盟委員會於 2020 年 11 月提出「歐洲資料治理規則」(Regulation on European data governance)，亦稱為資料治理法(Data Governance Act)，目的在促進歐盟資料共享，支持歐洲資料空間(European data spaces)的形成。資料治理是指資料利用的規則和手段，例如資料共享機制、協議和技術標準等；資料共享的架構與程序亦須具備安全性（例如透過受信任的第三方執行）。歐盟期望透過資料治理法，塑造新型態資料中介者(novel data intermediaries)成為受信任的(trustworthy)資料共享組織者(data-sharing organizers)。資料治理法將使歐洲民眾擁有更大的資料控制權，並確保各會員國資料治理規範上的一致，以利歐洲單一資料市場與歐洲共同資料空間的發展，強化歐洲數位主權(digital sovereignty)。

在促進公共利益的目標上，資料治理法將制定可信賴的資料利他主義(data altruism)原則，重視鼓勵非商業性、且具有社會公益的資料共享，以達到資料利他主義，並制定歐洲通用的資料共享同意書(common European consent)，提供各成員國之間資料蒐集與共享協議

[34] Commission proposes measures to boost data sharing and support European data spaces, European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2102; Proposal for a Regulation on European data governance (Data Governance Act), European Commission, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act (last visited Dec.7, 2020).

的統一格式(uniform format)，並可依據特定部門和目的進行調整。而自願遵守資料利他主義的單位或機構，得公開登記為「資料利他主義組織」(data altruism organization)。該組織必須為非營利性質、滿足透明性要求，並遵守保障民眾權益的特定措施，以達成「在最小的管理負擔下，提供最大信任」的目標。

歐盟期望在符合其價值觀和既有法律架構下，促進資料的流通與利用，並確保歐盟民眾的個人資料和具敏感性的資料受到良好的保護。資料治理法補充歐盟的整體資料管理體系，提供一個良好的資料治理架構，並將確保資料擁有者可以自願、信賴的提供資料共享，以創造更公平的經濟，發揮最大社會利益。

觀察上述 6 篇國際趨勢觀測資訊之重點，主要為國際間對於線上環境的消費者安全與隱私保護權益政策，以及資料治理與個資保護政策與法制整備發展趨勢。首先，在現行全球 COVID-19 疫情持續嚴峻的情況下，數位服務業者成為各國於防疫時期，為避免疫情大幅蔓延擴散，維護日常生活、休閒娛樂以及工作活動之運作的重要服務提供者，進而促進了全球數位經濟朝向更為蓬勃的成長發展。而在線上環境發展，於現今國家社會之日常運作，日漸更加顯著地重要時，許多線上服務及其科技應用，亦產生對於民眾個資隱私安全可能造成重大影響之情事。因此，各國政府對此陸續作出各種因應措施，包括近來的線上通訊服務，作為各國防止疫情擴散的重要數位應用科技，其近來引發許多的資安疑慮爭議，因而造成的線上隱私與安全問題，成為各國政府持續關注與積極處理的重要議題，如美國政府即採取措施要求業者改善；以及，歐盟議會針對數位服務市場的未來規管政策，提出為強化民眾使用線上服務之安全與個資保護權益之政策倡議；英國政府更針對兒少線上安全與隱私保護，採取「設計保護隱私」(Privacy by Design)規範途徑，要求數位服務提供者加強保護兒少的線上安全與個資隱私，均顯現出各國政府對於民眾使用線上服務的安全與隱私個資保護之重視。

其次，在國際間個資保護與資料治理政策與法制發展方面，無論是美國近來提出的安全資料法草案，除強化個人資料之隱私保護，並

對於數位平臺之數位服務納入規管，作為因應數位服務與資料經濟蓬勃發展下的個資保護規範法案；或是英國為能在完成脫歐程序後，順利取得歐盟 GDPR 適足性認證，持續進行的個資保護法制規範與機構等制度整備，以利英國未來資料經濟政策的發展；以及歐盟為強化促進安全的資料互通與共享利用，近來提出的資料治理規則草案，亦顯示各國對於資料治理政策之重視。

第二節 研究調查摘譯與分析重點資訊

每月提供研究調查摘譯與分析重點資訊 1 篇，定期彙整觀測主題與報告，參考通傳會官網之「國際通傳產業動態觀測」專屬網站資料，撰寫議題包含隱私保護發展趨勢、通傳產業數位經濟、大數據運用、異業合作（結合）相關研究等進行資料蒐整與研究。

瀏覽各國通訊傳播主管機關發布政策文件或調查，如美國聯邦交易委員會（Federal Trade Commission, FTC）、英國通訊傳播主管機關（Ofcom）、英國數位文化媒體暨體育部（Department for Digital, Culture, Media & Sport，DCMS）、日本總務省、經濟產業省等；或是國際組織、智庫、協會或公司提出之報告等，如 APEC、OECD、全球行動通訊系統協會（Groupe Speciale Mobile Association，GSMA）、國際電信聯合會（International Telecommunication Union，ITU）、Deloitte 等。以下整理從 109 年 4 月至 11 月研究調查摘譯與分析重點資訊 8 篇：

表 23 2020 年 4 月至 11 月研究調查摘譯與分析重點資訊

	研究調查摘譯與分析重點資訊
1.	WEF「理解媒體的價值：消費者與產業觀點」（Understanding Value in Media: Perspectives from Consumers and Industry）報告
2.	IBA Research「關注 2020 年 54 種技術趨勢」（54 TECHNOLOGYTRENDS TO WATCHIN 2020）白皮書
3.	世界經濟論壇發表「跨境資料流動藍圖：新資料經濟中永不過時的準備與合作」白皮書
4.	世界經濟論壇「行動資料的十項操作原則」白皮書
5.	Facebook「隱私交流：朝向以人為本與信賴的設計」白皮書

	研究調查摘譯與分析重點資訊
6.	開放通訊：電信領域的開放式可信賴資料生態系統
7.	世界經濟論壇「後疫情時代下數位媒體與技術設計的倫理原則」報告
8.	英國未能確保符合歐盟適足性認定的經濟影響

資料來源：本計畫製作

一、WEF「理解媒體的價值：消費者與產業觀點」（Understanding Value in Media: Perspectives from Consumers and Industry）報告[35]

WEF 於 2020 年 4 月發表關於媒體價值的報告，透過消費者之媒體收視相關資料調查，進而分析不同的利益關係者對於媒體內容的重視。首先，分析 6 個主要媒體市場（德國、韓國、英國、美國、中國和印度）;其二，提出媒體商業模式的影響;其三，提高人們對塑造未來媒體、娛樂和文化平台的興趣和關注的意識。

該報告指出消費者的媒體參與度高，但不到一半的消費者為新聞和娛樂付費；將來願意為媒體付費的人比例大於當前付費的比例，而年輕人（16-34 歲）更有可能為內容付費。至於如何為有價值內容的製作提供資金的問題仍然存在，且媒體策略的改變亦代表著不同獲利模式、消費者習慣改變與超級競爭者的到來，皆會影響未來媒體的發展。

綜上，媒體未來面臨的主要問題在於「說服消費者對於媒體提供有價值內容進行付費」，報告建議關注生態系媒體對於整體經濟的影響，應密切關注其將媒體整合到其活動中的方式；以及法規如何平衡創新、消費者福利和企業責任。

二、IBA Research「關注 2020 年 54 種技術趨勢」（54 TECHNOLOGYTRENDS TO WATCHIN 2020）白皮書[36]

資料通訊技術市場研究機構 ABI Research 於 2019 年 12 月

[35] Understanding Value in Media: Perspectives from Consumers and Industry, WEF, https://www.weforum.org/reports/value-in-media (last visited Aug.27, 2020).
[36] 54 TECHNOLOGYTRENDS TO WATCHIN 2020, IBA Research,

發布「關注 2020 年 54 種技術趨勢」(54 TECHNOLOGYTRENDS TO WATCHIN 2020)白皮書,提出將影響未來技術市場的趨勢,涵蓋 5G 相關技術與基礎設施、人工智慧與機器學習、增強和虛擬實境、數位安全、貨運與物流、工業和協作機器人、製造業、定位技術、物聯網、智慧城市和智慧空間、智慧家電、智慧移動、影視與雲端以及 Wi-Fi、Bluetooth、無線連接技術等。以上趨勢所蘊含的技術挑戰對於現今數位驅動市場係為關鍵,而值得關注的是既有技術與創新之衝擊與矛盾。

其中牽涉隱私的技術趨勢,即為「臉部辨識」(Face recognition)技術,在多種應用場景中,需評估實用性與安全性,且關於隱私權之侵害亦引發爭議。現階段中國大力投資且廣泛應用臉部辨識;而美國加州則是全面禁止臉部辨識,其他州亦針對生物辨識(biometric)立法;英國則要求執法者公開揭露對公共事務秘密監視議題等。生物辨識技術的發展,不僅影響政府相關政策,更反映企業風險。儘管未來該技術的發展仍待觀察,但臉部辨識應用特別是生物監視(biometric surveillance)將持續擴增,因此如何在監管與公共安全之間兼顧隱私保護將是未來的挑戰。

三、 世界經濟論壇發表「跨境資料流動藍圖:新資料經濟中永不過時的準備與合作」白皮書[37]

「世界經濟論壇」(World Economic Forum, WEF)與「巴林經濟發展委員會」(Bahrain Economic Development Board)以及世界各地組織的指導委員會共同合作,於 2020 年 6 月發表關於「跨境資料流通藍圖:新資料經濟中永不過時的準備與合作」白皮書(A Roadmap for Cross-Border Data Flows: Future-Proofing

https://cdn2.hubspot.net/hubfs/6705264/Marketing/Whitepapers/54%20Technology%20Trends%20To%20Watch%20In%202020/ABI_Research_54_Technology_Trends_to_Watch__In_2020.pdf?hsCtaTracking=095d6803-5017-4852-9028-6691d19085a4%7Cdc1a0ec9-b458-4e51-a3c2-e25c1a1ba80c (last visited Aug.27, 2020).

[37] A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy WHITE PAPER, WEF, https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy (last visited Aug.27, 2020).

Readiness and Cooperation in the New Data Economy WHITE PAPER），旨在促進資料密集技術（data-intensive technologies）的創新，並實現區域和國際關於資料跨境流通合作發展的最佳實踐政策。

對於任何依賴資本、商品、知識和人員自由流通，以與其他國家互動的國家而言，跨境資料流通係為關鍵發展優先政策。現階段資料的跨境流通不僅是各國第四次工業革命（the Fourth Industrial Revolution）的競爭關鍵，也是後疫情時代（the post COVID-19 era）國家發展之重要前提。跨境資料流動藍圖，主要有三大基礎對應六項規畫，分別為建立信任（1.允許資料流通預設、2.建立資料保護層級、3.重視資安保護）、鼓勵國家合作（4.國家責任、5.優先考量連接性、技術互操作性、資料可攜和資料溯源）、國際資料共享政策（6.永不過時的政策環境）。

然而，目前仍有部份國家限制資料跨境傳輸，如資料在地化（data localization），對於數位經濟發展以及相關技術（如 AI、blockchain）構成嚴重威脅。因此白皮書期能提供指導藍圖予跨境資料共享的國家，以制定強而有力的政策，從資料流通效益與風險取得平衡。

四、 世界經濟論壇「行動資料的十項操作原則」白皮書[38]

世界經濟論壇（World Economic Forum, WEF）於 2020 年 7 月發表關於「行動資料的十項操作原則」（10 Principles of Mobility Data Operationalization）報告，旨在提供建議予相關分析人員在規劃使用行動資料時，應考慮的關鍵原則，並以較易理解白話方式說明。

原則的核心在於為行動資料應用尋求解決方案，當今因科技發展與 COVID-19 疫情的影響，應確保解決方案的有效性。該報告分為三階段，第一階段，在開始前應避免主觀偏見，保持懷疑，包容多元觀點；接著進行經常性資料盤點，以利掌握其所擁有資

[38] 10 Principles of Mobility Data Operationalization, WEF, https://www.weforum.org/reports/10-principles-of-mobility-data-operationalization (last visited Aug.27, 2020).

料；同時應遵循既有資料交換框架、標準，與相關法律規範；資料的選擇往往涉及跨領域資料集，應避免過多重複資料，因此必須了解需求。

第二階段，於過程中應注意依據資料做出的決策，需先明確列出欲解決問題，並關注對使用者的影響；避免蒐集過多資料，並應了解資料間真正的差異，以質化（qualitative）和量化（quantitative）方式來思考；避免欲一次解決所有問題。

最後於第三階段，確保整體流程合理性，測試可能有利有弊，甚至可能迷失於資料集或致結果偏差；並應注意制衡，讓隱私保護不僅於法規遵循，還應於技術上建構整體框架；最後發掘問題也相當重要。

五、 Facebook「隱私交流：朝向以人為本與信賴的設計」白皮書[39]

Facebook 於 2020 年 7 月 14 日發布「隱私交流：朝向以人為本與信賴的設計」（Communicating About Privacy: Towards People-Centered and Accountable Design）白皮書，討論企業、監管機關和利益相關者，如何共同開發和測試新的交流方式，以符合各國的隱私相關法規，因此設計出「以人為本」的法律和監管制度。希望確保每個人都能了解企業是如何蒐集、使用和共享其資料。

隱私政策應針對各項服務或產品所制定，並以清晰且易理解之文字通知使用者，以確保其能夠更直觀且有效地決策。因此，監管機關應與企業和專家合作，共同討論該產品或技術應符合何種隱私政策標準，並在該隱私政策正式實施之前，對其可行性及有效性進行測試。具體作法是利用「監理沙盒」（regulatory sandbox），在嚴格的參數範圍內，使監管機關可以在封閉的監管環境中，針對特定隱私政策，測試新方法（例如透明度），並設

[39] Communicating About Privacy: Towards People-Centered and Accountable Design, Facebook, https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf (last visited Aug.27, 2020).

計適當的解決方案，以及鼓勵採取更多以人為本的設計。監管機關應建立完整流程，以確定各產業領域的審查標準。而企業則須建立隱私管理程序及問責制度，施行適合的隱私政策方案。綜上，企業所制定的隱私政策，除應滿足最低的法律標準外，更須告知並賦予使用者隱私選擇之權利。

瀏覽各國通訊傳播主管機關發布政策文件或調查。以下整理從109年9月至11月研究調查摘譯與分析重點資訊3篇：

六、 開放通訊：電信領域的開放式可信賴資料生態系統[40]

英國開放資料研究所(Open Data Institute, ODI)於2020年8月發表「開放通訊：電信領域的開放式可信賴資料生態系統」(Open communications: an open trustworthy data ecosystem for the telecommunications sector)報告，旨在後續回應英國的通訊傳播監理機關通訊局(Office of Communications, Ofcom)目前正在公眾意見諮詢的資料可攜規劃—「開放通訊：使人們能夠透過創新服務共享資料」(Open Communications – Enabling people to share data with innovative services)，此規劃將使人們和企業可以與電信服務提供者共享電信服務相關資料。開放通訊作為英國創新研發計畫(Innovate UK R&D Programme)的一部分，ODI與產業代表召開相關會議討論，重點聚焦在如何使人們和企業共享有關其使用通訊服務相關資料，以及加值利用該類資料的效益與風險。

報告以ODI從2018年開始之相關工作(如電信領域的開放API)為基礎，整理與業者討論之相關發現，包括如何提供消費者更好的產品，如何激發服務提供者的開發潛力，同時意識到應用資料之風險。促進產業資料更加開放是漫長的過程，Ofcom參考其他產業類似之規劃，如開放銀行(open banking)，期能尋求有效方法，且希望掌握如何從規範面與相關獎勵措施，促進組織轉型並能有利於資料經濟發展。

[40] Open communications: an open trustworthy data ecosystem for the telecommunications sector, ODI, https://theodi.org/article/open-communications-an-open-trustworthy-data-ecosystem-for-the-telecommunications-sector-report/ (last visited Dec.7, 2020).

七、 世界經濟論壇「後疫情時代下數位媒體與技術設計的倫理原則」報告[41]

世界經濟論壇(World Economic Forum, WEF)於 2020 年 9 月發表關於「後疫情時代下數位媒體與技術設計的倫理原則」(Ethical Principles for Digital Media and Technology Design in the New Normal)報告，介紹四個根據「安全設計」(Safety by Design, SbD)的數位媒體(ALHOSN app、Twitter、LEGO Life app、Zoom)實際應用案例，說明符合倫理的媒體與技術設計之間的關係。而安全設計的三個關鍵原則為：「服務提供者之責任」、「使用者授權及自主權」、「透明度和問責制度」。

以 ALHOSN app 為例，該應用程式是阿拉伯聯合大公國的中央與地方衛生單位聯合開發，系統設計使用去中心化模型(decentralized model)及後端加密技術，生成由時間組及匿名資料所組成的個人安全追蹤碼(Secure Tracing Identifier)。以灰色（未檢測）、綠色（健康）、紅色（確診者），以及橙色（可能曾與確診者接觸）區分個人健康狀況，並追蹤 COVID-19 的確診者。該條碼暫存於手機上為時三週，過程中不會蒐集個人身分資料。另外，ALHOSN app 由民眾自願下載註冊，僅在使用者同意的情況下，衛生單位方能取得民眾過去三週的安全追蹤碼，且使用者得自行決定與誰共享其 COVID-19 測試結果。

綜上，由於 COVID-19 大流行，更加強了社會對於數位產品的依賴。數位媒體產品在設計時應主動符合安全設計標準以保護線上數位空間，避免數位產品造成危害，並提高使用者隱私安全。

八、 英國未能確保符合歐盟適足性認定的經濟影響[42]

英國新經濟基金會(New Economics Foundation, NEF)與 UCL 歐洲研究所(UCL European Institute)於 2020 年 11 月發表「未符資料適足

[41] Ethical Principles for Digital Media and Technology Design in the New Normal, WEF, http://www3.weforum.org/docs/WEF_Ethical_Principles_2020.pdf (last visited Dec.7, 2020).

[42] The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision, NEF, https://neweconomics.org/uploads/files/NEF_DATA-INADEQUACY.pdf (last visited Dec.7, 2020).

性的代價：英國未能確保符合歐盟適足性認定的經濟影響」(The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision)報告，概述英國在 2020 年底退出歐盟過渡期結束後，未得歐盟適足性認定的經濟影響，並提出降低不確定性與資料保護的相關建議。

報告從經濟角度分析並訪談 60 多位法律專業人士、資料保護官、企業代表和學者，發現英國未符合歐盟適足性認定之嚴重性，後續影響也將相當複雜，同時因 Covid-19 疫情導致整體經濟極大不確定性。報告估計英國企業對於資料保護總成本約 10 至 16 億英鎊，作為繼續將資料從歐盟傳輸至英國的合規成本，如標準契約條款(standard contractual clauses, SCCs)制定等。

報告建議政府應提供資料建模工具，以利實證研究；並強化國家資料戰略(National Data Strategy)促進創新的資料保護制度；考量放寬跨境資料傳輸審查；提高企業對於資料風險和成本認知；提供簡單實用的工具，如資料保護措施；預留資金協助陷入困境的英國企業。報告最終認為若不符適足性認定，將可能成為破壞英國數位服務和技術競爭力的關鍵因素，因此希望脫歐談判協議能達成共識，以實現適足性認定。

第十章 通傳產業資料運用面臨議題與諮詢交流平臺機制解決方案

在數位時代下，資料利用驅動了數位經濟發展，如何促進產業資料流通與利用，並衡平個資與隱私保護，各國均積極進行資料治理政策與個資保護法制的調適。

為建立良好資料治理的基礎，計畫團隊於 108 年同案委託期末報告之「中長期建議」提出「建立中介平臺機制」，建議參考數位通訊傳播法草案中的網路治理與公眾參與之精神，提供適當的中介平臺機制，供通傳事業、民眾及政府代表作為監理法規釋疑與調整需求溝通的交流管道，彙整三方對於相關資料保護與加值利用的法規理解爭議，並對資料利用情境多方討論，以利通傳會或個資法主管機關參考。現階段我國雖尚未設立官方與通傳事業的單一交流平臺，但如國發會

「公共政策網路參與平臺」，係為全民參與公共事務之常設管道，因此，於通傳產業資料運用議題涉及公民參與時，該管道仍得應用。

至於面對更具體議題諮詢交流，考量到隱私與資料之合理利用之利益權衡，以及資料跨域創新應用複雜情況，要考量資料流通議題，同時也要考量隱私保護與安全，還有市場競爭議題。而計畫團隊本年度透過各國法制政策趨勢研析，以及與業者訪視溝通過程，也更進一步瞭解到，業者針對資料運用、個資法遵等相關法制議題或實務操作之諮詢需求相當迫切，如關於去識別化資料應用、當事人同意等，均為業者積極關心之議題。

是故，評估通傳產業業者對資料運用之服務需求，且當資料流通涉及跨產業之目的事業主管機關權責時，通傳會將需與跨產業的目的事業主管機關協調個資保護準則，以達成在現行單一個人資料保護法、個別目的事業主管機關的框架下監理之一致性。同時，當通傳業者提供資料商業運用或加值服務過程中，可能面臨法規適用疑慮與障礙時，計畫團隊亦須研擬並提出解決方案，並參考相關國家或組織相關政策或規範，以及實行之案例、運作模式及適法性等提出建議。

以下將由三大面向出發，以全面對應上述各項議題與需求。首先，將參酌國際資料應用相關政策與趨勢，先提出整體資料治理與創新應用規劃建議，在適當上位政策之規劃，建構資料治理與流通基礎，亦即從政策面著眼，了解整體國家在資料應用流通時將面臨議題。其次，再到產業面向，研析國際有關企業資料運用之管理與問責之法制發展，並提出我國個人資料保護法制修正需求，與主管機關因應企業運用資料的管理需求所應有之配套問責機制。企業運用資料的前提，在於其應負起妥善管理資料的責任，主管機關不僅須要求企業於運用資料時，應符合個資法規範，亦應對企業之資料管理加以問責，協助主管目的事業落實資料管理責任。最後，在上述資料治理政策與企業問責規範的基礎上，更應思考建構有利創造資料最大價值的法規環境，適合業者資料流通的規管框架，計畫團隊亦將整合國際政策與法制研析成果，並分析我國資料治理之法制環境及需求，提出跨產業之目的事業主管機關權責法規調適建議。

第一節 資料治理與創新應用規劃建議

資料透過共享、交換、再利用，以達成價值之極大化，而資料經濟仍是現階段整體社會關鍵發展之趨勢，當面對資料共享交流推動與可能面臨相關法律爭議，同時在全球企業因 5G 發展走向結合物聯網、雲端、大資料發展應用的同時，資料串接、加值應用不論在公私部門皆是相當可觀。全球資料量亦將急遽增長，而資料處理模式改變從集中式資料處理到分散式智慧聯網，也就是資料處理的去中心化，展望未來資料也將因科技發展，以更加多元創新的方式加值應用。

然而隨著資料經濟如火如荼發展，關於資料跨域應用、當事人資料賦權等議題，更是作為各國發展之重要策略之一，使不同領域、機關間相互激盪、創新資料應用，以促進整體社會利益。而國際間趨勢如歐盟於 2020 年 2 月提出歐洲資料戰略(The European Data Strategy)，預計投入 4-6 億歐元於歐洲共同資料空間和歐洲雲基礎設施與服務，期能成為資料經濟領導者，透過建立單一資料市場確保歐洲的全球競爭力和資料主權；對應歐洲資料戰略，英國政府也於 2020 年 9 月公佈國家資料戰略(National Data Strategy)，透過釋放資料的價值，推動該國的資料能夠更好、更安全、更具創新性的應用，藉以改善社會和公共服務，使英國成為資料驅動創新的領導者；日本也推動官民資料活用基本法與資料信託。

然而，在隱私與資料之合理利用之利益權衡下，隨著技術發展，資料加值應用廣泛，如因應 COVID-19 疫情，將位置資料應用於疾病預防、醫療衛生等，因此各國政府推動資料應用趨勢，甚至結合公私部門之資料、跨國資料之串接應用，形成不同型態資料交換機制甚至是平台，為了解目前國際資料交換共享趨勢，以下將針對目標國家相關資料治理與創新應用政策與現況觀察分析。

一、國際資料政策趨勢觀察

以下就歐盟、英國、日本關於資料政策或相關法制之觀察，與策略規劃進行研析，更利於我國公私部門共同促進資料共享應用之未來

發展。

（一）歐盟：歐洲資料戰略

因應科技發展與資料應用趨勢，如全球資料量急遽增長，從 2018 年到 2025 年將增長 5 倍之多；資料處理從過去集中式到 2025 年將以分散式智慧聯網 IoT 佔大宗，也就是資料處理的去中心化，而邊緣運算也是實現智慧物聯網(AIoT)應用的關鍵技術，因此短短五年可以期待資料將因為科技發展，以更加多元創新的方式加值應用。

因此作為資料經濟發展的龍頭之一，歐盟為了因應科技發展與資料應用趨勢，於 2020 年 2 月提出歐洲資料戰略(The European Data Strategy)[43]，投入 4 至 6 億歐元於歐洲共同資料空間和歐洲雲基礎設施與服務，期能成為資料經濟領導者。戰略主要是透過建立單一資料市場(single market for data)，確保歐洲的全球競爭力和資料主權(data sovereignty)。而資料單一市場的建構框架三大重點在於「資料可以在歐盟內部和跨部門流動，並使所有人受益」；同時也應「遵守歐洲資料應用相關法律規範，特別是隱私和資料保護以及競爭法規」；最後則是「資料近用(access)和使用的規範必須是公平、實用和且明確的」；並透過四大策略行動來實現：

1. 資料近用之跨部門治理調適框架(A cross-sectoral governance framework for data access and use)

   跨部門資料近用為歐盟就資料敏捷經濟(data-agile economy)建構之必要框架，避免部門間或成員國間的不一致行動而導致內部市場的分裂，同時考慮到各部門和會員國的差異。

   由於難以完全掌控所有資料敏捷經濟轉型要素，因此執委會傾向於採用有利於試驗的方式推動（例如監理沙盒），而非採取過分嚴格的事前監管。

   因此首要任務即在 2020 年第 4 季建立一個歐洲共同資料空間治理的立法框架(framework for the governance of

[43] European Commission, A European strategy for data, https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy (last visited Dec. 2, 2020).

common European data spaces)，針對在何種情況下可以使用哪些資料進行決策，以促進跨境資料的使用，並優先考慮互操作性要求和標準，並將促進創新業務的資料應用，透過加強歐盟和成員國跨部門資料使用以及公部門資料空間的治理機制，如標準化機制與資料互操作性規範；其次，則是致力於使更多高價值資料集(high-value data sets)於符合 GDPR 規範下再利用，並以免費、機器可讀，以及標準化的應用介面(Application Programming Interfaces, APIs)開放。其三，針對資料敏捷經濟主體間相互關係立法之必要性，以鼓勵跨部門的資料共享，透過 2021 年將提出之資料法釐清相關議題，如針對強化企業對政府(business-to-government)資料共享、企業對企業(business-to-business)資料共享，尤其是解決共同生成的資料（如工業環境中的 IoT 資料）的使用權等，在適當的情況下，應在公平、透明、合理、適當、非歧視(appropriate under fair, transparent, reasonable, proportionate and/or non-discriminatory)的條件下強制近用資料，以及評估智慧財產權相關規範，以期強化資料近用；也會評估建立資料池(data pools)，以進行資料分析和機器學習所需。此外，為使資料共享符合歐盟競爭相關規範，也將針對與歐盟競爭規範間的兼容性提供指引，如進行企業合併時，大規模資料累積可能造成的競爭影響。

關鍵行動除了前述將提出歐洲共同資料空間治理的立法框架，另一值得注意的是將於 2021 年資料法(Data Act)，完整建構有利於企業對政府或企業間的資料共享環境。

2. 對資料進行投資並強化管理、近用資料之能力與框架建構，以及資料互通性(Investments in data and strengthening Europe’s capabilities and infrastructures for hosting, processing and using data, interoperability)

透過投資歐洲資料空間，包括資料共享體系結構（資料共

享標準、最佳實踐、工具）和治理機制，以及歐洲雲基礎架構，旨在促進 4 至 60 億歐元的聯合投資，預計 2022 年將進入第一個實施階段；與會員國簽署關於雲端聯盟的諒解備忘錄，2020 年第三季度；2022 年第 4 季啟動歐洲雲端服務市場，整合雲端服務產品；編撰 2022 年第 2 季雲監管規則手冊。

3. 強化個人並投資中小企業有關其資料使用能力(Empowering individuals, investing in skills and in SMEs)

   前述提到的 2021 年資料法，透過歐盟 GDPR 第 20 條資料可攜權(data portability)之強化，使當事人有權控制其資料，如某些產品和服務（智慧家電或穿戴裝置）的資料必須具有可讀格式，且個資應用服務提供者或個人資料空間提供者的將是新型資料中介者，詳細內容也將後續提出之資料法為進一步探討。此外，數位歐洲計畫(Digital Europe programme)還將支持「個人資料空間」(personal data spaces)之推展，並將針對技能和一般資料素養投資，縮小大資料分析能力的差距，並擴大數位人才庫。

   此外，為了增強中小企業和初創企業能力，資料對其而言乃是重要資產，因為基於資料啟動或擴展公司的資本投入不是很高，他們通常會需要法規建議，才能充分把握基於資料的業務模型所帶來的眾多機遇。

4. 建構具戰略性與攸關公益領域之歐盟資料空間(Common European data spaces in strategic sectors and domains of public interest)

   針對戰略性經濟領域與攸關公共利益的資料使用需求，開發符合個資保護、資安法令標準、確保互操作性的機制之資料空間，主要用於九種資料空間，包含製造業(manufacturing)、綠色交易 (Green Deal)、智慧交通、健康、財務、能源、農業、公共管理(public administration)與技能(skills)資料空間等領域之資料。

以上相當值得關注的就是歐盟將於 2021 年將提出的資料治理相關法律框架建構，後續待法規提案得以對照思考與 GDPR 的適用關係，還有資料可攜權將如何被強化，亦即未來資料流通應用的關鍵。

而現階段歐盟執委會已於 2020 年 11 月提出促進資料共享並支持歐洲資料空間相關規範措施[44]，亦即有關資料治理的新規則提案(Proposal for a Regulation on European data governance)—資料治理法案(Data Governance Act)[45]，作為 2020 年歐洲資料戰略下的第一個提案，旨在透過增加對資料中介機構的信任，並加強歐盟資料共享機制來促進資料的可用性。該法案將促進整個歐盟以及各部門間的資料共享，從而為社會創造價值、增強公民和公司對資料的控制和信任，並為主要技術平台的資料處理提供替代性的歐洲模式(alternative European model)。

該法案將符合歐盟規範與相關原則（如 GDPR 規範之個資料保護、消費者保護和競爭規則等），並為新的歐洲資料治理方式奠定基礎。同時，為大型技術平台的資料處理提供替代模型，由於其業務模型隱含著控制大量資料的能力，因此可以獲得較高的市場支配力，因此提出具有中立性和透明度的資料中介機構(neutrality and transparency of data intermediaries)模型，作為資料共享的組織者，以強化信任。為了確保中立性，資料共享中介不能以其自己名義來處理資料（例如使用該資料開發自己的產品），並應遵守嚴格要求。

此外，由於缺乏信任是當前的資料共享的主要障礙，並導致高昂的成本，因此該法採取許多措施來強化對資料共享的信任；制定有關中立性的歐盟規則，以允許新型資料中介機構充當值得信賴的資料共享組織者；促進再利用公部門持有的某些資料，如應用健康資料研發現罕見或慢性疾病的治療方法；使公司和個人更容易、更安全地在明確條件下，為更廣泛的共同利益提供資料，從而使歐洲人民能夠控制所生成資料的應用。

---

[44] European Commission, Proposal for a Regulation on European data governance (Data Governance Act), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2102(last visited Dec. 2, 2020).

