NDC-MIS-110-002（委託研析報告）

個人資料授權應用與知情同意管理機制之研析（結案報告）

國家發展委員會編印

中華民國 **111** 年 **3** 月

NDC-MIS-110-002（委託研析報告）

個人資料授權應用與知情同意管理機制之研析（結案報告）

受委託單位：數位治理研究中心
計畫主持人：陳恭
協同主持人：戴豪君、曾憲立
顧問：朱斌妤
研究助理：徐詩雅、柯郁萱、葉雅雯

國家發展委員會編印
中華民國 **111** 年 **3** 月

目次

表次

圖次

摘要

我國「數位國家・創新經濟」以資料驅動、公私協力、以民為本的推動策略，透過獎勵機制，鼓勵機關提供創新優質服務，以有效回應民眾需求，智慧政府 2.0 重視資料價值與個人化服務，於 2020 年 7 月試營運個人化資料自主運用平臺（MyData）平臺（下稱「MyData 平臺」），2021 年 4 月正式上線，發布「個人化資料自主運用平臺介接作業要點」，民眾可於平臺經身分驗證及同意後，在個資安全與隱私保護下，享受多元化個人資料下載及線上介接服務。由於政府機關提供數位服務通常涉及各機關資料介接，而個人資料蒐集與處理屬於特定目的內利用，在進行跨機關個人資料介接時，需奠基於民眾的知情同意，近年國際社會對民眾知情同意的機制與設計甚為關注。

為落實知情同意之機制，本計畫以 MyData 平臺為例，在符合我國個人資料保護法等相關法規要求之下，研提 MyData 平臺對個人資料保護、知情同意機制、線上授權流程簡化等管理模式的改善建議與改進方向。為達前述研析目標，本計畫透過（1）文獻回顧，彙整歐盟一般資料保護規則（General Data Protection Regulation）、美國加州消費者隱私保護法（California Consumer Privacy Act）、新加坡個人資料保護法（Personal Data Protection Act）、以及亞太經濟合作會議的跨境隱私保護規則（Cross-Border Privacy Rules）體系所遵循之隱私綱領（Privacy Framework），對個人資料保護機制與法令之影響；（2）知情同意文本實驗，招募 309 位受試者以測試知情同意文件長度、圖像化呈現方式，對受試者解讀文本正確性的影響，試圖找出較佳的呈現方式與機制；（3）MyData 平臺的使用者體驗（User Experience）問題診斷，透過不同服務提供者線上申辦的流程診斷，以找出 MyData 平臺線上申辦的可能精進之作為；（4）專家訪談與座談，深度了解資料提供者與服務提供者對 MyData 平臺推動策略、個資保護方式、未來推動之建議；以及對本案所提出知情同意設計與資料保護之改善建議。綜合上述，本計畫規劃並實驗可行之知情同意形式，提出 MyData 平臺精進之作為，結果發現：（1）知情同意文件可採圖像化與階層化方式呈現，以利民眾閱讀；（2）個資稽核方式宜再優化；（3）同意管理平臺架構之規劃，仍有可精進的方向；（4）平臺服務流程再簡化，應朝資料營運者之目標；（5）因應個資生態系，個資目的外使用應完備。

對前述研究發現，本計畫具體提出短中長期建議如下：短期部分，針對知情同意管理方式建議：（1）MyData 平臺的服務條款與隱私保護政策可考慮以圖像化與階層化方式呈現，唯階層不宜過多，以三層為限；（2）可朝「特定期間」或依「年度更新會員制」驗證及授權方式，同時調整隱私權保護政策、個人化資料自主運用平臺介接作業要點等「單次同意」之內容，以減少同意疲勞；（3）優化會員專區功能，如知情同意授權方式、提供同意收執聯等；（4）建議 MyData 平臺主管機關應對服務提供者落實稽核，或預先推演當民眾發生個資危害事件，

的處置規則與流程，如發生人民向主管機關請求作出具體個案解釋時，主管機關應積極回應，以為人民釐清爭議；（5）平臺隱私政策聲明修訂方向建議增加特種資料之合法蒐集、處理或利用與特定目的外之利用；（6）針對使用者體驗建議身分驗證之方式，應由實體卡片放寬，並與各業務主管機關協商，持續精進或放寬資訊委託人或代理人制度、簡化再次造訪民眾之業務申辦流程、降低個人資料重複填寫、減少服務斷點。

中長期部分，建議 MyData 平臺應可朝向同意管理平臺（consent management platform）角色發展，提供標準化的應用程式介面與規範給服務提供者，集中管理民眾對服務提供者使用資料提供者個資所進行的知情同意。同時規劃未來法規增修方向及增修後平臺發展，如標準化圖示、撤回同意之規定、資料可攜權、接軌國際認證方式與標準、個資稽核指引等作為。

關鍵字：個人化資料自主運用平臺、知情同意、隱私保護

Abstract

Taiwan is pursuing its “Digital Nation, Innovative Economy” effort through information driven initiatives combining public and private efforts, focused on citizen centered policy promotion, deploying incentive mechanisms to encourage entities to provide exemplary innovative services. To efficaciously respond to the public’s demands, our SMART Government 2.0 offers value-added and personalized services, which began trial operations from July 2020 with the MyData platform (hereafter, “MyData”). The system was formally launched on April 2021, with concomitant release of the Personalized Data Governance Applications Platform Interface Operational Guidelines, providing regulations ensuring that after a user confirms their identity on the platform and consents, their personal data security and information protection will be assured to enjoy the diversified, personal data download and upload functional interface capabilities and services. Since government entity digital services provision often entails various entity’s information interfaces, while personal data collection and processing usually relates to specified use purposes, when allowing access to personal data between entities, it is essential to ensure the citizenry are duly informed and consent, and the international community in recent years has become rightly focused on concern with mechanisms and design ensuring citizens’ informed consent.

To implement informed consent mechanisms, this plan relies on the MyData platform in conformity with Taiwan’s regulations implementing the Personal Data Protection Act in elucidating the provisions for personal data protection in the MyData platform, informed consent mechanisms, and streamlined online consent processes, among the management mode recommendations and improvement directions. To achieve these policy study objectives, this plan relies on: (1) literature review, collating the European Union General Data Protection Regulation, the California Consumer Privacy Act from the United States, Singapore’s Personal Data Protection Act, and the APEC Privacy Framework under the Cross-Border Privacy Rules, and their impacts on personal data protection mechanisms and regulation; (2) Informed consent written experimentation, with 309 study subjects participating in varying length of informed consent provisions and graphical display, to elucidate influence on correct participant understanding of the text, seeking to elicit the optimal display method and means; (3)MyData platform User Experience related problem diagnosis, through online process diagnostics offered by different service providers, to elicit potential improvements to the MyData platform online processes; (4) Expert interviews and discussions, for in-depth elucidation of data providers and service providers’ promotional strategies for the MyData platform, personal data protection measures, and

suggestions for future promotion and development; as well as recommendations for this plan's suggested Informed Consent design and data protection. In sum, this plan's experimental determination of feasible informed consent measures, to elicit best practices for streamlining the MyData platform, found that: (1) informed consent documents can deftly rely on graphic display and heirarchical presentation, to assist the citizenry in reading and understanding; (2) personal data approval methods should be optimized; (3) the consent management platform structure planning, can still be further streamlined; (4) the platform service process should be streamlined, in the direction of information operators' objectives; (5) in response to the personal data ecosystem, uses outside existing personal data objectives should also be fully complete.

As for the aforesaid study findings, this plan specifically suggests the following short-term, medium-term, and long-term recommendations; for the short-term, it is recommended that informed consent management methods: (1) should consider the MyData platform service conditions and privacy protection policities include graphic display and hierarchical presentation, without excessive hierarchies, or less than three; (2) Efforts should proceed toward "specified times" or "annual membership renewal" means to confirm identity and obtain consent authorization, while duly amending or adjusting privacy protection policies, personalized data autonomy in use and platform interface operational guidelines for "single consent" contents, reducing fatigue from duplicative expression of consent; (3) optimize member area functions, such as the informed consent authorization means and providing consent to receive services, etcetera; (4) recommend the MyData platform administrative competent authorities ensure service providers are duly authorized, or ensure advance staging exercises in the event of personal data incidents adversely affecting the public, as to handling rules and procedures, or in the event a member of the public applies to the competent authorities for assistance in resolving specific cases, and how the competent authority should assiduously respond, so as to resolve any dispute for members of the public; (5) Platform privacy policy terms and conditions should be amended in the direction of adding lawful uses for special data, its processing or uses, along with use outside of specified uses; (6) To enhance user experience, it is recommended to adopt relaxation in identity verification by adopting a physical card, and in consultation with operational competent authorities, continue streamlining or relaxing information principal or agent systems, simplifying application processes for revisiting users, reduce duplicative personal information re-entry, and reduce service breakpoints.

Over the medium and long-term, it is recommended that the MyData platform should evolve in the direction of developing a consent management platform, offering standardized application program interfaces and guidelines for service providers, for concentrated management of expression of informed consent by members of the public

for service provider use of personal data. There should also be concomitant planning for future regulatory agendas with likely amendment directions and advances in the platform development after such modifications, such as standardized graphics, regulations governing withdrawal of consent, data portability rights, international harmonization with certification and accreditation methods or standards, and personal data audit guidelines.

Keywords: MyData, Informed Consent, Privacy Protection

第一章　緒論

第一節　研究背景

我國「數位國家・創新經濟」方案的核心理念為資料驅動、公私協力、以民為本，推動策略包含基礎環境數位化、協作治理多元化、產業營運智能化、數位服務個人化。在創新數位服務面向，透過獎勵機制鼓勵機關提供創新優質服務，有效回應民眾需求，智慧政府 2.0 重視資料價值與個人化服務，國家發展委員會（下稱國發會）於 2020 年 7 月試營運個人化資料自主運用平臺（MyData）平臺（下稱「MyData 平臺」），平臺在 2021 年 4 月正式上線，民眾可於平臺經身分驗證及同意後，在個資安全與隱私保護下，享受多元化個人資料下載及線上介接服務。值得注意的是，在個資賦權的國際趨勢下，如歐盟提出一般資料保護規則（General Data Protection Regulation, GDPR），GDPR 對於個資保護賦權概念、技術與程序要求甚嚴，與歐盟政經合作與貿易往來者都需檢視自身國內相關法規之適足性，因此，個人資料（personal data）蒐集與處理的相關議題更顯重要，已從過去被動的資料保護，轉變為主動的資料賦權（data empowerment），如：英國 Midata、芬蘭 MyData、歐盟 GDPR 與支付服務指令（Payment Service Directive 2, PSD2）[1]，及澳洲消費者資料權（Consumer Data Right）等，均涵蓋此類概念。民眾在公私部門所留存的個人資料，擁有知情同意（informed consent）後自主使用、分享與調閱刪除的主動權利，是故，相關服務的前瞻議題研析更顯重要。

由於政府機關提供數位服務（例如：MyData 平臺服務、社福補助等）通常涉及各機關資料介接，而個人資料蒐集與處理屬於特定目的內利用，在進行跨機關個人資料介接時，需奠基於民眾的知情同意。個人資料應用涉及個人資料保護法（下稱個資法）問題，目前，國內的應用領域以金融和醫療領域較為領先，前者搭配全球的開放銀行（open banking）風潮，金融監督管理委員會（下稱金管會）已於 2019 年發布開放銀行的三階段實施策略，由銀行公會與財金公司共同推動，並依循銀行公會訂定的開放業務種類和期程，訂定不同階段的開放應用程式介面（Application Programming Interface, API）技術規格與資安規範。第一階段「公開資料查詢」已於 2019 年 10 月上線；第二階段「消費者資訊查詢」與第三階段「交易面資訊」則涉及消費者個資保護，較為複雜。第二階段甫於 2021 年四月上線，第三階段則仍在規劃中。衛生福利部中央健康保險署（下稱「健保署」）也於 2019 年開發完成健康存摺的軟體開發套件（Software Development Kits, SDK），可以讓第三方服務提供者（例如各醫療院所的 App）介接健康存摺；在

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, 35-127.

使用者授權同意下，經由使用者就特定期間內的個人就醫、用藥及檢驗結果等資料，下載並提供給第三方服務提供者使用，協助進行健康管理。相關應用如臺大醫院行動服務、大樹健康 GO、WaCare 等（健保署，2019）。

MyData 平臺 2021 年 4 月正式上線後，國發會後續又發布「個人化資料自主運用平臺介接作業要點」，以該平臺為例，同意管理（consent management）機制是此平臺運作的核心功能之一，讓民眾理解對於其個人資料的處理及利用，他們有選擇權與主控權，以對此平臺產生信任。

第二節　研究目的

延續前述研究背景，本計畫主題為個人資料授權應用與知情同意管理機制之研析，主要研究目的有下列四點：

第一，彙整歐盟一般資料保護規則（GDPR）、美國加州消費者隱私保護法（California Consumer Privacy Act, CCPA）、新加坡個人資料保護法（Personal Data Protection Act, PDPA）、以及亞太經濟合作會議的跨境隱私保護規則（Cross-Border Privacy Rules, CBPR）體系所遵循之隱私綱領（Privacy Framework，下稱 APEC 隱私綱領）對個人資料保護機制與法令，在符合我國個資法等相關法規要求之下，研提個人化資料自主運用 MyData 平臺對個人資料保護、知情同意機制、線上授權流程簡化等管理模式的改善建議與改進方向。內容包含：（1）業務主管機關或個資稽核的行動指引；（2）預先因應可能之跨領域、跨部門加值服務生態體系，發展所需之同意管理平臺（Consent Management Platform, CMP）架構；（3）資料提供端—使用者—服務提供端間資料轉拋、介接之服務流程簡化等，期望能發展出跨平臺（平臺由政府或民間單位開發，以民眾個資為服務之資格確認或其他模式）、多元、豐富且合規的個人化數位服務。

第二，為優化現行 MyData 平臺數位服務流程中，個人資料之蒐集、知情同意表單或文件處理方式，避免同意陷阱（consent trap），如在快速滾動大量網頁內容時，可能不經意間錯過相關內容等人為操作之可能情事，研提包含（但不限於）授權的時間區間、單次授權方式、知情同意查閱與存取等機制改進模式與方法。

第三，透過使用者調查等形式，規劃並實驗可行之知情同意操作介面或管理平臺架構，提出精進 MyData 服務平臺設計原則，及可供政府及第三方服務提供者參考之規範指引，以提高公部門、使用者及第三方服務提供者的操作便利性與使用意願。

第四，彙整國內外作法，提供可供國內業者參考之政府或研究機構公布 GDPR 或 CBPR 體系之知情同意指引，如法規遵循、個資保護技術等內容。

第二章　文獻回顧

本章將依序說明知情同意的重要性，和民眾對於知情同意文件的不當使用與認知不足（第一節）、接著說明知情同意文件的技術面相關議題，如知情同意授權與同意範圍的相關技術及管理方式（第二節）、相關的國內外法令與規範（第三節）、最後彙整各國案例（第四節）。

第一節　知情同意的使用與認知

知情同意，或稱告知後同意原則，其做法是透過增加個資蒐集程序的透明性，使資料當事人收到完整、清楚的說明，旨在充分認識所有事實的基礎，「同意」係指資料當事人基於其意思，透過聲明或明確肯定之行動，所為具自主性、具體、受充分告知且明確之表示同意，確保經由資料主體的同意，以合意成立契約方式，來蒐集、利用個資[2]。雖然目前並未有知情同意的統一呈現方式或規範，服務提供者可自行決定並交由業務主管機關審查，但一般涵蓋四個原則，分別是使用者具理解其選擇的能力（decision capacity）、同意的紀錄（documentation of consent）、服務提供者應提供足夠的資訊揭露（disclosure）、使用者在法律認定上應為行為能力人（competency）。在前述原則之下，知情同意的樣式與種類繁多，本計畫聚焦於線上服務的知情同意，即便如此，在不同數位載具上呈現知情同意的方式也有所不同，以滾動式、彈跳式及頁面式居多，並以文字敘述為主，圖片為輔。

首先，使用認知與行為指的是使用者在閱讀知情同意文件時，使用者的行為會受到什麼原因影響。The Exchange Lab 與 Populus 的調查結果有高達 72%的民眾覺得接受 cookie 的知情同意文字很干擾（annoyed），僅有 2%的民眾不會同意 cookie 的追蹤（Feeley, 2018）。Whitley 與 Pujadas（2018）透過文獻分析、情境問卷以及訪談，將影響民眾對個人金融財務資料分享與第三方的知情同意的態度與行為之因素分為三大類，包括：（1）提供方（包括知情同意內容與條件，以及隱私政策如何被呈現，例如長度和清晰程度、相關性等）；（2）民眾個人行為（包括個人對於分享個資的利益與風險認知、知情同意內容閱讀多寡與了解程度、個人的隱私態度）；（3）社會情境（對於相關領域法規的了解與預期程度）。但該研究也發現，多數民眾並不閱讀知情同意內容，或是不甚理解到底同意了什麼、到了什麼程度，甚至多數民眾再次閱讀知情同意條款後，仍無法正確回答問題。World Economic Forum（2020）的白皮書也指出[3]，知情同意機制存在的問題

[2] 張陳弘（2019）。新興科技下的資訊隱私保護—「告知後同意原則」的侷限性與修正方法之提出。**臺灣大學法學論叢**，**47**（1），201-297。

[3] World Economic Forum (2020). Redesigning Data Privacy: Reimagining Notice & Consent for humantechnology interaction. Retrieved August 23, from http://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

都是廣泛且有據可循的，當出現點擊同意、隱私政策或條款時，大多數人會反射性地直接選擇「我同意」。研究顯示（Luger, Morgan & Rodden, 2013），大部分的民眾（使用者）並不會閱讀同意、隱私政策或條款，且有一部份民眾不能理解同意書的意思或誤解同意書的目的，條款提供的選項只有接受或放棄（leave it），使用者如果選擇放棄就等於放棄原本的服務或產品，導致使用者除了「接受」之外沒有其他選擇。以下列舉了目前告知（notices）的問題：

一、 告知的篇幅（Length of notices）

由於告知的篇幅過長，無論是線上或書面的隱私政策及條款，大部分的民眾都不願意花時間去閱讀。知情同意內容過度冗長及繁瑣，龐大資訊量會干擾到使用者去理解真正與自己相關的內容，建議應使用輔助工具，如關鍵字超連結（如**圖 1**），將條款改為檢附，使用者有興趣再點進去，讓版面簡潔明瞭。

圖 1：App Store App 隱私權超連結

資料來源：本計畫自行整理。

二、 告知的近用性（Accessibility of notices）

由於告知、隱私條款通常是律師撰寫的，內容常常包含法律術語或艱澀的文字，使用者難以理解。資訊系統學者 Luger et al.（2013）的研究指出：在英國，告知條款和條件的文件超出一般成年人所能理解的閱讀水準[4]。World Economic Forum（2020）中引用 2019 年《紐約時報》對隱私政策的研究，同樣顯示出在美國科技公司的隱私條款撰寫水準也遠遠超過美國大眾所能理解的。簡而言之，時間的投入多寡及可閱讀性成為使用者做出明智決定的罩門。以民眾的角度撰寫文字更能幫助其使用者抓住核心概念。

[4] Luger, E., S. Moran, & T. Rodden (2013). Consent for all: revealing the hidden complexity of terms and conditions. ***CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*** (pp. 2687–2696). NY: Association for Computing Machinery.

三、 頻繁的告知頻率以及流程的可擴展性將造成同意疲勞（Frequency of the notices and scalability of the process, i.e., consent fatigue）

即使把同意、隱私條款內容縮短並增加可閱讀性，但還是無法解決使用者被頻繁要求對個人資料做出決定的問題，且這些決定通常是有拘束力、持續性（lasting），重複地閱讀知情同意，將造成同意疲勞（consent fatigue）。多數使用者有視覺上的比重差異，圖片的效果大於文字，知情同意介面搭配標誌（icon），可以使民眾視線停留較久，願意繼續瀏覽文字，減少同意疲勞（consent fatigue）。

四、 告知的表示和時效性（Presentation and timing of the notices）

首次註冊服務時，使用者常在無法充分參與當前告知系統所要求的過程下，僅得做出「接受」或「放棄」之選擇。研究顯示，當使用者閱讀告知書時，會受到告知的時效性、告知書的視覺設計及其語言框架（framing language）表達方式而影響使用者決策，隨著使用者熟悉服務，使用者會希望與網站之間的互動不同於第一次註冊，使用者註冊時進行過一次知情同意，但在後續程式更新時，使用者每次都需要重新進行同意。故而得出，由於企業蒐集和利用資料的方式未達使用者一般所期望的明顯（obvious）程度，使消費者對企業產生不信任，進而領會出告知在當前模式下的問題與重要性。可將重覆性的一次性知情同意改為特定期間同意之方式，使用者在特定時間內申請相同服務時，可不用重複閱讀知情同意，以減少使用者同意疲勞的情況。

圖 2 為 IOS 系統 App store 隱私政策的階層圖，其操作介面以階層式與圖像式的方式呈現。使用者點選安裝頁面，即可下滑頁面以了解 App 隱私權，如**圖 3** 所示，App store 的操作介面使用區塊加上標誌將內容分為三大類，分別是用來追蹤您的資料（資料可能用於在其他公司的 App 和網站上追蹤您）、會與您連結的資料（系統可能會蒐集以下資料，並將其與您的身分連結）及不會與您連結的資料（系統可能會蒐集以下資料，但不會與您的身分連結），一目了然且明確告知使用者 App 存取的資料項目，並另外提供「檢視詳細資訊」，告知民眾 App 將資料處理程度（如**圖 4**）、「開發者的隱私權政策」直接連結到該廠商的隱私權政策、「更多內容」可以連結到 App 隱私權的介紹（如**圖 5**）。

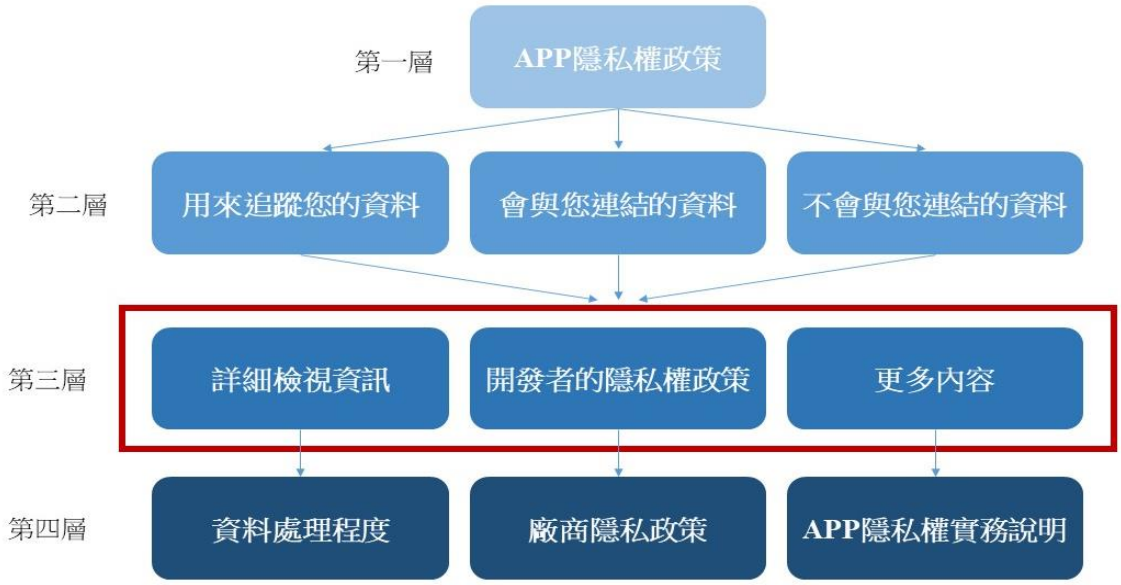


圖 2：App Store 階層圖

資料來源：本計畫自行整理。

圖 3：App Store 操作介面

資料來源：App Store。

圖 4：App Store「檢視詳細資訊」介面

資料來源：App Store。

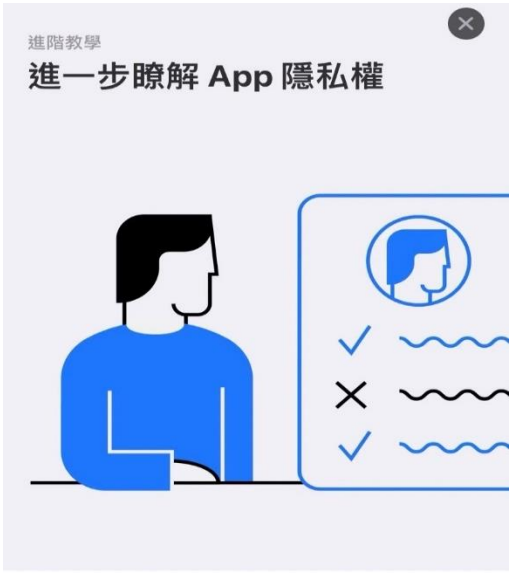


圖 5：App Store「更多內容」介面

資料來源：App Store。

另外，**圖 6** 為 Android 系統 Google Play 隱私政策的階層圖，和 IOS 相較，是將開發者隱私以階層式、列點式的方式呈現，對隱私權政策有興趣的民眾可點選開發人聯絡資訊中的隱私權政策（如**圖 7**），即可直接連結到該廠商的隱私權政策。

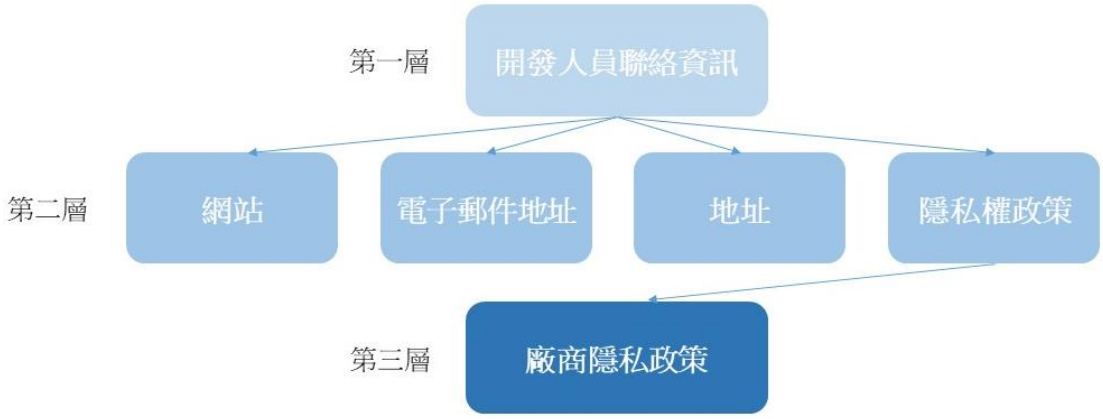


圖 6：Google Play 階層圖

資料來源：本計畫自行整理。

圖 7：Google Play 操作介面

資料來源：Google Play。

綜上所述，我們可以得知，現有的知情同意機制大多是以「使用者能夠閱讀並理解隱私權政策、能權衡服務帶來的利益與其需要被蒐集的資訊，並能夠做出明智選擇」的前提下設計的，卻忽略很多使用者在認知與行為上的限制。知情同意機制應採用「以人為本的設計（Human-Centred Design, HCD）」，透過直接與使用者接觸來了解其需求並考慮到所有參與使用的人。

第二節　知情同意的技術與管理面

一、　知情同意的技術配合

技術性問題包含兩面向，第一，同意管理平臺介面的呈現方式，不同的設計所產生的效果差異甚大，也就是使用者介面（User Interface, UI），法國個資保護主管機關國家資訊自由委員會（Commission Nationale de l'Informatique et des Libertés, CNIL）就有要求與個人資料處理相關的資訊必須被簡潔、透明地告知使用者，並應使用簡短、易懂的語句呈現（詳細案例請見本章第三節知情同意各國案例介紹）；第二，同意管理平臺應給予民眾主動權及選擇權，使用者是否可以回頭查看後臺端的資料，例如下載時間、下載範圍、甚至變更同意項目等。

由於政府數位公共服務通常會涉及個人資料應用，蒐集與處理個人資料，以MyData 平臺為例[5]，同意管理機制是平臺運作的核心功能之一，讓民眾理解對於其個人資料的使用本身具有選擇權與主控權，以對此平臺建立信任感。現行MyData 平臺經身分驗證及同意後，提供民眾多元化個人資料下載及線上介接服務，平臺未存留民眾個人資料，民眾僅當次同意下載，非永久同意資料取用，且民眾後續可於平臺查詢個人資料使用紀錄，知道個人資料運用流向。但目前MyData 平臺面對民眾僅能進行一次性的同意授權使用，無法設定同意授權期限；當涉及第三方服務（如金融、保險等服務）須同時在 MyData 平臺與服務提供端進行同意授權。部分服務需由服務提供端到 MyData 平臺下載檔案，依個人資料保護法第 6 條第 1 項無法直接向資料提供機關介接民眾的資料。若因個別服務需要，未能於八小時內下載檔案，則無法順利介接民眾同意提供之資料。

有關民眾個資交換及利用另有一案例可供參考，衛生福利部於 2011 年起建置電子病歷交換中心（E.M.R. Exchange Center, EEC），提供互通格式的電子病歷交換，並為因應公共衛生或緊急醫療或公部門給付作業需求，陸續進行跨機構系統介接，然面對如：知情同意之病人授權自主性及便利性的相關倡議、電子病歷系統及資料庫儲存安全等議題，於 2019 年針對電子病歷交換環境與存取控制進行全面性資通安全評估，王儷玲等人（2019）並提出技術架構與安全管理策略之建議。在身分識別部分，電子病歷交換皆為實名制管理，王儷玲等人（2019）所開發之手機申辦服務，透過區塊鏈技術，於民眾手機端註冊後，經過在醫院的臨櫃確認身分證件程序後，產製區塊鏈公私鑰，私鑰儲存於手機內，公鑰儲存於區塊鏈上，並綁定手機與身分證號。手機中之區塊鏈私鑰為民眾數位身分識別信物，並可作為數位簽署申請書或同意書之用；民眾於網頁調閱或下載所申請的電子文件時，必須使用雙因子身分驗證，目前以健保卡驗證，也建議可擴充自然人憑證的驗證方式。若其他服務提供端欲調閱或下載電子文件，如保險機構，同樣須以雙因子身分驗證，所用裝置為符合 FIDO 標準之 YubiKey 硬體驗證器。將來可以擴及以政府憑證總管理中心（Government Root Certification Authority, GRCA）相關憑證（工商憑證或政府憑證），是目前國內少見以手機方式完成個人資料（電子病歷）申請與授權查閱的原型（prototype）。

第三方服務部分，王儷玲等人（2019）以民眾、公務部門（法院及勞保局）及 6 家保險機構（台灣人壽、中國人壽、國泰人壽、新光人壽、富邦人壽及富邦產險）為電子文件之申請者角色。以臺北市立聯合醫院、馬偕紀念醫院（臺北及淡水）及衛生福利部雙和醫院 3 家為電子文件之釋出者角色。以中國信託金控扮演金流服務的角色，提供民眾繳費虛擬帳號機制；民眾繳費後與該服務平臺應用程式介面（API）交換繳費資訊；撥款申請費用予各醫療機構及收款交易手續費。90%的使用者（民眾）覺得線上申請及領取病歷，比親赴醫院更能節省時間及交

[5] 依個人化資料自主運用平臺介接作業要點，第一條第一項的定義：個人化資料自主運用（MyData）平臺：指由國發會建置，經自然人或法人（下稱當事人）完成身分驗證及同意後，單次即時提供該當事人個人化資料下載及介接應用之平臺。

通成本；有 80%的使用者覺得 App 使用介面設計清楚，操作相當容易；有 79%的使用者願意爾後於線上申請病歷時，支付新臺幣 10 元手續費。另有使用者建議其他功能（照護資訊授權）、同意書簽署儘早開通、操作及流程應再優化等意見回饋。