[45] European Commission, Proposal for a Regulation on European data governance (Data Governance Act), https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act (last visited Dec. 2, 2020).

提案具體規定的說明，總共有八個章節（共 35 條）：

1. 第一章包含適用主體、範圍與定義。
2. 第二章建立某些受保護之公部門資料的再利用機制，以尊重他人的權利為條件（特別是基於保護個人資料以及智慧財產權和商業機密的基礎），不影響歐盟特定部門關於近用和再利用該資料的立法，且並非創造再利用此類資料的權利，而是規定了一系列允許再利用此類資料的統一基礎。允許在技術上確保充分資料保護、隱私和機密性；會員國將建立一個單一的聯絡點，以支持研究人員和創新企業獲得合適的資料。
3. 第三章旨在透過為資料共享服務提供者建構通知機制，來強化對共享個人和非個人資料的信任，並降低與 B2B 和 C2B 資料共享成本，提供者必須遵守許多要求，尤其是在交換資料方面保持中立的要求，不能將此類資料用於其他目的。
4. 第四章促進資料利他主義(data altruism)，亦即個人或公司出於共同利益自願提供的資料。從事資料利他主義組織得註冊為「歐盟認可的資料利他主義組織」(Data Altruism Organisation recognised in the EU)，以增加對其營運的信任。此外，還將研擬通用的歐洲資料利他主義同意書(a common European data altruism consent form)，以降低蒐集同意書的成本，並促進資料的可攜性（當欲提供的資料非由個人持有時）。
5. 第五章規定監管機關監督和實施資料共享服務提供業者和從事資料利他主義組織的通知框架(notification framework)，以及關於此類機構的決定提出申訴的權利和司法救濟的相關規定。
6. 第六章則設立正式的專家小組—亦即「歐洲資料創新委員會」(European Data Innovation Board)，以促進成員國發展適當措施，特別是受他人權利的約束之資料再利用

要求（第二章），確保有關資料共享服務提供業者（第三章）和資料利他主義（第四章）通知框架的一致作法。此外，該委員會將針對跨部門標準化的治理提供協助，並向執委會提出建議。

7. 第七章允許執委會依據有關歐洲資料利他主義同意書實施法案。
8. 最後，第八章則是關於資料共享服務提供者通用授權計劃運作的過渡性規定。

該法案為實現歐洲資料主權邁出良好的一步，歐盟執委會後續將於 2021 年提出更多與歐洲資料空間相關法規提案，以促進企業間以及企業與政府間的資料共享。

（二）英國：國家資料戰略

對應歐洲資料戰略，英國政府亦於 2020 年 9 月發布國家資料戰略(National Data Strategy)[46]，透過釋放資料的價值，推動英國的資料能夠更好、更安全、更具創新性的應用，藉以改善社會和公共服務，使英國成為資料驅動創新的領導者。該策略著眼於如何利用英國現有的優勢來促進企業、政府、公民社會和個人之間更好地應用資料。同時因應脫離歐盟後的國際上定位，持續發會對於全球資料共享和應用之影響力；以及 COVID-19 疫情下資料應用的跨域合作。此外，對於供部門資料可以被運用和共享，以造福社會，前提是建立在可信任的基礎之上，當共享個人資料時將更具彈性。

理論上資料是一種不會消耗的資源(non-depletable resource)，但是它的使用受到近用限制，因此戰略將確保可以利用資料來提供創新服務，促進競爭以及為消費者和小型企業提供更好的選擇，使所有人都能從負責任的使用資料中受益。

從戰略整體架構觀察（參下圖），可知綠色部分透過確立 5 項創新的機會為促進生產力和貿易(Boosting productivity and trade)、支持

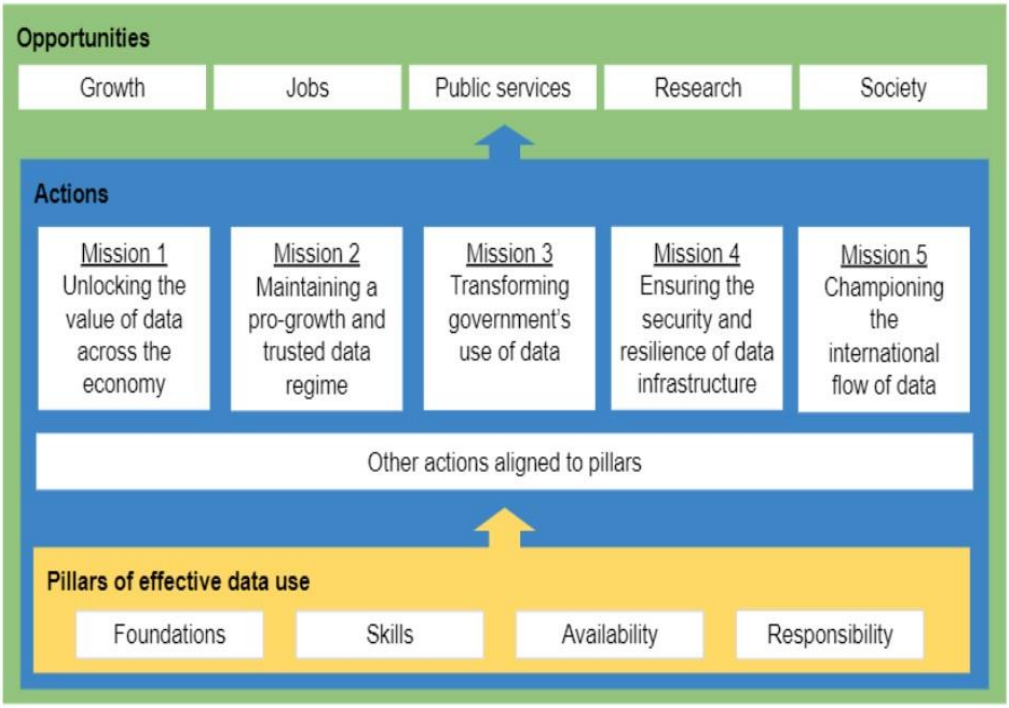
[46] Department for Digital, Culture, Media & Sport, National Data Strategy, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-1-3 (last visited Dec. 4, 2020).

創新和相關工作機會(Supporting new businesses and jobs)、提高科學研究效率和範圍(Increasing the speed, efficiency and scope of scientific research)、推動更好政策和公共服務(Driving better delivery of policy and public services)，以及為所有人創造更加公平的社會(Creating a fairer society for all)。

藍色部分則是英國政府具體採取 5 項優先行動任務，包含：釋放整體經濟中資料的價值(Unlocking the value of data across the economy)、確保促進持續增長與可信賴的資料機制(Securing a pro-growth and trusted data regime)、改變政府資料利用以提高效率和改善公共服務(Transforming government's use of data to drive efficiency and improve public services)、確保資料基礎架構的安全性和韌性(Ensuring the security and resilience of the infrastructure on which data relies)，以及促進國際資料流通(Championing the international flow of data)。

黃色部分對應 5 項優先行動任務的 4 大支柱分別為：

1. 資料基礎(Data foundations)：資料在完備基礎上始得真正發揮其價值，如標準格式、能因應未來發展的機制(standardised formats on modern, future-proof systems)，且容易查找、可近用性、具互操作性，並得再利用(findable, accessible, interoperable and reusable)。
2. 資料技能(Data skills)：確保人民具備應用資料相當技能，所學具持續發展性。
3. 資料可用性(Data availability)：確保資料得適當近用、移動和再利用，並鼓勵公私部門與第三方間共享資料，以及國際資料流通的適當保護。
4. 負責任的資料(Responsible data)：確保以合法、安全、公平、倫理、可持續和負責任(lawful, secure, fair, ethical, sustainable and accountable)利用資料，並支持創新與科學研究。



資料來源：英國國家資料戰略

圖 143 英國國家資料戰略整體架構

從以上可知現階段英國對於資料應用政策趨勢，為了建構整體資料經濟生態系，不論是政府對企業，企業對企業之資料共享再利用都需要有完整規劃，其中值得關注的是涉及資料經濟中產業面的個人資料流通，若要建構資料交換共享機制，除了從基礎建設、培養技能還有負責任利用資料外，推動之關鍵重點即在於資料必須先具備可用性，同時這也是促進資料流通應用的關鍵。

戰略中關於資料可用性，在於確保適當地近用資料，分別從三大面向切入，包含經濟社會、政府和公部門內，以及國際資料可用性，由於資料交換機制本報告主要針對產業需求導向，因此以下將聚焦於經濟社會面向。

首先，戰略中關於「資料可用性」(data availability)說明，由於該詞彙常與資料共享(data sharing)、資料可發現性(data discoverability)、資料近用(data access)、資料可攜性(data portability)、資料移動性(data mobility)經常組合互用。在此策略中，以資料可用性表示一種可促進公私部門、第三部門間以及彼此之間的適當資料近用、移動和再利用。

此外，由於科技發展，近用資料方式多元且得由多方進行，因此政府在關於資料相關技術以及資料共享或資料治理亦將發揮其重要作用，尤其是面臨 COVID-19 疫情，公私協力提供相關因應措施與服務時，即證明資料共享之重要性。而不同資料加值應用也將產生全新商業模式與服務，如醫療資料匿名處理與串接後，更能有助於醫學發展。甚至是在特定領域資料共享下，英國政府試圖在具有明顯的消費者利益方面，如在開放銀行與智慧資料。政府還投資研發更好的資料共享機制，如創新英國(Innovate UK)與開放資料研究所(Open Data Institute)的合作關係，以探索資料信任。

然而，資料可用性所面臨的障礙如風險規避(risk aversion)的文化、現行許可授權相關法規、資料再利用之市場障礙、公部門資料格式不一致、與資料可發現性有關的問題、隱私與安全、因資料蒐集與維護成本以致組織未能發覺資料共享的好處等。英國政府考量如何克服已知的可用性障礙，如限制特定資料使用者獲得監管機關之認可或是符合規範、在協作組織中共享資料、建立合成資料(synthetic data)共享與其他增強隱私(privacy-enhancing)技術，以支持研究和創新。

關於「經濟社會的資料可用性」(Data availability for the economy and society)面向，英國相關智庫研究顯示[47]目前市場上的資料應用尚未完全實現資料價值，政府干預對於解決特定領域之市場失靈仍有其必要性，且資料過度集中和缺乏互操作性(data concentration and lack of interoperability)，導致數位市場競爭和創新不彰關鍵因素。因此英國政府採取具體行動如下：

1. 智慧資料(Smart Data)計畫

   該計畫使消費者能與獲授權的第三方簡單、安全地共享資料，從而使第三方服務提供者(third party service provider, TPPs)能提供創新服務。第一個智慧資料計畫，即「開放銀行」(Open Banking)[48]，透過具互操作性格式

[47] 英國國家資料戰略中引述相關研究報告如“Online platforms and digital advertising Market study interim report”, “Online platforms and digital advertising Market study interim report, “DATA MOBILITY: The personal data portability growth opportunity for the UK economy”等。

[48] 英國競爭及市場管理局(CMA)2016 年 8 月發布「零售銀行業市場調查的最終報告」(Retail

和資料流通，使創新服務得以發展，並在銀行與其他領域促進競爭。此外，英國通訊傳播管理局(The Office of Communications, Ofcom)於 2020 年 8 至 11 月進行「開放通訊：使人們能夠透過創新服務共享資料」(Open Communications: Enabling people to share data with innovative services)公開意見徵詢，開放通訊將使消費者能將通訊資料與獲授權第三方簡單安全地共享，消費者應能控制其所共享之資料，且必須獲其同意，要求業者共享更多有關產品的資料，確保提供 TPP 可用資料，任何經認可第三方都得依消費者的要求近用其資料。目前諮詢已經結束，Ofcom 下一步將持續與利益相關者溝通，後續也將思考訂定相關規範，以及確保資料移動安全性與消費者控制權限，並期能循序漸進開放資料，如風險低但對消費者有較高利益的資料。

對於消費者而言，掌控服務提供者所擁有關於他們的資料或近用該資料之創新服務，是相當困難且耗時。因此政府致力於使消費者資料可以為其服務，而創新業務亦得蓬勃發展，透過鼓勵新競爭者進入市場，驅動創新資料服務，降低創新者的壁壘，保護消費者權益。

此外，英國資料保護法(Data Protection Act 1998)亦賦予消費者權利，即參照 GDPR 資料可攜權規定，而 Smart Data 亦可謂對資料可攜權擴展，提供共享消費者資料框架。戰略也提出將考量立法，作為所有智慧資料計畫法律依據。

---

banking market investigation Summary of final report) 調查結果指出英國大型銀行間競爭疲弱，且銀行間帳戶轉換成本高、資訊不夠透明，因此推動改革制定開放銀行標準(Open Banking Standard)；同年 9 月則由英國 9 大銀行(CMA9) 出資成立開放銀行實施組織(Open Banking Implementation Entity, OBIE)，其主要任務即在制定開放銀行 API 與共同標準，使消費者資料透過開放 API 提供給獲授權的第三方服務提供者(TPPs)。

英國開放銀行的下一步為「開放金融」(Open finance)，開放金融將開放銀行的資料共享和第三方資料近用概念，擴展到更廣泛的金融產品服務（退休金、投資保單、資產管理等），藉此改變消費者和企業使用金融服務的方式，使其更輕鬆地比較價格、產品功能以及轉換產品或服務提供業者。

2019 年 Smart Data Review 重點即在於「如何改善消費者對於其資料控制與應用」，建議加速開發創新的資料驅動服務，包含建立跨部門的智慧資料工作組(Smart Data working group)，並拓展應用領域於通訊、金融、能源和退休金領域，以及監管者得於資料受到適當保護的情況下，協助弱勢消費者，並確保對第三方服務提供者資料保護要求，使消費者對創新資料驅動服務的信任。

2. 確保數位市場有效運作

資料是競爭市場的核心，因此需建構適當機制來安全地共享應用資料，英國政府原則上接受數位競爭專家小組(Digital Competition Expert Panel)提出 6 項建議，並成立一個跨監管機關的數位市場工作組(Digital Markets Taskforce)，確保監管框架是適當且能夠支持創新。

3. 開放資料(Open data)

英國於 2012 年關於「釋放潛力」(Unleashing the Potential)白皮書，政府對所有公部門資料均採原則開放(Open by Default)，促進發布開放資料的概念，實現許多預期的結果，如透過公開發布資料和政策背後的證據基礎，提升人民對於政府決策的信任；提升效率，避免重複、浪費和其他系統性問題；以及以資料作為新產品和服務的基礎，促進創新創公司的成長。透過改善對政府擁有的資料集的近用，不僅釋放其價值亦得改善市場。

透過審查開放資料的發布和決策過程，以確保其一致性；並支持開發可互操作的指標以衡量發布資料的影響，以及針對能源資料工作組(Energy Data Taskforce)的建議，並推動現代化的能源資料近用計畫(Modernising Energy Data Access)。

4. 從公私資料中獲取價值的共享模型(Shared models for deriving value from public and private data assets)

英國政府除了對開放資料的承諾外，也意識到需要新的模型方法來從跨越公私部門資料與其系統中獲取價值，尤其是在資料本身不適合公開的情況下（隱私、國家安全或商業原因等）尤其重要。而後續也將進行線上危害（如兒童性虐待、仇恨言論、自我傷害、自殺等）審查和監控的資料基礎架構，還有相關案例如建成環境(built environment)、地下設施資產登記(National Underground Assets Register)相關資料。

綜上，英國透過擬定國家資料戰略作為整體推動方向，從確立 5 項創新的機會，並採取 5 項具體優先行動任務，對應 4 大支柱，而其中針對經濟社會的資料可用性推動可知，智慧資料計畫係為英國政府推動特定領域資料應用，也是當事人資料可攜權之擴展，作為英國共享消費者資料框架，透過資料賦權，使消費者應對未來更多元跨域資料應用情況下，都能掌握自己的資料也能從中獲益，同時第三方業者亦得開展出不同的資料商業模式與服務。除了智慧資料計畫，英國政府也考量資料對於數位市場競爭，還有政府開放資料對於民間影響，並發展從公私資料中獲取價值的共享模型。

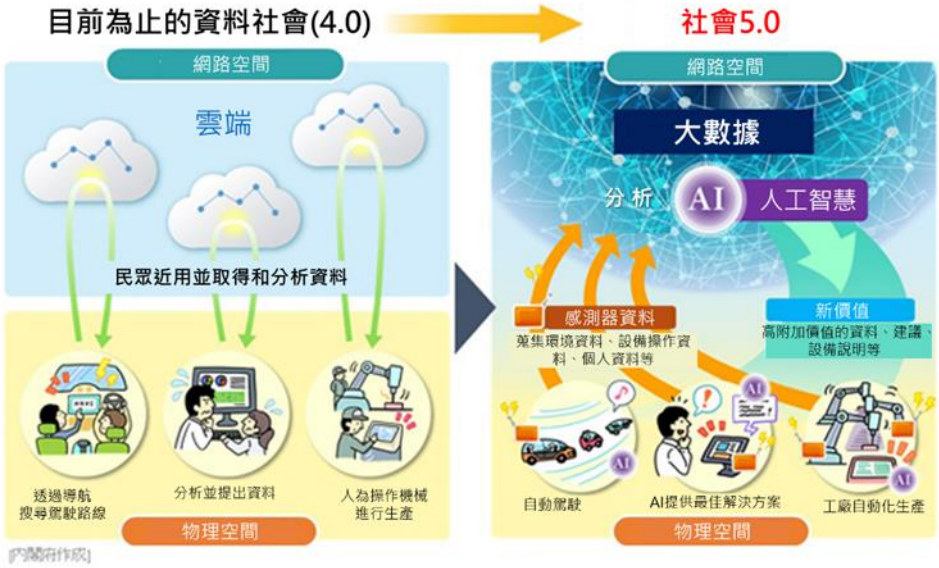
（三）日本：社會 5.0 政策資料信託機制

日本首相安倍晉三於 2016 年提出「社會 5.0」政策[49]，期以在以人為本的思維下，建立串聯人工智慧、機器人、物聯網和量子運算科技的超智能社會（超スマート社会）。「社會 5.0」是透過網路（虛擬空間）與現實（物理空間）結合而成，將物理空間中感測器的大量資料累積在網路空間中，並由網路空間中的 AI 進行大數據分析，再將分析結果反饋給人類。因此，資料的累積對於「社會 5.0」的發展至關重要。

目前資料僅限於蒐集公司內部使用，資料無法發揮所能產生的最大價值。資料信託機制即是以此為概念，將個人資料視為「財產」，

[49] 石山大晃，日本国内のデータ利活用に係る昨今の制度検討の状況，富士通総研，https://www.fujitsu.com/jp/group/fri/businesstopics/data-economy/regulation-domestic/（最後瀏覽日：2020/12/3）。

將個人資料儲存到「資料銀行」並委由其進行託管，透過出售的方式交給想要利用個人資料的營運商，並將所得利益返還給個人。



資料來源：內閣府

圖 144 社會 4.0 到社會 5.0

綜上，資料串接即是在進行建構超智能社會首先面對之挑戰。日本對於資料共享的態度回歸資料自主理念，以個人為出發點，決定資料是否釋出以及流通形式。以下討論資料信託建立背景及運作模式，並說明成立資料銀行之認定方式。

1. 日本資料信託機制建立背景

日本資料流通與運用所面臨的挑戰在於對新興科技在個人資料保護方面存有疑慮、資料交易信任度不足，以及難與資料霸權者相競爭的困境。為此，日本於 2016 年通過施行「官民資料活用推進基本法」(官民データ活用推進基本法)，積極推動包括開放資料在內等公私部門資料之加值運用。

2017 年 2 月，日本 IT 總合戰略總部下設置之「數據資料流通環境整建檢討會　AI、IoT 時代之數據資料活用工作小組」舉行期中匯報，認為建立實現資料流通與靈活運用的個人資料儲存系統(Personal data storage,

PDS)[50]、資料銀行，或資料交易市場平台[51]，有益於實現個人資料在多種類且大量的數據資料庫中流通[52]。

有鑑於此，日本總務省於 2017 年 2 月設置「資料市場支援工作小組」（データ取引市場等サブワーキンググループ(SWG)），主要討論資料信託機制（即資料銀行，又稱情報銀行）相關議題。並在 2017 年 11 月至 2018 年 4 月間召開六次「資料信託功能認定機制檢討會」（情報信託機能の認定スキームの在り方に関する検討会），檢討具備資料信託功能的資料銀行認定基準和契約建議記載事項等。

2018 年 6 月公布「資料信託功能認定指引 ver1.0」（情報信託機能の認定に係る指針 ver1.0）[53]，藉此實現利於個人資料流通並創造新服務型態[54]，該指引於 2019 年 10 月更新為 2.0 版[55]。

2. 資料銀行運作模式

為提高資料主體實際參與度（可控制性）並促進個人資料流通、活用，資料銀行旨在期望獲得資料主體同意的一定範圍內，委託資料主體信賴的其他主體，將個人資料提供予第三人。

資料銀行建立在既有的 PDS 或資料交易市場平台之上，

---

[50] 所謂 PDS(Personal Data Store)是指「包括其他持有數據資料的彙整在內，個人依自我意志而蓄積和管理自身之數據資料而作的設計（系統），具備提供第三方相關控管作用（包含移交）」。再者，關於 PDS 及「資料銀行」等的定義為「根據民間企業及外國等先行配套措施和提案，在現階段能彙整如下，但根據今後商業動態，有再度檢討的可能性。此外，各自並非排他性質，而是設想同一物具備複數的作用」。

[51] 資料交易市場是一種促使雙方通過買賣等方式進行交易之仲介機制。本身具有媒合之功能，但以匿名化資料及非屬個人資料為大宗。且須保持中立性，本身不會參與資料之蒐集、保存、處理和交易活動。

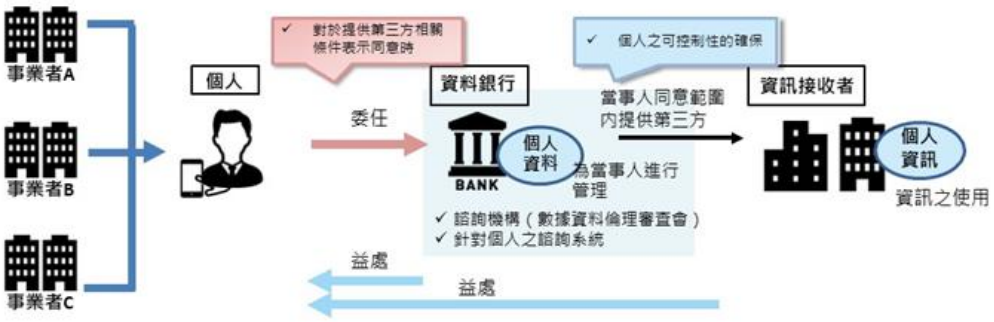
[52] 情報信託機能の認定スキームの在り方に関する検討会，〈情報信託機能の認定に係る指針 ver1.0〉，https://www.meti.go.jp/press/2018/06/20180626002/20180626002-2.pdf（最後瀏覽日：2020/12/3）。

[53] 同前註 52。

[54] 石山大晃，同前註 49。

[55] 情報信託機能の認定スキームの在り方に関する検討会，〈情報信託機能の認定に係る指針 ver2.0〉，https://www.meti.go.jp/press/2019/10/20191008003/20191008003-3.pdf（最後瀏覽日：2020/12/3）。

同時結合二者特性，進行資料的蒐集、保存、處理和交易行為。透過與個人簽訂之個人數據資料活用相關契約，在管理個人的數據資料的同時，基於個人指示或預先設定之條件管理個人資料，為資料主體作出適當的評判，且在必要時對資料作匿名化，將數據資料提供予第三方(其他事業者)。並將數據資料的提供與運用獲得的相關利益，由數據資料接收事業者直接或間接回歸給當事人。



資料來源：資料信託功能認定指引 ver2.0

圖 145 資料銀行示意圖

資料銀行作為提供資料信託的關鍵角色，在接獲個人委託後，管理包含該個人相關個人資料在內的所有資料。此制度的建立即在希望未來出現跨產業資料流通應用時，有良好的流通管道及平台，能使資料加值創造更多效益。因此，2017 年 11 月，由經濟產業省和總務省共同組成的「資料信託功能認定機制檢討會」經過六次會議後，共同研議公布「資料信託功能認定指引 ver1.0」。雖然該指引是由業者自由參加認證，並非成為資料銀行之必要條件，但仍希望該藉此提供相關利害關係人一個可遵循的框架。

(1) 認定標的

涉及個人資料之取得方法和使用目的之明示。一是依照當事人的委託，判斷資料利用者處理個資的合

理性，後才協助提供資料；二是單純由當事人自行判斷是否提供資料。惟指引中未提供認定標準，故在認定標準上應從消費者角度出發，以易於理解的方式向消費者說明所提供的服務，以取得消費者信賴。針對資料當事人與資料銀行如何進行委任及個自之權利義務，則提供定型化契約範本，說明業務範圍以及事業告終時等的處理。

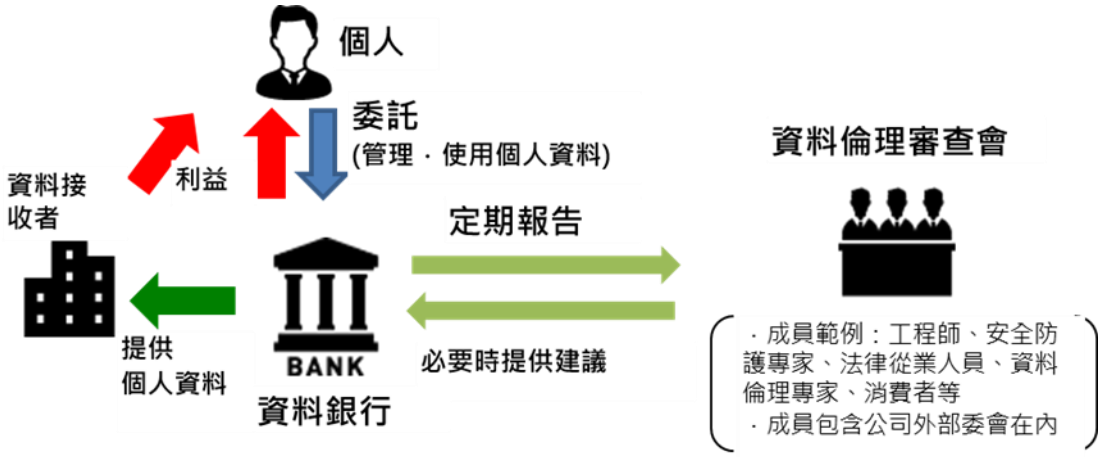
(2) 資料信託機能

認定標準討論業者資格、資料安全要求與隱私保護要求，以及治理體制三個部分。業者資格部分分為兩個面向。在經營條件上，應具備法人資格，且應擁有足夠的財產基礎作為執行業務、確保資訊安全需求，以及處理損害賠償的能力。在業務能力方面，應遵守包括個人資料保護法等相關法規的要求，並制定隱私政策與安全防護政策，確保擁有足以確實執行使用個人資料相關業務的知識及經驗，且建立實施、治理體制，以獲得社會信賴。

基於風險管理的考量，應建立人員資料安全防護和隱私相關體制，確保有足夠的人力與組織體系保護資料安全和隱私，以因應未來資料當事人、資料量或資料接收者的增加。具體遵守的標準主要參考國際標準或國內規範，例如 JISQ15001 個人資料保護管理系統、ISO/IEC29100(JIS X 9250)隱私保護框架。而在使用個人資料、安全管理基準皆取得隱私權標誌或通過 ISMA 認證，並定期更新認證。

在治理體制部分，企業應以資料是為了讓個人享受成果、豐富個人生活而使用的「以顧客本位的業務營運體制」，建立公司管理架構，並設有諮詢窗口，以接受消費者或其他業者的詢問並立即給予回應。再者，應聘請外部專家擔任顧問，建立「資料倫理審查

會」(データ倫理審査会),成員組成應包含工程師(分析資料和技術累積整合等)、資安防護專家、法律從業人員、資料倫理專家、消費者等,就資料銀行業務多角度審核使用資料相關契約和使用方法、第三方接收者等的適當性,在必要時提供建議。在透明性方面應以淺顯易懂的方式揭露重要資訊,確保系統完整性。而業者與認定機構之間的契約上,內容應包含遵守認定基準、更新程序、違反認定基準時的處置等內容,以及通過認定的項目大幅度變更時,須向認定團體申報等。



資料來源:資料信託功能認定指引 ver2.0

圖 146 資料倫理審查委員會

3. 成立資料銀行的認定方式

(1) 認定團體資格:應確保其獨立性、中立性和公平性。

(2) 審查作法:申請認定的資料銀行須填寫申請表單,在接受申請後,由事務局根據申請表單內容進行聽證,由學者等組成的「認定委員會」進行審查。最後設定認定費用及設定認定有效期間(2 年)和設計更新程序。

(3) 認定證書:在通過資料銀行的申請後,認定團體會頒給認定證書,證書上載有業者名稱。業者在收到證書

後，應在自己的網頁上進行揭露，同時，認定團體也會在官網上公布認定書通過的結果。

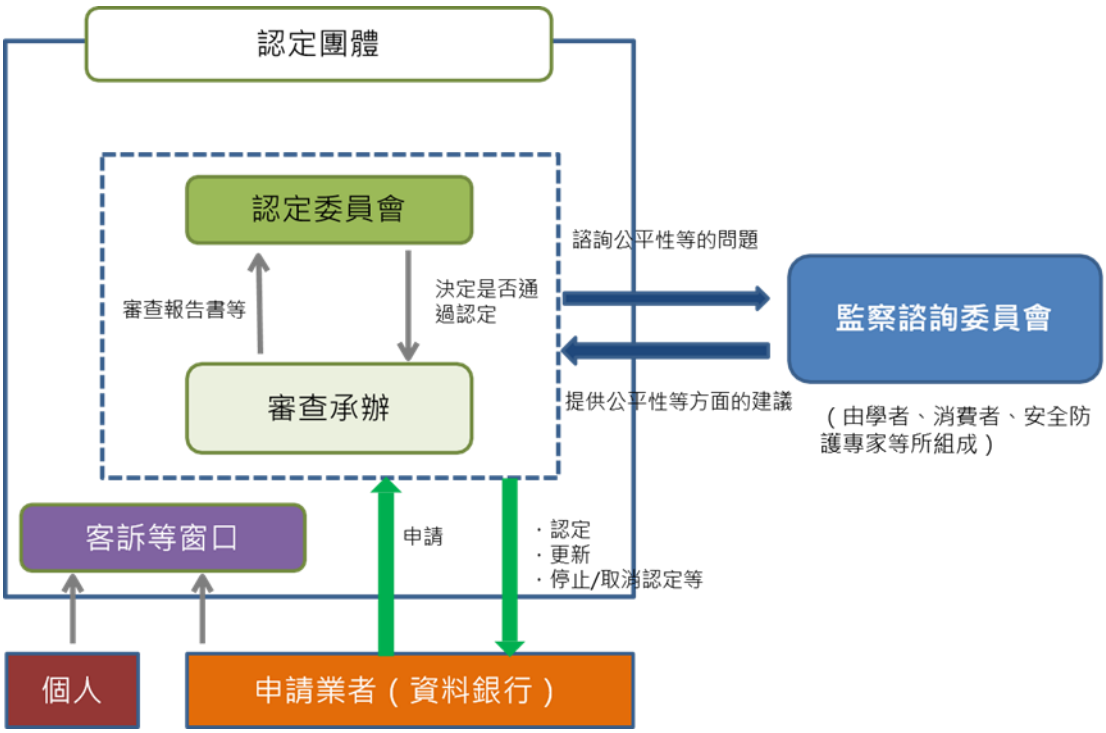
(4) 特殊情況：當認定事業者判定違反認定內容與標準，或是發生個人資料外洩的情況時，認定機構可以向第三方委員會（監督諮詢委員會）諮詢或委託，進行資料銀行資格的保留、暫時停止、停止認定，以及註銷認定資格，或是公佈業者名稱及公布監督諮詢委員會的評估報告。

(5) 契約：認定團體與受認定的資料銀行業者之間須締結契約。契約內容包含業者應遵守的認定標準、更新程序、違反認定標準的後果，以及認定團體可以對認定業者，進行認定等所必要的檢查或要求提供報告。

(6) 認定團體運作：應包含事務局、認定委員會、客訴窗口，以及第三方委員會（即監督諮詢委員會，應由學者、消費者和資安專家組成）。目前，日本政府委託「日本 IT 團體聯盟」（一般社団法人日本 IT 団体連盟）擔任「資料銀行推進委員會」，擔任資料銀行認定之第三方委員會。截至 2020 年 2 月為止，日本 IT 團體聯盟進行了三波資料銀行認定，共三井住友信託銀行、FiliCa Pocket Marketing、J.Score、中部電力株式會社等四家業者通過情報銀行認證[56]。並在 2020 年 3 月進行第四波資料銀行認定，DataSign 成為第一家取得一般性認定的資料銀行[57]。

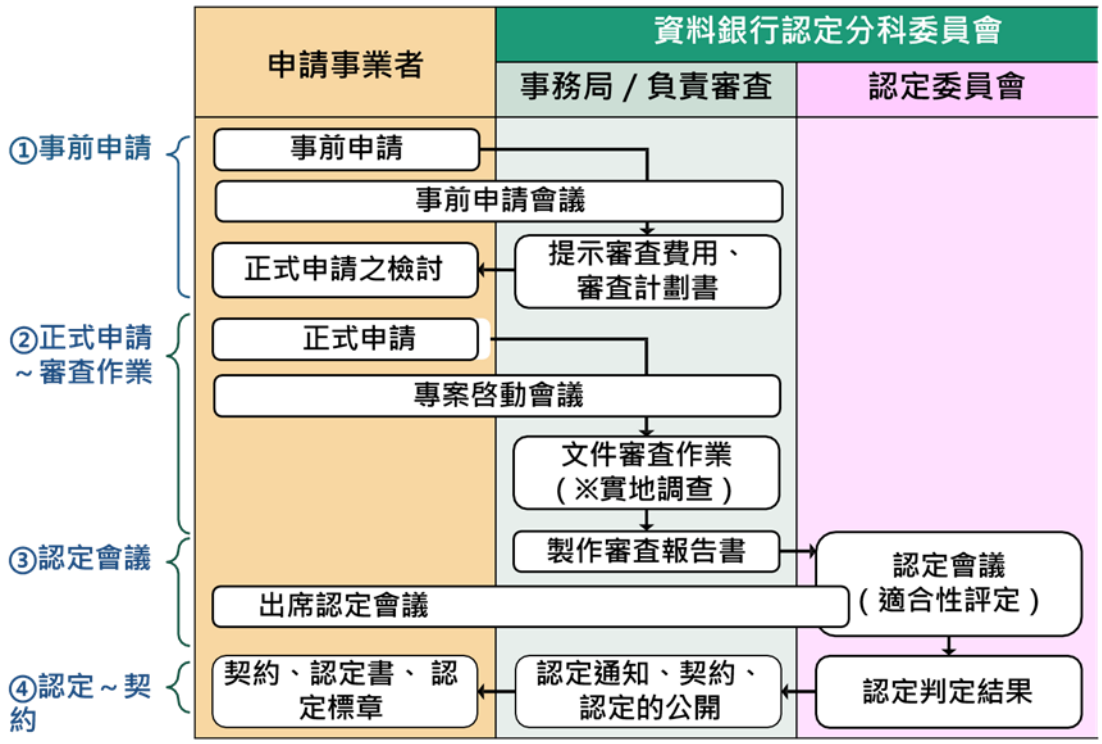
[56] 一般社団法人日本 IT 団体連盟，〈日本 IT 団体連盟、「情報銀行」認定（第１弾）を決定〉，2019/06/26，https://itrenmei.jp/topics/2019/3646/；一般社団法人日本 IT 団体連盟，〈日本 IT 団体連盟、「情報銀行」認定（第２弾）を決定〉，2019/12/25，https://www.itrenmei.jp/topics/2019/3652/；一般社団法人日本 IT 団体連盟，〈日本 IT 団体連盟、「情報銀行」認定（第３弾）を決定〉，2020/02/17，https://www.itrenmei.jp/topics/2020/3657/（最後瀏覽日：2020/12/04）。

[57] 一般社団法人日本 IT 団体連盟，〈日本 IT 団体連盟、初の通常認定となる「情報銀行」認定（第４弾）を決定〉，2020/03/12，https://www.itrenmei.jp/topics/2020/3662/（最後瀏覽日：2020/12/04）。



資料來源：資料信託功能認定指引 ver2.0

圖 147 認定機制



資料來源：「情報銀行」の推進に向けた取組みについて

圖 148 申請認定流程

綜上，日本在社會 5.0 中的「資料驅動型社會的改革」(データ駆動型社会への変革)，其中特別提到「資料霸權主義」(データ覇権主義）的現象[58]。與此同時，國際上正面對資料、財富和人才向 GAFA(Google、Amazon、Facebook、Apple)集中，產生一種「新壟斷」的局面，而對 GAFA 任意蒐集、使用個人資料不滿的情緒逐漸增加時，「資料銀行」或許能為這種新壟斷的現象提供解決方案。

大量的資料有助於開發新產品和改善服務，資料銀行之目的即是希望在資料主體具備資料自主控制權的情況下取得同意使用個人資料。資料主體也可以透過資料分析取得更多個人化服務，且資料利用所產生的利益也將回饋於己，形成一種企業與資料主體互利的資料使用模式。並由民間機構分別負責驗證、擔任「資料銀行」的方式，將個人資料商業化，利用個人資料進行大數據分析。另一方面，引入資料倫理審查會，透過公正之第三方審查資料流通平台業者是否公允，以促成資料經濟發展與保障個人資料之環境的形成，利用個人資料的同時也保護個人隱私。

二、國際資料創新應用策略觀察

以下就英國與日本關於資料創新應用策略觀察，透過國際相關策略研析，作為我國於促進資料創新應用模式參考。

（一）英國：ICO 資料監理沙盒

英國資訊專員辦公室(Information Commissioner's Office, ICO)於 2018 年 9 月提出監理沙盒之公眾意見徵詢(Call for evidence: Regulatory Sandbox)[59]，係依據 2018-2021 年科技策略(Technology Strategy for 2018-2021)，沙盒提供組織應用個人資料於創新產品與服務於安全空間之中，雖然不會豁免於英國資料保護法，但可以獲得 ICO 於資料保護專業知識和建議，同時確保適當的保護措施。當時為

[58] 意即國家或是特定企業獨占特定資料。

[59] Call for evidence: Regulatory Sandbox, ICO, https://ico.org.uk/media/about-the-ico/consultations/2259746/regulatory-sandbox-call-for-evidence.pdf (last visited Dec. 6, 2020). Blog: ICO regulatory sandbox, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/first-reports-published-from-the-regulatory-sandbox/(last visited Dec. 6, 2020).

了解沙盒的可行性，公眾意見徵詢重點在於範圍、是否需要針對特定的部門或類型的組織、好處以及有利於組織運作之相關機制，如提供技術指導、工具等。

2018 年 10 月 ICO 建立監管機關業務和隱私創新中心(Regulators' Business and Privacy Innovation Hub)，為企業提供資料隱私專業知識，以確保法規與未來的技術同步發展，該中心也將與 ICO 的監理沙盒共同合作，支持組織和企業以不同方式使用個人資料開發創新產品和服務。

2018 年 11 月 ICO 對監理沙盒的初步回應，參與資格設定為具創新、公共利益，以及現階段適合參加組織，並說明該機制並非提供測試環境、虛擬資料集或工具的沙盒，而是經過指導和諮詢與創新業者合作。2019 年 3 月開放沙盒測試，申請截止為 5 月底，總共收到 64 份申請，沙盒 Beta 階段將選擇約 10 個項目，7 月通知成功申請者。2020 年 7 月 ICO 發布揭示 ICO 與試驗階段 2 個組織的合作成果：

1. 「JISC—福祉實踐準則」(Wellbeing Code of Practice)[60]

   JISC 為非營利組織，提供高等教育、技能領域相關服務，強調了數位技術對英國教育和研究的重要性和潛力；並於沙盒中製定福祉實踐準則，希望透過調查學生活動資料的使用，以改善高等教育對於學生行政支持相關服務(support services)，以協助他們保護自己的隱私和福祉。JISC 的 Sandbox 計劃達成如下目標：確定大學可以在分析中使用哪些個人資料；提供有關精神健康的相關證據研究，並解釋其分析將如何幫助避免危機，證明福祉實踐準則必要性；確保關鍵資料保護，包含蒐集資料時隱私聲明中應包括的內容、若未成年學生資料保護、如何以及何時進行資料保護影響評估。

   透過兩項機制設計達成：其一為「目的相容性矩陣」(Purpose compatibility matrix)設計，以便大學根據其列出

[60] Regulatory Sandbox Final Report: Jisc, ICO, https://ico.org.uk/media/for-organisations/documents/2618023/jisc-regulatory-sandbox-final-report.pdf (last visited Dec. 6, 2020).

要在資料分析中使用的資料，並評估是否將資料用於分析，並符合 GDPR 第 89 條（1）為實現公共利益、科學或歷史研究目的或統計目的之處理的規定。

其二為是 DPIA 模板，該模板針對大學在為此目的進行資料分析之前需要考慮和評估的風險提供有針對性的指導，以及有關如何減輕已識別風險的建議。

2. 希斯洛機場—旅客旅程自動化程序(Heathrow Airport Ltd - Automation of the Passenger Journey programme)[61]

旨在透過使用生物識別技術來簡化旅客旅程，應用臉部識別技術於辦理登機手續、自助行李托運和登機處，為旅客創造順暢便利的機場體驗。旅客在旅途中的不同地點將不再需要出示不同形式的文件，例如登機證和護照，以證明其身份。沙盒中與 ICO 諮詢資料保相關議題：複雜的資料控制權問題，即控制者、聯合控制者或處理者判斷；擴展該計畫現有法律義務；如何蒐集明確的同意，以確保機場提供最好的服務；以及旅客驗證服務(Traveler Verification Service, TVS)資料庫得否用於進行身份驗證等。

2020 年 11 月 ICO 接續發表沙盒中的最新合作成果為協助企業應對金融犯罪的創新技術：

1. Onfido：減輕客戶身份驗證中的偏見(Onfido: Mitigating bias in customer identity verification)[62]

透過識別和減輕其設計的生物特徵身份驗證技術中存在的偏見，旨在使顧客能夠證明其所宣稱之真實身份。如金融機構可能會使用該技術來證明欲開戶的顧客之身份，透過客戶提供其身份證件的照片以及使用手機或其他設備拍攝的照片，由 Onfido 分析這些圖像，以確定

[61] Regulatory Sandbox Final Report: Heathrow Airport Ltd. , ICO, https://ico.org.uk/media/for-organisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf (last visited Dec. 6, 2020).

[62] Regulatory Sandbox Final Report: Onfido, ICO, https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf (last visited Dec. 6, 2020).

身份證明文件的真實性。確保其產品對所有進行身份驗證的用戶是公平且無偏見。沙盒中與 ICO 諮詢資料保相關議題：Onfido 是否為改善臉部識別模型時處理個人資料的控制者；依據 GDPR 第 6 條，開發其身份驗證服務時最適合處理個人資料合法的基礎；得否在處理 GDPR 第 9 條(1)所定義的任何特殊類別的個人資料時開發其身份驗證服務；應如何向資料主體提供有關其活動的隱私資訊；在處理資料時應如何賦予資料主體個人資料權利等。

2. 未來流：資料流通(Future Flow: Data flows)[63]

Future Flow Research 公司提供一個分析平台，監視金融系統中具犯罪可能的的資金流動，使金融機構可以提供假名交易資料，使金融、監管和代理機構協力發現並解決金融犯罪。沙盒中與 ICO 諮詢資料保相關議題：複雜的資料控制權問題（即在不同模式下的資料處理，如何判斷控制者、聯合控制者或處理者；該公司處理的資料是否可以視為匿名資料；以及關於英國資料保護法遵循。

推動至今，已有以上 4 項成果，而 ICO 也持續推動提出 2020-2021 年監理沙盒的主要重點領域包含「資料共享」(data sharing)，特別是在衛生、政府、金融、教育或執法領域等；以及「適齡服務設計準則」(Age Appropriate Design Code)，如線上兒童隱私保護、物連網玩具、未成年人之定位資訊等，鼓勵以上領域相關業者參與沙盒的下一階段[64]。

（二）日本：資料信託示範實驗

2017 年 6 月 9 日，日本首相官邸舉行第 10 次未來投資會議，提

[63] Regulatory Sandbox Final Report: FutureFlow, ICO, https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf (last visited Dec. 6, 2020).

[64] Our key areas of focus for the Regulatory Sandbox 2020-2021, ICO, https://ico.org.uk/media/for-organisations/documents/2618112/our-key-areas-of-focus-for-regulatory-sandbox.pdf (last visited Dec. 6, 2020).

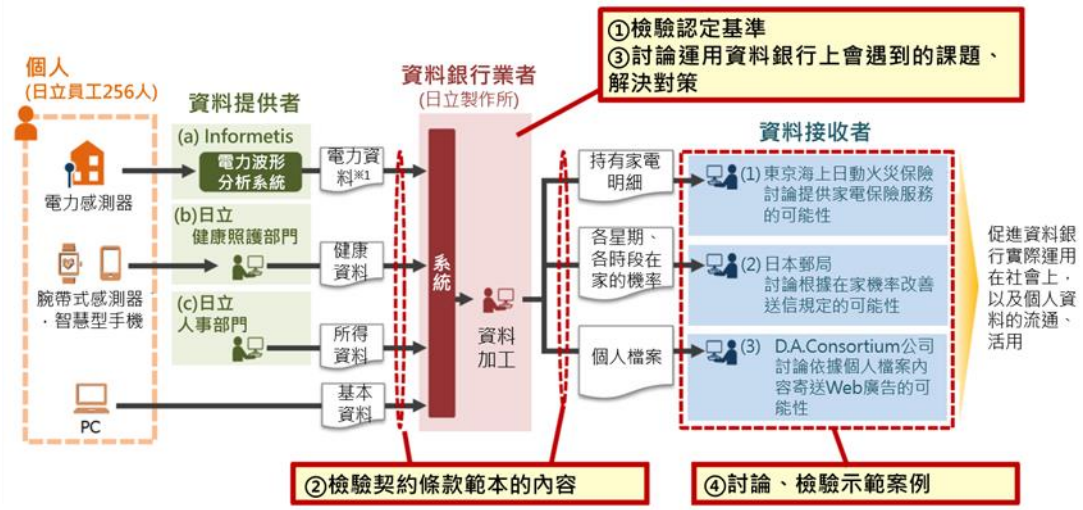
出日本「未來投資戰略 2017」(未来投資戦略 2017)以實現「社會5.0」為目標。戰略中提到將以公私協力的方式支持開創性工作，並創建具體實驗項目[65]。其中，巨量資料的使用被認為是驅動數位轉型的力量，「資料銀行」的概念即是個人透過資料信託的方式將個人資料提供給第三方營運商，建立對資料處理的信任，將可以為個人及企業製造雙贏的局面。因此，日本總務省推出「資料信託功能運用推動計畫」(情報信託機能活用促進事業)並進行示範實驗，希望透過實驗的方式確認資料銀行的可行性，並檢查此機制在運作過程中可能會遇到的問題以建立解決方案。自計劃開始後，日本企業積極建立各領域資料信託實證實驗，以下舉例說明之。

1. 日立「活用個人 IoT 資料等之生活支援事業」

   日立製作所(資料銀行業者)、Infometis 公司(インフォメティス)、東京海上日動火災保險(東京海上日動火災保険)、日本郵局(日本郵便)和數位廣告聯盟(デジタル・アドバタイジング・コンソーシアムは)在 2018 年 9 月 10 日宣布將根據「資料信託功能認證指引 ver1.0」進行示範實驗，推動「用個人 IoT 資料等之生活支援事業」[66]。旨在討論在資料銀行中蒐集、管理和提供個人資料，以及使用個人資料進行服務的可行性。除了性別和家庭組成等一般個人資料之外，也關注未來將可能快速發展的物聯網議題。

[65] 首相官邸，〈未来投資戦略 2017〉，2017/6/9，https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf (最後瀏覽日：2020/12/10)。

[66] 日立トップ，〈個人データの活用の新しい仕組み「情報銀行」の実現に向けた実証実験を開始〉，2018/09/10，https://www.hitachi.co.jp/New/cnews/month/2018/09/0910.html；株式会社日立製作所，〈情報銀行に係る日立の実証実験について〉，2019/02/12，file:///C:/Users/cindyhsu/Desktop/000600133.pdf (最後瀏覽日：2020/12/04)。



資料來源：HITACHI

圖 149 日立資料信託實證實驗

本實驗的參與對象為日立公司員工約 256 人，實驗期間從 2018 年 8 月到 2019 年 3 月。參與者將配有電力感測器、穿戴式裝置以及個人電腦，以蒐集參與者的資料。電力感測器產出的電力資料[67]由 Infometis 公司保存；穿戴式裝置產出的健康資料由日立公司健康管理部門保存；員工的其他基本資料及所得資料則由日立公司人力部門保存。公司員工（資料主體）與日立製造所（資料銀行業者）簽訂契約後，將資料信託給日立製作所，日立製作所即須依照符合資料信託功能認定指引 ver1.0 的標準，提供資料給資料利用者作後續使用。例如可以由電力感測器蒐集到的電力資料知悉家電使用情況，提供家電清單給東京海上日動火災保險公司，研議後續家電保險服務的開發可能性；員工其他基本資料中的出缺勤資料可以知道員工平時與假日的在家時間，可以提供給郵局做為分配宅配路線之參考，藉以改善物流情形；或是提供員工的側寫(profiling)資料給數位廣告聯盟，驗證基於側寫發送的廣告效果如何。

[67] 除了各家電的耗電量外，亦包括依家電使用狀況分析生活模式的結果。

本實驗檢討標的包括(1)認定標準；(2)定型化契約；(3)運作上可能會出現的問題；(4)示範實驗遇到的其他問題等。實驗結果茲分述如下：

(1) 認定標準

應重新思考資安防護是否有義務確認受託人是否已取得 ISMS 認證及隱私標章 P-mark，以及除了規定有責任調查資料及資料處理設施相關資產、指定該資產及採取適當之保護措施外，是否應根據保護等級分類資料，並制定使用基準。再者，為提升監督諮詢委員會的組織獨立性，是否應要求委員有一半為外部成員，並在發生事故時向資料銀行建議對外說明事故狀況。第三，為提高個人資料控制權，資料銀行是否有義務揭露將資料提供給哪一個資料接收者、提供何種資料及何時提供。對資料接收者而言，是否應該劃分成「停止提供資料」及「停止使用資料」。最後，當資料銀行發生事故狀況時，是否有義務向全部資料提供者和資料接收者揭露事故相關資料並說明之。

(2) 對定型化契約條款的檢討從以下三個面向進行討論

A. 個人-資料銀行：就信賴觀點而言，從資料提供者蒐集而來的資料，是否應記載「資料銀行可以不接受個人提出修訂之要求」。另外，依法進行匿名加工、統計個人資料時，是否應明確告知資料主體，並將因為資料流通帶來的利益回饋給資料提主體。

B. 資料提供者-資料銀行：為確保提供資料的正確性，資料接收者有權要求資料提供者公開資料取得方法、資料產生方法，以及預測準確度等相關資料。在資料提供者有不願意提供資料

的企業時，是否有權要求資料銀行「選擇資料接收者」的要求，資料銀行是否應考量並接受該要求。

C. 資料接收者-資料銀行：是否應追加記載「使用衍生資料」的規定，以及當提供匿名加工資料時，是否應適用不同檢驗標準。

(3) 運作上可能會出現的問題

當參加者非獨居生活時，可能同時蒐集到其他家庭成員之資料，故在簽約時應向家庭全部成員說明並取得同意。在建立及管理帳號方面，為確認本人真實性及同一性，應提出身分證明資料，並經由日本公開金鑰基礎建設(JPKI)確認身分。應同意資料主體可自行修改自己註冊的資料，或是和資料提供者合作，委託其處理，但當個人退出時應立即刪除資料。對於資料取得、提供的紀錄應保存 3 年以上。資料提供者可要求資料接收者一定期間後停止使用。最後，資料價格應依項目數量、交易件數設定費用。

(4) 示範實驗遇到的其他問題

應修正每個資料接收者和資料主體在資料價格上的落差，目前即使是同一筆或同一種資料，資料提供的價格可能不同，如此一來，可能會被視為個資販售者。第二，資料使用者加工、販售已取得的資料時應該制定加工標準，例如加工到何種程度的資料就不適合再轉手販售。最後，未來資料銀行蒐集的資料種類將越來越多，資料提供者應制定共通性標準格式(例如查詢目錄、資料提供介面、API 參數名稱、表頭資料的內容等)，以提高資料接收者的便利性及資料流通性。