然不可忽視的是，對於新流程與系統操作的熟悉程度，將對經年習慣於審閱紙本病歷、醫院進行身分核對過程及解說的人力負荷。是故，宜對診所、區域醫院或地區醫院採分級、分階的導入。此外，考量民眾個資數位化傳遞過程，應符合資通安全管理法，甚至 ISO 27001、27701 等規範，針對健康與醫療產業的資訊安全管理需求，國際標準組織另提供了 ISO 27799:2016，指引如何保護個人健康的資訊，規範健康資訊的儲存、傳輸與防護要求，確保達成機密性、完整性、可稽核性、可用性，與隱私保護。

就線上服務提供個人資料之方式進行分析，國際間可分為以第三方提供者（Third Party Providers, TPPs），作為資料集中的「中介管理者」角色，或創建個人資料帳戶兩種方向。前者如金融領域中，例如歐盟支付服務指令（PSD2）經個人授權後可將使用者的各個銀行帳戶交由提供帳戶資訊服務（Account Information Services, AIS）之第三方提供者—帳戶資訊服務提供者（Account Information Service Provider, AISP）。使用者可由單一管理者得知個人總資產或信用。芬蘭等歐盟國家較常以創建個人資料帳戶的方式管理個人資料，使用者可自行設立該帳戶資料，業者有利用需求時，經同意後可與個別帳戶接取[6]，但如何確保個人知情權與同意權至為關鍵。

二、 資料存取控管機制

不管是政府機關或是民間機構近年都投入了大量資源來確保組織能夠符合個資法的要求，加上歐盟 GDPR 的規範，在在都顯示必須在應用系統的架構設計上，建立完善的資料存取控管（access control）機制來保護個資，可分為三個面向：所謂 3A 或 AAA（Authentication, Authorization, Accounting）（陳恭，2013）。

(一) 驗證（Authentication）

驗證是 3A 架構的第一道關卡，指的是要辨識與驗證使用者（可以是人員或程式）的身份，線上驗證使用者具有一定的挑戰，不同強度的驗證方式必伴隨不同程度的風險，各種線上服務必須斟酌風險，選用適當的驗證方式。

(二) 授權（Authorization）

其次要判定使用者是否有權使用特定的資料，授權是資訊安全與隱私保護政策管理的核心工作項目，主要精神在於根據安全政策給予使用者所能擁有的權限，使用者若不是資料當事人，則必須先取得當事人的同意（consent），才能使用。

[6] 環球生技（2020）。突破智慧健康科技資料蒐集挑戰資策會邀醫電跨界對談共尋解方，2021 年 8 月 5 日，取自：https://store.gbimonthly.com/Article/Detail/46079?lang=zh-TW。

(三) 紀錄（Accounting）

紀錄的工作項目包括量測（measuring）、監控（monitoring）、報告（reporting）各種資源使用量及事件紀錄（log），以提供後續的稽核（audit）、計費（billing）、分析（analysis）與規則管理之用，因此紀錄的主要精神在於收集必要的使用者與系統之間互動的資料，最完備的作法就是「凡走過必留下痕跡」，鉅細靡遺地記錄所有的互動。

在 3A 要求下，現行個人化服務可能存在技術與流程、法規等面向不一致與可優化的精進作為，本計畫將著重在授權（Authorization）與紀錄（Accounting）的處理。**表 1** 摘錄本研究以 3A 模式檢視現行線上個人服務的重點。

表 1：以 3A 模式檢視現行線上個人服務

	技術與流程問題	法律問題	研究目標與方法
授權	● 格式未統一 ● 各服務提供者要求民眾先完成不同的驗證程序與個資填寫，才能進行資料授權，使用體驗不佳 ● 各項服務為一次性申請與一次性授權，無法設定同意授權期限	● GDPR 規定資料主體須先知情，才能有效同意，包含控管者之身分、徵求同意的各個處理行為之目的、蒐集與處理之個資（類別）為何、有權撤回同意、利用個資以作出自動化決策之資訊 ● 申辦服務另有法律要式行為的要求	● 研究國外同意管理機制與實驗 ● 研擬使用者身分驗證機制以改善使用第三方線上服務之使用者體驗 ● 研究授權期間、目的、知情同意查閱與存取等機制改進模式與方法
紀錄	● 本人操作紀錄依資料類別之清單方式瀏覽，缺少依時間查詢等之功能 ● 授權服務提供者之紀錄與資料下載紀錄以合併方式顯示	GDPR 與電子隱私指令（Directive 2002/58/EC）都將 cookie 列為個人資料的一環	

資料來源：本計畫自行整理。

本計畫參考國際間針對 GDPR 與 CCPA 所發展的同意管理平臺與同意收執聯（consent receipt）等機制與工具，參考如新加坡政府的 SingPass App，如**圖 8** 手機畫面截圖，民眾可透過手機 App 確認個人資料、政府資訊、線上服務、身分驗證等項目，研提精進個人化服務與知情同意管理的改善方向。

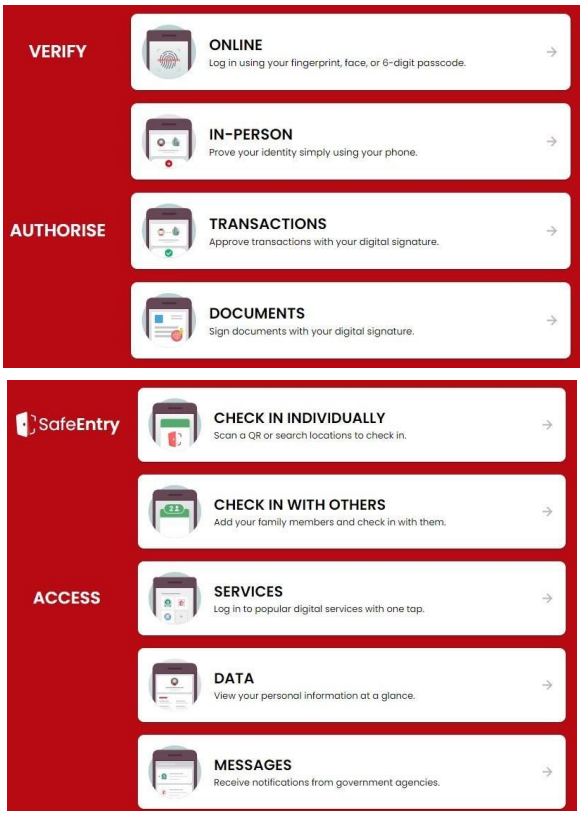


圖 8：SingPass App

資料來源：SingPass App。

三、 同意管理平臺（Consent Management Platform, CMP）

GDPR 規定了如果網站使用的資料含有「個人可辨識資料」，也就是關聯於一個已識別或可識別資料主體的任何資料（如：cookie、網路 IP 位址等）都屬於需要被保護的內容，而且資料主體可以同意其個人資料是否能使用、刪除、或搬移。然而，第一方 cookie 是每個網站的命脈，它使企業能夠記住有關資料主體的關鍵資訊並蒐集分析資料。第三方 cookie 是 AdTech 的基礎，其允許發布商通過其網站獲利，允許品牌開展廣告和行銷活動。

GDPR 規定網站的所有者需要先獲得資料主體的同意，然後才能允許在提供商品時處理個人資料、服務或監控資料主體的行為。GDPR 對網站和企業蒐集、存儲和使用這兩種類型的 cookie 的運作方式產生了重大影響，也因為 GDPR 的嚴格控管以及嚴厲懲罰，諸多大型的跨國企業、網站都逐漸開始規劃相關的應對方案，為了要讓該網站的功能以及撰寫同意書的方式能符合 GDPR 的條款，有些網站每天接待的訪問者數量眾多，因此如何有效的管理此過程的需求也就越趨重要。同意管理平臺使同意收集的過程變得更加容易，同意管理是一個協助網站符合歐盟關於同意收集的監管要求的過程。有了同意管理平臺，網站就有技術能力去告知網站的訪問者：該網站將蒐集的資料類型為何，並提前為網站的特定資料處理目的去徵求訪問者們的同意，藉此去確保網站的作為符合 GDPR 的規定。

(一) 同意管理平臺的主要作為與收集過程

Zawadziński 與 Wlosik（2020）提到，如果有以下情形發生時，網站就必須要有同意管理平臺的存在：（1）個人資料的處理：將個人的資料數據用於行為廣告、再銷售、分析、電子郵件銷售等目的；（2）自動決策：例如行為分析；（3）海外資料傳輸：當公司蒐集歐盟公民的資料以在歐盟外進行處理時。

同意管理平臺促成的一些監管義務包括：（1）向使用者顯示同意用的彈出窗口（consent pop-ups）和實用小工具（widgets）；（2）蒐集和儲存訪客所有關於同意決定的資訊，並記錄其異動；（3）在獲得同意之前，僅透過觸發接受的標籤來蒐集預先批准的資料（即只有在使用者同意後才會觸發下一步的標籤）；（4）蒐集和管理資料主題的請求，例如處理訪問者對於存取、修改、移動和刪除其資料的請求。

圖 9 為同意管理平臺收集和存儲使用者同意的過程（Zawadziński & Wlosik, 2020）。資料當事人在訪問網站時，首先會先以彈出窗口方式顯示同意的要求通知（consent pop-ups），同意管理平臺希望可以基於網站的特殊資料處理目的以蒐集訪問者資料；再來就是依訪問者所勾取的同意或不同意去存取資料，在獲得明確同意之前，同意管理平臺都還只是資料控管者（data controller），獲得同意之後才能對資料進行相關的處理（process）[7]，此時才會變成資料處理者（data processor）。

[7] 依 GDPR 第 4 條第 2 項規定，所謂「處理」係指對個人資料或個人資料檔案執行任何操作或系列操作，不問是否透過自動化方式，例如蒐集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀。

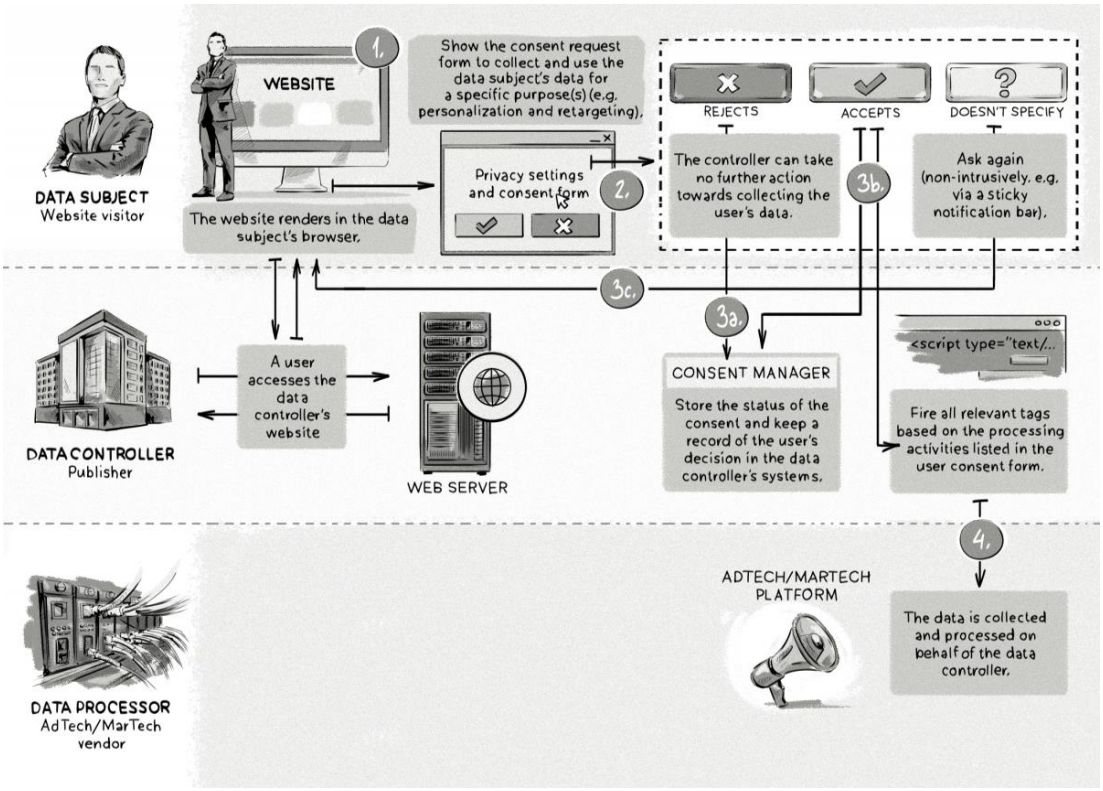


圖 9：CMP 收集和存儲使用者同意的過程圖

資料來源：https://clearcode.cc/blog/consent-management-platform/。

因為 GDPR 對於資料控管者及資料處理者的合規措施與責任有不同的規範。故常見的同意管理平臺有以下兩種特徵：

1、 資料控管者：指掌握個人資料，並決定處理個人資料之目的、用途、條件與方法者，例如蒐集、處理或利用個資之企業。資料控管者必須要合法且公平的去獲得資料，同時也要達到透明度的要求。

2、 資料處理者：依據資料控管者的指示而為實質處理資料者，即為代表控制者處理個人資料的其他主體，例如受委託之資料處理業者。當同意管理平臺被定位成資料處理者時，必須遵守 GDPR 的相關規定義務，否則就會被嚴厲處罰。

Santos、Nouwens、Toth、Bielova 與 Roca（2021）透過實證分析認為同意管理平臺承擔「控管者」的角色，因此，在以下的四種情況時應該對處理活動負責：

1、 包含額外的處理活動時；

2、 使用追蹤技術執行資料掃描和預先分類時；

3、 當默認包含第三方供應商時；

4、 當在部署知情同意過程的界面操作設計策略時。

(二) 同意管理架構

在知情同意的管理上，如**圖 10** 所示，同意管理架構由五項要素組成（PwC, 2019）：

1、 使用者互動及同意收集者（user interaction and consent collector）：

使用者與產品互動並行使同意的介面。在此介面中，使用者得知悉有哪些個人資料將被存取，使用者同時可以要求網站刪除其個人資料。

2、 同意管理者（Consent Manager）：

將獲得的同意轉化為各種類型，如同意有效性，同意義務和同意授權（consent permission），之後將不同類型之同意儲存、進行個人資料處理。同意管理者僅會儲存、並且就當前使用者行使之同意進行資料處理，但除此之外的其他資訊（例如：誰行使同意、何時同意）是由調解管理者（Reconciliation manager）儲存。

3、 資料管理者（Data Manager）：

確保個人資料蒐集與個人資料使用，遵照同意書的規定執行，方有足夠權限用於後續資料之用途和處理，並負責保護使用者之個人資料。

4、 脈絡處理者（Context Handler）：

作用為管理產生變化的新同意，並通知同意管理者和資料管理者。由於個人資料之儲存與蒐集，可能隨著時間的推移而發生變化，脈絡處理者將會檢視前後變化，並將這些變化通知給同意管理者和資料管理者。前者將會更新相關同意資訊，而後者將停止資料處理，直到接獲使用者再次授權進行個人資料使用。

5、 調解管理者（Reconciliation Manager）：

負責維護、核對與個人資料、同意有關之紀錄，要求資料處理以及收集同意皆必須合規。調解管理者記錄同意管理者如何處理使用者的同意。並持續檢視資料管理者提供的資料生命週期，包含儲存資料和共享資料等活動。此外，如有資料更改和同意撤銷，調解管理者仍會保留過去同意和資料的紀錄。

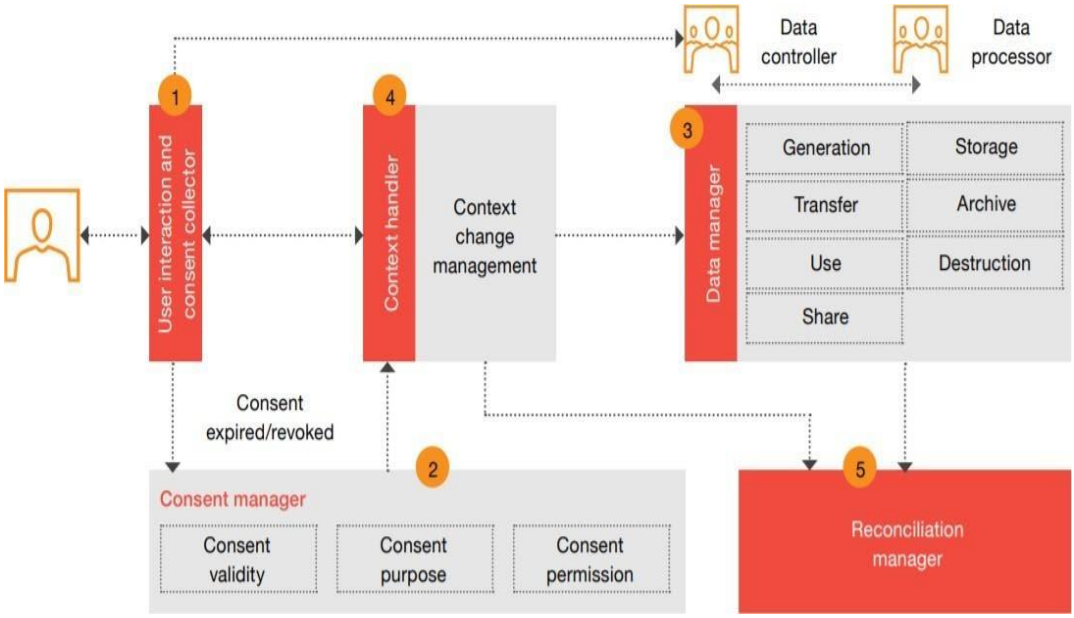


圖 10：同意管理架構圖

資料來源：https://www.pwc.in/consulting/technology/data-and-analytics/govern-your-data/insights/a-blueprint-for-robust-consent-management.html。

(三) 同意機制

圖 11 提及的同意機制將有助於開發有效之同意管理平臺，主要為提供企業去開發一個合規的同意管理平臺之指引（PwC, 2019）：

1、 分析：

分析當前的實踐之同意是否與遵照隱私架構，並評估架構中是否有任何要素需要改進。

2、 設計：

修改目前實踐之同意，並設計新的同意模板，有助於同意架構中不同單位之間資訊之流通。

3、 發展與實施：

開發在同意管理者、資料管理者和脈絡處理者之間使用的互動模型。創造行動計畫以實施同意管理流程的工具，並訓練員工使其能夠配合計畫。

4、 運作：

不斷監督同意管理過程，並根據對法規和政策標準進行必要的修改。

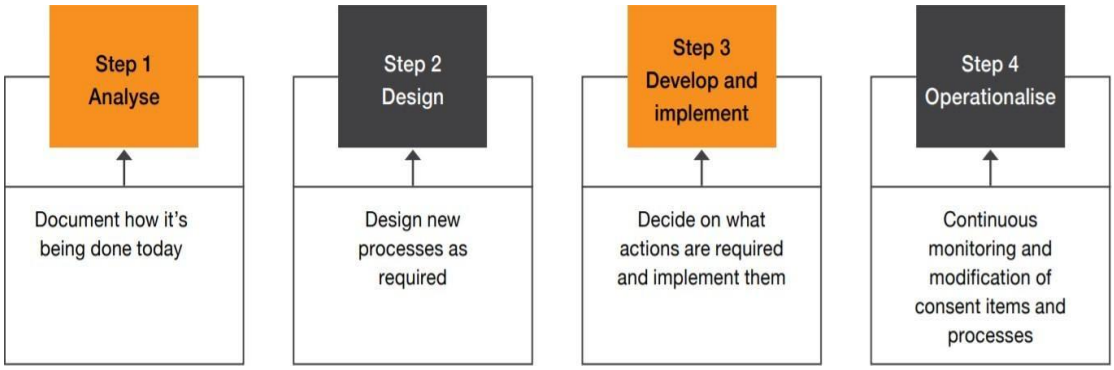


圖 11：同意機制處理步驟圖

資料來源：https://www.pwc.in/consulting/technology/data-and-analytics/govern-your-data/insights/a-blueprint-for-robust-consent-management.html。

(四) 同意管理平臺的核心功能（Zawadziński & Wlosik, 2020）

如果要成為一個具有功能性的同意管理平臺，應涵蓋整個訪問者的生命週期，從獲得新訪問者的同意到處理他們的資料主體之請求。

1、 同意書的收集：

首先，必須通知使用者他們的個人資料正在被處理。有關資料處理範圍的詳細資訊應包含在隱私政策或彈出通知（或兩者）中。同時必須讓使用者決定他們是否同意處理的具體目的。雖然GDPR沒有明確說明同意請求應該是什麼樣子，但彈出框（pop-up boxes）被認為是行業標準並且是最常見的實施方式。必須允許使用者以自由方式表示同意，且必須允許使用者有選擇地決定他們的資料可用於哪些類型的追蹤、分析和其他活動。資料的使用將僅用於使用者同意的目的及內容。

2、 記錄蒐集的資料：

可以降低GDPR對於處理資料主體請求的複雜性所造成的負擔，同意管理平臺會協助記錄以下內容：誰給予同意（個人姓名或其他標識，通常是電子郵件地址、cookie或設備ID）、獲得同意的時間（包含時間戳的線上紀錄）、使用者同意的內容（他們同意使用個人資料的具體目的列表）、是否以及何時撤回或更改同意（包含時間戳的線上紀錄）。

除了向使用者顯示的小工具及彈出窗口之外，同意管理平臺還提供了一個管理面板，可以在其中觀察和檢查所有同意和資料主體的請求。

3、 為使用者提供一種改變他們的同意和移動資料的方法：

同意管理平臺讓使用者可以自由訪問同意彈出窗口，讓他們根據特定目的調整同意決定並隨時行使其他使用權利。根據GDPR規定，有關資料主體的個人資料必須以結構化、常用和機器可讀的格式提供給使用者。這被稱為資料近用權（Right of access by the data subject）（Art.15）；且使用者必須

有權輕鬆地將此類資料傳輸給另一個控管者，資料可攜權（Right to data portability）（GDPR Art.20），也就是當事人應有權接受控管者提供以有結構的、共通使用的（commonly used）、機器可讀形式（machine-readable）的檔案。是故，同意管理平臺提供了一種處理同意決定更改的方法，如**圖12**。

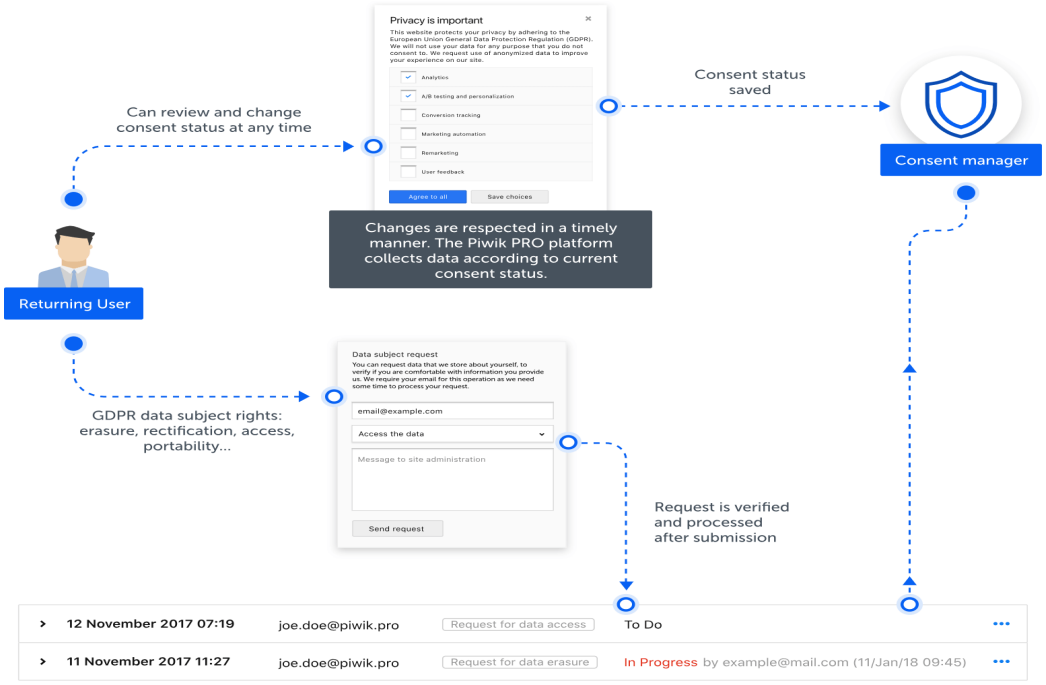


圖 12：CMP 管理使用者同意狀態

資料來源：https://clearcode.cc/blog/consent-management-platform/。

4、 透明與同意框架（Transparency and Consent Framework, TCF）：

歐洲互動廣告局（Interactive Advertising Bureau, IAB Europe, IAB）為了要能夠「標準化」蒐集和使用個人資料的同意過程而開發透明與同意框架。該框架旨在支持出版商、技術供應商和廣告商滿足GDPR所規定的透明度和使用者同意要求。

從**圖13**可以發現，透明與同意框架的運作模式可以分為三步驟：首先，發行網站從全球供應商列表中選擇它想與之合作的技術供應商，之後再安裝同意彈出視窗；再來，當使用者第一次訪問發布者的網站時，他們都會被要求選擇發布者可以與其共享資料的公司，蒐集使用者的選擇資訊並儲存在使用者瀏覽器的第一方cookie中；最後，一旦使用者做出選擇，發布者就可以與選定的技術供應商共享使用者資料。

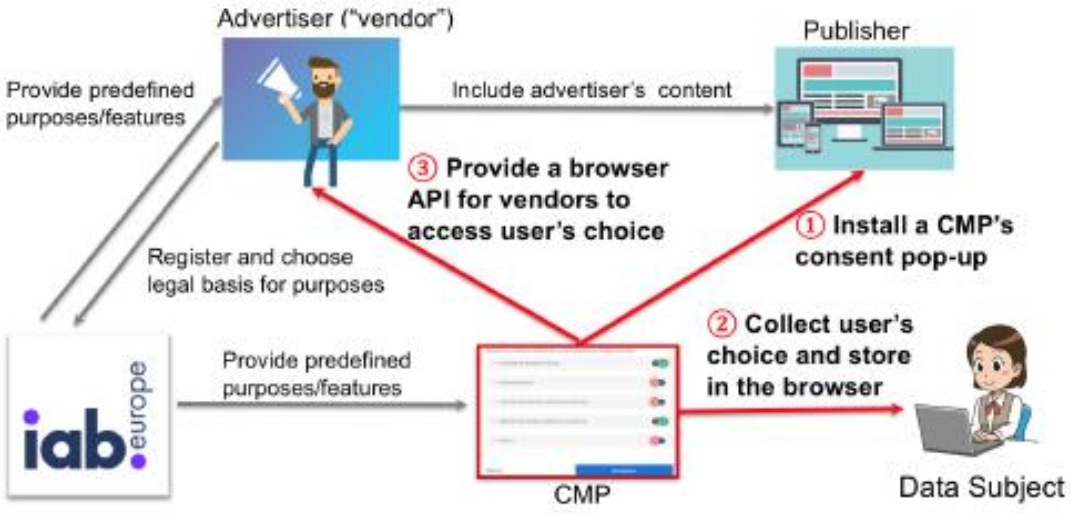


圖 13：TCF 運作模式及行動者

資料來源：https://www.ieee-security.org/TC/SPW2021/ConPro/papers/santos-conpro21.pdf。

四、 資料系統管理者（MyData operator）介紹

隨著個人資料越來越受重視，確保個人能夠瞭解和控制自己的資料也隨之變得迫切。許多廠商甚至願意免費提供服務，只為取得使用者的資料，然而，這種將服務與個人資料綑綁的做法不但會抑制競爭、削弱市場的力量，最後還可能扼殺創新。若個人沒有能力選擇不同的服務以及服務提供者，就無法產生有意義的同意，個人也會失去影響市場的權力。

此時資料系統管理者相當重要，其在信任架構或生態系統中扮演著資料來源和資料使用服務的中介。主要功能在於建立信任、創造使用者驅動的市場，使個人能夠安全地近用、管理和使用其資料，不但可自行管理，亦可委託管理者代為管理，此時管理者就可以根據該使用者之偏好代為決定。此外，管理者也掌控資料來源和使用者之間的過程，MyData 生態系統之架構如**圖 14** 所示。

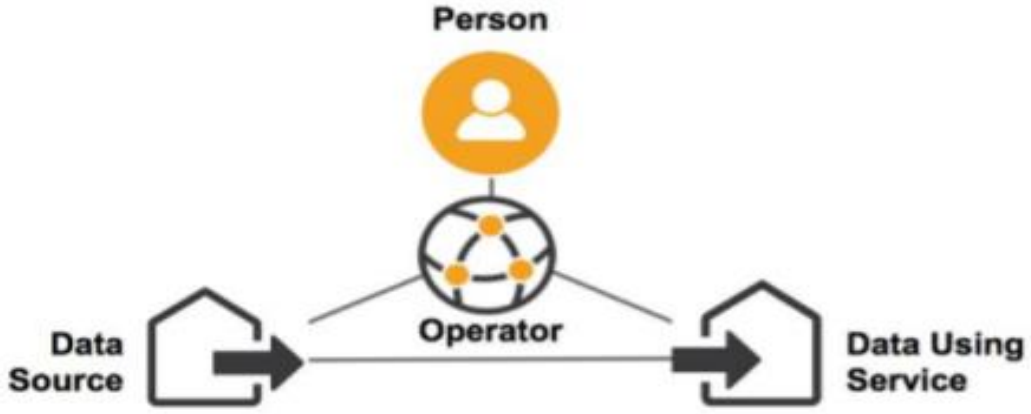


圖 14：MyData 生態系統

資料來源：https://mydata.org/mydata-operators/。

(一) 資料系統管理者的功能要件

如**圖 15** 所示，資料系統管理者的功能要素可以被分為四大類九要件。第一類型（橢圓圓框部分）主要調和（mediate）了參與者和權限方面的資料交易；第二類型（方形部分）描述 MyData 生態系統中啟用了哪些服務以及價值要如何在生態系統參與者們之間被交換；第三類型（打勾部分）主要在管理資料及其含義、交換、存取等；第四類型則為其他功能要素，主要是提供其他七個功能要素的背景脈絡，其對於生態系統的透明度及信任度至關重要。