2. My Data Intelligence「資料銀行試辦計畫」

日本電通集團旗下的「My Data Intelligence」公司於2019 年 7 月 3 日宣布推出資料銀行服務，實驗期間從2019 年 7 月至 2019 年 12 月，約有 12000 名消費者申請加入。本項實驗除了電通集團，包括麒麟控股和明治安田人壽保險在內的 10 家公司也將參與其中[68]。

本實驗蒐集存放多達 250 項資料，包括個人資料、人口統計資料、個人興趣偏好、位置資料、購物紀錄、家庭收支、可穿戴式裝置資料等。蒐集時明確指出資料的使用目的和所需要提供的資料類型，由資料主體自行決定是否提供，提供資料後則會有金錢或服務等獎勵機制回饋資料主體[69]。

資料來源：My Data Intelligence

圖 150 My Data Intelligence 運作流程

3. NTT Data「個人資料同意管理服務實證實驗」

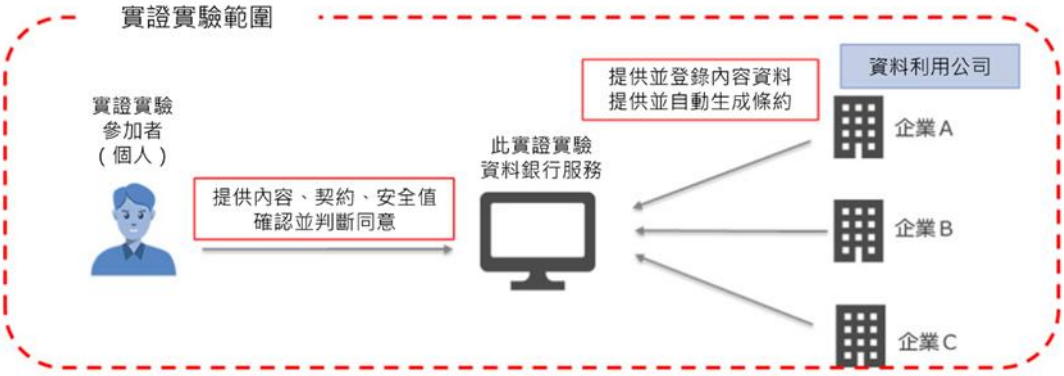
從個人資料保護委員會及公平交易委員會的趨勢來看，企業應以透明的方式處理個人資料被日漸重視。惟目前各項契約條款大多分散式記載，且大多數民眾時常在不了解各項契約條款的情況下即同意各項契約條款，導致

[68] 〈国内初の情報銀行、サービス開始 購買履歴など提供〉(2019)，産経新聞社，https://www.sankei.com/economy/news/190703/ecn1907030015-n1.html(最後瀏覽日：2020/12/10)。

[69] My Data Intelligence，〈パーソナルデータの預託と活用をする情報銀行を生活者と企業が体験！大規模「情報銀行トライアル企画」スタート〉，2019/7/23，https://www.mydata-intelligence.co.jp/news/2019/07/20190703_01.html（最後瀏覽日：2020/12/10）。

資料主體很難掌握自己向公司提供何種個人資料。因此，NTT Data 公司（株式会社 NTT データ）長期發展及管理跨行業共享大型網路系統。2020 年 4 月 28 日宣布，將在 2020 年 5 月 7 日至 2020 年 5 月 14 日期間進行「個人資料同意管理服務實證實驗」，參與人數約 400 人[70]。

本實驗將驗證使用資料銀行系統的資料使用者和資料提供者對於個人化功能的有效性。實驗中，NTT 公司將建立虛擬的資料庫，讓資料使用者和個人協調和集中管理各項服務條款和協議，以建立一個「安全值」顯示對個人資料處理的清晰程度和安全程度。若安全程度越低則資料接收及使用程度越低。本實驗對資料使用者優點在於，可以建立易於理解且令人信賴的契約條款，且在協議內容變更時可以有效通知資料主體；對資料主體的優點在於透過統一格式，可以輕易識別需要確認的項目及確認該資料提供是否安全，且可以集中掌握及管理自己以提供哪些資料給資料提供者或資料使用者。未來，將根據此實驗結果，預計在 2021 年末建立個人資料同意管理服務。



資料來源：NTT Data

圖 151 實證實驗流程

[70] NTT Data，〈情報銀行を活用したパーソナルデータ同意管理サービスの実証実験を開始〉，2020/04/28，https://www.nttdata.com/jp/ja/news/release/2020/042800/（最後瀏覽日：2020/12/04）。

資料信託服務目前尚處於起步階段，隨著資料銀行逐漸成熟，未來將有更多個人資料能夠透過加值利用取得更高的附加價值。根據日本總務省引用 IDC JAPAN 的研究報告指出，資料利用市場規模將以8.4%的年均增長率增長，2021 年將達到 3419.8 億日元[71]。根據調查，一般民眾有意願提供資料的產業領域包括醫療、購物、交通等。換言之，對於具有高度公共利益的醫療健康服務，或是針對個人化服務以及日常小確幸的福利和便利服務都是一般民眾較為願意參與的領域[72]。因此，在計劃推動方面，未來應減輕資料提供者的不信任感並加強資料提供後所產生之價值另外，也需要加強建立資料洩漏時的恢復措施即補償機制，以及制訂有助於資料利用的標準化規則，以促進民眾資料提供的意願。

三、 資料治理與創新應用規劃建議

前述關於國際資料策略與資料創新應用策略觀察可知，國際上透過上位政策驅動整體資料經濟發展，2020 年歐盟提出歐洲資料戰略、英國政府也提出國家資料戰略，皆是希望充分發揮資料的價值，引領資料應用潮流，同時建構適合資料創新應用生態系；同時因 COVID-19 疫情影響，資料如何應用於防疫，甚至是未來後疫情時代因應措施皆是關鍵所在。此外，下階段資料應用也朝向跨域共享再利用、當事人資料賦權前進，透過創新應用，以促進整體社會進步。就以下面向提出關於資料治理與創新應用規劃之相關建議：

（一）資料應用溝通主管部會與機制建議

當涉及隱私與資料之合理利用之利益權衡，且資料跨域創新應用更加複雜之情況下，不僅是要考量不同型態資料交換機制、可用性、互操作性等資料流通議題，同時也要考量隱私保護與安全，還有特定領域甚至是因資料壟斷於特定公司，也必須考量市場競爭議題。因此

---

[71] 〈「情報信託機能の認定スキームの在り方に関する検討会」の論点について〉(2017)，總務省，http://www.soumu.go.jp/main_content/000553637.pdf（最後瀏覽日：2020/12/10）。

[72] 庄司昌彦，〈我が国における データ活用に関する意識調査〉，第 6 回データ流通・活用ワーキンググループ，http://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/dai6/siryou1.pdf（最後瀏覽日：2020/12/10）。

參酌國際資料應用相關政策與趨勢可知，英國個人資料專責機關 ICO 其所提出資料監理沙盒。雖然稱為「沙盒」，但重點是在「提供進入沙盒的組織關於資料應用之法制建議」，而無沙盒測試認證機制或是豁免相關資料法規之機制存在，且不提供測試資料集等。因此英國資料沙盒反而更類似於提供法制意見溝通機制，讓參與沙盒之組織可以直接面對主管機關，並向其諮詢資料應用規範面問題。因此若借鏡英國，由於我國目前尚無單一個資專責主管機關，而現階段將成立科技發展部會，資料也將會是該部會重要一環，亦得作為思考資料應用溝通主管機關。

日本則是透過資料信託機制，在加強資料流通以利資料加值應用的同時，避免資料過度集中於科技巨頭造成壟斷，並加強個人對資料之自主控制權。我國目前尚無類似資料銀行之第三方資料蒐集的機構，未來在思考資料加值服務時，可以借鏡日本之運作方式，透過公平之第三方機構審查個人資料使用是否公平並符合個人對於資料的利用期待，在促進資料經濟發展的同時也保護個人隱私。

（二）資料應用相關法規之訂定與現行法修訂

資料交流應用建構之基礎，應通盤考量借鏡歐盟、英國、日本皆有上位資料應用政策，從各面向規劃，如資料基礎環境建構、當事人資料相關權利、資料應用人才與技能培養、資料跨部門流通應用與相關機制、資料跨境傳輸等，以及對應之相關立法提案與治理框架等，如歐盟將於 2021 年提出資料治理法，英國也研擬相關資料應用立法，日本亦有提出相應指引。

而我國除了政府資訊公開法、個資法與散見各領域相關法規中資料應用規範外，尚無完整適當法律框架，面對未來真正資料驅動的經濟，必須考慮開放各種來源的資料，現階段我國並無資料應用基本法規，且目前爭取歐盟適足性認定，我國個資法亦須有相對之修正，目前亦待觀察修法進度，因此建議應一併考量資料應用基本法規訂定，以及現行個資法之修訂，甚至應通盤考量製定總體性策略，以實現長期資料治理應用與共享。

（三）資料賦權概念融入與機制設計

最後，針對資料賦權趨勢，對於當事人資料自主權利，由於我國並無類似GDPR可攜權之規定,但在我國金融監督管理委員會於2019年推動開放銀行推動，以及2020年國家發展委員會推動數位服務個人化(MyData)，當事人對於資料掌控權利概念已逐漸融入政策推動中，且此亦為數位經濟的重要關鍵。若當個人得以自由、安全的控制其個資，並同意授權第三方在新的資料驅動創新服務或技術應用個資，並確保其對個資流動有足夠的信任和了解，得使其知悉資料流向以及如何被使用，建議由政府提供指引或相關機制設計，甚至是參考日本資料銀行作為受信任的中介機構建立，協助消費者管理其資料，相信資料對於未來整體社會經濟發展帶來利益，是相當值得期待的。

第二節 企業資料運用之問責及管理

網際網路的普及、社群媒體的使用以及物聯網技術的演進，全球資料流通量呈現指數性增長。資料利用已成為國家社會、經濟和民眾生活的重要組成。消費者已習慣透過資料驅動技術，實現高度個人化的訂製服務，同時並期望企業為使用不同類型的資料使用負責，並積極保護資料安全。在主要國家的個人資料保護制度發展上，新加坡正進行個人資料保護法的修正，強化企業資料運用的問責、促進企業間資料共享，以及降低創新服務的資料運用限制。本研究以下將透過對新加坡個人資料保護法的修正，及一系列的配套指南，說明在個資法下，企業資料運用之問責及管理的發展。

一、新加坡資料問責制的修正

為因應數位經濟發展，同時強化資料保護信賴之法制環境，新加坡於 2012 年即公佈個人資料保護法(Personal Data Protection Act, PDPA)；而後，為了在數位經濟趨勢下加強消費者保護，同時使企業組織有信心利用個人資料進行創新，新加坡國會於2020年11月通過個人資料保護法修正案(Personal Data Protection (Amendment) Bill

2020)。個人資料保護委員會(Personal Data Protection Commission, PDPC)認為，本次 PDPA 的修正，係以強化問責性(Accountability)，為本次修法重點，期望藉由企業問責制加強消費者對資料使用的信任，並提高執法效率，增強消費者的自主權，加強創新資料使用。

對此，個資法修正草案有四項重要修正。首先，將問責性增列於法規之篇名，將問責性明文化為 PDPA 的重要法律原則；第二，增列企業資料外洩通知之義務規範；第三，確保第三方事業受政府機關委託，代為進行個人資料之蒐集、使用與揭露行為，亦受個資法規範；第四，強化個人資料利用之問責性。分述如下：

（一）增列問責性於法規篇名

首先，為了增強消費者信任，企業必須對其擁有或控制的個人資料承擔責任，因此，主管機關透過對企業資料管理的問責，加強消費者信任企業資料使用。

新加坡本次 PDPA 的修正，將問責性列為修法重點，將問責性增加明列於 PDPA Part III 的篇名，將原本「有關個人資料保護之一般規範」(General rules with respect to protection of personal data)的篇名，調整為「有關個人資料保護與**問責性**之一般規範」(General rules with respect to protection of and accountability for personal data)，以明確闡明此一重要法規原則並強調其核心地位。

問責性的具體條文包括 PDPA 第 11 條與第 12 條。第 11 條主要規範事業對於其所持有或控管之個人資料，負有遵循 PDPA 規範之責；事業應設置資料保護專責人員，以確保事業遵循本法之規範，並應將專責人員聯絡資訊公開[73]。第 12 條之規範內容，主要為事業應制定與執行符合 PDPA 所規定之資料保護政策與準則，並設立申訴機制與聯絡窗口，同時上述政策、準則與機制亦應資訊公開[74]。

（二）增設資料外洩通知法定義務

為能強化個人資料保護及事業問責性，本次修正草案新增第 VIA

[73] Section 11 of Personal Data Protection Act 2012.
[74] Section 12 of Personal Data Protection Act 2012.

部分(Part VIA)，增列資料外洩通知(Notification of data breaches)規定。將事業發生資料外洩事件時，所應遵循之評估與通知義務，設為法定義務規範。此項要求，能促進事業內部建構更為健全的資料侵害之風險控管及回報系統機制，進而強化事業對於資料侵害因應與補救之能量[75]。

對此，本文分就個資法修正草案對於事業資料外洩通知義務之規範內容，包括：資料外洩之定義；應為資料外洩事件通知之法定要件與標準；事業對於資料外洩事件之評估義務；資料外洩事件之通知對象；以及，事業資料外洩通知義務之例外規定，介析如下：

1. 資料外洩(Data breach)定義

   個資法修正草案，將資料外洩定義為：(A)任何未經授權而進行個人資料之接取、蒐集、使用、揭露、複製、修改或移除行為；或(B)因遺失任何存有個人資料之設備或裝置，而導致可能發生未經授權的個人資料之接取、蒐集、使用、揭露、複製、修改或移除情形[76]。

2. 應踐行資料外洩事件通知義務之法定要件與標準

   依個資法修正草案規定，事業發生資料外洩事故，經評估後，若認為已構成該法所規定，應為資料外洩通知(Notifiable data breaches)之情形時，該事業應踐行資料外洩事件之通知義務[77]。

   事業是否負有資料外洩通知義務，依照個資法修正草案之規定，以該資料外洩對於受影響之人，是否造成或可能造成顯著性影響(significant harm)；或因該資料外洩之侵害而受影響之人，其人數已達最低數量規模[78]。此外，若是特定的個人資料類型受到侵害，亦可能被認定為，

[75] MCI & PDPC, *Public Consultation paper: draft Personal Data Protection (Amendment) Bill, including related amendments to the Spam Control Act* (2020),p.6, *available at* https://www.mci.gov.sg/-/media/mcicorp/doc/public-consultations/public-consultation-on-pdp-amendment-bill---14may2020/public-consultation-on-pdp-amendment-bill.ashx (last visited Dec. 5, 2020).

[76] Section 26A of Personal Data Protection (Amendment) Bill 2020.

[77] See Section 26D of Personal Data Protection (Amendment) Bill 2020.

[78] Section 26B(1)(b)of Personal Data Protection (Amendment) Bill 2020.

對於受影響人造成顯著性影響[79]。

基此，事業發生資料外洩之事件，是否構成資料外洩法定通知義務，主要係（A）對於受影響人是否造成顯著性影響；或是（B）受影響人之人數達到顯著性規模(a significant scale)；或是（C）侵害特定個人資料之類型而造成顯著性影響而論。對此，未來新加坡通訊與資訊部(Ministry of Communications and Information, MCI)與PDPC，擬於法規進一步規範，構成顯著性規模之受影響人數標準，以及可能構成顯著性影響之受侵害個人資料類型。

對於顯著性規模之標準，PDPC 根據過去執法經驗，目前傾向採取以受影響人數至少 500 人以上作為認定基準[80]。

另一方面，未來 MCI 與 PDPC，對於何種個人資料之類型發生資料外洩時，將可能認定為構成顯著性之影響，將於法規進一步規範。其觀測國際間實務作法，例舉如社會安全號碼(social security numbers)、駕駛執照號碼、身分證字號、信用卡號碼、健康保險資訊以及醫療歷史資訊等個人資料類型，若發生資料外洩時，即要求事業應踐行通知義務，可作為參考[81]。

3. 資料外洩評估之法定義務

一旦事業具有合理可信基礎，足以認為該事業所持有或管控之個人資料已發生外洩之侵害，個資法草案規定，事業應即時採取適宜評估措施，以檢視該資料外洩之侵害程度，是否已達應為資料外洩通知之標準[82]。對此，事業應以書面為之，以證明事業已即時執行合宜之評估措施。事業若無故遲延評估措施或資料外洩通知義務，均

[79] See Section 26B (2)(b) of Personal Data Protection (Amendment) Bill 2020.
[80] *Id.*
[81] *Id.*
[82] Section 26C of Personal Data Protection (Amendment) Bill 2020.

構成法定義務之違反。

另外，個資法修正草案亦要求資料中介業者，受他事業之委任代為處理個人資料時，若具有合理可信基礎，足以認為發生資料外洩之情事，該中介業者應盡速通知委任之事業，發生資料外洩之情事。而受通知之事業，即須採取適宜之評估措施，以檢視該資料外洩之侵害，是否已達法定資料外洩通知之標準[83]。

4. 資料外洩事件之通知對象

事業發生資料外洩事件時，其應通知之對象，依個資法修正草案第 26D 條之規定，分別為 PDPC[84]以及因個人資料外洩而受影響之人[85]。

個資法修正草案要求事業應通報 PDPC 之規範目的，係讓事業於必要時，取得 PDPC 提供資料侵害事後補救措施之指導（例如執行資料外洩管理計畫）且讓 PDPC 對於哪類型的產業部門，在維護資料保護標準之品質時需要更多協助，能有更確切認知掌握。對此，個資法修正草案要求，若事業認為其所發生資料外洩事件，為依法應為資料外洩通知之情形時，事業應於認定之日起，應於三日內通知 PDPC。

而個資法修正草案要求事業應於合理情況下，告知因資料外洩而受影響之當事人，[86]目的在於能讓受影響之人，對於資料外洩之侵害發生能早日知悉，並使受影響之人，得以盡速地採取可能因應之自我保護措施；亦確保事業對於個人資料應有適當處理與安全防護措施。

5. 資料外洩通知之例外

個資法修正草案設有免除事業向受影響人為資料外洩

[83] Section 26C (2) of Personal Data Protection (Amendment) Bill 2020.
[84] Section 26D (1) of Personal Data Protection (Amendment) Bill 2020.
[85] Section 26D (2) of Personal Data Protection (Amendment) Bill 2020.
[86] Section 26D (2) of Personal Data Protection (Amendment) Bill 2020.

通知義務之例外規定，其一為補救措施之例外；第二為技術保護之例外；此外，當政府機關依法禁止事業進行通知時，事業亦不得通知當事人。對此分述如下：

(1) 補救措施之例外

事業若已採取減少對受影響人可能造成損害與影響之措施，因而使資料外洩事故之侵害，對受影響之人，應不致於造成顯著性損害(significant harm)時，免除該事業之通知義務。[87]

(2) 安全技術保護之例外

再者，若事業對於資料侵害之個人資料，於資料外洩之事故發生前，已使用安全保護技術措施（例如加密措施[88]），因而使該資料外洩事故之侵害，對於受影響之人，應不致於造成顯著性損害時，亦免除事業之通知義務[89]。

(3) 禁止事業通知當事人

此外，PDPC 或政府機關亦得依法要求事業禁止通知，而事業因此不得通知任何受影響之人[90]。事項規範要求，係防止企業向受影響人所進行的資料外洩通知，可能造成阻礙任何調查行為或影響法律執行之效果，以及基於國家安全、重大公益之維護[91]。

（三）第三方事業受政府機關委託蒐集個人資料亦受個資法規範

由於新加坡對於公部門（政府機關）處理個人資料之法律，規範於「2018 年公部門（治理）法」(Public Sector (Governance) Act 2018, PSGA)。因此，現行個資法第 4 條（1）（C）規定，政府機關之個人資料蒐集、使用與揭露之行為，不適用於個人資料保護法第三部分與

87 Section 26D (4) of Personal Data Protection (Amendment) Bill 2020.
88 *Id*.
89 Section 26D (5) of Personal Data Protection (Amendment) Bill 2020.
90 Section 26D (6) of Personal Data Protection (Amendment) Bill 2020.
91 *Supra* note 75, at 9.

第四部分之規範，亦即不適用該法對於個人資料保護之一般規範，以及個人資料蒐集、使用與揭露之規範[92]；同樣地，第三方事業受政府機關委託，代政府機關所為之個人資料蒐集、使用或揭露行為，依照現行個資法第 4 條（1）（C）規定，亦不受該法對於個人資料保護之規範條款所規範[93]。

本次修法，於既有現行個資法第 4 條（1）（C）之排除條款，刪除事業受政府機關委託，代政府機關進行個人資料之蒐集、使用以及揭露行為之部分。以確保第三方事業受政府機關之委託，代政府機關進行個人資料之蒐集、使用以及揭露行為，應適用於個資法、遵循問責性之規範要求。

（四）強化個人問責性

本次個資法修正，為能強化對於個人問責性，個資法修正草案於第 35B 條、第 35C 條以及第 35D 條分別增列規定，要求持有或管控個人資料之自然人，應遵循下列行為：

1. 不得因故意或重大過失(reckless)，未經授權而揭露其所持有或管控之個人資料[94]；
2. 不得因故意或重大過失，未經授權而不當使用其所持有或管控之個人資料，因而使行為人受有利益，或使他人取得利益，或造成他人受有損害[95]；
3. 不得因故意或重大過失，未經授權而將匿名化資訊(anonymised information)再識別化[96]。

對於上述規範，個資法修正草案第 35B 條、第 35C 條以及第 35D 條均設有刑事處罰之規定，對於違反上述規範之行為人，均規定可科處兩年以下有期徒刑，以及 5000 元以下罰金。

對於上述之違法行為，個資法修正草案亦設有阻卻違法條款，阻卻違法事由包含個人資料可公開取得、依法律之行為、依法院之命令、

[92] Section 4(1) (c) of Personal Data Protection Act 2012.
[93] *Id*.
[94] Section 35B of Personal Data Protection (Amendment) Bill 2020.
[95] Section 35C of Personal Data Protection (Amendment) Bill 2020.
[96] Section 35D of Personal Data Protection (Amendment) Bill 2020.

執行公司政策準則或經雇主授權、出於專業研發目的或學術研究目的之行為。如行為人對於所持有或管控之個人資料，有前述之揭露、使用，或將匿名化之資訊再識別化時，若該個人資料已可公開取得(publicly available)；或是行為人之行為，係依據個資法或其他法律之規定；或是行為人之行為，係基於法院所授權或要求之行為，個資法修正草案第 35B 條、第 35C 條以及第 35D 條均設有行為人得主張阻卻違法之規定。

此外，PDPA 也修正對於匿名化資訊為再識別化之行為，如該再識別化行為係基於特定目的，且該識別化行為已適時通知 PDPC、其他政府機關或是事業者，亦得主張阻卻違法之規定[97]。基此，員工在業務執行範圍內之再識別化行為，若係依據公司政策或準則，或是基於雇主之授權，進行專業研發，或學術研究目的之再識別化行為，將不會受到該法之處罰。

具體而言，依據 MCI 與 PDPC 的說明，如網際網路安全專家、資料科學家、AI 工程師，以及資訊安全與密碼產業的統計人員，其對於匿名化資料進行再識別化之行為，若是基於執行研究發展之目的、基於測試其事業產品與服務或其客戶資訊安全系統之目的，且經由於雇主之授權者，該行為將不會受到本法之處罰[98]。此外，學術研究者，於進行研究工作或匿名化或去識別化之相關課程之教學時，將匿名化資料為再識別化之行為，亦不會受到本法之處罰[99]。

（五）創新改善服務或產品之目的可豁免同意

新加坡個資法修正草案於第 17 條(1)(b)規定，可未經同意使用個人資料，而相關的定義與限制則規範於附表 2 (Second Schedule)第 2 部份(PART 2)。在此次 PDPA 修正中，為能促進創新發展、活絡數位經濟，增設了資料創新條款，允許業者基於「商業增進的目的」

97 Section 35D(2)(c) of Personal Data Protection (Amendment) Bill 2020.
98 *Id*.
99 *Id*.

(business improvement purposes) [100]時，可未經同意使用個人資料[101]。

在「創新」的詮釋上，研究團隊由草案條文分析為三個層次，其一為商品或服務的創新，其條文定義為「改善或加強該組織提供的任何商品或服務，或開發該組織要提供的新商品或服務」；其二則為創新的商業模式，其條文定義為「改善或加強組織運作的方法(methods)或程序(processes)，或發展新的方法或程序；其三係為消費者提供更為精準與量身訂製的服務，其定義為「學習並了解(learning about and understanding) 與組織的商品或服務有關連的個人行為(behavior)和偏好(preferences)，以及「辨識(identifying)該組織所提供，可能適合個人的其他商品或服務，或為個性化或定制任何的商品或服務。」

此外，依循資料創新以及資料市場競爭的議題，也於 PDPA 的第 6 部份納入資料可攜權(Data Portability)，強化對於個人資料的保護及控制性。

二、新加坡個資保護法的問責指南

數位經濟與網際網路蓬勃發展下，全球的資料保護格局產生許多變化，且在數位平臺競爭之下，個人線上活動產生大量資料，但處理個人資料的「核取方塊」(check-box)之法規框架卻越來越不符實際，不足以跟上資料處理發展，更不利於以此為遵循法規的組織[102]。在無法創新於資料使用得情況下，技術演進與資料驅動創新，就對數位經濟有著至關重要的地位。

新加坡以資料作為數位經濟的基石，引導資料保護措施，不僅是遵循法規的步伐，考量符合規範的方法，繼而著重於責任歸屬之制度。作為個資保護的主要原則之一，問責制(Accountability)在 1980 年由經

[100] 商業創新目的包括（1）營運效能與服務改善、（2）產品與服務發展、（3）增進對顧客之瞭解。PDPC, Public Consultation on Review of the Personal Data Protection Act 2012–Proposed Data Portability and Data Innovation Provisions 19 (2019), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Public-Consultation-Paper-on-Data-Portability-and-Data-Innovation-Provisions-(220519).pdf?la=en (last visited Dec. 8, 2020).

[101] 然而對於個人資料的蒐集與公開揭露，原則上仍應告知個人並取得其同意。*Id.*

[102] PERSONAL DATA PROTECTION COMMISSION[pdpc], *GUIDE TO ACCOUNTABILITY UNDER THE PERSONAL DATA PROTECTION ACT, PERSONAL DATA PROTECTION COMMISSION SINGAPORE*（2019）, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Accountability.pdf (last visited Dec. 5, 2020).

濟合作暨發展組織(Organization for Economic Cooperation and Development, OECD)提出，並獲得國際廣泛關注；而後，問責制也成為 APEC 隱私架構(APEC Privacy Framework)下關鍵原則之一；歐盟於 GDPR 中也強調問責制作為個資保護義務之一[103]。

PDPC 於 2019 年 7 月 15 日發布「新加坡個資保護法問責制指南」(Guide To Accountability Under The Personal Data Protection Act，以下簡稱問責指南)，將資料保護的原則進行重點移轉，鼓勵組織將其個人資料管理從基於法規遵循的方法，轉換採行問責制的方式[104]，換言之，在個資的蒐集、處理與利用上，組織不是僅追求合乎法律規定，而需更進一步對其所蒐集、控制的個人資料負責，並藉此方式給予組織業務合作夥伴提供更紮實的保證，並且加強客戶信任度。

問責制落實於 PDPA Part III 的第 11 條與第 12 條，根據 PDPA 規範，組織必須對所擁有或控制的個資負責，並且需制定並實施資料保護政策；組織也必須溝通並告知員工相關政策、及履行 PDPA 義務所必須之流程與作法。

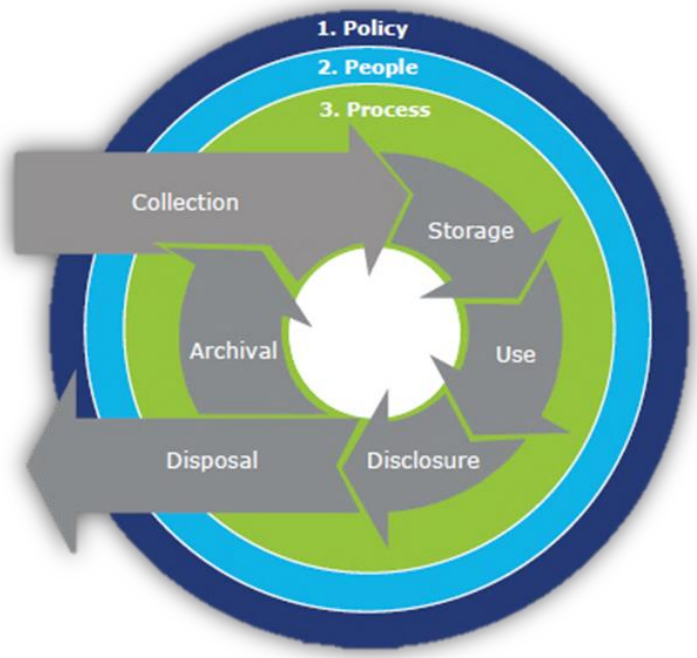
問責指南的目的，在於闡述問責制概念的轉換，以及可採用之步驟範例與資源，並要求組織確實遵守 PDPA 之規範[105]。問責指南在政策、人員、流程等領域中指出，透過資料生命週期的循環，確立組織責任歸屬。簡言之，問責指南涵蓋組織內部、業務內及執行過程三大領域之責任歸屬。在個人資料的保護上，除了具有遵守法律要求的能力外，負責任的組織應具有能力，可適當管理和保護個人數據，包括將法律義務落實於組織政策和行為，利用稽核機制和控制措施來確保政策和流程得到有效實施，並透過人員培訓和宣傳計劃，建立負責任的組織文化。

---

103 *Id.*

104 PERSONAL DATA PROTECTION COMMISSION[pdpc], *Keynote Speech by Mr Tan Kiat How, Commissioner of PDPC, at the IAPP Asia Privacy Forum 2019 on Monday, 15 July 2019, at the Sands Expo and Convention Centre, Marina Bay Sands*（2019）, https://www.pdpc.gov.sg/pdpc/news/press-room/2019/07/keynote-speech-by-commissioner-of-pdpc-at-the-iapp-asia-privacy-forum-2019 (last visited Dec. 5, 2020).

105 Osborne Clarke, *Singapore introduces new concept of accountability for personal data*, LEXOLOGY（Aug. 29, 2019）, https://www.lexology.com/library/detail.aspx?g=3f402921-0643-4950-a0c7-764119269b5a(last visited Dec. 5, 2020).



資料來源：新加坡個資保護法問責制指南

圖 152 資料生命週期循環圖

問責指南從政策(policy)、人員(people)與流程(process)三方面，闡明問責制如何落實於組織內部。例如在組織面，需將個資保護落實於治理政策中，指派管理層級監督個資保護計畫的落實；在人員面，為了確保員工了解並遵守資料保護政策，必須將資料保護與管理納入員工培訓與溝通；在流程面，則是依據資料生命週期（從蒐集、處理、除存到利用），均要建立管理流程，例如在產品或服務的開發階段，即導入隱私保護設計(privacy by design)的概念。

在國家政策部份，PDPC 也建立資料保護信任標章(The Data Protection Trustmark, DPTM)的認證機制，以協助企業或組織驗證其符合 PDPA 的個人資料保護標準和最佳做法(best practices)[106]。

個資保護問責制度的建立，在於組織對個資保護的承諾與責任表示，透過問責制，組織的資料保護制度更加井井有條，在資料隱私政策與落實之制定更為妥適；再者，從有效管理層面來看，因 PDPC 的推動，組織建立責任制措施並獲得認可；最後，由全球角度觀察，責

[106] IMDA, Data Protection Trustmark Certification, https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification (last visited Dec. 5, 2020).

任歸屬制使企業能與相類似做法之境外公司建立聯繫橋梁，使資料更容易進行跨境傳輸，從而為跨境資料建立安全且可信賴的網路渠道。

三、新加坡資料共享機制運作

致力運用數位科技發展成智慧國家的新加坡，以政府、社會以及產業三方面的數位轉型發展為國家智慧轉型政策發展主軸，資料運用的創新促進為產業數位轉型發展之重點。而在 2015 年 8 月所發布未來十年的資通訊發展政策「資通訊 2025」(Infocomm Media 2025)計畫中，即表示資料數據為 21 世紀的「新石油」能源，在連網技術不斷提升且電腦運算科技更為強大的發展下，數據資料分析為產業發展強而有力的工具[107]，政策上以創造安全信賴的、共通的數據資料市場(data marketplace)為目標。

有鑒於私部門的資料集取得不易、且即便資料可取得，亦需耗費相當的時間與資源成本在分散的資料集中進行搜尋外，資料集的關鍵資訊通常亦無法取得。因此將促進私部門資料交換與共享之發展環境，並透過資料市場的建構，以創造資料相關產品與服務之發展環境，達成資料經濟發展；另一方面政府亦持續促進公部門資料開放平台發展，並應致力於建構涵括公部門與私部門數據集的數據資料平臺，讓公部門與私部門的資料，都能以有系統的取得與搜尋[108]。

（一）資料共享指南

為朝此目標前進，2017 年 7 月 27 日 PDPC 發布「資料共享指南」(Guide to Data Sharing)[109]。其目的在於協助企業、組織遵守 PDPA，並提供組織內部與組織間之個資共享。也就是對於得否共享個資、確保如何應用個資以符合 PDPA 共享個資之適當方法，以及將特定資料共享而豁免的 PDPA 規範。而對於資料共享指引分別有三個部分，如下

---

[107] Ministry of Communications and Information, *Infocomm Media 2025* 19 (2015), https://www2.imda.gov.sg/who-we-are/corporate-publications/infocomm-media-2025-plan (last visited Dec. 5, 2020).

[108] *Id.*

[109] PERSONAL DATA PROTECTION COMMISSION [PDPC], *GUIDE TO DATA SHARING*, https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-data-sharing-(270717).pdf?sfvrsn=8 (last visited Dec. 5, 2020).

分述：

第一部分為引言，探討三大資料共享類型[110]：

1. 在同一組織內或關係組織間共享：共享包含向一或多組織為利用、揭露或後續蒐集個資；
2. 與資料中介機構共享（依契約約定資料留存與保護義務）：在組織內共享個人已同意利用之個資，組織還應制定內部政策，防止濫用，並避免未經授權的處理、利用與揭露；
3. 與一個或多個組織共享（在不同私部門間、公私部門間）：還應考慮共享的預期目的，以及共享可能產生的潛在利益與風險。若組織在未經同意的情況下共享個資，必須確保根據 PDPA 的相關例外或豁免之規定。

第二部分為決定共享資料前應考量之要素[111]，包含共享目的、是否適當、共享個資之類型、與預期目的相關性、於預期目的下，匿名資料具備個資替代性、共享是否需要獲得同意、是否有例外、如無須同意，是否需要通知共享目的、以及共享是否涉及跨境傳輸等。

第三部分為共享資料的方式與具體案例[112]，在此一部份，主要由各種不同的情境，討論個人資料保護法的核心要件─「當事人同意」的狀況。

首先，根據 PDPA，組織必須將其個資蒐集目的告知當事人，並徵得當事人同意。如果組織在共享個人資料時，與獲得同意的原始目的不同，組織必須將重新告知並再度獲得當事人同意，除非有例外情況。此處則透過四個不同情境來說明，什麼是正確的「告知並取得同意」。

其次，在上述取得同意的基礎上，進一步探討如何設計動態(dynamic)或多次(iterative)的同意，以因應技術與環境的變化，需要多次重複取得當事人同意，或是讓當事人可以控制/選擇同意的項目等。例如許多應用程式(APP)會將資料利用分成許多項目，當事人可隨時

[110] PERSONAL DATA PROTECTION COMMISSION [PDPC], *New Guide to Data Sharing*, https://www.pdpc.gov.sg/news/latest-updates/page/0/year/2017/month/All/new-guide-to-data-sharing (last visited Dec. 5, 2020).
[111] *Id.*
[112] *Id.*

調整同意/不同意；或者，組織在第一次取得同意時，已告知未來可能變動事項，後續的事項變動就僅做到告知，不再取得同意，但當事人仍可隨時退出的權利。最後則是告知並同意的例外狀況。

資料共享指南具體說明如何共享個資、與資料共享應注意規範、提供具體案例參考，並值得作為組織遵守個人資料保護相關規範與資料共享之法源依據。

而 PDPC 也說明依序 PDPA 可申請資料共享協議(Data Sharing Arrangements, DSA)的法規豁免(exempted)，用於資料共享的公共利益高於個人保護權益時的情境。PDPC 也於文件附錄中，將前述各種考量事項做成清單，供組織參考使用。

另外，為協助產業的商業競爭能力發展，並建構消費者信賴，新加坡資通訊與媒體發展管理局(Infocomm Media Development Authority, IMDA)亦協助 PDPC 推動資料保護信賴標章制度(Data Protection Trustmark Certification, DPTC)，以發展安全信賴與促進創新的資料利用環境[113]。

（二）資料共享協議

上述之資料共享協議(DSA)，係 PDPC 與公司組織合作，建立監理沙盒(regulatory sandboxes)的機制[114]，主要在落實 PDPA 的前提下進行資料共享。而 PDPC 與 IMDA 進一步合作建立了資料共享信任架構（Trusted Data Sharing Framework），該框架提供系統性的原則，以協助公司組織建立一套資料共享的實施基準(baseline practices)。這一套信任架構結合了現有 PDPC 指南中有關個人資料匿名化和資料共享的內容，也包含資料共享所需的資料評估指南以及法規範本。

前述的資料共享信任架構，目前被 IMDA 應用於推動產業導入人工智慧的資料運用上[115]，稱為 AI Singapore(AI SG)，AI SG 為私部

[113] Infocomm Media Development Authority, *Data Protection Trustmark Certification*, https://www2.imda.gov.sg/programme-listing/data-protection-trustmark-certification (last visited Dec. 5, 2020).

[114] Personal Data Protection Commission, Data Sharing Arrangements, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/exemption-requests/data-sharing-arrangements (last visited Dec. 5, 2020).

[115] Infocomm Media Development Authority, Artificial Intelligence, https://www.imda.gov.sg/AI-and-Data (last visited Dec. 5, 2020).

門提供了詳細且易於實施的指南，協助產業在導入 AI 解決方案時，解決關鍵的 AI 道德和資料治理問題，AI SG 解釋如何為 AI 系統建立良好的資料問責制，以及建立開放和透明的溝通模式，以促進公眾對 AI 技術的理解和信任。

四、新加坡個資法下的替代性爭議處理機制

不斷變化的數位產業環境與資料分析的興起，企業運用個人資料的範圍越來越廣泛，為消費者提供了許多新興服務。數位社群平台連接更多的人、電子商務產品更多元也更個性化、數位服務可依據消費者需求，提供更具互動性、客製化的服務。企業一方面蒐集和處理資料，以便提供量身訂做的服務，但另一方面，開發新服務和增進服務品質的資料分析需求，也帶來更高的資料濫用風險，進而產生爭議。

PDPC 認知到，個人資料保護的爭議，多數發生在私人與企業之間，因此，透過雙方的調解或其他替代性爭議處理機制(Alternative dispute resolution, ADR)，也許是較佳的解決方案。在 PDPA 規範中，原本需得雙方當事人同意，PDPC 才能將爭議轉移至 ADR；在 PDPA 修正後，PDPC 可在未經雙方當事人同意的情形下，即將爭議移至 ADR 機制解決。

未來 PDPC 將進一步針對 ADR 機制的以下事項制定配套規範：

1. ADR 服務的標準或要求；
2. 提供 ADR 服務的業者收取費用的基準；
3. ADR 業者必須保存的記錄，以及這些記錄的保存期限；
4. ADR 業者必須依據 PDPC 規定的方式與時間，向 PDPC 提交機制的執行報告；
5. 有關爭議處理結果的生效與執行事項

若參酌新加坡的法制架構，我國則是各目的事業主管機關需要設立各自的爭議處理機制，以快速解決爭議，降低對創新服務利用資料的限制。

五、小結與建議

新加坡個人資料保護法(PDPA)的修正重點，與本研究關聯較深的

部份為問責制及資料創新目的可免於告知義務的增列。PDPC 依據 PDPA 規定，發布有關資料問責指南，就各組織在資料利用上，如何承擔責任進行非常詳細的說明；另一方面，PDPC 則透過資料共享指南，說明組織在進行資料共享前，應有的準備與評估，包括個資法上最重要的「告知並取得同意」原則的具體情境。此外，在問責制的落實上，PDPC 則與資通訊主管機關(IMDA)合作，建立資料保護信任標章(DPTM)。IMDA 不但公佈詳細的自我評估清單[116]供各組織參考。特別的是，IMDA 同時也說明，通過 ISO/IEC 27001 或 27701 認證的組織，因為具有良好的資訊安全性和隱私資訊管理標準，因此可能更容易獲得 DPTM 認證；這意味著 IMDA 的資料保護要求，與國際標準的一致性相當高。

（三）資料治理應納入數位產業職能部會之權責

而目前我國個人資料保護法採取目的事業機關立法模式，與新加坡相比，欠缺個人資料保護的專責主管機關；另一方面，我國目前的通傳會，相較於新加坡 IMDA 為一跨資通訊傳播網路的大型主管機關，我國通傳會主管產業範圍也較為受限。

而我國目前則正研議成立跨資通訊傳播網路產業的新數位產業職能主責部會，未來在個人資料保護的事務上，則可參酌新加坡 PDPC 的職能，將個人資料保護事務納入為其主責事務。進一步說明的是，PDPC 與 IMDA 在新加坡政府體制下，皆屬於通訊與資訊部(MCI)，而 MCI 尚管理新加坡網路安全局(Cyber Security Agency of Singapore, CSA)，可知在政府職能規劃上，資安事務、個人資料保護事務與資通訊傳播網路產業之管制，已然密不可分。

數位經濟下，組織負擔起資料管理責任，已經成為組織資料利用所必須承擔的義務，而為了能靈活的運用資料管理機制，參酌新加坡的作法與經驗，主管機關必須協助、監督企業組織負起完善的資料管理責任。

[116] IMDA, DPTM Certification Checklist, https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Checklist-041220.pdf?la=en (last visited Dec. 5, 2020).

（四）法規修正建議

1. 將問責制納入個人資料保護法

參酌新加坡個資法修正，強化組織對個人資料的保護及問責，我國亦應將問責制納入個資法修正。問責制的重點在於檢視組織如何負擔起個資保護的作為；現行個資法對於利用個資之組織所應遵守的義務有相當詳細規範，但卻欠缺問責的考量，業者在法規的自我詮釋上僅能採用最保守的方向，對於發展以資料為主要驅動力的新興服務相當不利。

問責制以要求資料利用的業者負起資料保護責任為原則，因此賦予主管機關更多用以督促的手段，以要求業者擔負起個資保護的責任；相對的，主管機關則必須積極協助業者建立起適當的保護機制。

2. 新增資料可攜權

資料利用成為數位經濟的主要支柱，為了促進資料流通，除了業者間的資料共享外，讓資料主體能自由的選擇服務提供者、並將資料轉移，也是促進資料市場活絡的手段之一，同時也增進了資料主體的控制權，也能具有促進創新服務發展的效益。

然而，為了落實資料可攜，主管機關尚必須有配套的資料互通的政策，並且對於可攜的範圍也需加以界定，畢竟資料除了由蒐集而來，亦可能由觀察、分析、側寫等衍生方式為之。

3. 納入替代性爭議處理機制

當個資運用出現爭議時，並未必然代表利用資料的企業違反個資法，有時可能是對於蒐集、處理或利用的範圍有所爭執，此時可由第三方爭議處理機構介入調解，以快速維護、處理當事人兼之爭議。

由於個資爭議的態樣與專業性高，因此若僅依照一般民事

法規的處理方式，由當事人自行尋求調解或和解，在專業性與信賴性方面可能有所不足;此時可於個資法中增訂處理機制的規範，連結、補充我國既有的調解制度或仲裁法規，以增加主管機關執法的彈性。

4. 將創新服務納入特定目的外之利用事項

PDPA 此次的修正，將創新服務納入可未經同意使用個人資料之事由，此一法規內容的修正可與個資保護主管機關 PDPC 的資料共享指南一起觀察。PDPC 在資料共享指南中，已針對同意並告知的作法進行詮釋，其中包含對未來可能新增的特定目的所為的預先同意告知;而在 PDPA 修正中，則進一步將個資利用於商業改進目的(business improvement purpose)納入例外事由。

因此，本研究建議，在我國將數位經濟發展視為重要經濟政策的同時，應將創新服務的提供或開發，納入我國個人資料保護法第 20 條上的特定目的外之利用事項；其定義可參酌新加坡個資保護法的附表 2 內容，以業者改進或開發新商品及服務為限，並配合主管機關的監督措施，要求業者必須具體說明，對商品或服務的改進或創新之處，以提供數位創新服務更寬廣的發展環境。

（五）配套措施建議

1. 協助通傳產業建立資料保護問責機制

如前所述，個資法納入問責制的用意，在於主管機關需督促、協助業者建立保護機制。在本計畫的執行上，已透過個資保護手冊與相關資料編排與提供、個資法規課程規劃及業者實際訪視等，了解通傳業者對於個資的保護狀況，並設計相關法規遵循的課程，使業者了解個資法的要求，並進而達成法規的要求。研究團隊在其他的專案或與業者交流的機會中，也得知部份業者為能達成個資保護的責任，會於組織內導入 ISO/IEC 27701 隱私資訊管理系統

(Privacy Information Management System, PIMS)，尤其在歐盟 GDPR 實施後，相當深遠的影響全球隱私法規的走向。

然而，並非所有類型、規模的通傳業者皆有能力或需求導入 PIMS 機制，大型、主要業者可藉由國際標準的導入而符合個資法要求，但規模較小的業者、新創業者等，就難以達成。因此，研究團隊建議，未來主管機關可參酌新加坡 PDPC 與 IMDA 合作，建立資料保護信任標章(DPTM)的作法，協助不同規模、需求、創新的業者建立適當的個資保護機制，而大型、主要業者則可自行導入類似 PIMS 的機制，正如 IMDA 也認為，通過 ISO 27001 的組織也比較容易取得 DPTM。

2. 監督創新服務資料利用

參酌新加坡 PDPA 修法，將創新服務納入免告知同意的例外，未來在個資法若納入類似的修法，則目的事業主管機關將擔負起監督、定義「創新服務」的責任；同時，當爭議產生時，主管機關也需要設立相應的訴訟外的替代爭議處理機制(ADR)，以快速解決爭議，降低對創新服務利用資料的限制。

另一方面，當創新服務之資料利用需求範圍更大、程度更深時，便可能需要利用到資料沙盒機制，實際觀察創新服務對於個人資料的利用，以決定資料利用組織可如何負起資料保護責任。

3. 跨產業個資保護準則協調機制

在數位經濟趨勢下，通訊傳播產業除了提供人與人的通訊，或是資訊傳遞的媒介之外，也扮演消費者與其他產業之間的中介管道。尤其在各領域的產業進行數位轉型時，將既有的服務數位化、轉移到線上平臺之後，通訊傳播業者掌握了接觸使用者的管道，因此，通傳業者所掌握的個人資料，也可能因為產業合作而有跨產業使用的需求。

此時，通傳主管機關需與其他主管機關協調個資保護的一致準則，在我國現行體制下，不同產業的個資保護措施與思維可能不同，例如，合乎通傳產業的措施，未必符合金融產業的標準。此時，需要通傳主管機關與金融產業主管機關針對個資保護事項協調，使兩個產業的保護標準能夠一致化。

另一方面，政府在推動產業創新發展時，也可能面臨新興產業主管機關不明的狀態，此時由於通傳產業的中介者特性，主管機關可扮演跨產業溝通的角色，邀集相關利害關係人組成溝通平臺，初期以自律方式建立一致的個資保護責任要求，適當完善資料治理的目標。

第三節 跨產業之目的事業主管機關權責法規調適具體之建議

由上研究可知，資料經濟已是先進國家數位發展的趨勢，我國政府刻正積極推動數位轉型，當應致力於建構有利創造資料最大價值的法規環境。其中，資料流通既是發展資料經濟的關鍵，如要促進資料價值最大化，政府即須打造適於業者資料流通的規管框架。特別是為了發揮資料的創新價值，講求資料多樣性、即時性、巨量性的大數據應用仍至為重要。因此，跨產業間的資料流通更是政府推動資料經濟發展的首要目標。

然而，當資料涉及特定個人時，個人資料蒐集機關的資料共享、交換或再利用，將可能危害當事人（資料主體）的資訊隱私權或自主權，此時即有個人資料保護法規介入的必要。雖然我國現行有單一部個人資料保護法，拘束所有公、私領域的資料蒐集機關，但在法規架構下，除由國家發展委員會職司該法的統一解釋之外，對於各個非公務機關涉及個人資料之行為的違法事實認定與監理規管，均由該非公務機關所屬事業的中央目的事業主管機關負責[117]。

從而，在涉及跨產業的個人資料流通時，如有法規調適的需求，雖然直接增修個人資料保護法相關規定似為正辦，但修法工程仍應由

[117] 相較之下，先進國家如有單一部個人資料保護法律者，多有專責機關職司該法的解釋與執法。例如歐盟會員國、英國、日本、新加坡、南韓、菲律賓、馬來西亞、澳大利亞、紐西蘭等。

該法的主管機關國家發展委員會啟動。至於各中央目的事業主管機關如欲推動跨產業的個人資料流通，僅能在個人資料保護法授權的範圍內，調整依授權訂定的法規命令；抑或跳脫個人資料保護法的限制，在所主管的法律或法規命令中，以特別法形式增修關於個人資料流通的規定。

但無論是在個人資料保護法授權範圍內調整法規，或於特別法中增修規定，此兩種方式都有造成不同中央目的事業主管機關規範歧異的風險。以通傳產業為例，如某電信事業同時為公開發行公司，除應遵守通傳會就電信事業訂定之規範外[118]，也受金融監督管理委員會在證券交易監理權責下的監督[119]；又如某電視購物頻道業者同時經營電子商務網站，則除受通傳會規範之拘束外，亦應遵循經濟部就個人資料保護、管理訂定的法規命令[120]。是若不同中央目的事業主管機關對個人資料流通的規範存有落差時，業者恐仍將有所顧慮，無法有效達成流通之目標，難以釋放巨量資料的潛在價值。

因此，跨產業之目的事業主管機關權責法規調適有其難度，整體政策的戰略思維應有完整規劃，如能在現行法規框架下，透過解釋、輔導等方式達到促進資料流通的需求，則尚無需更動法規。

本研究認為，通傳會如欲促進個人資料的跨產業流通，應可由下列方向著手：

一、彙整通傳事業及利害關係人之需求與意見

主管機關推動法規調適，應立基於監理事業與利害關係人的具體需求平衡。因此，通傳會如欲適當調適法規以輔導通傳事業創造資料經濟，首應彙整通傳事業對資料利用的具體需求，並掌握利害關係人的關注議題。對此，金融監督管理委員會（金管會）於 109 年 8 月發布「金融科技發展路徑圖」，對金融科技發展提出長期制度與規劃，

[118] 例如電信管理法（特別法）、國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法（依個資法授權訂定的法規命令）。

[119] 例如公開發行公司建立內部控制制度處理準則第 8 條第 1 項第 15 款：「公開發行公司之內部控制制度，除包括前條對各種營運循環類型之控制作業外，尚應包括對下列作業之控制：15、個人資料保護之管理」。

[120] 例如網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法（依個資法授權訂定的法規命令）。

其方法論應可作為通傳會之參考，簡述如下：

（一）舉辦座談會收納監理事業與利害關係人意見

1. 金管會為提出金融科技發展路線圖，於 109 年 6 月起舉辦 3 場座談會，廣邀金融機構、金融科技業者、電信業者、證券交易所、期貨交易所、集保結算所、消基會、學者、專家等生態圈促進者出席座談，就資訊共享、建立單一窗口平臺、法規調適、人才培育、消費者保護等議題交換意見，納入金管會規劃方向。
2. 通傳會亦可參考此作法，以座談會方式徵集通傳業者與通傳資料生態圈的利害關係人（包含跨產業的資料需求者，例如金融機構、金融科技業者、行銷與廣告科技業者等）之意見，彙整各方對通傳事業（個人）資料交換、共享、再利用、行銷等需求，作為通傳事業資料流通政策長期規劃的第一步(本研究試規劃座談會焦點議題於第十一章)。

（二） 建立單一諮詢交流平台

1. 金管會於座談會中獲得數項反饋，其中之一乃是業者認為「金融科技之發展已跳脫傳統機構別之框架，甚至多與相關領域結合，業務範圍亦拓展至金融服務以外」，因此常遇有跨機構、跨部會之議題，亟需單一窗口協助釐清法令與監理等問題。因此，金管會於金融科技發展路徑圖揭示的推動措施第一項即是強化「單一窗口溝通平台」。
2. 相較之下，通傳事業握有之資料也益發存在跨產業流通的需求，即便在通傳事業之間也不乏資料流通之利益。因此，通傳會應可評估指定單一窗口作為通傳事業與利害關係人對溝通管道，並建立諮詢交流平台以定期彙整業者對資料經濟發展的需求，甚至納入跨產業主管機關窗口作為平台參與者，共同創造資料經濟的最大規模。

二、優先處理通傳事業之間的資料流通法規調適

通傳事業之間的資料流通，可透過資料交換、資料共享或資料可

攜等方式達成。此外，異業行銷雖不必然需要資料交換，但涉及資料的（目的外）再利用行為，不妨視為廣義的資料流通：

（一）資料交換

1. 法規現狀檢視

(1) 在通傳事業之間傳輸個人資料的情形，業者首應評估該行為之目的對應所欲傳輸之個人資料（內容），是否符合必要性原則（包含目的限制與資料最小化），並應考量可否以匿名資料的形式提供，以避免特定客戶身分遭資料接收者識別。

(2) 如依具體情形，匿名資料無法滿足需求時，業者即應審查該傳輸個人資料予他事業的利用資料行為，是否構成目的外利用，如是，則應依個人資料保護法規定取得當事人之同意，或檢視是否符合個人資料保護法第 20 條第 1 項但書的其他例外事由。

2. 通傳會調適法規措施

(1) 特別法規

由於資料交換涉及的個人資料利用行為，於個人資料保護法上已有規範，通傳會如欲以特別法放寬利用個人資料的要件，恐將使通傳資料當事人的保障低於個人資料保護法之標準，尚不宜貿然為之。

(2) 匿名（或假名）措施

本研究認為，通傳會應可考量在現行個人資料保護法第 27 條第 2 條「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」及第 3 條「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之」的授權範圍內，於「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」增訂有關資料匿名（或假名）措施之規定，以「防止個人資料（於資料

交換時）洩漏」（參考調適法規見第十一章）。

(3) 當事人同意方式

此外，姑不論我國個人資料保護法尚未如歐盟 GDPR 等先進國家法規，明確對當事人同意的形式要件（任意性、特定性、知情性、積極性、可撤回性）設下規定，實務上的當事人同意機制缺陷多在於當事人需於有限的契約文件審視期間勾選框格，或以機械性的點擊（螢幕或網頁）方式表達同意，恐將弱化當事人對其同意事項的理解；且一經同意，除非業者主動提醒，否則當事人恐不知仍有權撤回同意，甚或時日久遠早已忘記曾同意的目的外利用個人資料行為。凡此均將削減個人資料保護法對當事人資訊自主權所欲強化的保障。