1、 身分管理（Identity management）：

鏈接不同的身分服務提供者並將身分鏈接到權限以處理組織及個人的身分驗證和授權。

2、 權限管理（Permission management）：

使人們能夠管理、概覽資料交易和聯繫，並行使他們的合法權利。同時包括維護資料交換的紀錄（通知、同意、許可、授權、法律依據、目的、偏好等）。

3、 服務管理（Service management）：

使用連接和關係管理工具來鏈接操作員、資料源及資料使用服務。資料可以從不同的來源獲得，並且可以從多個資料使用服務當中被使用。

4、 價值交換（Value exchange）：

促進可量化及可獲取價值（貨幣、其他形式信用或聲譽）在資料交換中被創建。

5、 資料模型管理（Data model management）：

關於管理資料的語義（含義），包括從一種資料模型到另一種資料模型的轉換。

6、 個人資料傳輸（Personal data transfer）：

以標準化及安全的方式實現了資料交換與生態系統參與者之間的接口，例如開放應用程式介面（API）。

7、 個人資料儲存（Personal data storage）：

在個人的控制下，允許資料從多個來源（包括個人創建的資料）中整合進個人資料儲存區（personal data storage, PDS）。

8、 治理支持（Governance support）：

使其符合底層治理框架，並致力於個人和組織之間建立可信賴的關係。

9、 記錄日誌與課責（Logging and accountability）：

追蹤所有資訊交換的位置並創造關於誰存取什麼及何時存取的透明度。

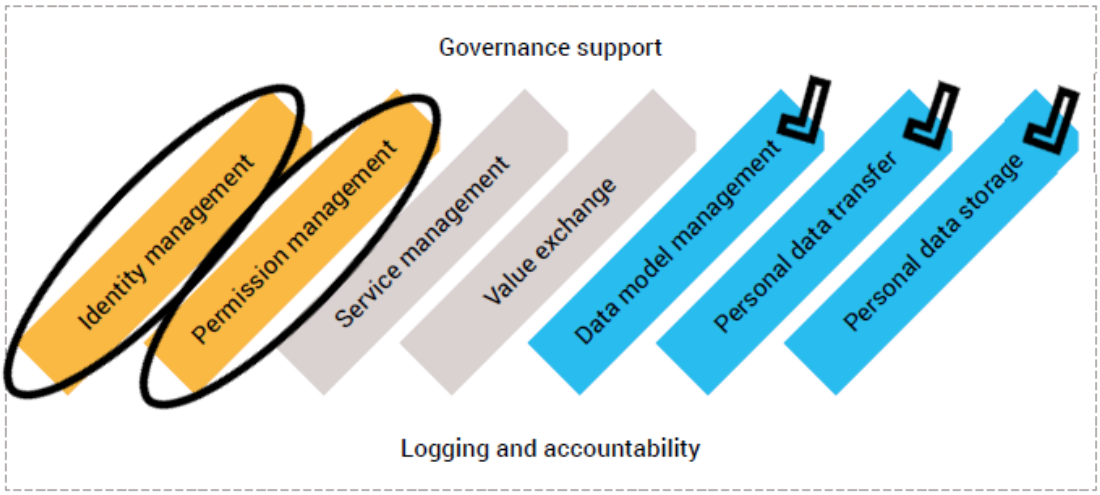


圖 15：MyData operator 的九大功能要素

資料來源：https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf。

(二) 資料系統管理者的爭議

1、 可信度：

可信度是資料系統管理者的關鍵，因為他們在生態系統中為新興的角色，與人關係最密切。因此，信任的要素有哪些、如果過程透明是重要的、要如何在大量個人資料和資料交換中確保過程透明等疑慮需再作考量。

2、 平臺獨立管理或是管理者網絡：

目前有一些平臺為使用者提供多種服務，若平臺遵守芬蘭MyData的以人為本（human centric），資料可利用性（usability of data）和開放的商業環境（open business environment）原則，是否可以被視為資料系統管理者；若不由平臺獨立管理，是否需要創造一個可互通（interoperable）的管理者網路（參照**圖16**），仍須考量。

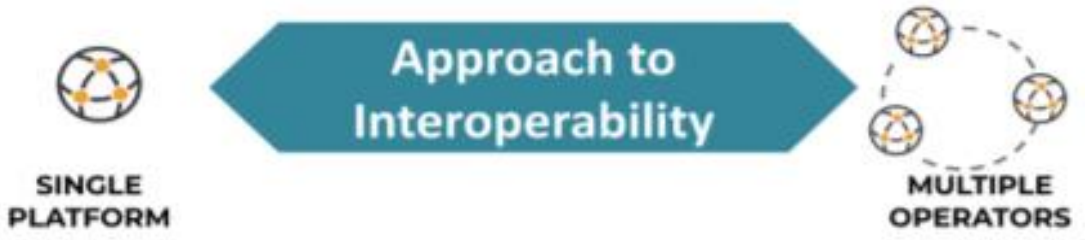


圖 16：管理型態

資料來源：https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf。

3、 管理者的商業模式：

生態系統需要由穩定的商業模式支持，才能永續經營。雖然管理者並非商業組織，但它們仍然可以進行價值交換。然而，在什麼條件下才允許營利、個人資料是否可以出售、政府在商業模式中扮演什麼角色，這些都是商業模式必須被探討的問題。

4、 互通性：

互通性是管理者網絡蓬勃發展的關鍵，內容包含資料可移植性，其能賦予使用者選擇和移動至不同資料系統管理者的權力。

5、 不同領域中的資料系統管理者是否應該不同：

如果管理者能夠滿足使用者明確的需求，將更容易被使用者接納。如同病患需要醫療服務，對資產管理有需求的人則需要金融服務。因此，如**圖17**所示，不同領域的管理者功能是否應該因應特定領域的需求而有所區別，是否應該積極創造資料的互通性，皆有待討論。

圖 17：管理之領域範圍

資料來源：https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf。

第三節　知情同意的法規面

由於民眾個人資料乃至於數位生活與消費動態成為數位足跡（digital footprint），政府與企業可從民眾資料中獲得有價值的資料經濟，然而隱私與資安的問題日益嚴重，歐盟於 2018 年 5 月正式實施「一般資料保護規則（GDPR）」，配合資料保護執法指令（Directive (EU) 2016/680 establishing rules for the protection of individuals with regard to the processing of personal data by competent authorities for purposes of law enforcement）[8]，達成個人資料保護的目標。GDPR 加強了個人對其資料處理及儲存方式的掌控權，使其得以享有重要的權利及自由，例如刪除權、同意權、知情權、資料可攜權以及拒絕權等。也就是如果一個人在不完全且易於理解的情況下，不知道處理目的而給予同意，那麼它將不是有效的同意。同時，單純沉默、預設為同意之選項或不為表示，皆不構成有效的同意。資料主體有權隨時撤回其同意（GDPR 第 7 條）（李世德，2018）。然而，有相當比例企業輕忽且未落實知情同意，民眾覺知也不足（Whitley & Pujadas, 2018），要處理 MyData 平臺同意管理機制，需讓民眾對於其個人資料的使用本身具有選擇權與控制權，本計畫認為應從我國個人資料保護法著手。個人資料保護法就當事人同意規範，分為明示同意與默示同意兩類。明示同意包括在個資法第 7 條第 1 項、個資法第 15 條第 2 款及第 19 條第 1 項第 5 款所稱同意，指當事人經蒐集者告知本法所定應告知事項（個資法第 8 條或第 9 條）後，所為允許之意思表示。

另就特種個人資料[9]之蒐集、處理及利用，則依個資法第 6 條第 1 項第 6 款進行書面同意，但當事人之同意不得逾越特定目的之必要範圍或其他法律之限制。針對「特定目的外之其他利用之同意」，規範於同條第 2 項：第 16 條第 7 款、

[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89–131.

[9] 依個人資料保護法第 6 條第 1 項所示，特種個人資料為：病歷、醫療、基因、性生活、健康檢查、犯罪前科。

第 20 條第 1 項第 6 款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。「單獨所為之意思表示」依個資法施行細則第 15 條係指，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。默示同意則指，依同條第 3 項規範公務機關或非公務機關明確告知當事人第 8 條第 1 項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第 15 條第 2 款及第 19 條第 1 項第 5 款之規定表示同意。不論明示同意或默示同意方式，均由個資蒐集者就當事人同意之事實，負舉證責任。

本計畫透過主要國際組織或國家法制政策面研議的方向，以及政府數位服務政策研析意見的看法，甚至於執法層面的規劃或作法，對於評估國內後續法制政策或個資管理規範，將有所幫助。因此本計畫將擇定歐盟一般資料保護規則（GDPR）、美國加州消費者隱私保護法（CCPA）、新加坡個人資料保護法（PDPA）及亞太經濟合作會議的跨境隱私保護規則（CBPR 體系）之隱私綱領（APEC 隱私綱領）等國際法制探討。研析如何落實知情同意及服務提供者的法規遵循原則等，以下分別說明之。

一、 歐盟一般資料保護規則之知情同意機制研析

歐盟個人資料保護立法自 1995 年公布之資料保護指令（Data Protection Directive）[10]，旨在確保人民隱私基本權。由於指令所要求事項，對會員國具有拘束力。為確保歐盟基本權利憲章（Charter of Fundamental Rights of the European Union[11]）第 8 條所規定的個人資料保護之基本權利實現，同時考量將來數位經濟的發展，由歐盟於 2015 年完成修正個人資料保護規範：一般資料保護規則（GDPR）[12]。GDPR[13]自在 2018 年 5 月 25 日開始施行，受到國際社會的高度重視，成為多個國家個資法立法或修法的圭臬。其對個人資料處理的完整規範與因應數位化資料環境，而提出的新興資料管理技術與管理措施的要求，具有重要參考價值。

歐盟 GDPR 中個人資料之處理應具自主性，為避免資料控管者與資料主體間資訊不對稱對後者個人資料保護產生負面影響，強調「知情同意」（informed consent）制度作為個人資料保護之重要基石。以透明性為前提，資料主體得以明確同意之方式使資料處理者合法處理個資，更是個人資料控制權之體現。故有效之知情同意從「知情」及「同意」二部分分析，成立要素分別為充分告知資訊義

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.

[11] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, 391–407.

[12] EU Press Release Database (2016). Building on modern and unified rules to strengthen fundamental rights and create a Digital Single Market - Joint Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the 2016 Data Protection day. Retrieved April 28, 2021, from http://europa.eu/rapid/press-release_STATEMENT-16-181_en.htm.

[13] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, 1–88.

務、透明度要求、出於自由意志同意，且同意者能力健全（兒童同意取得另有特別規定）[14]。

GDPR 規定資料主體須先知情，才能有效同意，使資料處理者合法處理個資。其資訊揭露方式可為書面、言詞、影音等，須以清楚、簡白的語言[15]，不可為冗長而難以理解的隱私權政策或法律用語聲明，及將必要資訊隱藏於其他條款中。2020 年所發布之 Guidelines 05/2020 on consent under Regulation 2016/679，該指引提及應告知之內容，包含控管者之身分、徵求同意的各個處理行為之目的、蒐集與處理之個資（類別）為何、有權撤回同意、利用個資以做出自動化決策之資訊，以及未取得適足性判定且未有適當安全維護措施而傳輸個資之潛在風險[16]。為符合 GDPR 透明性原則要求，英國資訊專員辦公室(Information Commissioner's Office, ICO）建議得使用以階層方式（layered approach）或即時通知（a just-in-time notice）[17]（如**圖 18**）作為有效的資訊揭露方式。

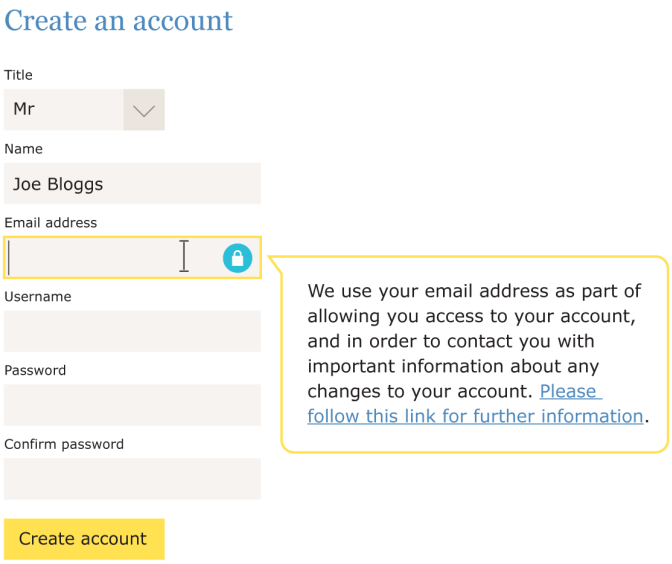


圖 18：ICO 即時通知範例

資料來源：ICO。

[14] 李沛宸（2019）。GDPR 當事人同意之實務採行建議。**商業法律與財金期刊**，**2**（1），81。

[15] 王慕民（2019）。跨境隱私管理機制—GDPR 下的透明與同意，2021 年 4 月 6 日，取自：https://www.ncc.gov.tw/chinese/files/19120/5162_42306_191202_3.pdf。

[16] 國家發展委員會（2020）。EDPB 同意指引文件中英翻譯對照：Guidelines 05/2020 on consent under Regulation 2016/679 關於第 2016/679 號規則（GDPR)中的同意之指引，2021 年 4 月 6 日，取自: https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9hNTI2ZmUyYy0wZjNlLTQ1NzAtOTFiYS1jYzkzZTExNTc0NDguc GRm&n=44CQ5paw44CRMeWQjOaEjyBHdWlkZWxpbmVzIG9uIGNvbnNlbnQgKEFkb3B0ZWQgb24gNCBNYXkgMjAyMCkucGRm&icon=..pdf。

[17] Information Commissioner's Office, ICO (2018). What methods can we use to provide privacy information? Retrieved May 19, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/.

國際個人資料保護法執法層面，對於資料驅動的數位服務，已陸續有相關執法個案出現。部分個案更引發國內外學說及實務的關注。尤其歐盟於 GDPR 已經有多個違反知情同意機制重要案例，亦有政府服務涉及違反 GDPR 而被裁罰。本計畫蒐集因個資在組織內之管理流程與技術與程序，未能達到 GDPR 第 6 條同意要求或違反 GDPR 第 13 條、第 14 條告知當事人資訊之規定而被裁罰之案件，包括歐盟各國個人資料主管機關與歐盟個資保護委員會（The European Data Protection Board, EDPB）公布之處分與歐盟法院之判例如**表 2**。

藉此實際案例之分析，研析 MyData 平臺同意管理機制與個人資料保護措施應有之規範。

表 2：違反歐盟 GDPR 知情同意機制之案件表

日期	裁罰機關	違法行為	違反法條
2019 年 1 月 21 日	法國 CNIL	● 使用者建立 Google 帳戶後，需點擊「更多選項」來修改帳戶選項，包括配置個人化廣告，Google 預先勾選個人廣告的同意選項 ● 資料當事人無法得知處理操作涉及的如 Google 搜尋、YouTube、Google 地圖等服務網站或應用程式，以及其如何進行資料的處理與組合	● 違反 GDPR 第 6 條，既不具體也不符合清楚之要求 ● 違反 GDPR 第 13 條、第 14 條告知當事人資訊之規定
2019 年 8 月 20 日	瑞典 DPA	● Skellefteå 市中學委員會利用臉部辨識查核學生出席，屬於 GDPR 第 9 條第 1 項的特種個資，未能取得當事人明確的同意	● 違反 GDPR 第 9 條第 2 項 a 款之規定
2019 年 9 月 19 日	比利時 DPA	● 線上商店因讀取電子身分證（eID）以發放會員卡，因未提供其他選擇方案給客戶，若客戶拒絕使用其 eID 來申請會員卡，無法享受優惠和折扣等於變向受到不利益。此時當事人的同意不能被視為自主提出的同意	● 違反 GDPR 第 6 條第 1 項 a 款同意
2019 年 10 月 1 日	歐盟法院 C-637/17	● 德國公司 Planet49 網站用透過網頁上預先勾選選框，讓使用者同意網站儲存和訪問 cookie，該同意為無效；使用者必須使用積極的同意（active consent）	● 違反隱私及電子通訊指令第 2 條 f 項所規範的同意與 GDPR

日期	裁罰機關	違法行為	違反法條
		● 網站未向使用者提供資訊，應包括 cookie 的操作持續時間，以及有無第三方業者可以存取 cookie 資料	第 6 條 1 項 a 款同意 ● 違反 GDPR 第 13 條 1 項與第 2 項規定控管者應提供當事人資訊
2019 年 11 月 6 日	波蘭 UODO	● ClickQuickNow SP 在取得當事人蒐集資料同意時，只要點選同意鍵即可。當客戶點選撤回同意的案件時，並非立即處理。而是寄出一封郵件，要求客戶連到其他網站，點選撤回理由後方得撤回同意	● 違反 GDPR 第 7 條第 3 項，同意之撤回應與給予同意一樣容易，並違反不得在當事人行使撤回同意時要求說明原因
2020 年 12 月 10 日	法國 CNIL	● 當使用者訪問 Amazon 網站時，Amazon 提示使用該網站即代表使用者同意 cookie 存放，而 Amazon 未明確說明 cookie 是用來發送個人化廣告、未告知使用者有權拒絕，及如何行使，也未取得使用者明確同意即存放非服務必要之 cookies ● 另外，當使用者透過其他網站廣告導向 Amazon 網站時將在未受告知且同意下被 cookie 追蹤 ● Google 在未經使用者事先同意下在其電腦中存放廣告目的之 cookies ● 當使用者訪問 Google.fr 頁面時，網頁底部資訊橫條所顯示的隱私提醒，並未提供使用者任何有關 cookies 資訊 ● 當使用者停用個人化廣告時，其中部分 cookies 仍於其電腦中執行	● 違反法國資料保護法第 82 條關於未事先取得同意，而存放對服務非必需的 cookies ● Google 設立的反對機制有部份缺陷，同樣違反法國資料保護法第 82 條
2021 年 1 月 13 日	西班牙 AEPD	● CAIXABANK, SA 在不同文件使用資訊不一內容，且隱私政策具不準確之術語，以及有關處理的個人資料類別、使用者資料，及其特定用途，與權利之	● 違反 GDPR 第 6 條基於正當利益處理的資料，以及不符合有效同意的要

日期	裁罰機關	違法行為	違反法條
		行使和資料保留期限之說明皆不夠充分 ● APED 指出 CaixaBank 在獲得使用者同意以處理其個人資料的過程中有缺陷，且將個人資料傳輸到 CaixaBank 集團內的其他公司是非法行為	件，即具體、明確和知情
2021 年 6 月 13 日	瑞典 DPA	● 針對斯德哥爾摩公共運輸（Stockholm Public Transport, SL），為其員工提供隨身攝影機，且要求 SL 員工上班期間都要戴隨身攝影機，並拍攝經過身邊所有乘客之行為，處約 156 萬歐元罰鍰	● 違反 GDPR 第 13 條未提供蒐集個資時應提供資訊 ● 違反 GDPR 第 6 條第 1 項未取得同意 ● 違反 GDPR 第 5 條第 1 項 c 款資料最少蒐集原則

資料來源：本計畫自行整理。

二、 美國加州消費者隱私保護法之知情同意機制研析

美國加州消費者隱私保護法（CCPA）[18]，於 2018 年 6 月 28 日通過。作為美國最具代表性之隱私權法，其立法目的係為消費者提供有效方式來控管其個人資料（personal information）。確保消費者享有以下權利，包含知情權、選擇退出（opt-out）權利、刪除權、近用權、資料可攜權，以及不受歧視之權利，避免如資料探勘公司等濫用個人資料、侵害消費者隱私權。為解決當初匆促通過 CCPA 所產生之內容等問題，經多次修正，於 2019 年 10 月 13 日簽署生效，並於 2020 年 1 月 1 日施行。CCPA 為美國各州首部一般性之個人資料保護法[19]，極具參考價值，佛羅里達州隱私保護法（Florida Privacy Protection Act 2021, FPPA）[20]即相當程度參照 CCPA 制定。

(一) CCPA 適用範圍

企業根據 CCPA 不得濫用居住於加州之自然人所擁有的個人資料。所謂「企業」即於加州境內有營業行為並符合以下條件之一的事業：第一，年營業額總額達 2,500 萬美元以上；第二，每年基於商業目的之購買、接收（receive）、銷售或分享超過 5 萬個消費者、家戶或裝置之個人資料；第三，每年有 50%以上營業

[18] California Consumer Privacy Act of 2018/Assembly Bill No. 375.
[19] 國家發展委員會（2019）。加州消費者隱私保護法（CCPA）規範重點說明，2021 年 5 月 18 日，取自：https://www.ndc.gov.tw/Content_List.aspx?n=48BEF57F071432E0。
[20] FPPA 雖眾議院通過，然於 2021 年 4 月 30 日被參議院否決。

額來自於銷售消費者之個人資料。滿足前述情形之一者企業所控制或分享商業品牌之關係企業，同受 CCPA 管轄。

所謂「個人資料」係指任何能直接或間接識別、關聯、描述足以合理關聯或可合理連結特定消費者或家戶之資料，包含：聯絡資訊、社會安全碼、生物識別資訊（biometric information）、商業資訊、地理位置資料、帳戶資料、學歷、商業資訊、網路或裝置識別碼，以及網路搜尋瀏覽及其他活動之紀錄等；不包含經聯邦、州或地方政府合法公開之個人資料，以及已經去識別（de-identified）或總合性（aggregate）之消費者資料。

雖然 CCPA 已明確規定僅適用於營利性質實體，不包含非營利及政府機關，然倘若政府機關定期與營利性公司簽訂契約為政府機關提供之服務收費、政府機關與私人微型移動裝置（腳踏車等）供應商簽訂契約，甚至將一些個資銷售給私營公司等情狀，此時政府機關將有可能因獨立承包商違反 CCPA 而受影響[21]。

此外，加州於 2020 年 8 月 30 日通過 AB-1281 修正案[22]，除原先賦予員工資料及 B2B 通訊資料豁免期外再延長一年：對企業在招募過程中所蒐集的求職者個人資料、緊急聯絡資訊；以及對於其他組織提供商品或服務、或進行盡職調查時，所蒐集到該組織雇員、股東、經理人之個人資料（即於 B2B 經營情境，所蒐集對方組織成員資訊）[23]。換句話說，企業目前僅需向加州員工提供有關蒐集其個人資料類別及如何使用其資料之告知（若雇主未能實施合理安全措施，員工仍有對資料外洩採取私人訴訟之權利）。須注意，AB-1281 修正案因《加州隱私權法》（California Privacy Rights Act, CPRA）通過而失效，但員工及 B2B 通訊資料豁免期因 CPRA 規定自動再延長兩年，直至 2023 年 1 月 1 日。

(二) CCPA 知情同意制度

CCPA 號稱全美最嚴格的隱私權法，賦予消費者控制其個人資料之權利，並針對蒐集消費者個人資料之企業給予責任義務。

1、 知情權：

按CCPA規定，蒐集消費者個人資料之企業，應向該消費者揭露該企業蒐集之個人資料及類別和具體內容[24]、蒐集的企業或商業用途、個人資料為「分享」之第三方（third parties）類別、「已銷售」的個人資料類別，以及銷售的每一類個資之「第三方」類別、已因商業目的（business purpose）而揭露的個資類別，以及已轉接的第三方類別等。相對來說，企業應於蒐集個

[21] Kettles, G. (2020). The CCPA's impact on public agencies. Retrieved July 13, 2021, from: https://www.jdsupra.com/legalnews/the-ccpa-s-impact-on-public-agencies-40892/.

[22] Assembly Bill No. 1281, An act to amend Section 1798.145 of the Civil Code, relating to privacy.

[23] 王德瀛（2020）。簡評加州消費者隱私保護法-規範重點與其對美國隱私保護的影響，**科技法律透析**，**32**（03），21。

[24] CCPA Art.1798.100. (a).

人資料時或前，告知消費者將蒐集個人資料之類別及類別目的，不得任意將蒐集之個人資料用於其他目的[25]。

此外，CCPA規定企業於其所提供的線上隱私權政策，應至少每12個月更新資訊[26]，包括：對消費者權利之描述、消費者向企業提交揭露請求之方法、企業所蒐集個人資料之類別及目的、列出過去12個月中蒐集、銷售或無銷售關於消費者個人資料之類別、線上隱私政策應確保企業盡告知義務，且應指示消費者如何行使其權利（特別是選擇退出權），及從消費者那蒐集的任何個人資料用於企業對消費者請求之驗證僅用於驗證目的。

2、 近用權：

消費者得請求企業免費提供近12個月內所蒐集該當事人之個人資料類型、資料來源與揭露之第三人類型，且企業應指定提供兩種以上請求方法，其中至少包括一個免付費電話號碼。若企業有經營網站，應讓消費者透過該網站申請；或提供電子郵件地址[27]。企業應於收到消費者可覈實請求後45天內回覆消費者，不得任意延長，僅有在合理必要時得再延長45天，前提應於收到請求後45天內將延長告知消費者，且企業不得以要求消費者於企業創建帳號作為提出可覈實請求之前提要件[28]。消費者得向蒐集消費者個人資料之企業要求揭露下列資訊：

(1) 其蒐集關於該消費者的個人資料類別；

(2) 個人資料正在被蒐集的事實；

(3) 蒐集個人資料之目的；

(4) 可能向其揭露個人資料之個人或組織的類型；

(5) 個人資料控管者的身分及位址，包括如何和個人資料控管者就其實踐（practices）和個人資料處理（handling）的聯絡資料；

個人資料控管者為限制個人資料的利用和揭露以及近用和更正個人資料提供的選擇和方法。

3、 選擇退出權：

消費者有權於任何時候指示向第三方銷售消費者個人資料之企業，不得銷售消費者個人資料，該權利CCPA稱為「選擇退出權利（the right to opt out）」[29]（又稱事後退出選擇權／拒絕販售權）；向第三方銷售消費者個人資料之企業應通知消費者該個資得銷售，消費者有權選擇不銷售其個人資料，並禁止企業於收到消費者指示後銷售其個人資料，除非消費者隨後為銷售其個人

[25] CCPA Art.1798.100. (b).
[26] CCPA Art.1798.125 (5).
[27] 若企業僅單純於網路營業，則僅需提供電子郵件信箱（CCPA Art.1798.130. (a).）。
[28] CCPA Art.1798.130. (a).
[29] CCPA Art.1798.120. (a)

資料提供明確之授權[30]。同時第三方不得銷售企業銷售給第三方的個人資料，除非消費者已收到明確通知，並有機會根據第1798.120條行使選擇退出的權利[31]。

企業應以消費者合理近用的形式，在企業的網站首頁（Homepage）上提供明確且顯眼之連結（不得僅在隱私政策聲明處理），標題為「不要銷售我的個人資料」（Do Not Sell My Personal Information），使消費者或消費者授權之人得選擇不銷售消費者之個人資料，而企業不得因此要求消費者創建帳號。

4、 不受歧視之權利：

企業不得因消費者行使依CCPA享有權利而歧視消費者，包括但不限於：（1）拒絕向消費者提供商品或服務；（2）對商品或服務收取不同的價格或費率，包括通過使用折扣或其他優惠或實施處罰；（3）若消費者行使權利，則向消費者提供不同級別或質量的商品或服務；（4）建議消費者將收到不同的價格或價格的商品，或服務或不同的水平或質量的商品或服務[32]（非指禁止企業向消費者收取不同價格或費率，或提供不同級別、質量的商品或服務）。

5、 財務誘因措施：

企業得就蒐集、銷售或刪除個人資料提供財務誘因（financial incentive），包括向消費者支付報酬[33]。如價格或差價與消費者資料提供給消費者之價值直接相關，企業得向消費者提供不同價格、費率之商品或服務質量。提供財務誘因之企業，具向消費者通知財務激勵措施之義務，僅有在消費者事先同意企業時，才得將消費者納入財務誘因措施。消費者可隨時撤銷。須注意，企業不得使用不公正、不合理、強制性或高利貸之措施[34]。

6、 損害賠償及民事處罰規定：

企業違反義務執行、維持與保護個人資料性質相適應的合理安全程序和做法，可因企業違反義務而未經授權近用（access）、滲透（exfiltration）、竊盜（theft）或揭露（disclosure），可對下列任何情況提起民事訴訟，要求：（1）賠償損失每起事故或實際損失不低於100美元，且每起事故或實際損失不大於750美元，以較大者為準；（2）禁制令或確認性救濟（declaratory relief）；（3）以及法院認為適當的任何其他救濟[35]。

[30] CCPA Art. 1798.120. (c)
[31] CCPA Art. 1978.115. (d)
[32] CCPA Art. 1798.125. (a) (1)
[33] CCPA 最終法規評論中提及企業以服務或產品換取資料，則該行為將受到「財務獎勵」及「價格差異（price difference）」約束，與以現金支付程度相同。
[34] CCPA Art.1798.125. (4)
[35] CCPA Art. 1798.150. (a)

企業必須在收到違法通知的30天內糾正其違法行為，又該企業未遵守上述CCPA補救規定，將對每項違法行為處以不超過2,500美元之「民事罰鍰」（Civil Penalty），或對每項故意違反行為最高可判罰7,500美元民事罰鍰[36]。

(三) 加州消費者隱私保護法施行細則（California Consumer Privacy Act Regulation 2021, CCPAR）

加州檢察長於 2021 年 3 月 15 日宣布通過加州消費者隱私保護法施行細則（California Consumer Privacy Act Regulation 2021, CCPAR），對企業應盡告知義務作出更進一步的規定，並提供「選擇退出」之標誌。

1、 選擇退出個人資料銷售權之通知（notice of right to opt-out of sale of personal information）[37]：

選擇退出之通知目的，為告知消費者其有權指示銷售其個人資料之企業停止銷售其個人資料。該通知之設計和呈現方式，應為消費者容易閱讀和理解的方式，且應以簡單明瞭的語言，避免使用技術或法律術語，同時使用特定格式，吸引消費者注意該通知，更應使該通知得以在較小螢幕上閱讀；企業以其通常商業程序或做法（ordinary course）的語言文字，向加州消費者提供契約、免責聲明、銷售公告和其他資訊。應使殘疾人之消費者得合理地獲得。對於線上提供之通知，該企業應遵循公認的行業標準，如2018年6月5日參照的全球資訊網聯盟（World Wide Web Consortium, WWWC）發布的Web內容可近用性指引第2.1版（Web Content Accessibility Guidelines, version 2.1）。最後，於其他情況下，企業應提供有關殘疾消費者如何以其他格式訪問通知之資訊。

銷售消費者個人資料之企業應當向消費者提供選擇退出權之通知，如下規定：

(1) 當消費者於網站首頁或下載並登入行動裝置頁面，並點擊「不要出售我的個人資料」連結後，企業應當發布選擇退出權之通知於其網站上。此外，通過行動應用程式蒐集個人資料之企業得提供應用程式內通知之連結，例如透過應用程式之設置目錄（setting menu）。且通知應包含「指定資訊」，或連結到包含相同資訊之企業隱私政策部分；

(2) 企業未經營網站者應建立、記錄並遵守另一種告知消費者選擇退出權的方法；

(3) 線下與消費者互動過程中銷售其蒐集之個人資料的企業，也應當通過線下方式告知消費者選擇退出的權利，並說明如何提交選擇退出請求。說明性舉例如下：第一，銷售在實體店向消費者蒐集的個人資料的企

[36] CCPA Art. 1798.155.
[37] CCPAR Art.999.306.