因此本研究認為，通傳會應可於在不逾越個人資料保護法有關當事人同意之規定的前提下，輔導業者以適切方式取得、維護當事人之同意（參考措施見第十一章）。

（二）資料共享

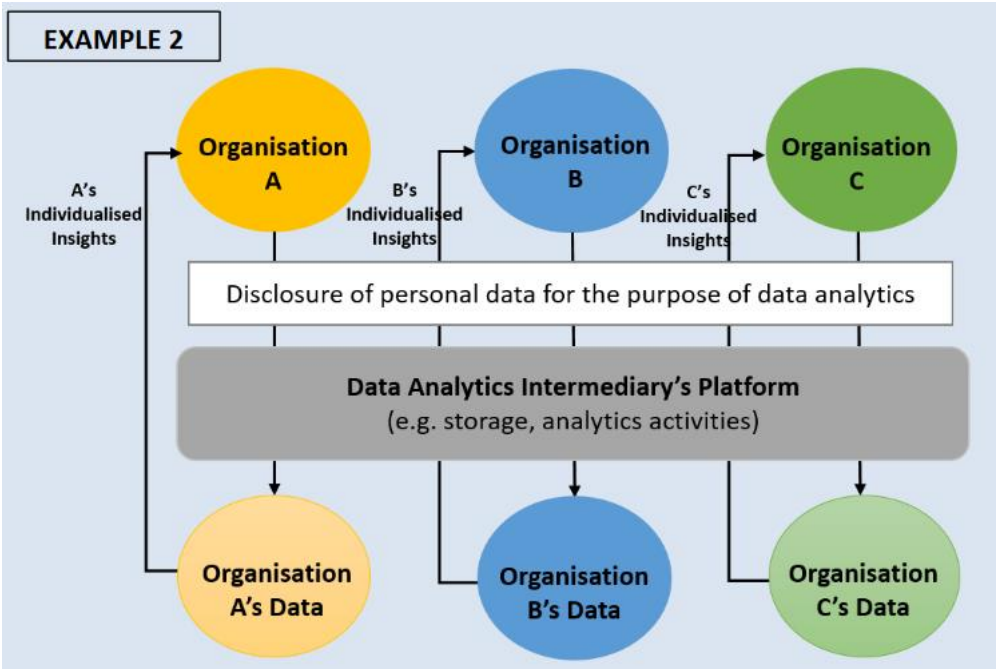
1. 法規現狀檢視

(1) 資料共享與資料交換不同之處在於資料共享並非由資料蒐集機關傳輸資料予特定機關，而是不同資料蒐集機關將資料置於特定平台，供其他機關依需求取得所需資料。

(2) 如以現行個人資料保護法檢視，通傳業者將個人資料傳輸至第三方平台，不必然構成目的外利用個人資料的行為（例如使用第三方雲端儲存服務、資料分析服務）；且在資料共享的概念下，由於通傳業者上傳平台之個人資料是否由其他業者取得尚屬未知，因此也不盡然須以「利用個人資料」之行為合法要件予以審查。

(3) 對此，本章第二節提及的新加坡資料共享指南為資料共享的法遵情境提供了數項分析，值得參考：

A. 情境 1：業者於第三方平台儲存或分析資料



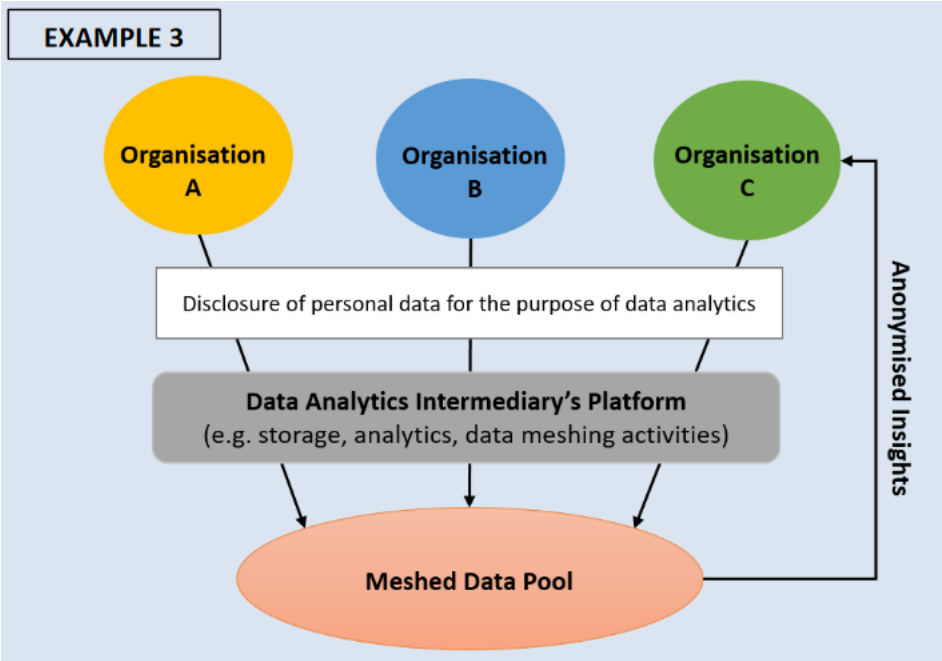
資料來源：PDPC 資料共享指南，第 8 頁

圖 153 業者於第三方平台儲存或分析資料

a. 此情境是指各個業者使用同一第三方平台儲存或分析資料，不涉及資料共享。

b. 在此情形下，即便各個業者使用同一第三方平台儲存或分析資料，但該平台係對個別業者提供服務，個別業者上傳的資料尚未由其他業者取得，不會構成目的外利用個人資料的行為。

B. 情境 2：第三方平台提供匿名資料



資料來源：PDPC 資料共享指南，第 9 頁

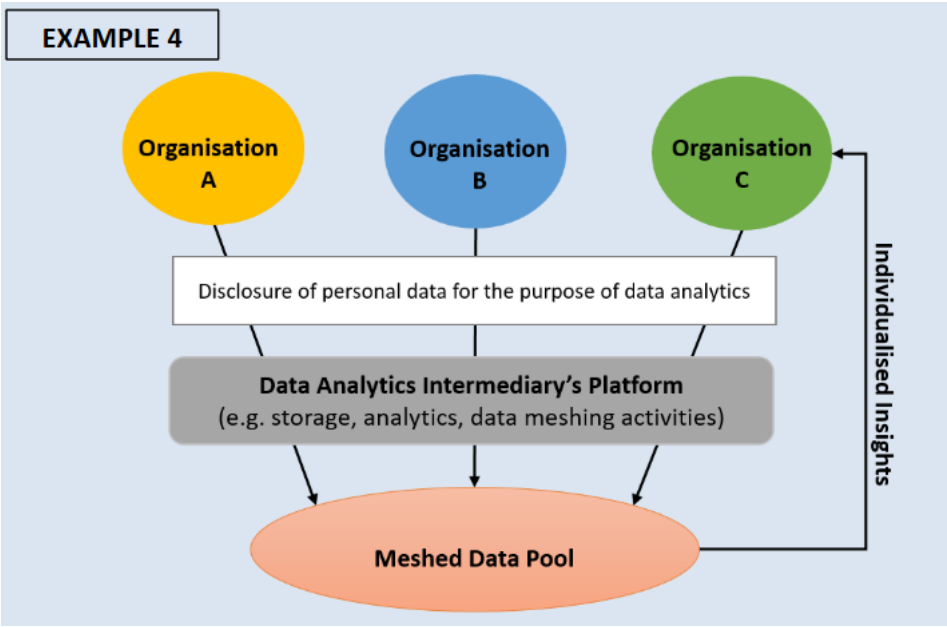
圖 154 第三方平台提供匿名資料

a. 此情境是指在各個業者上傳個人資料至同一第三方平台分析後，該平台將彙整各個業者上傳資料的分析結果，以匿名方式供特定業者取得。

b. 在此情形下，由於業者能取得者為匿名資料，該資料無法識別其他業者上傳之資料所屬的當事人，因此不須以個人資料保護法之要件審查。

c. 惟此處應留意者為資料匿名程度是否足夠，否則即有資料遭再識別的風險。而匿名程度應由該第三方平台控管，業者擇定平台時也應一併考量。

C. 情境 3：第三方平台提供非匿名資料



資料來源：PDPC 資料共享指南，第 10 頁

圖 155 第三方平台提供非匿名資料

a. 此情境是指各個業者上傳個人資料至同一第三方平台分析後，該平台將彙整各個業者上傳資料的分析結果，以非匿名方式供特定業者取得。

b. 在此情形下，業者上傳的個人資料（可識別特定當事人身分）將由其他業者取得，因此，除非符合個人資料保護法第 20 條第 1 項但書所列事由之一（包含取得當事人同意），否則將構成違法的目的外利用個人資料行為。

2. 通傳會調適法規措施

由上分類可知，資料共享之基礎在於第三方資料平台的存在，此於通傳事業實務運作上亦非鮮見：

(1) 業者於第三方平台儲存或分析資料

有線電視多系統經營者與有線電視業者之間常存在關係企業之集團關係。為有效分配資源，區域性的有線電視業者不乏將（客戶）資料儲存或分析之需求，委託所屬的有線電視多系統經營者執行。

在此情形下，只要該資料的流動仍存在一對一的關係，委託第三方儲存或分析客戶資料，不必然構成（目的外）違法處理或利用個人資料的行為。

(2) 第三方平台提供匿名資料

承前例，如有線電視多系統經營者提供的平台服務，因彙整各別有線電視業者之客戶資料，而產生潛在的資料經濟價值，此時若能確保資料的匿名程度，在可充分保障當事人的不可識別性之前提下，應無禁止業者共享匿名資料之必要。

在此情形，通傳會之監理方向應在於為業者提供有效的匿名措施。進一步言，如能評估此為多數業者的共通需求，通傳會亦可考量輔導建置獨立的通傳事業資料共享平台，供通傳業者以資料共享方式取得其他業者的匿名資料。

(3) 第三方平台提供非匿名資料

由於非匿名資料可識別當事人身分，必須有當事人額外同意或嚴格遵守個人資料保護法第 20 條第 1 項但書的其他例外事由始可為之。

本研究認為，如取得非匿名資料為多數業者的共通需求（例如電信事業欲建立用戶黑名單以預防或識別詐欺行為），通傳會可考量積極提供資料共享平台，並制定規則，促成通傳事業及資料當事人在可受通傳會控管風險的框架內達成非匿名資料共享的目標。

（三）資料可攜

1. 法規現狀檢視

(1) 資料可攜的內涵係指當事人（資料主體）可向資料蒐集機關請求以結構化、一般性、機器可讀之格式提供其個人資料檔案供再利用，或請求將其個人資料檔案傳輸予另一資料蒐集機關。實務上，目前先進各國並非均認為資料可攜式當事人的「法律上權利」，我國亦尚未於個

人資料保護法中賦予當事人該項權利。

(2) 然而，具有國際隱私與個資保護領先地位的歐盟 GDPR 已將資料可攜規定為當事人在法律上享有的權利，以此補足當事人對其個人資料的近用權。此權利或將成為國際立法趨勢，值得我國借鏡。

(3) 歐盟第 29 條個資保護工作小組於 2016 年 12 月 13 日通過（2017 年 4 月 5 日最近修訂）「資料可攜權指引 (Guidelines on the right of data portability, WP242 rev.01)」該指引指出，資料可攜權旨在賦予當事人關於自身個人資料之能力，該權利有助於當事人輕易地將個人資料從一個 IT 環境中移動、複製或傳輸至另一個 IT 環境（無論是其本身之系統、可信任第三方之系統亦或其他新的資料控管者之系統）[121]。

(4) 除強化當事人的資料自主性之外，WP242 指引認為，此權利也將支持歐盟個人資料之自由流通和促進控管者競爭的重要工具，即資料可攜權將增進不同服務提供商之間的轉換，從而促進在數位單一市場背景下開發新服務。

(5) 資料可攜權的內涵之一是當事人可接收資料控管者掌控的個人資料，自行儲存於裝置設備或雲端空間。WP242 指引指出，此內涵可謂補充當事人的近用權，為當事人提供一種簡單的方式來管理和再使用個人資料[122]。例如，當事人可能想從串流音樂服務中取得目前的播放清單（或收聽曲目的歷史紀錄），找出特定曲目收聽次數，或用以比對在另一平台上想要購買或收聽的音樂；當事人也可能想從其網路郵件應用程式中取得聯絡人列表，或取得使用不同會員卡的購買資訊。

(6) 另一方面，資料可攜權要求在技術可行之情況下，依據

[121] Guidelines on the right of data portability, WP242, rev01, 2017, p4.
[122] Guidelines on the right of data portability, WP242, rev01, 2017, p5.

當事人之請求，資料可直接從一資料控管者直接傳輸至另一資料控管者。GDPR 更鼓勵資料控管者建立資料互通的格式，以實現資料可攜性[123]。WP242 指引認為，此資料可攜權的內涵不僅為當事人提供了取得和再使用資料之能力，亦使其可就所提供之資料傳輸予另一服務提供商（無論是否在同一產業類別內）。除了透過賦予消費者權利以防止「被鎖在」某服務提供商，資料可攜權被預期可在當事人控制下，以安全可靠之方式促進創新及資料控管者間個人資料共享之機會。資料可攜性可增進個人資料用戶在組織之間對個人資料在受控制的情形下進行有限之分享，從而豐富服務和客戶體驗。在用戶感興趣的各種服務中，資料可攜性可促進相關用戶個人資料之傳輸和再使用[124]。

(7) 在資料可攜權涉及的可攜資料內容方面，WP242 指引強調，只有與當事人相關的個人資料屬於資料攜帶請求的標的，因此，匿名資料或與當事人無關之資料皆不屬之。不過，可清楚與當事人連結的假名資料則落入資料可攜的範圍[125]。

(8) 在此情形下，資料控管者不應對「與當事人相關之個人資料」一詞採取過度限縮之解釋。例如，電話、個人間通訊或網路電話(VoIP)之記錄可包括（在用戶帳戶歷史中）來電或去電第三方之資訊細節。雖然該記錄包含相關數個當事人之個人資料，但用戶應仍能夠依資料攜帶請求取得這些記錄，因該記錄（亦）與該當事人相關。

(9) 此外，可攜資料限於由當事人「提供」的資料，然而，為了充分發揮資料可攜權的價值，WP242 指引認為，經由當事人使用服務或設備而觀察其活動所得之資料，亦屬由當事人「提供」之資料。例如位置資料、流量資料、

[123] GDPR, Recital 68.
[124] Guidelines on the right of data portability, WP242, rev01, 2017, p5.
[125] Guidelines on the right of data portability, WP242, rev01, 2017, p9.

線上搜尋歷史記錄等[126]。

(10)相反地，資料控管者基於「由當事人提供」之資料所創建之推論資料和衍生資料，例如關於用戶健康狀況評估之結果，或在風險管理和財務法規背景下創建之檔案（例如，給予信用評分或遵守反洗錢法規），則不得被視為由當事人「所提供」。WP242 指引指出，即使此類資料可能係資料控管者所存留檔案之一部分，並且係透過當事人所提供之資料分析推論或衍生而來（例如透過當事人之行為），這些資料通常不會被視為「由當事人提供」，因此不屬於此項新權利之範圍[127]。

(11)最後，WP242 指引認為，作為一種優良實務範例，資料控管者應開始建立有助於回應資料攜帶請求之方法，例如可供下載之工具和應用程式介面。控管者應確保個人資料以結構性、一般性和機器可讀性之格式傳輸，並應鼓勵其在執行資料攜帶請求時，須確保所提供資料格式之互通性。

2. 通傳會調適法規措施

(1) 由於由當事人發起的資料攜帶，亦可達到通傳事業之間資料流通之目的，因此，在通傳事業的特別法中增加「資料可攜權」的規定，賦予用戶、客戶可請求攜帶其個人資料的權利，應可作為促進資料流通的法規調適選項。

(2) 然而，一方面作為基本法的個人資料保護法尚未承認資料可攜權為我國人民的當事人權利之一，二方面將資料可攜定為當事人權利，對通傳事業必將課予額外負擔，增加營運成本。因此，在資料可攜「權」成為我國普遍共識之前，如貿然在通傳事業的特別法中增列該項權利，修法過程恐遭遇阻礙。

(3) 本研究認為，通傳會初步或可參照金管會推動「開放銀

[126] Guidelines on the right of data portability, WP242, rev01, 2017, p10.
[127] *Id.*

行(Open Banking)」之例，推動資料可攜成為促進產業發展的政策，非將資料可攜定為通傳事業的義務，而是鼓勵通傳事業滿足用戶、客戶的資料可攜要求，促進資料流通。

(4) 據此，通傳會或可優先擇定個人資料內容較豐富的電信事業，與業者溝通利弊需求後，試辦推動「電信資料可攜政策」，逐步嘗試電信用戶的資料可攜，並據以觀察其對資料經濟之成效。

（四）異業行銷

1. 法規現狀檢視

(1) 通傳事業的異業行銷是指業者利用用戶、客戶的個人資料（例如地址、電子郵件信箱、手機號碼），行銷其他事業的商業資訊（例如在紙本或電子帳單中夾寄或刊登其他公司的商品、服務廣告，或對用戶發送其他公司的商品、服務的簡訊）。

(2) 對此情形，法務部（時為個人資料保護法解釋主管機關）於 102 年 7 月 5 日曾以法律字第 10203507340 號函指出「非公務機關使用基於契約或類似契約關係下取得之個人資料，對該個人當事人進行行銷，應合乎社會通念下當事人對隱私權之合理期待，故『行銷行為內容』與『契約或類似契約』二者間，應有正當合理之關聯，始符合本法第 20 條第 1 項本文規定特定目的內利用之範疇，而無需再得「當事人書面同意」（同條項但書第 5 款）。如行銷與當事人契約或類似契約內容無涉之商品或服務資訊，則除符合本法第 20 條第 1 項但書第 1 款至第 5 款事由外（例如：為增進公共利益或免除當事人生命、身體、自由、財產上之危險等事由），應依同條項第 6 款規定經當事人書面同意者（同意方式請依個資法第 7 條第 2 項規定），始得為之」。依法務部之見，如通傳業者對用戶行銷之資訊與雙方契約內容無涉者，將構成目的

外利用個人資料的行為。

(3) 然而，業者對用戶行銷之資訊究竟與雙方契約內容存有正當合理關聯與否、是否符合用戶內心的合理隱私期待，在個案中似均屬事實認定問題，因此在我國個人資料保護架構下，將歸由中央目的事業主管機關依權責分別認定。實務上，目前通傳業者有取得用戶同意接受異業行銷與否者，亦有在行銷資訊中強調該第三方提供的商品、服務係通傳業者用戶專屬優惠者，應是以此方式企圖滿足「行銷（第三方商品、服務）之資訊與雙方契約存有正當合理關聯」。

(4) 除前述異業行銷之外，由於通傳事業現今多涉及跨領域的多角化業務經營，因此，同一業者對於申辦 A 服務的用戶可否行銷其 B、C、D 商品或服務，亦會涉及法務部所稱「正當合理關聯」之判斷。

(5) 誠然，從實務操作角度而言，只要業者能夠取得用戶的同意，行銷何種資訊均不違反個人資料保護法規定，但必然增加業者的行銷成本，或阻礙業者的行銷機會。

2. 通傳會調適法規措施

(1) 跨產業主管機關協調定義行銷範圍

如將行銷內容區分為「與契約有關之商品或服務」、「同一業者的其他商品或服務」、「其他業者的商品或服務」，本研究初步認為，業者對當事人行銷與契約有關之商品或服務（例如行動網路方案的升級優惠），尚不致逾越當事人的合理期待，也與該契約有正當合理關聯；但業者對當事人行銷自己的其他商品或服務（例如對寬頻上網用戶行銷居家監控服務），或業者對當事人行銷其他業者的商品或服務（例如對手機門號用戶行銷異業的旅遊商品）時，由於「正當合理關聯」乃一「不確定法律概念」，如由通傳會自行認定何者與契約有無正當合理關聯，恐導致不同主管機關之間的適用矛盾，使業者無

所適從。

因此，由於異業行銷的需求相對明確，通傳會似可彙整業者需求，與跨產業主管機關共同協調一致性的行銷範圍，甚至評估可否由國家發展委員會推動將行銷內容的定義具體納入個人資料保護法。

(2) 於特別法中訂定規範

退步言之，如跨產業主管機關間未能達成共識，通傳會也仍不宜自行認定前述異業行銷之範圍。本研究認為，利用個人資料行銷一事涉及當事人資訊自主權的保障，應有法律或法律授權之命令支持，始有正當性。

據此，通傳會應可參考金融控股公司法第 43 條促成金控集團子公司間利用客戶資料共同行銷，並據以授權金管會訂定金融控股子公司間共同行銷管理辦法之精神，提案於特別法中放寬通傳事業的行銷規定，以此取得民意基礎（參考法規調適見第十一章）。

三、跨產業主管機關合作

誠如本章第二節所述，為促進跨產業間的資料流通，通傳會需與跨產業的目的事業主管機關協調個資保護準則，以在現行「單一個人資料保護法、各別目的事業主管機關」的框架下達到監理一致性。

本研究認為，如作為跨產業個資保護協調的表率，通傳會首應提升監理高度，參考國際規範趨勢，將資料治理與問責之概念納入通傳事業的安全維護計畫之中，以此促進通傳事業對資料經濟發展的因應成熟度。此外，通傳會亦可促成跨產業主管機關的監理執法合作，以確保通傳事業與其他產業之間的資料流通法遵監督。

（一）導入資料治理與問責制度於通傳事業安全維護計畫

1. 法規現狀檢視

(1) 在現行個人資料保護法第 27 條第 3 項的授權下，目前各中央目的事業主管機關共訂定 38 份個人資料檔案安全維護辦法，經研究發現，各份安全維護辦法之內容多

以個人資料保護法條文規範，或個人資料保護法施行細則第 12 條第 2 項共 11 款的安全維護措施作為依據，並未強調監理事業的資料治理或問責機制。

(2) 本研究認為，資料控管者的資料治理與問責，已成為國際上關於個人資料與隱私保護的法規監理趨勢，應是我國未來個人資料保護法修正的方向。因此，雖然目前個人資料保護法並未明確提及資料治理與問責，但該法第 27 條第 2 項及第 3 項既已授權中央目的事業主管機關對監理事業指定個人資料檔案安全維護計畫，防止個人資料遭竊取、竄改、毀損、滅失或洩漏，則通傳會在經授權的法規命令中納入資料治理與問責規範，仍是為了達到避免個人資料遭受侵害之目的，應未逾越法律授權之範圍。

2. 通傳會調適法規措施

(1) 參考英國 ICO 發布之問責性框架

英國個資保護主管機關 ICO 在 2020 年 9 月發布「問責性框架（Accountability Framework）」草案[128]，旨在協助業者建立內部制度規範，落實資料運用的法遵需求，承擔資料治理的責任。該框架將資料管理區分 10 個面向，要求業者針對各項目均應建置對應措施，簡述如下：

A. 領導與監督(Leadership and Oversight)

建立堅實的領導與監督機制是資料問責的第一步，包含從策略面與執行面充分賦予個資保護成員特定職責。無論是否設立或指派個資保護長(DPO)職位，業者都應配置足夠的資源協助個資保護人員執行任務，且應由內部高階管理階層負責推動與監督個人資料保護的落實。

B. 政策與程序(Policies and Procedures)

[128] Accountability Framework, ICO, https://ico.org.uk/for-organisations/accountability-framework/ (last visited Dec. 9, 2020).

有效的政策與程序能為業者的個人資料保護提供明確指示並確保一致性，並且能夠作為業者內部涉及個人資料蒐集、處理、利用之行為的具體操作依據。

C. 認知訓練(Training and Awareness)

個資管理程序需由人員執行予以落實，因此，對員工提供充足的認知訓練亦至關重要。業者應確保對員工提供相關、正確且即時的法規資訊或內部管理程序規範。

D. 當事人權利(Individuals' rights)

個人資料保護法旨在強化當事人的權利，因此，業者如能有效遵守當事人權利的行使規定，將有助於降低當事人與業者自身的隱私風險。此外，良好的當事人權利行使機制，也能增加業者的名聲，並加大與其他業者之間的差異性,對業者亦有商業利益。

E. 透明性(Transparency)

透明性（踐行告知義務）原則是「資料保護設計與預設(Data Protection by Design and by Default)」的重要基礎，業者如能高度揭露如何蒐集、處理或利用個人資料（特別是將與第三方分享資料的情形），除能讓當事人對其個人資料享有更充足的掌握之外，也能藉此提高公眾的信任感。

F. 法律依據與業務紀錄(Records of Processing and Lawful Basis)

記錄各項蒐集、處理或利用個人資料之業務流程以及對應的法律依據，可協助業者通盤掌握個人資料的法遵程度，也有助於受主管機關調查時能有效溝通。

G. 契約與資料共享(Contracts and Data Sharing)

當涉及委託他人蒐集、處理利用個人資料，或與第三方交換、共享個人資料時，業者除應檢視法律依

據之外，如能適當由事前評估與事後控管的角度，透過稽核與契約等方式降低風險，將更有助於資料的合法使用。

H. 風險與資料保護影響評估(Risks and Data Protection Impact Assessments)

個人資料的法規遵循不僅應由資產面檢視個人資料的靜態威脅，也應由流程面審視個人資料作業的動態風險，因此，有效的資料保護影響評估應涵蓋資安風險評鑑與管理風險識別，以協助業者事前導入足夠的安全維護措施。

I. 記錄管理與資訊安全(Records Management and Security)

優良的記錄管理始能確實達到資料治理的目的，業者應將各項個資管理過程及管理制度作成紀錄（包含資料交換或共享、資訊安全事件），以利永續經營。

J. 事故回應與監控(Breach Response and Monitoring)

最後，業者應有能力偵測、調查、評估及記錄各次個資事故，並應有效通報（主管機關）或通知（當事人）。

(2) 修訂通傳會指定之安全維護計畫辦法

A. 現行「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護計畫辦法」共計 7 條，除第 1 條說明法源、第 2 條列舉規範對象及第 7 條規定施行日外，其餘條文對應上述英國 ICO 的問責性框架如下表所示：

表 24 ICO 問責性框架與通傳事業個資檔案安全維護計畫辦法對照表

ICO 問責性框架	國家通訊傳播委員會指定非公務機關個人資料檔案安全維護計畫辦法
A.領導與監督	**第 3 條** 非公務機關應依其業務規模及特性，衡酌經營資源之合

ICO 問責性框架	國家通訊傳播委員會指定非公務機關個人資料檔案安全維護計畫辦法
	理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）。 本計畫及處理方法之訂定或修正，應經非公務機關負責人或法定代理人簽署。 非公務機關蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫。
B.政策與程序	**第 5 條** 非公務機關應就下列事項，訂定個人資料之管理程序： 一、蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。 二、檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。 三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條第一項規定。 四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合本法第七條第二項規定。 五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。 六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。 七、進行個人資料國際傳輸前，檢視是否受本會相關法令限制並遵循之。 八、當事人行使本法第三條所定權利之相關事項：

ICO 問責性框架	國家通訊傳播委員會指定非公務機關個人資料檔案安全維護計畫辦法
	（一）當事人身分之確認。 （二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 （三）對當事人請求之審查方式，並遵守本法有關處理期限之規定。 （四）有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。 九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。 十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理。 十一、設置聯絡窗口供當事人申訴與諮詢。
C.認知訓練	無
D.當事人權利	**第 5 條第 8 款** 非公務機關應就下列事項，訂定個人資料之管理程序： 八、當事人行使本法第三條所定權利之相關事項： （一）當事人身分之確認。 （二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 （三）對當事人請求之審查方式，並遵守本法有關處理期限之規定。 （四）有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。
E.透明性	**第 5 條第 2 款** 非公務機關應就下列事項，訂定個人資料之管理程序： 二、檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。
F.法律依據與業務	無

ICO 問責性框架	國家通訊傳播委員會指定非公務機關個人資料檔案安全維護計畫辦法
紀錄	
G.契約與資料共享	無
H.風險與資料保護影響評估	無
I.紀錄管理與資訊安全	**第 6 條** 非公務機關應就下列事項，訂定相關紀錄、證據保存機制： 一、因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之個人資料使用情況、軌跡資料及相關證據。 二、依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄： （一）刪除、停止處理或利用之方法、時間。 （二）將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。
J.事故回應與監控	**第 4 條** 非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制： 一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。 二、事故發生後應受通報之對象及其通報方式。 三、事故發生後，其改善措施之研議機制。 非公務機關遇有重大個人資料事故者，應即通報國家通訊傳播委員會（以下簡稱本會）。 前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。

資料來源：本計畫整理

B. 由上對照表可知，目前通傳會對監理事業訂定的個人資料檔案安全維護計畫辦法，對應英國 ICO 發布的問責性框架仍有落差。由於該辦法乃基於個人資料保護法授權而來，且亦參考個人資料保護法施行細則第 12 條第 2 項的 11 款措施而定，本研究認為，通傳會可適當調整該辦法，納入資料治理與問責機制，以作為跨產業資料流通的主管機關法規調適依據（參考調適見第十一章）。

（二）跨產業主管機關的監理合作

1. 建立定期會報或溝通機制

(1) 各別中央目的事業主管機關在個人資料保護法的規範下，各自有其對監理事業的執法任務。當涉及跨產業的資料流通時，各別主管機關將因所監理事業於該個案中扮演資料蒐集者、資料處理者或資料利用者之不同，而有監理事項上的差異。

(2) 然而，若主管機關之間未能溝通合作而有一致性的監理標準，將可能造成單一服務過程中的不同參與者，因主管機關監理強度不同而受有相異拘束，恐無助資料經濟的發展。例如在 5G 時代的強大網路運算與傳輸功能之下，物聯網設備業者、應用程式業者、網路提供業者可能共同作為特定商品或服務的供應者，但可能各自受到不同主管機關對於個人資料保護的規管，若執法標準未能統一，業者恐怕難以放心參與創新服務的推行。

(3) 此外，單一業者如受不同主管機關監理（例如公開發行的電信業者），若因個資保護不慎而遭其一主管機關裁罰，相同事件是否可由另一主管機關另行處罰，或須以

行政救濟途徑維護權利？更有甚者，如該業者的某行為已經某一主管機關許可或僅限期改正，另一主管機關可否作出不同認定，或須受前一主管機關見解之拘束？類似情形恐將對業者造成無法控管的風險，對於創造資料價值似無助益。

(4) 據此，通傳會應評估在跨產業主管機關之間（初期可先納入關鍵資料流通產業主管機關，例如國發會、金管會、經濟部等）建立定期會報或溝通機制，就各別監理事業的資料流通行為於個人資料保護法上的適用交換意見，以逐步達成共識。

2. 評估網路監理的可行性

(1) 比利時資料保護署於 2020 年 11 月底宣布，與比利時的域名管理機構 DNS Belgium 簽定協議[129]，就.be 域名網站合作執行個人資料保護法遵監理。DNS Belgium 為非營利組織，負責比利時國家頂級域名.be 的登記、分發、使用監督與受理投訴，雖無權認定.be 網站的特定行為是否違法，但可依法院或主管機關作出的決定，對該網站採取特定管理措施，包含暫停域名使用，甚至收回域名。

(2) 依照該合作協議，比利時資料保護署與 DNS Belgium 的合作分為兩部分：

A. DNS Belgium 將配合比利時資料保護署調查處(Inspection Service)的違法調查，當該調查除對特定.be 網站為行政檢查時，得要求 DNS Belgium 提供與該網站有關之資訊。

B. 針對故意嚴重違反資料保護法規的網站，採取「通知－行動」(Notice & Action)程序。依據比利時資料保護署的組織法規定，該署如認定特定網站涉及個

[129] PROTOCOLE DE COOPÉRATION ENTRE DNS BELGIUM ASBL ET L'AUTORITÉ DE PROTECTION DES DONNÉES, https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-dns-belgium-et-l-autorite-de-protection-des-donnees.pdf (last visited Dec. 9, 2020).