業，得告知消費者具有以紙本表單選擇退出蒐集個人資料之權利，或於蒐集個人資料之區域張貼標記，引導消費者於線上找到選擇退出資訊之所在地；第二，銷售通過電話蒐集的個人資料之企業，可告知消費者，在蒐集資訊時，消費者有權於通話中以口頭選擇退出。

企業應於其選擇退出權通知中包含以下內容，向消費者說明其有權拒絕（選擇退出）該企業販售其個人資料；且消費者得於線上提交選擇退出請求（request to opt-out）的互動表單，若無營運網站之企業，消費者得提交選擇退出請求的線下方法；以及消費者得提交選擇退出請求之任何其他方法之說明。

若不銷售個人資料，則企業不需要提供選擇退出的權利通知，及在隱私政策中規定不出售個人資料。企業在未發出選擇退出通知時，不得銷售其蒐集的個人資料，除非獲得消費者之肯定授權。

除了發布選擇退出權通知外，還可以使用選擇退出標誌（如**圖19**），惟不得代替發布選擇退出權通知或「不要出售我的個人資料」連接之任何要求。且該標誌的大小應與企業在其網頁上使用的任何其他標誌大致相同。

圖 19：選擇退出標誌（Opt-Out icon）

資料來源：CCPAR Art. 999.306 (f)。

2、 選擇退出之請求（requests to opt-out）[38]：

企業應提供兩種或兩種以上指定方法，以提交選擇退出請求，包括通過在企業網站或行動應用程式上名為「不要銷售我的個人資料」，為明確且醒目的連接近用互動式表單。提交該請求之其他可接受方法，包括免付費之電話號碼、指定電子郵件地址、親自提交的表格、通過郵件提交的表格，以及支持全球使用者的隱私控制（如瀏覽器擴充功能或隱私設置、設備設置或其他機制）等，這些控制能夠傳達或指示消費者選擇退出銷售其個人資料。

企業在確定消費者可使用何種方法提交選擇退出請求時，應考慮其與消費者互動之方式、企業向第三方銷售個人資料之方式、可用技術以及消費者的易用性。應至少提供一種方法反映企業主要與消費者互動之方式。

企業應盡快滿足「選擇退出的請求」，不得超過企業收到請求之日起15個工作日。企業在消費者提出請求後，但在企業滿足該要求之前向第三方銷售消費者個人資料者，應當通知第三方消費者行使選擇退出之權利，並應指示第三方不得出售該消費者個資。

倘若消費者提供消費者簽署的授權代理人書面許可，消費者得使用授權代理人代表消費者提交選擇退出請求。若代理人不能向企業提供消費者簽名的許可，證明消費者已授權他們代表消費者行事，則企業得拒絕授權代理的請求。

企業提交選擇退出請求的方法應便於消費者執行，且需要最少的步驟才能允許消費者選擇退出。企業不得使用旨在或具有顛覆或損害消費者選擇退出的重大效果的方法。其說明性示例如下：於消費者選擇退出後，企業提交選擇退出請求之過程，不得比消費者選擇同意銷售其個人資料之步驟還要多；提交選擇退出請求的步驟數目，是從消費者點擊「不要銷售我的個人資料」連結至完成請求時加以計算；而提交選擇同意銷售個人資料請求的步驟數目，為自消費者對其利益所在業務的首次指示，到選擇加入到完成請求的衡量；企業向消費者提供選擇退出選項時，不得使用令人混淆的語言，例如雙重否定（Don’t Not Sell My Personal Information）；除CCPAR允許外，企業不得要求消費者在確認其請求前點擊，或聽取（listen to）其不提交退出請求之原因；企業提交選擇退出請求的過程中，不應要求消費者提供實施請求所不需要的個人資料；最後，在點擊「不要出售我的個人資料」連結時，企業不應要求消費者搜索或滾動瀏覽隱私政策，或類似文檔或網頁的文本，以查找提交選擇退出請求的機制。

[38] CCPAR Art.999.315.

3、 授權代理（authorized agent）[39]：

當消費者使用授權代理提交知情請求或刪除請求時，企業可能要求授權代理提供證明，證明消費者已簽署請求的代理權限。企業還可能要求消費者提出：（1）直接與企業覈實自己的身分；（2）直接向企業確認其已獲得授權代理人提交請求的許可。另外，當消費者若根據「遺囑認證法（Probate Code）」向授權代理人提供委託書時，則無須提供前述證明。授權代理人應實施並維護合理的安全程序和做法，以保護消費者的個資，且不得將消費者的個人資料或從消費者那裡蒐集任何資料用於滿足消費者的要求、覈實或防止欺詐以外的任何目的。

4、 通知 16 歲以下之消費者（notices to consumers under 16 years of age）[40]：

企業應於其隱私政策中說明流程。未經13歲至15歲消費者其同意模式為選擇加入同意（opt-in），或未經其父母或法定代理人對13歲以下消費者，同意模式同為選擇加入同意，不得銷售該消費者個人資料，且無須提供選擇退出通知。

三、 新加坡個人資料保護法之知情同意機制研析

自新加坡於 2012 年 10 月 15 日通過個人資料保護法(Personal Data Protection Act 2012, PDPA 2012）後，時隔 8 年後，基於 PDPA 2012 第 5 條規定，於 2016 年成立之個人資料主管機關ー新加坡個人資料保護委員會（ Personal Data Protection Commission, PDPC)於 2020 年發布「個人資料保護法修訂草案(Personal Data Protection (Amendment) Act 2020, PDPA 2020）」[41]，該修正法案於 2021 年 2 月 1 日起將分階段生效。

新加坡個人資料保護法之立法目的，為承認個人保護其個人資料之權利，並強化個人對其個人資料之控制權。PDPA 要求涉及在新加坡處理個人資料之組織應遵守相關義務，包含課責、同意、目的限制、告知、近用與更正個資（access to and correction of personal data）、準確性（accuracy）、保留限制、保護、資料可攜權、資料外洩告知以及傳輸限制義務[42]。

[39] CCPAR Art. 999.326.
[40] CCPAR Art. 999.332.
[41] PDPA 2020 修正案中，透過修改視為同意和同意之例外條款，來避免嚴重依賴同意之高要求所造成之「同意疲勞」。
[42] Personal Data Protection Commission (n.d.). Data Protection Obligations. Retrieved July 13, 2021, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act/Data-Protection-Obligations.

(一) PDPA 適用範圍

PDPA 為規範所有私人組織（private organisations）蒐集（collection）、利用（use），和揭露（disclosure）特定人[43]之個人資料的法規。所謂「組織」（organisation）包含任何個人、公司、協會或個人團體、公司或未註冊公司，無論是否依據新加坡法律所設立，或在新加坡設有辦事處或營業地點，皆受 PDPA 規範[44]。為監督資料保護並確保組織遵守 PDPA，組織須設立至少一位資料保護長（Data Protection Officer, DPO）[45]。

而「個人資料」（personal data）係指無論真實與否，僅需為足以個人可識別之資料。雖新加坡個人資料保護法並未定義敏感（特種）個資，但新加坡衛生主管機關「健康科學局（Health Sciences Authority, HSA）」，得針對醫療院（所）自行制訂法規命令，將病歷、個人健康資料等特別加以保護與管制[46]。

(二) 例外不適用

PDPA 涵蓋以電子和非電子格式儲存之個人資料，但不適用下列情形：（1）以個人或家庭身分所為之個人活動；受雇人於其組織僱傭期間所為之活動；（2）任何政府機關，或組織於其代表政府機關之期間，蒐集、利用、公開揭露個人資料相關之行為；（3）業務工作聯絡資訊，例如姓名、職稱、公司電話、公司地址、公司電子郵件或傳真號碼或其他類似之個人資訊[47]；（4）已經存在至少 100 年的紀錄中包含的個人資料[48]，或已故當事人的個資[49]等。

(三) PDPA 知情規定

組織應在下列情況下告知當事人：

1、 於蒐集個人資料時或之前，告知蒐集、利用或揭露個人資料之目的；

2、 在利用或揭露先前未告知目的的個人資料之前，對個人告知此額外之目的；

3、 代表組織之聯繫人所提供的資訊[50]，能滿足當事人有關其個資被蒐集、利用或揭露的問題；

---

[43] 自然人。惟 PDPA 對此限縮，原則上不適用於已存在 100 年之個人資料，及已故者個人資料（關於該資料揭露部分有例外規定）。（PDPA Section 4 (4)）

[44] PDPA Section 2.

[45] Personal Data Protection Commission, (n.d.). Data Protection Officers. Retrieved November 27, 2021, from https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers.

[46] 財團法人資訊工業策進會科技法律研究所| TPIPAS 制度維運小組，新加坡個人資料保護法之現況與比較。**集保結算所雙月刊 TDCC BIMONTHLY**，（213），59。

[47] Personal Data Protection Commission (n.d.). PDPA Overview. Retrieved July 13, 2021, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.

[48] PDPA Section 4 (4).

[49] 但有關揭露個人資料規定和第 24 條個人資料保護可適用於已故 10 年或更短時間之當事人個資。

[50] PDPA Section 20.

4、 當事人撤回同意方式；

5、 當事人近用或更正其個資方式以及組織的保留政策等[51]。

在向其他組織蒐集有關特定個人資料之組織，應向該其他組織提供有關蒐集目的足夠資訊，以讓該其他組織確定揭露該資料是否符合本法的規定要求。

(四) PDPA 同意規定

1、 需要同意（consent required）：

組織應於蒐集、利用或揭露個人資料時或之前，告知當事人該行為之目的[52]，且須為合理之目的。不得於指定日（appointed day）[53]或之後蒐集、利用或揭露有關當事人之個人資料（personal data）[54]，除非當事人已根據PDPA同意蒐集、利用或揭露其個人資料；以及經PDPA或其他法律規定，該個人資料得未經同意蒐集、利用或揭露（視情況而定）。

2、 提供同意（provision of consent）：

當事人未根據本法同意組織出於某種目的蒐集、利用或揭露有關該其個人資料[55]，除非：已提供第20條所要求的資料，和當事人根據本法為此目的提供了同意書[56]。

新加坡於《PDPA關鍵概念諮詢指引》[57]（Advisory Guidelines on Key Concepts in the Personal Data Protection Act）（下稱「諮詢指引」）中規定，同意之方式包含以書面形式（表達同意）及口頭同意等多種方式獲得同意，其中在獲得口頭同意後，為證明，組織應取得個人書面（或電子方式）之確認同意形式，或於適當情況下以書面或電子形式書面證據，紀錄當事人已提供口頭同意之事實。

若組織有下列情事時，當事人的同意即屬無效：第一，組織不得以提供產品或服務為條件，要求當事人同意蒐集、利用或揭露個人資料，超出向當事人提供產品或服務之合理範圍；第二，組織以虛假或誤導性資訊、利用欺騙性或誤導性做法，獲取或試圖獲取當事人之同意[58]。諮詢指引進一步說明禁止提供虛假或誤導性資訊獲得同意，形式包含以模糊或不正確之術語、難以辨認之字體或將其放置在文檔晦澀區域等。

---

51 同前註。

52 通知目的外，應當事人要求，組織應給予其能夠代表組織回答個人有關相關問題這業務聯絡資訊。（PDPA Section 20 (1) (c)）

53 為該法指定生效日期。

54 PDPA Section 13.

55 An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose…

56 PDPA Section 14 (1).

57 Personal Data Protection Commission (2021). ***Advisory Guidelines on Key Concepts in the Personal Data Protection Act***. Singapore: Personal Data Protection Commission, 1-164.

58 PDPA section14 (2).

另外，在本法中，提及當事人為蒐集、利用或揭露有關該當事人個資而給予或認為已給予的同意，應包括代表該當事人有效行事的任何人就蒐集、利用或揭露該當事人給予或視為已給予的同意[59]。

3、 視為同意（deemed consent）：

PDPA認為以下情形，視為當事人已同意組織為蒐集、利用或揭露其個人資料：（1）若當事人沒有實際同意時，自願向此組織提供其個人資料，且為合理之行為；（2）當事人同意組織出於特定目的向另一組織揭露其個人資料時，視為同意另一組織為特定目的蒐集、利用或揭露其個人資料[60]等情形。

企業組織蒐集、利用或揭露個人資料對於訂立或執行契約或交易為必要性等特定情形下[61]，在未明確徵得當事人同意之下（且當事人未於合理期限屆滿前通知組織其不同意），向另一個組織揭露其個人資料，以利履行契約（fulfil contracts），但該組織與該當事人之間的契約中需有明示條款（express terms）[62]。該組織必須評估確定對個人資料之蒐集、利用或揭露可能對當事人產生之影響、採取合理步驟提請當事人注意相關資訊[63]，以及減少負面影響發生可能性或減輕負面影響，以及遵守其他規定之要求。

PDPA 2020修正法案中，新增「通過通知視為同意（deemed consent by notification）[64]」，若當事人已被告知蒐集、利用或揭露其個人資料之目的，但未能在合理期限內選擇退出，視為已同意。

4、 撤回同意（withdrawal of consent）：

係指當事人向組織發出合理通知時，可隨時撤回該組織為任何目的蒐集、利用或揭露其個人資料所給予或認為根據PDPA規定已給予之任何同意[65]。組織於收到該通知後，應告知當事人撤回同意可能產生之後果，並且不得禁止當事人撤回同意[66]。另外，若當事人出於任何目的撤回其同意，組織應停止（並導致資料中介者和代理人停止）蒐集、利用或揭露個人資料，除非為未經當事人同意，而PDPA或其他成文法律要求獲授權者例外。

---

[59] PDPA Section14 (4): In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data.

[60] PDPA Section 15.

[61] PDPA Section 15 (3).

[62] 財團法人資訊工業策進會科技法律研究所（2020）。新加坡國會於 2020 年 11 月通過個人資料保護法之修正案，2021 年 5 月 19 日，取自：https://stli.iii.org.tw/article-detail.aspx?tp=1&i=180&d=8580&no=64。

[63] 資訊包含該行為目的、是否為合理期限，並且當事人得以合理之方式通知組織其不同意等。

[64] PDPA Section 15A.

[65] PDPA Section 16.

[66] 但不影響提取個人資料產生之任何法律後果。（PDPA Section 16 (3)）

5、 同意之例外（collection, use and disclosure without consent）[67]：

PDPA提出例外情況下，組織得於未經當事人同意之情況下，或出於當事人以外之來源蒐集、利用或揭露有關當事人之個人資料[68]。惟蒐集前應向其他組織提供有關蒐集目的之充分資訊，以便其他組織確定該揭露是否符合PDPA規定[69]。

根據該法規定，在與個人切身利益（vital interests of individuals）、影響公眾事項（matters affecting public）、正當利益（legitimate interests）、企業資產交易（business assert transactions）、業務改善目的（business improvement purposes）[70]，或其他依據[71]時，組織得未經當事人同意下蒐集、利用或揭露其個人資料。

(五) 其他與知情同意有關規定

1、 近用權規定：

原則上，當事人得請求組織提供其被該組織擁有或控制的個人資料[72]，以及該組織在過去一年內所使用或揭露當事人個人資料之方式[73]，而該組織應於合理期限內向當事人提供相關資料[74]。然而在某些特殊的情況下，組織依法不應向當事人提供資料，例如組織在未經當事人同意之情況下，依法向執法機關揭露該個人資料[75]。除此之外，還包含該個人資料涉及當事人或其他人的人身安全與身心健康、[76]`違背國家利益[77]以及有洩露他人個人資料或身分之虞[78]等情形，組織在提供資料前，經合理評估後認為以上情形有可能會發生時，應拒絕當事人提供資料之請求。

除了上述情形之外，PDPA 亦於附表五列舉了不需提供資料之例外情形，大致上可劃分為 3 種情形，首先涉及訴訟程序、仲裁或調解程序等受法律保障之個人資料[79]，組織不需向當事人提供；第二，尚未公布的考試成績與用於評估目的的意見資料[80]，這類資料因其特殊性，組織亦不需向當事人提供；第三，當事人的不合理請求，這類情形通常會干擾到組織的

67 PDPA Section 17.
68 PDPA Section 17 (1).
69 PDPA Section 20 (2).
70 PDPA FIRST SCHEDULE, Collection, use and disclosure of personal data without consent.
71 PDPA SECOND SCHEDULE, Additional base for collection, use and disclosure of personal data without consent.
72 PDPA Article 21(1)(a).
73 PDPA Article 21(1)(b).
74 PDPA Article 21(1).
75 PDPA Article 21(4).
76 PDPA Article 21(3)(a)(b).
77 PDPA Article 21(3)(e).
78 PDPA Article 21(3)(c)(d).
79 PDPA Fifth Schedule 1(d)(e)(f)(h)(i).
80 PDPA Fifth Schedule 1(a)(b).