人資料之行為違反 GDPR 時，有權要求相關資料控管者限期改正，逾期未改正者，比利時資料保護署即可請求 DNS Belgium 執行「通知－行動」程序，即：

a. 比利時資料保護署將違法網站的相關資訊通知 DNS Belgium，後者收到該通知後，須於 1 個工作日內通知該網站的域名註冊人，要求於 14 日內改正違法行為。在該 14 日期間內，該網站的瀏覽者在開啟開網站網頁時，將被導向警示頁面，提醒瀏覽者該網站存在違反個人資料保護法規的風險。

b. 如(1)域名註冊人於 14 日期間內改正違法行為並獲得比利時資料保護署認可，(2)域名註冊人於 14 日期間內通知 DNS Belgium 其已改正違法行為，而比利時資料保護署未於期限內對此主張作出回應，或(3)該 14 日期間屆滿後，比利時資料保護署未向 DNS Belgium 確認須繼續執行程序，DNS Belgium 將停止程序、移除警示頁面，網站將回復正常造訪。

c. 但若域名註冊人於該 14 日期間內未改正違法行為，且經比利時資料保護署確認仍有必要繼續執行程序時，DNS Belgium 將持續上述「將網頁導向警示頁面」之措施 6 個月。6 個月期滿後，該網站之域名將被收回（網站移除），其域名將進入 40 日的保管期，期滿後即開放公開註冊。

(3) 上述事例為比利時的個資保護主管機關對於違反個人資料保護法行為的網路監理手段。無論數位通訊傳播法如何發展，目前通傳會為財團法人台灣網路資訊中心(TWNIC)的主管機關，在網路監理方面即有工具可

採。

(4) 然而，網路監理必將涉及言論管制爭議，通傳會雖可考量以此作為跨產業的個資保護監理工具，但執行上仍應與各產業主管機關溝通以具體權衡所追求的公益與所侵害的權利間的平衡保障。

四、小結

綜上研究發現，本研究認為通傳會可評估下列措施作為跨產業間法規調適的參考作為，具體調適建議則參第十一章：

（一）彙整通傳事業及利害關係人之需求與意見，包含：

1. 舉辦座談會收納通傳事業與利害關係人意見
2. 建立單一諮詢交流平台

（二）優先處理通傳事業之間的資料流通法規調適，包含：

1. 於「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」增訂有關資料匿名（或假名）措施之規定。
2. 在不逾越個人資料保護法有關當事人同意之規定的前提下，輔導業者以適切方式取得、維護當事人之同意。
3. 如資料共享為多數業者的共同需求，通傳會可評估建置獨立的通傳事業資料共享平台，供通傳業者以資料共享方式取得其他業者的匿名資料，或在通傳會可控管風險的規則內取得非匿名資料。
4. 考量優先擇定個人資料內容較豐富的電信事業，試辦推動「電信資料可攜政策」，逐步嘗試電信用戶的資料可攜，並據以觀察其對資料經濟之成效。
5. 彙整業者需求，與跨產業主管機關共同協調一致性的異業行銷容許範圍；或參考金融控股子公司間共同行銷管理辦法之精神，於特別法中放寬通傳事業的異業行銷規

定。

（三）跨產業主管機關合作，包含：

1. 導入資料治理與問責制度於通傳事業安全維護計畫
2. 建立跨產業主管機關的監理合作，例如：

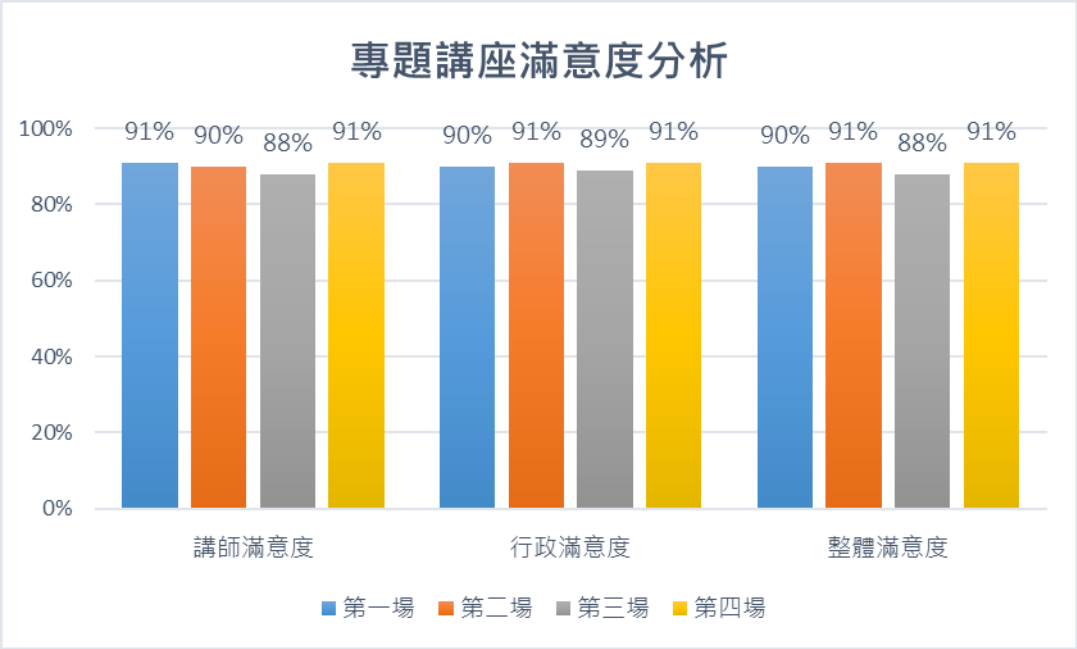
(1) 建立定期會報或溝通機制

(2) 評估網路監理的可行性

第十一章　執行與研究發現

第一節 通傳產業之實務專題講座

本團隊今年度執行 4 場專題講座，專題講座總報名人數共 305 人，實際總人數為 195 人，整體平均滿意度為 90%。



資料來源：本計畫製作

圖 156 109 年專題講座各項滿意度分析

本團隊將滿意度調查問卷進行分析後，發現以下幾點：

1. 業者對個資法遵教育訓練課程回應熱烈；
2. 約有 80%的學員想更加瞭解的主題為「公司內部風險控管及個資運用實務」。

因此，建請通傳會未來持續為通傳業者辦理輔導訓練，並區分受眾，一方面持續對通傳業者（尤其是新進同仁）提供個資法遵教育訓練，強化對個資法基礎的理解程度；二方面為通傳業者的個資保護人員提供內稽內控進階課程，協助尚未導入個資管理制度的業者瞭解管理制度的制定基準，亦對通傳事業的稽核人員或法務人員提供內部稽核的經驗分享；三方面以資料經濟發展趨勢為主題，供通傳業者的決策、管理、研發人員掌握資料經濟下的個人資料運用趨勢。

第二節 通傳產業法制諮詢、問答模擬題庫與參考手冊

本團隊除於教育訓練、專題講座時由專業律師回答參與者個資保護相關問題外，從 9 月起共執行 4 次通傳產業法制諮詢議題回覆，均於規定時間內回覆通傳業者。

本團隊亦撰寫 109 年 4 月至 11 月模擬問答，每月 3 題，共計 24 題，除了針對通傳業者常遇見的個資疑義撰寫模擬問答外，在 109 年 9 月、10 月及 11 月的模擬問答中，特撰擬有關告知義務、安全維護措施等相關個資議題，供通傳產業參酌。

此外，本團隊亦彙整問答模擬題庫，依照個資保護各項主題編寫「通傳事業個資案例參考手冊」，分為「個人資料定義」、「必要範圍」、「特定目的外利用」、「委外監督」、「告知義務」、「當事人權利」、「安全維護」、「事故通報」、「屆期刪除」9 篇，共 25 題常見問題模擬題庫，供通傳會處理通傳產業個資案例參考。

第三節 通傳產業個人資料保護與管理實作指引手冊

本計畫前兩年執行成果發現國內通傳產業於落實過人資料管理制度建置上，仍有持續精進空間。因此，計畫團隊結合我國當前法制、我國常見個人資料管理制度及資訊管理制度（包含國家標準 29100、國家標準 27005、國家標準 31000、台灣個人資料保護與管理制度 TPIPAS、英國標準協會 BS10012 等），透過執行流程的呈現形式，協助產業能更容易地藉由此工具書逐步建立其個人資料管理制度，以持續改善通傳產業的個資保護。

本次手冊初次發放時間為 11 月 10 日研討會，發放過程中可發現業界參與者對於手冊的詢問度高，並有業者在領取並查閱內容後至手冊發放處，詢問是否可以幫公司未至現場的同仁代為領取。由此可見，業者對於個資管理之落實確實有資訊需求。並且藉由手冊領取者的反應情況也顯示，本手冊編制之內容確實有觸及業者需求。

第四節 通傳事業輔導訪查（談）作業

一、通傳事業個資法遵因應評估報告

本團隊期中執行 7 間、期末執行 8 間，共執行 15 間通傳業者個資保護輔導訪查項目（5 間電信事業、5 間有線電視事業、5 間電視購物頻道事業）。輔導訪查發現以種類區分，可統計如下表：

表 25 導訪查發現分類彙整表

種類	電信事業	有線電視事業	電視購物頻道事業	小計
蒐集、處理個人資料	3	3	3	9
法定告知義務	12	11	17	40
跨境傳輸個人資料	0	0	1	1
利用個人資料	11	4	7	22
當事人權利	1	6	0	7
保存個人資料／保存期限	2	3	4	9
委外監督	9	12	11	32
事故通知	2	0	0	2
安全維護	10	18	21	49

資料來源：本計畫製作

本團隊 15 間輔導訪查之主要發現如下：

1. 大型電信事業之個資保護制度與資訊安全措施之落實均較領先，同仁普遍具備個資保護與資訊安全之法規遵循意識。惟因事業體大，業務繁多，除本次訪查鎖定的行動寬頻業務（客戶資料流程）之外，尚有其他電信與加值服務，可取得同一特定客戶的多種個人資料（使用服務所產生之紀錄）。仍須留意在其他業務中的個人資料串接整併（可能供作大數據

分析、線上行為追蹤、輪廓側寫、分群貼標等用途）的適法性。

2. 有線電視業者屬多媒體系統經營者之集團下關係企業，經集團安排，在個資保護制度與資訊安全政策方面均遵循多媒體系統經營者的統一規定，但具體落實程度仍須定期確認，避免說、寫、做不一致性。且因集團事業存有業務互相委託情事，涉及個人資料的委託蒐集、處理或利用行為。有線電視業者與所屬的多媒體系統經營者間就個資委託事項如何互為監督、稽核，宜由主管機關續為留意訪查。
3. 新開播的電視購物頻道業者因仍處於開發商品與客戶市場階段，在個資保護與資訊安全方面仍有不足，整體法規遵循意識尚未完整建立，應仍有賴主管機關持續追蹤輔導。
4. 多數業者仍未全面落實法定告知義務，包含無個資告知聲明、蒐集目的與必要性不明、隱私權政策之明確性不足或疊床架屋等。
5. 多數業者之安全維護措施不足，恐有資安風險，包含仍使用不安全之電腦作業系統、帳號密碼管控待加強等。
6. 多數業者與個資委外廠商（物流、資料儲存、資料處理）普遍就個資保護事項未約定完整的監督權利義務，尤未約定委託事項執行完畢後的資料刪除、銷毀（多表示以口頭或文字告知廠商，但如未以契約約定為廠商義務，究責上較有難度）。
7. 少數業者利用個人資料之適法性尚有疑慮，包含目的外利用個人資料（提供客戶個資予關係企業）所取得之當事人同意未完全符合法定要件、未於首次對客戶行銷時，提供表示拒絕接受行銷之方式等。
8. 少數業者個人資料保存未訂定適當保存期限，或是保存期限屆至未依規定銷毀或刪除。

二、電信事業個資告知義務秘密客抽查報告

本團隊另針對五大電信事業進行個資告知義務秘密客抽查，相關結論整理如下：

1. OOOO：
   (1) 本次抽查人員申辦預付卡過程中，門市人員蒐集、處理抽查人員之個人資料，並未積極向抽查人員揭露個人資料保護法第 8 條規定的應告知事項，亦未告知或提醒於何處可取得相關資訊。但申請書 B 欄第 8 點記載「立同意書人/法定代理人/代理人已知悉個人資料告知事項」，恐與實際情形不相符合。
   (2) 另申請書 B 欄第 7 點提供勾選是否同意接受優惠或服務訊息之選項，似表示該公司以「經當事人同意」作為利用個人資料行銷之依據。然而門市人員未向抽查人員說明須請勾選以表達意願，更在系統中於申請書 B 欄第 7 點預設勾選同意，此同意非屬當事人所為之意思表示，應屬無效。
2. OOOO：

   本次抽查人員申辦行動寬頻試用專案過程中，門市人員蒐集、處理抽查人員之個人資料，並未積極向抽查人員揭露個人資料保護法第 8 條規定的應告知事項，亦未告知或提醒於何處可取得相關資訊。但申請書記載「本人已知悉 OOOO 依個人資料保護法第 8 條告知事項」，恐與實際情形不相符合。
3. OOOO：
   (1) 申辦過程中，OOOO 服務中心門市人員向抽查人員收取身分證件前後，均未告知有關蒐集個資的法定應告知事項，亦未提出任何有關隱私權保護政策及個人資料使用同意事項之書面或電子畫面等供抽查人員檢視。
   (2) 抽查人員簽名時，電子簽名板上除申請表外，已列有個人資料使用同意書的字體，此記載貌似代表抽查人員只要簽

名後即同意 OOOO 使用個人資料，惟使用範圍及內容抽查人員卻一概不知。

4. OOOO：

本次抽查人員申辦行動寬頻試用專案過程中，門市人員蒐集、處理抽查人員之個人資料，除已踐行個資告知聲明外，並就該蒐集行為取得當事人同意，應以符合個人資料保護法第 8 條等相關規定。

5. OOOO：

本次抽查人員申辦行動寬頻試用專案過程中，門市人員蒐集、處理抽查人員之個人資料，雖於櫃檯桌面貼有個人資料保護法第 8 條規定的應告知事項，但並未積極向抽查人員提醒促請閱讀。

綜上所述，本團隊執行五大電信事業「個資告知義務秘密客抽查」，發現只有一間符合個人資料保護法第 8 條告知義務相關規定，其餘四間均有改善及進步空間。建議通傳會未來可持續進行「個資告知義務秘密客抽查」，以敦促通傳事業（包含電信事業）依照個人資料保護法第 8 條規定履行告知義務。

第五節 通傳事業個資管理機制或資料加值運用相關研討會

本計劃案執行研討會舉辦工作項目，分別就行政方面及實際研討會研討內容整理觀察及發現如下：

一、行政部分之觀察

本次研討會有別於去年的研討會設置，設有線上直播管道供線上參與。就行政執行層面而言，可分為研討會前與研討會當日兩部分為觀察分析。計劃案執行過程中，於研討會報名期間，除報名現場參與的情況熱烈以外，亦陸續接獲來電詢問網路直播參與注意事項。整理來電者的說法，主要係基於以下原因選擇線上參與：公司位在中南部北上不便、當天部分時間另有要事安排至現場參與有困難、公司與參與者多無法全體至現場參與、研討會現場可容納人數有限等原因。此

外，從研討會當日的線上即時觀看紀錄，以及當日所接獲有關線上參與技術性問題等，皆印證本次研討會設置線上參與管道的必要性。

二、實際研討內容之歸納

本次研討會分別以「通傳產業資料應用與法制研析」、「通傳產業資料應用與法遵運作」、「通傳資料應用與疫情防制議題研析」三議題進行討論，根據三位主講人報告之內容及與談人之回應與建議，歸納整理如下：

第一場次的報告主題中，主講人介紹資料市集概念以及歐洲目前就此一概念的發展狀況，並指出對我國現行個人資料保護法未規範資料可攜權等法制不足之觀察，並建議以類似沙盒程序等方式實驗資料流動的機會，同時加強保護消費者權益、注重資料安全與隱私保護，以推動資料共享。

第一場次與談人針對此部分議題之回應如下，

1. 政府應對通傳產業業者間資料相互連接性，與第三方外部業者提供個資蒐集等服務，採較開放的態度，以避免業者常礙於擔憂蒐集資料責任過重，而避免蒐集消費者資料。
2. 目前許多資料加值應用的商業作法都仍處於試驗階段，該等商業操作方法是否合法，以及販售價格及行為是否合理，主管機關給予較明確的規範。
3. 建議部分個資法上的權益維護及管理規定，如當事人退出機制等，應聚焦於要求業者提出創新技術或執行上之技術性機制，以確切落實權益之維護。
4. 前端人員的判斷及執行能力將會是特別需要注意之處，資料資產化的趨勢下，最困難的部分將會是個資盤點時資料欄位的設計，若操作者未能進行適法性評估，將致法規準備及實務操作上存在很大的落差。

第二場次報告主題中主講人指出，根據其在實務上之觀察，現行管理制度難以滿足創新應用的法遵需求。其中最主要的兩大困難分別為，(1)去識別化不在程序中；以及(2)取得當事人同意部分缺乏操作

性。而在資料經濟崛起的浪潮下，差異化的個人資料保護、隱私保護將成為未來業者競逐的亮點。

第二場次與談人針對此部分議題之回應如下，

1. 對於「有效的」去識別化，我國目前未有明確規範，因此需要主管機關提供相關指引以利遵循。
2. 在實務操作中「合法的」當事人同意亦需要被明確界定，否則將阻礙資料蒐集，並影響業者提供完整的加值服務。因此，業者期待主管機關更明確界定當事人同意範圍，或提出更便利取得用戶同意的執行模式。
3. 在數位轉型的過程中，許多新型態的服務並沒有明確的規範可以依循，因此在業者的立場上呼籲主管機關在法規尚未明確的情況下，給予較低度的管制，讓業者有較高的彈性嘗試創新。
4. 在集團內部的行銷應用方面，業者期待主管機關，在個資修法前，能先透過函釋使業者集團內之個資使用有所依循，達成創新與法規的雙贏，並降低企業經營風險及營運不確定性。

第三場次報告主題中主講人指出在疫情時代，我們可以觀察到目前世界各國透過手機定位等資訊，以資料的流通追蹤人的流動，並透過流程、資料與資訊、互動溝通的數位化，以資料的流動來取代人的流動等現象。面對防疫下半場，政府應思考科技防疫的合理界線，重新構思數位化下流程及組織的安排規劃。

第三場次與談人針對此部分議題之回應如下，

1. 就目前的技術而言，可依照追蹤對象不同、追蹤方式定位與否、追蹤結果分散式或集中式儲存方式等方案進行資料管控，建議政府預先界定傳染性疾病，依照嚴重程度落入何種象限中，以強化政府防疫手段的正當性。
2. 雖然政府在疫情期間蒐集之個資資訊，係基於高度公益目的，然應注意實際應用上使否符合個資法比例性應用之規定。

3. 在疫情緩和後，已蒐集的資料將如可處理政府應有明確說明，以消弭人民之憂慮。
4. 現行的個資法主要係一般性規定，可能不完全適合作為我國政府採取防疫措施，蒐集、處理、利用個資的依據。應作法規盤點並針對目前法規可能存在的不確定法律概念，或無法完全涵蓋的議題，進一步討論。另建議針對個資監管，設置專責監督機關，以利特殊形況發生時為統一之解釋。

運用科技方式處理疫情，應特別注意隱私權與科技濫用的風險，以及對基本權利的影響。相關的因應措施包括在開始設計時，即嵌入隱私保護概念以降低侵害隱私風險；執行過程中應注意是否符合比例原則；最後針對已蒐集資料的保存，及防疫資料蒐集機制之退場應有通盤規劃。

第六節 國際個資保護管理及資料加值創新應用發展趨勢活動報告

由於疫情影響，為能有效掌握國際間個資保護管理機制及資料加值創新應用之重要之議題，提供主管機關參酌，相關實體研討會已取消或改採線上會議進行，因此在不影響本工作項目之實行，變更參與3場（4人次）之國際發展趨勢活動線上會議。

本次參與3場研討會主要為美國、歐盟產官學研專家對於個資隱私保護、資料創新應用等議題討論。GDPR施行以來，對全球個人資料保護法制影響深遠，且科技迅速發展之下，國際社會對於隱私保護、資料合理利用、充分發揮資料價值等議題皆相當重視，資料也是現代社會發展關鍵基礎。因此2020年歐盟執委會於提出歐洲資料戰略，英國也提出國家資料戰略，美國亦有聯邦個資法立法趨勢，不僅是因為重視隱私保護，還有產業發展面向，積極促進資料得以應用於創新商業模式或服務。因此為能掌握國際上資料相關法律框架，如資料治理、近用與再利用方面，還有可能會影響全球的2021年歐盟資料法案、公私資料共享、如何負責任應用資料，都是我國未來發展資料經濟重要參考依據。就實際研討會研討內容歸納如下：

一、歐洲國家執行 GDPR 之方式大致相同，各國一致期待 EDPB 制定一套全歐盟國家能共同執行的、簡單的 GDPR 執行標準和方式。另外，Schrems II 的作成影響世界所有科技產業，目前美國和歐盟積極討論擬定出新隱私盾，同時，各國積極期盼 EDPB 頒布額外措施指引。本研討會後，EDPB 已於 2020 年 11 月 10 日頒布針對額外措施之建議(Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data)。

二、歐盟今年提出歐洲資料戰略中，預計於 2021 年提出關於資料治理、資料空間相關立法規劃，值得後續密切關注。

三、愛爾蘭隱私保護長 Helen Dixon 分享執行 GDPR 之經驗，主要較擔心未來各國將相繼競爭誰開出比較高的罰鍰使企業誤以為 GDPR 之執行只有裁罰一種方式。另，Dixon 期待歐洲各國開始在國內法院中提起訴訟，目的係讓國內法官開始詮釋 GDPR。

四、近年國際隱私議題日重，美國正積極提倡制定一套聯邦隱私法，民主黨、共和黨參議員都已向國會提出草案，何者將會被選定通過，成為最終美國聯邦隱私法將需持續關注，惟無論是何版得標，美國聯邦隱私法首重消費者權利，亦會與 GDPR 不同，係一部美國人的法律承襲美國隱私法沿革。目前，CCPA 係美國最完整及強大的州隱私法，賦予消費者諸多權利，研討會時逢 Prop 24 公投案前，那時專家預估加州司法部長未來執行 CCPA 時趨向於起訴累犯或重大違反事件。另外，CPRA 已於 2020 年 11 月 3 日通過，將在 2023 年 1 月 1 日正式生效。CPRA 是 CCPA 的附錄，旨在加強加州民眾的權利，限制關於使用個人資料的商業法規，以建立新的保護規則。

五、數位醫療隱私議題日重，尤其後 COVID-19 時代數位醫療將更貼近生活，美國聯邦醫療隱私法 FTC Act 和 HIPAA 之管轄權需多加留意，尤其是 FTC 擁有非常廣的管轄權。

六、COVID-19 促使非接觸式科技的崛起，世界各國相繼投入研發、使用接觸者追蹤技術。惟接觸者追蹤技術涉及隱私疑慮，在此即

可以看出中西方在面對隱私及公益進行衡平時態度差異：西方國家較重視隱私，東方國家則較以公共衛生利益為主。當資料蒐集成本降低，隱私成本就會增加，因此，COVID-19 大流行即提供科技與隱私衡平的一個很好的測試機會，以利在未來建立更適當的資料保護機制。另外，科技的使用並非黑即白，對於技術使用是否會產生偏見或歧視的疑慮，人類應保有完整的自主權。

七、「從設計包含隱私」係隱私法的核心原則，專家一致認為企業在實務上落實此原則的關鍵三元素為：找到重視隱私的公司高層、重用對隱私熱忱的員工執行公司內隱私制度的建置與落實、詳細對員工說明為何需重視隱私以及隱私對企業的影響。

八、在資料蒐集向大企業聚集，造成新的「數位壟斷」的現象下，目前線上服務遇到的問題在於競爭性、公平性及進入市場的可能性。當線上平台業者大量資料串連後，即能夠透過自己平台的優勢來改善或開發新服務，創造完整的生態系統，造成市場傾斜。資料市場的特點在於沒有國界的限制，因此在資料跨境傳輸與競爭法規的設計上，應重新思考數位環境與傳統法規的差異，並保持彈性，以因應數位發展的快速變化。

第七節 國際資料經濟與個資保護趨勢動態資訊與研究調查摘譯

一、趨勢動態資訊

觀測近期國際動態趨勢，先進各國仍持續關注民眾於線上環境的安全與隱私權益保護，以及資料治理發展與個資隱私保護間之調和議題。

首先，在新冠疫情持續對全球帶來嚴重影響下，各類線上服務的蓬勃發展，雖帶來數位經濟的活絡，然其所引發的隱私個資保護與線上安全爭議，使得各國政府均積極採取因應措施，包括美國 FTC 對於線上視訊會議軟體服務提供者所造成的資安與隱私疑慮，採取措施要求業者進行改善之規管發展，或是歐盟議會為健全線上環境發展、保護民眾線上安全與個資權益，對於未來數位服務市場與人工智慧規

範所提出之規範政策倡議，以及英國為保護兒少線上環境安全與個資隱私，發布適齡線上服務設計規範，要求數位服務業者應遵循規範，均展現出國際間政府積極維護消費者的線上環境安全與隱私權益之態度。

另外在國際資料治理與個資保護政策與法制發展上，美國為強化個資隱私保護而提出的安全資料法草案，或是英國為脫歐後順利取得歐盟 GDPR 適足性認證，持續進行的個資保護法制規範與相關制度整備，以利英國資料自由流通與運用政策未來發展，以及歐盟為強化促進安全的資料互通與共享利用，近來提出的資料治理規則草案，均顯示國際間對於資料治理政策發展的關注重視。.

二、研究調查摘譯

透過定期彙整觀測主題與報告，以提供研究調查摘譯與分析重點資訊，協助通傳會掌握包含隱私保護發展趨勢，以及通傳產業數位經濟發展。現階段持續關注世界經濟論壇(WEF)所提出白皮書與報告，其中針對後疫情時代下數位媒體與技術設計的倫理原則，說明「安全設計」關鍵原則在於服務提供者之責任、使用者授權及自主權，以及透明度和問責制度，並以數位媒體實際應用案例，說明符合倫理的媒體與技術設計之間的關係。同時於通傳資料流通應用觀測，值得關注如 2020 年英國 Ofcom 資料可攜規劃公眾意見諮詢，將開放通訊相關資料，使人們和企業可以與電信服務提供者共享電信服務相關資料，透過其他產業借鏡，如金融產業的開放銀行，期能未來促進公私部門資料流通應用，也賦權資料當事人，以利於資料經濟蓬勃發展。此外，英國將於 2020 年底脫歐，然而因應資料跨境傳輸，若未獲歐盟適足性認定，將可能破壞英國數位服務和技術競爭力，脫歐談判協議關於資料國際傳輸部份，我國亦爭取獲得歐盟適足性認定，以利我國資料跨境傳輸至歐盟，此一趨勢亦相當值得後續關注。

第八節 通傳產業資料運用面臨議題與諮詢交流平臺機制解決方案

一、資料治理與創新應用規劃建議

依據前述相關國際資料策略與資料創新應用策略觀察，透過整體上位政策制定，作為整體資料經濟發展驅動基礎。期能充分發揮資料潛在價值，建構適合資料創新應用的蓬勃生態系；今年 COVID-19 疫情影響，資料之應用於更是未來在因應後疫情時代之關鍵。同時觀察到資料應用逐漸朝向跨域共享再利用、當事人資料賦權方向，因此因應以上觀察發現提出關於資料治理與創新應用規劃之相關建議面向：其一，就資料應用溝通主管部會與機制建構，因我國無單一個資專責主管機關，而現階段密集討論科技發展部會之成立，關於資料應用亦可能成為該部會重要職掌，後續得思考資料應用溝通主管機關，此外目前我國於資料應用面並無沙盒機制，參考英國資料於提供法制意見溝通機制，諮詢資料應用規範面問題。

其二，關於資料應用相關法規之訂定與現行法修訂，最值得關注為歐盟 2021 年資料治理法，我國除政府資訊公開法、個資法與散見各領域相關法規中資料應用規範外，尚無完整適當資料應用法律框架，且目前仍與歐盟協議關於適足性認定，因此我國個資法亦須有相對之修正，現階段修法進度仍未見進展，因此一併考量資料應用基本法規訂定，以及現行個資法之修訂，同時為實現長期資料治理應用與共享，應通盤考量製定總體性策略。

最後，則是就資料賦權概念融入與機制設計，國際上資料賦權趨勢，使當事人更能自主控制其資料，我國金管員會開放銀行推動以及國發會 MyData 亦是融入此概念，因此建議由政府提供指引或相關機制設計，甚至是參考日本資料銀行機制關於中介機構建立，協助消費者管理其資料，皆是後續得作為機制參考設計方向。

二、企業資料運用之問責及管理

在本研究各有關的研析國家中，新加坡與我國的相似之處在於，

兩國均以數位經濟發展作為國家主要經濟策略，而新加坡在促進資料運用的法制設計，較我國更為積極。是故，在主管機關針對企業資料運用之管制上，本研究以新加坡個人資料保護法的修正，主要著重於加強問責制的規範，並與既有一系列之準則指南配套運作，由新加坡個資法的變遷，可觀察到主管機關對企業在資料運用上可參考之作法。

首先，我國既有規範傾向於法規遵循，而非問責要求，主要重點仍在於資料的安全維護以及是否遵守個資法的規定，例如我國「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」的主要目的即在於個資利用的法律遵循。然而，所謂的問責，是主管機關必須監督企業的資料保護措施以及政策的落實，而非僅是形式上符合法條文字敘述。

次而觀察到新加坡將創新使用納入免為告知同意的例外，亦可知新加坡相當積極的解決資料運用於數位經濟發展的需求；資料可攜權的納入，也代表強化資料主體的控制。此部份的修正均與新加坡積極發展其智慧國家的政策有關，也代表主管機關更為積極的監督企業在資料的利用上。我國在數位經濟發展需求上，對於資料利用的規範也需更加的開放與細緻。

最後則是在執法手段上的彈性增加，主管機關可透過調解或其他替代性爭議處理機制(ADR)的導入，更加快速的解決當事人間對於資料利用的爭議；同時，PDPC 認知到不同產可能存在特定的問題，因此制定了針對特定產業的的諮詢指南，PDPC 指出，這些指南是根據 PDPC 與相關產業有關的合或、諮詢和反饋，並與產業目的事業主管機關緊密合作而製定。

因此，我國當下雖然欠缺個資專責主管機關，但仍然可先建立跨產業協調與溝通平臺，跨部會合作先行整合個資保護的相關標準，以利數位經濟下產業創新的需求。

三、跨產業之目的事業主管機關權責法規調適具體之建議

在我國現行「單一個人資料保護法，各別中央目的事業主管機關」

的規範下，跨產業之目的事業主管機關權責法規調適有其難度，整體政策的戰略思維應有完整規劃，如能在現行法規框架下，透過解釋、輔導等方式達到促進資料流通的需求，則尚無需更動法規。本研究認為，通傳會如欲促進個人資料的跨產業流通，應可由下列方向著手：

（一）彙整通傳事業及利害關係人之需求與意見

透過座談會方式徵集通傳業者與通傳資料生態圈的利害關係人（包含跨產業的資料需求者，例如金融機構、金融科技業者、行銷與廣告科技業者等）之意見，彙整各方對通傳事業（個人）資料交換、共享、再利用、行銷等需求，作為通傳事業資料流通政策長期規劃的第一步；並可建立單一諮詢交流平台，定期彙整業者對資料經濟發展的需求，甚至納入跨產業主管機關窗口作為平台參與者，共同創造資料經濟的最大規模。

（二）優先處理通傳事業之間的法規調適

針對資料交換、資料共享、資料可攜、異業行銷等特定議題，採取法規修訂或提供輔導、推行政策等方式促成通傳事業之間的資料流通，並未跨產業之間的資料經濟發展建立典範。

（三）跨產業主管機關合作

為有效推動跨產業個資保護準則協調，通傳會可適當提升監理高度，參考國際規範趨勢，將資料治理與問責之概念納入通傳事業的安全維護計畫之中，以此促進通傳事業對資料經濟發展的因應成熟度。此外，通傳會亦可促成跨產業主管機關的監理執法合作，以確保通傳事業與其他產業之間的資料流通法遵監督。

第十二章　結論與建議

綜合本案整體執行與研究發現，本研究提出以下「立即可行建議」與「中長期建議」供委託機關卓參：

第一節 立即可行建議

一、持續追蹤輔導業者進行改善訪查發現

本團隊進行 15 間通傳業者輔導訪查，得知輔導對象仍有未落實法定告知義務、利用個人資料之適法性存疑、委外監督機制不明、安全維護措施尚待加強等情況，亦即本次訪查項目之說、寫、做尚有不一致之處，有待主管機關持續追蹤並輔導通傳業者進行改善。此外，本團隊執行五大電信事業「個資告知義務秘密客抽查」時，發現只有一間符合個人資料保護法第 8 條告知義務相關規定，其餘四間均有改善及進步空間。建議通傳會應持續辦理電信事業「個資告知義務秘密客抽查」，敦促五大電信事業依照個人資料保護法第 8 條規定履行告知義務。

二、提高實作指引手冊觸及率與容易取得

從計畫執行手冊發放過程可觀察到，業者對於個資管理管理實作資訊確有其需求。因此建議，手冊的印刷版本及電子檔可置於相關從業人員聚集場合或慣用網站，以拉高觸及率並可加速文件之流通，使有需求者更容易取得。

三、建議提出個資檔案安全維護說明指引

從研討會中產官學各界專家所提供的實務說明及建議可發現，就個資法遵之執行部分，研討會中針對「有效的」去識別化及「合法的」當事人同意多有討論，並有業者代表提出由主管機關提供相關指引以利遵循之需求。因此建議，或可針對目前已公布之國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法中之規範內涵及範疇等，給予業者進一步的說明指引。

四、持續參與關注線上國際會議，以利獲得第一手資訊

趨勢活動報告受到疫情影響，應變措施為參與國際發展趨勢線上研討會議，為利於後續能持續有效掌握國際間個資保護管理機制及資料加值創新應用之重要之議題，仍得透過參與線上會議方式與國際交流，而不受到時空限制。

參與國際線上研討會獲得資訊，皆為直接從國際上產官學研界各專家學者第一資料，因此對於國際針對資料趨勢更能掌握，現階段最值得關注莫過於歐洲資料戰略後續具體策略將於 2021 年陸續提出，立法提案也有規劃時程，不僅是歐盟內部資料應用關鍵法規，也將與 GDPR 有異曲同工之效，進而影響全球資料治理、應用法制趨勢，後續應持續追蹤關注。

五、持續掌握國際資料經濟與個資保護產業及法制趨勢

當前國際間受新冠疫情持續影響，各式線上服務蓬勃的發展，活絡全球數位經濟趨勢，於此同時，對民眾線上環境的安全與隱私保護權益，成為目前各國政府積極維護之政策目標。另一方面，適逢國際政經局勢詭譎多變的 2020 年，各國政府除為強化個資保護，同時促進安全的資料流通與運用，均積極發展資料治理政策與法制整備，以促進資料經濟發展。

在本計畫執行上，研究團隊經由持續觀測國際資料經濟與個資保護之重要發展動態，提供主管機關掌握國際情勢及國內外相關規範、隱私保護發展趨勢，確保了解並與全球發展脈動一致。此不僅協助主管機關擬定、推動通傳產業資料治理政策，亦有助於未來政府因應數位經濟發展，調整數位事務主責機關之職能架構，使臺灣具備更強之數位競爭力。

六、主管機關強化企業資料運用之問責與管理措施

本部份建議雖然與個資法的修正有所關聯，然而在法規修正之前，主管機關仍有相應之措施可先進行，差異在於因法規尚未修訂，僅能仰賴業者自願遵行，而欠缺強制要求的法源依據。

（一）協助通傳產業建立資料保護問責機制

主管機關協助企業建立問責制，可落實、協助業者建立個資保護機制，承擔個資保護責任。例如落實隱私設計（Privacy by Design, PbD）原則；還有具規模企業可導入 ISO/IEC 27701 隱私資訊管理系統 (Privacy Information Management System, PIMS)，達成負擔責任的要求；但規模不足的業者，就需藉由主管機協助。主管機關可參酌新加坡 PDPC 與 IMDA 合作模式，建立資料保護信任標章(DPTM)，協助不同規模、需求、創新的業者建立適當的個資保護責任機制；以及落實 PbD 原則，此亦為新加坡問責機制之一環。

（二）跨產業個資保護準則協調

通訊傳播產業在資料利用上，時常扮演消費者與其他產業間的中介者，通傳業者所掌握的個人資料，也可能因為產業合作而有跨產業使用的需求，例如身份認證或需求評估。

在我國現行體制下，不同產業的個資保護措施與思維可能不同，尤其新創產業發展時，面臨新興產業主管機關不明的狀態，透過通傳產業的中介者特性，由通傳主管機關進行跨產業協調，邀集相關利害關係人組成溝通平臺，以自律方式協調跨產業同步一致的個資保護責任要求。

七、修訂通傳會指定非公務機關個資檔案安全維護計畫辦法

為促成資料交換與資料共享，在個人資料保護法規範與授權的範圍內，通傳會應可於「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護計畫辦法」中強調資料去識別（匿名）的重要性，並參考日本個人資料保護法第 36 條的規定，另行訂定通傳產業資料去識別的規則基準（此僅涉及技術性事項，應以行政規則訂定即可，未逾法律保留原則）；又為作為跨產業資料交流的表率，通傳會亦可將資料治理與問責概念導入該辦法，在個人資料保護法第 27 條第 2 項及第 3 項授權的範圍內，強化通傳產業對個人資料的保障。辦法之修正建議如下：

表 26 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案建議

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
第一條 本辦法依個人資料保護法(以下簡稱本法)第二十七條第三項規定訂定之。	第一條 本辦法依個人資料保護法(以下簡稱本法)第二十七條第三項規定訂定之。	本條未修正。
第二條 本辦法所稱非公務機關包括下列各款： 一、第一類電信事業。 二、第二類電信事業。 三、有線廣播電視系統經營者及有線電視節目播送系統。 四、電視事業。 五、訂戶數達三千戶以上之直播衛星廣播電視服務事業。 六、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業。	第二條 本辦法所稱非公務機關包括下列各款： 一、第一類電信事業。 二、第二類電信事業。 三、有線廣播電視系統經營者及有線電視節目播送系統。 四、電視事業。 五、訂戶數達三千戶以上之直播衛星廣播電視服務事業。 六、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業。	本條未修正。
第三條	第三條	一、為明確非公務

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，**以執行下列任務：** **一、**規劃、訂定、修正、執行**與監督非公務機關**個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）。 **二、檢視非公務機關蒐集、處理及利用個人資料之法規遵循程度並提出建議。** **三、向非公務機關報告應履行個人資料保護法規之義務。** **四、執行第四條之個人資料現況查核。**	非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）。 本計畫及處理方法之訂定或修正，應經非公務機關負責人或法定代理人簽署。 非公務機關蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫。	機關為個人資料保護事宜所配置管理人員之具體任務，以明文規範管理人員之職責，爰參考歐盟 GDPR 第 39 條及英國 ICO 問責性框架，修正本條第一項。 二、為使非公務機關之個人資料保護管理人員獲得足以執行任務之相當資源，爰參考歐盟 GDPR 第 38 條及英國 ICO 問責性框架，新增本條第四項。

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
五、執行第五條之風險評估。 **六、統籌規劃並執行非公務機關內部人員個人資料保護法規與實務之認知教育訓練。** **七、稽核本計畫及處理方法之落實。** 本計畫及處理方法之訂定或修正，應經非公務機關負責人或法定代理人簽署。 非公務機關蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫。 **第一項所稱相當資源，應至少包含：** **一、適當之經費、設施及人力支援。** **二、使第一項所稱管理之人員獲得非**		

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
公務機關蒐集、處理及利用個人資料之業務內容的必要資訊所需之資源。 **三、對第一項所稱管理之人員持續提供必要之法規與實務訓練。**		
第四條 **非公務機關應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。**		一、本條新增。 二、為促使非公務機關確實查核個人資料現況，並得供本會作為行政檢查之依據，爰參考金融監督管理委員會指定非公務機關個人資料安全維護辦法第4條及英國ICO問責性框架，新增本條規定。
第五條 **非公務機關應依前條界定之個人資料範圍**		一、本條新增。 二、為明確非公務機關除對個人

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管理機制。		資料檔案之資訊安全執行風險評鑑之外，亦應將業務流程納入評估範圍，爰參考歐盟GDPR第35條、金融監督管理委員會指定非公務機關個人資料安全維護辦法第5條及英國ICO問責性框架，新增本條規定。
第六條 非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制： 一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人	第四條 非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及改善機制： 一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人	條次變更，內容未修正。

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
之適當方式及內容。 二、事故發生後應受通報之對象及其通報方式。 三、事故發生後，其改善措施之研議機制。 非公務機關遇有重大個人資料事故者，應即通報國家通訊傳播委員會（以下簡稱本會）。 前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。	之適當方式及內容。 二、事故發生後應受通報之對象及其通報方式。 三、事故發生後，其改善措施之研議機制。 非公務機關遇有重大個人資料事故者，應即通報國家通訊傳播委員會（以下簡稱本會）。 前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。	
第七條 非公務機關應就下列事項，訂定個人資料之管理程序： 一、蒐集、處理或利用之個人資料包含本法第六條所	第五條 非公務機關應就下列事項，訂定個人資料之管理程序： 一、蒐集、處理或利用之個人資料包含本法第六條所	一、條次變更。 二、為促成非公務機關以去識別之匿名方式利用個人資料，以創造資料的最大價值，並平衡保障當事

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。	定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。	人不受識別之權利，爰參考日本個人資料保護法第三十六條之精神，增訂第五款，明訂非公務機關應訂定遵守本會就資料去識別標準制定之規則的管理程序。
二、檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。	二、檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。	三、原第五款至第十一款款次變更。
三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條第一項規定。	三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條第一項規定。	
四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否	四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否	

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
符合法定情形，經當事人同意者，並應確保符合本法第七條第二項規定。	符合法定情形，經當事人同意者，並應確保符合本法第七條第二項規定。	
五、依本會訂定之規則將個人資料作成無法識別特定當事人之去識別資料。	五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。	
六、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。	六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。	
七、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於	七、進行個人資料國際傳輸前，檢視	

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
委託契約或相關文件中，明確約定其內容。 八、進行個人資料國際傳輸前，檢視是否受本會相關法令限制並遵循之。 九、當事人行使本法第三條所定權利之相關事項： （一）當事人身分之確認。 （二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 （三）對當事人請求之審查方式，並遵守本法有關處理期限之規定。 （四）有本法所定	是否受本會相關法令限制並遵循之。 八、當事人行使本法第三條所定權利之相關事項： （一）當事人身分之確認。 （二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 （三）對當事人請求之審查方式，並遵守本法有關處理期限之規定。 （四）有本法所定得拒絕當事人行使權利之事由者，其理由記載及	

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。 十、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。 十一、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理。 十二、設置聯絡窗口	通知當事人之方式。 九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。 十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理。 十一、設置聯絡窗口供當事人申訴與諮詢。	

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
供當事人申訴與諮詢。		
第八條 非公務機關應就下列事項，訂定相關紀錄、證據保存機制： 一、因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之個人資料使用情況、軌跡資料及相關證據。 二、依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄： (一)刪除、停止處理或利用之方法、時間。 (二)將刪除、停止處理或利用之個人資料移轉其他對	第六條 非公務機關應就下列事項，訂定相關紀錄、證據保存機制： 一、因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之個人資料使用情況、軌跡資料及相關證據。 二、依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄： (一)刪除、停止處理或利用之方法、時間。 (二)將刪除、停止處理或利用之個人資料移轉其他對	條次變更，內容未修正。

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法修正草案		
修正草案	現行條文	說明
象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。	象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。	
第九條 本辦法自發布日施行。	第七條 本辦法自發布日施行。	條次變更，內容未修正。

資料來源：本計畫製作

第二節 中長期建議

一、持續辦理通傳事業個資法遵教育訓練及專題講座

建請通傳會未來持續為通傳業者辦理輔導訓練，並區分受眾，一方面持續對通傳業者（尤其是新進同仁）提供個資法遵教育訓練，強化對個資法基礎的理解程度；二方面為通傳業者的個資保護人員提供內稽內控進階課程，協助尚未導入個資管理制度的業者瞭解管理制度的制定基準，亦對通傳事業的稽核人員或法務人員提供內部稽核的經驗分享；三方面以資料經濟發展趨勢為主題，供通傳業者的決策、管理、研發人員掌握資料經濟下的個人資料運用趨勢。

二、持續辦理通傳事業輔導訪查或稽核作業

本團隊進行通傳業者輔導訪查時，因有許多業者仍有未落實法定告知義務、利用個人資料之適法性存疑、委外監督機制不明、安全維護措施尚待加強等情況，除持續追蹤並輔導通傳業者就相關訪查發現

進行改善外，亦建議通傳會可持續辦理通傳事業輔導訪查或稽核作業，以持續監督通傳業者落實「個人資料保護法」、「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」及其個資保護管理制度等。

此外，本團隊執行五大電信事業「個資告知義務秘密客抽查」時，發現只有一間符合個人資料保護法第 8 條告知義務相關規定，其餘四間均有改善及進步空間。建議通傳會除持續辦理電信事業「個資告知義務秘密客抽查」外，亦可持續辦理通傳事業「個資告知義務秘密客抽查」，以敦促通傳事業依照個人資料保護法第 8 條規定履行告知義務。

三、建議持續通傳產業個資管理訪查項目追蹤輔導

以中長期角度而言，關於通傳產業個人資料保護與管理實作指引手冊之工作項的主要目的，旨在提供業者個資管理資訊，建構並加強個資管理概念，並提供著手落實之路徑。然而，文字理解與實際執行難免存在落差，此外，也因應各公司業務型態及組織管理架構之差異，在手冊所提供的原則概念下，個別組織實際上的個資管理方式以及側重點皆有不同。故後續若有業者輔導訪查項目，宜對此部分進一步追蹤輔導，一方面蒐集通傳產業類別的個資管理特有型態與案例，另一方面也可協助業者更有效的以符合其公司實際需求之方式進行個資管理。

四、建議訪查實地瞭解業者實際需由及困難規劃輔導方案

從研討會中產官學各界專家所提供的實務說明及建議可看出，在資料加值應用的推動方面，通傳產業業者可能因為資料蒐集責任及新興服務適用之法規範模糊等情況而怯步。此外，目前實務在個資管理的執行方面，也面臨法遵落實過程中實務行為適法性與否不易判斷的情形。因此建議針對加值應用之推動，可以藉由訪查等方式，實地瞭解蒐集分析業者目前在資料加值應用方面所面臨的實際需由及困難，以進一步規劃擬定輔導方案。

五、建議提出修定個資保護法之跨境傳輸條款

貴會應可建議國家發展委員會修訂「個人資料保護法」中跨境傳輸條款部分，參考歐盟 GDPR、巴西、印度、美國加州、日本等研討會中討論到的國家之隱私法。考量我國個資法需保有我國隱私法之文化，惟又需與國際隱私法趨勢接軌，可按 GDPR 和其他國家隱私法中跨境傳輸要件修訂並考量保有或納入哪些我國隱私元素。

此外，由本案輔導訪查中得知近年來，通訊傳播事業涉及跨境傳輸資料比例大幅增加，通訊傳播事業業者亦日漸重視，再者 GDPR 近年來加強執行力，我國既然有跨境傳輸需求應加入眾多國家行列修定個人資料保護法。

六、建議提出國家級之資料戰略與召開資料應用 SRB 會議

我國現階段仍在積極爭取歐盟資料適當足性認定，因此掌握歐盟資料保護相關法制趨勢發展，亦能有利於我國在個資法修訂時參考依據，同時更應全面通盤思考我國未來對於國家級之資料策略，從各面向不同領域來考量，如基礎環境建構、機制標準建立、公私部門資料交流、人才培育等，還有特定領域如金融、電信、能源、醫療等資料共享與應用，由各該主管機關提出因應策略，並整合作為國家資料策略的具體行動計畫，同時亦得透過針對資料應用 SRB 策略會議之交流溝通，廣納國內產學研各方意見。

七、修訂個資法以強化企業資料運用之問責與管理

（一）將問責制納入個人資料保護法

參酌新加坡個資法修正，強化組織對個人資料的保護及問責，我國亦應將問責制納入個資法修正。現行個資法對於利用個資之組織所應遵守的義務有相當詳細規範，但卻欠缺問責的考量，主管機關要對企業進行問責與監督，則必須有個資法的授權，才能有效的要求業者擔負起個資保護的責任，並業者建立起適當的保護機制。

（二）新增資料可攜權

在數位經濟下，為促進資料流通，除了業者間的資料共享外，也需解除企業對於資料鎖定的限制，強化資料主體的控制權，促進資料市場活絡。故不僅新加坡，許多國家在修正個資法時，也紛紛將資料可攜權加以納入。此外，為了落實資料可攜，主管機關尚必須有配套的資料互通的政策，並且對於可攜的範圍也需加以界定。

（三）納入替代性爭議處理機制

由於個資爭議的態樣與專業性高，因此若僅依照一般民事法規的處理方式，由當事人自行尋求調解或和解，在專業性與信賴性方面可能有所不足；此時可於個資法中增訂處理機制的規範，連結、補充我國既有的調解制度或仲裁法規，以增加主管機關執法的彈性，由第三方爭議處理機構介入調解，以快速維護、處理當事人兼之爭議。

（四）將創新服務納入特定目的外之利用事項

參酌新加坡 PDPA 修正將創新服務納入可未經同意使用個人資料之事由，本研究建議，在我國將數位經濟發展視為重要經濟政策的同時，應參酌新加坡個資法修正內容，將創新服務的提供或開發，納入我國個資法第 20 條的特定目的外利用事項；其定義亦參酌新加坡個資法修正之附表 2，限制於業者改進既有、或開發創新商品或服務，並將之納入我國個資法施行細則中。而業者尚須配合主管機關的監督措施，具體說明其商品或服務的改進或創新之處，以提供數位創新服務更寬廣的發展環境。

八、舉辦座談會彙整通傳產業與利害關係人之需求與意見

為能有效掌握通傳資料生態圈的各方意見，建議參考金管會推動金融科技發展路線圖之策略，廣邀生態圈的利害關係人（包含通傳產業、跨產業的資料需求者、資料平台業者、廣告科技業者等）與會，可初步就下列議題交換意見尋求聚焦：

（一）業者對異業行銷之需求，如何滿足當事人的合理期待，或必

須取得當事人的同意始得為之。例如業者對當事人行銷自己的其他商品或服務(例如對寬頻上網用戶行銷居家監控服務)、業者對當事人行銷其他業者的商品或服務（例如對手機門號用戶行銷異業的旅遊商品)。

（二）業者對於資料共享之需求，注重者為匿名資料（例如不須當事人身分的行動軌跡）或非匿名資料（例如為精準行銷或建立黑名單等目的)。是否需要通傳會為業者建立資料共享平台。

（三）業者對資料交換的需求，如欲提供可識別當事人身分之資料予第三者，如何有效取得並維護當事人的同意。

（四）業者對資料可攜的態度，是否認為可促進資料流通且有益於其商業利益，並可試辦推行資料可攜政策。

九、推動通傳產業異業行銷法規修正

由於利用個人資料行銷一事涉及當事人資訊自主權的保障，如無法由跨產業主管機關間取得共識，通傳會亦不宜自行認定異業行銷的容許範圍，應有法律或法律授權之命令支持，始有正當性。

因此，通傳會應可參考金融控股公司法第 43 條促成金控集團子公司間利用客戶資料共同行銷，並據以授權金管會訂定金融控股子公司間共同行銷管理辦法之精神，提案於特別法（例如電信管理法、有線廣播電視法等）放寬通傳事業的行銷規定，例如：

「電信事業利用用戶資料為他事業行銷者，應事先向主管機關申請核准，且不得有損害用戶權益之行為。(第一項）依前項規定申請核准之程序、應備資訊、用戶資料範圍、行銷範圍及其他應遵行事項之辦法，由主管機關定之。(第二項)」。

此修法方向雖要求業者需經主管機關核准始得為異業行銷，但一經核准，即無須各別取得用戶的同意，應對業者利大於弊。

十、與跨產業主管機關合作

各別中央目的事業主管機關在個人資料保護法的規範下，各自有其對監理事業的執法任務。當涉及跨產業的資料流通時，各別主管機關將因所監理事業於該個案中扮演資料蒐集者、資料處理者或資料利

用者之不同，而有監理事項上的差異。若主管機關之間未能溝通合作而有一致性的監理標準，將可能造成單一服務過程中的不同參與者，因主管機關監理強度不同而受有相異拘束，恐無助資料經濟的發展。

因此，通傳會應與跨產業之目的事業主管機關建立定期會報或溝通機制，以共同就不同事業的同類行為協調一致性的監理標準，例如目前即可由各別產業主管機關就異業行銷的容許範圍協商基準以取得共識，俾利業者遵循。