運作，並造成組織須承受不合理之費用或負擔，故 PDPA 第 21 條第 2 項明文排除這類請求[81]。

2、 傳輸限制（transfer limitation obligation）：

PDPA 原則禁止個人資料的跨境傳輸，若有符合 PDPA 所定之要件，則例外允許跨境傳輸[82]。依據 PDPA 第 26 條第 1 項之規定，組織如有進行跨境傳輸個人資料的需求，首先該組織須以 PDPA 之規定為基礎，建立並實行一套針對個人資料跨境傳輸之保護標準，其次，該保護標準對於個人資料的保護程度須與 PDPA 水準相當。

PDPA 第 26 條第 2 項給予 PDPC 豁免的權限，有進行跨境傳輸個人資料需求的組織得向 PDPC 提出申請，PDPC 審查通過後，會以書面通知該組織，針對 PDPA 第 26 條第 1 項之規定予以豁免[83]。除此之外，PDPC 亦可依個案之不同，視情形增加、更改或撤銷本條之要求[84]。

四、 亞太經濟合作會議的隱私綱領研析之知情同意機制研析

亞太經濟合作組織（Asia-Pacific Economic Cooperation, APEC）於 2011 年通過了 APEC 跨境隱私保護規則（CBPR 體系）。該體系具自願性、可執行性，基於課責制之特色，通過制度化機制處理隱私保護等議題[85]，以確保 APEC 經濟體間尊重隱私之資料流（data flows）。

CBPR 體系建立一套標準原則，目的在於為提高消費者信心及確保電子商務之增長和創新合作，以促進亞太地區內有效之資訊隱私保護和資訊自由流通。同時尊重會員體國內法律法規、適用國際資訊隱私保護綱領，以及加強亞太地區資訊安全[86]。若要成為 CBPR 體系之成員，首先須為 APEC 會員經濟體（member economy）、參與跨境隱私執法機構協議（Cross-border Privacy Enforcement Arrangement, CPEA）[87]、將國家法律體系對應到 APEC 隱私綱領（APEC Privacy Framework 2015）之原則規定、建立當責機構（Accountability Agent, AA），審查申請之企業有無符合 APEC 隱私綱領，並給予標章受到持續監督[88]。

---

81 PDPA Fifth Schedule 1(j).
82 PDPA Article 26(1).
83 PDPA Article 26(2).
84 PDPA Article 26(4).
85 陳宏志（2017）。網路無國界，跨境個資傳輸如何管—以 APEC CBPRs 為例，**科技法律透析**，**29**（8），31。
86 CBPRs (2011). Cross-border data flows are a vital part of our vibrant and growing digital economy in the Asia-Pacific region. Retrieved May 25, 2021, from http://cbprs.org/consumers/.
87 為一種實用多邊機制，透過創建一架構，隱私執法機構可在自願的基礎上共享資料、請求和以某種方式提供幫助。（APEC Privacy Framework Principle 13.）
88 張瑞星（2019）。臺灣個人資料保護與管理制度（TPIPAS）之現況與挑戰，2019 年 11 月 26 日，取自：https://www.ncc.gov.tw/chinese/files/20011/5162_42529_200110_5.pdf。

通過 CBPR 體系，該 APEC 經濟體之參與企業和政府確保個人資訊跨境傳輸時，應遵循 APEC 隱私綱領規定之標準。我國於 2018 年獲准加入 CBPR 體系，我國並於 2021 年 6 月 3 日獲准財團法人資訊工業策進會成為 CBPR 體系當責機構（AA）。我國係繼美國、日本、新加坡、南韓之後，第 5 個擁有當責機構的 APEC 會員經濟體[89]。應針對 APEC 隱私綱領中知情同意制度部分，與他國比較分析，為確保我國於 APEC 隱私綱領規定下之法律調和，進行個人資料告知、蒐集限制個人資料利用等知情同意機制相關規定之研析。

(一) APEC 隱私綱領

APEC 隱私綱領旨在推廣亞太地區的電子商務，重視實務運作以及資訊隱私保護，平衡資訊隱私（information privacy）、企業需求和商業利益，同時調和各會員經濟體之文化及其他各種差異性[90]。該綱領提供清楚明白的指導方向，使企業組織在符合 APEC 隱私綱領原則情況下認知到消費者之隱私利益[91]。

APEC 隱私綱領著重對個人資料（personal information）執行適當隱私保護措施，特別是避免個人資料受侵害後果和濫用個人資料；促使於 AEPC 會員經濟體內蒐集（collection）、近用（access）、利用（use）或處理（process）資料的全球性組織在其組織內部制定和執行近用和利用個人資料之全球化標準程序；授權隱私執法機構[92]履行其保護個人隱私之職責；推動國際和區域機制，包括 APEC CBPR 系統，以促進和加強隱私，並維持各會員經濟體間及其貿易夥伴的資訊流；鼓勵組織對其控管的所有個人資料負責；促進隱私綱領與其相關實施措施（CPEA 和 CBPR 系統）以及其他地區隱私協議間互用性（interoperability）[93]。

(二) APEC 隱私綱領適用範圍

APEC 隱私綱領為規範個人資料控管者（personal information controller）於蒐集、持有（holding）、利用、傳輸（transfer）或揭露（disclosure）個人資料之規定[94]。主要適用於自然人之個人（natural living persons）資料保護，不適用於法人（legal persons）。

所謂「個人資料控管者」係指蒐集、持有、處理、利用、傳輸或揭露的個人或組織（persons or organizations）[95]，以及授權他人代為蒐集、持有、處理、利

[89] 國家發展委員會（2021）。我國獲准設立 APEC 跨境隱私保護規則（CBPR）體系當責機構，2021 年 7 月 13 日，取自：https://www.ndc.gov.tw/nc_27_35052。
[90] APEC Privacy Framework Preamble 6.
[91] APEC Privacy Framework Preamble 7.
[92] 定義於第 14 原則，指負責執行隱私法並有權進行調查和／或進行執法程序之任何公共機構（public body）。
[93] APEC Privacy Framework Preamble 8.
[94] 在適用上基於各會員經濟體兼社會、文化、經濟和法律的差異，應彈性地執行 APEC 隱私綱領所訂立之原則。並且需注意有關隱私保護例外原則，包括與國家主權和安全、公共安全和政策相關者在適用上應限縮與例外條款相關之目的並符合比例原則；以及為公眾所知悉或符合法律規定。（規定於第 17 原則及第 18 原則）
[95] 無論為政府機構或私營機構皆適用。

用、傳輸或揭露個人資料者。APEC 隱私綱領不適用於受他人指示而為前列行為者，亦不包括因個人之私人、家庭事務而蒐集、持有、處理或利用個人資料者[96]，例如個人持有通訊錄和電話簿或準備家庭聯絡（prepare family newsletters）[97]。而「個人資料」係指任何有關可識別個人或足以識別該個人之資料[98]。

另外，公開可獲得之資料（publicly available information）APEC 隱私綱領認為不需要受告知及選擇要求（notice and choice requirements）規定所規範。所謂「公開可獲得之資料」為當事人明示同意公開或是經由下列合法途徑取得的個人資料：（1）合法公開之政府檔案；（2）新聞報導；（3）依法公開之個人資料[99]。

(三) APEC 隱私綱領知情同意制度

個人資料之蒐集應限於與蒐集目的相關的資料，依合法或公平的方式為之，並在適當情況下告知或取得當事人同意（with notice to, or consent）[100]；個人資料之利用（包括傳輸或揭露）僅限於與蒐集目的一致或相關的範圍內，但若為取得當事人同意、為提供當事人所要求之產品或服務所必要者、或法律明文規定者[101]。

1、 告知原則（notice）：

個人資料控管者對於其所蒐集和持有之個人資料應要向當事人提供清楚且易於近用的聲明（statements），該聲明應包含以下資訊[102]：

(1) 個人資料正在被蒐集的事實；

(2) 蒐集個人資料之目的；

(3) 可能向其揭露個人資料之個人或組織的類型；

(4) 個人資料控管者的身分及位址，包括如何和個人資料控管者就其實踐（practices）和個人資料處理（handling）的聯絡資料；

(5) 個人資料控管者為限制個人資料的利用和揭露以及近用和更正個人資料提供的選擇和方法。

應採取合理措施以確保個人資料被蒐集前或蒐集時，提供此類通知。否則當無法於蒐集前或蒐集時立即告知當事人時(例如當事人行為造成電子科技自動地蒐集其個人資料，如使用cookies時），應於切實可行的情狀下，盡快提供此類告知[103]。此外，當個人資料之來源非自當事人，而來自第三方時，亦不適用於蒐集前或蒐集時告知當事人前述通知，例如保險公司基於提供醫

96 APEC Privacy Framework Principle 10.
97 APEC Privacy Framework Commentary 10.
98 APEC Privacy Framework Principle 9.
99 APEC Privacy Framework Principle 11.
100 APEC Privacy Framework Principle 24.
101 APEC Privacy Framework Principle 25.
102 APEC Privacy Framework Principle 21.
103 APEC Privacy Framework Principle 22.

療保險服務之目的而向僱傭人蒐集員工之個人資料。除此之外，蒐集及利用公開可獲得的資料，或業務聯繫資料，已識別當事人企業中的專業能力在時（例如名片），不適用於告知原則。

2、 當事人自主原則（choice）：

於適當的情況下，個人資料控管者應提供當事人清楚明白、淺顯易懂、可近用和可負擔之機制（此機制得以電子格式、書面或其他方式為之，且應將該機制容易性及方便性納入考量），使當事人就其蒐集、利用和揭露其個人資料方面做出選擇[104]。

3、 課責原則（accountability）：

個人資料控管者應負責確保APEC隱私綱領原則之實踐。於傳輸個人資料於無論國內或國外之第三方時，個人資料控管者應取得當事人之同意，或必須竭力確保該第三方會採取和APEC隱私綱領一致的措施，以保護個人隱私資訊之安全[105]。為確保個人資料控管者對其持有的個人資料負責，制定隱私管理計畫為有用方法之一。

五、 我國個人資料保護法

我國 2015 年新修正個人資料保護法（下稱個資法），其立法目的為規範個人資料之蒐集、處理[106]及利用[107]，以避免人格權受侵害，並促進個人資料之合理利用。個資法賦予個人資料之本人知情、請求查詢、閱覽或製給複製本（請求閱覽或製給複製本權）、補充更正（更正權）、請求停止蒐集、處理或利用和請求刪除（拒絕和刪除）等[108]，上述權利不得預先拋棄或以特約限制。

(一) 個資法適用範圍

適用個資法之主體包含依法行使公權力之中央或地方機關或行政法人之公務機關，及指自然人、法人或其他團體之非公務機關；另外受「公務機關或非公務機關（下稱「機關」）」委託蒐集、處理或利用個人資料者，於個資法適用範圍內，視同委託機關。

機關在中華民國領域內外對中華民國人民個人資料蒐集、處理或利用者，適用個資法。於我國領域內有違反個資法之行為，無論是否為中華民國人民原則上

104 當僱傭人基於僱傭關係而利用受僱者個人資料時，無須提供選擇機制，例如一機構欲將其人力資源的資料集中化處理。

105 APEC Privacy Framework Principle 32.

106 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

107 利用：指將蒐集之個人資料為處理以外之使用。

108 另有「限制使用權利」。

皆適用個資法；至於於我國領域外，僅有從事蒐集、處理或利用個人資料者為我國之機關，或者該個人資料為我國人民之個人資料者始有個資法之適用[109]。

所謂「個人」，指現生存之自然人[110]，個人資料包含指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式[111]識別該個人之資料[112]。其中病歷、醫療、基因、性生活、健康檢查及犯罪前科為特種資料，原則上不得蒐集、處理及利用，除特種資料以外之個人資料下稱「一般個人資料」。

(二) 不適用個資法之資料

1、 自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料；

2、 以及於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料[113]；

3、 匿名化資料非屬我國個資法所稱之個人資料[114]；

4、 死亡者個人資料；

5、 法人資料。

(三) 合法蒐集、處理或利用個人資料

個資法第 5 條明文規定：「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」。換句話說，合法的個人資料蒐用，機關應向資料當事人通知法定告知事項，取得經當事人充分知情後之同意；在資料蒐集最小化原則下，蒐用行為須有特定目的或法定特定目的外之情形，不得逾越必要範圍內。個資法採告知後同意機制以保障資料當事人資料自主權，以下對個資法中「知情權」、「同意」、「合法行銷行為之拒絕權」、「特定目的外之利用」、「特種資料」規定，分別說明：

1、 知情權：

個資法第7條規定，蒐集者在取得資料當事人同意前，有告知義務。針對知情權規定，個資法區分機關欲蒐集之個人資料由當事人提供或非由當事

109 李世德（2018）。GDPR 與我國個人資料保護法之比較分析。**台灣經濟論衡，16**（3），74。

110 個人資料保護法施行細則第 2 條規定。

111 指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

112 涵蓋網路識別碼。

113 個人資料保護法第 51 條規定。

114 李世德，同註 109。

人提供，因此是否為個人資料之當事人所提供，將產生不同的應告知事項、免為告知之事項，及告知之時間，相關整理如**表3**：

表 3：我國個人資料保護法知情權整理

	蒐集由當事人提供之個人資料（直接蒐集）	蒐集非由當事人提供之個人資（間接蒐集）
法條	個資法第 8 條：「公務機關或公務機關依第 15 條或第 19 條規定向當事人蒐集個人資料時，應明確告知當事人下列事項…」	個資法第 9 條：「公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知…」
應告知之事項	1、 公務機關或非公務機關名稱 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	1、 個人資料來源 2、 公務機關或非公務機關名稱 3、 蒐集之目的 4、 個人資料之類別 5、 個人資料利用之期間、地區、對象及方式 6、 當事人依第三條規定得行使之權利及方式
免為告知之情形	1、 依法律規定得免告知 2、 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要 3、 告知將妨害公務機關執行法定職務 4、 告知將妨害公共利益 5、 當事人明知應告知之內容個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響	1、 依法律規定得免告知 2、 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要 3、 告知將妨害公務機關執行法定職務 4、 告知將妨害公共利益 5、 當事人明知應告知之內容 6、 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響 7、 當事人自行公開或其他已合法公開之個人資料 8、 不能向當事人或其法定代理人為告知 9、 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐

	蒐集由當事人提供之個人資料（直接蒐集）	蒐集非由當事人提供之個人資（間接蒐集）
		集者依其揭露方式，無從識別特定當事人者為限 10、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料
告知時間	蒐集個人資料時完成告知	依個資法第 9 條第 1 項規定，通知應於處理或利用前，惟又依同條第 3 項規定告知得於首次對當事人為利用時併同為之，故告知時間點即為「利用時間點前」
告知方式	得以言詞、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	

資料來源：個人資料保護法。

按個資法第8條第1項規定，機關依第15條或第19條規定向當事人蒐集個人資料時，應盡告知義務。當機關依同法第16條或第20條規定對當事人之個資為特定目的外之利用時，除第7條第2項規定第16條第7款及第20條第1項第6款「經當事人同意」事由，機關須向當事人明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響外，對於其他事由，個資法無規定機關法定應告知之事項。簡言之，除經當事人同意外，其他特定目的外之利用事由的情形下，機關對當事人不負告知義務。

2、 同意：

機關對於個人資料的蒐集、處理或利用，除有其他法定原因外，應經當事人同意：

(1) 告知後同意和明示同意：

公務機關及非公務機關得分別依個資法第15條第2款、第19條第1項第5款規定經當事人同意後，對當事人之一般個人資料為蒐集或處理。此所稱之同意，依同法第7條第1項規定，指當事人經蒐集者（公務機關及非公務機關）明確告知本法所定應告知事項後，所為允許之意思表示，此即明示同意。另外，同法第6條第1項但書第6款規定，若機關經當事人書面同意得例外蒐集、處理或利用特種資料[115]。

[115] 但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

(2) 推定同意：

指同法第7條第3項規定，公務機關或非公務機關於蒐集、處理及目的內利用本人之個人資料時，已明確告知當事人應告知事項，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已表示同意。

(3) 特定目的外利用個人資料之同意：

原則上，機關對一般個人資料之利用，應與蒐集之特定目的相符（當蒐集者為公務機關時應於執行法定職務必要範圍內為之）。惟依同法第16條第7款、第20條第1項第6款規定，機關取得當事人同意時屬例外情形，得合法於特定目的外利用。此所稱之同意，依第7條第2項規定，指當事人經蒐集者明確告知特定目的外之其他處理或利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。即機關須向當事人明確告知特定目的外之其他處理或利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示[116]，且該同意須為明示同意。

個資法第7條對於當事人同意，僅規定蒐集者有告知義務，至於是否尚須具備其他要件方為有效之同意，並無明確規定。唯針對蒐用特種資料時有須經當事人「書面」同意之明文規定，及個資法施行條例說明特種資料的「書面」同意方式，依電子簽章法規定得以電子文件為之；而一般個人資料蒐用之同意，於2015年三讀通過的個資法修正案中規定，不再限於書面方式。此外，同意存在與否之事實，蒐集者依同法第7條第4項規定，負舉證責任。

3、 請求停止蒐集、處理或利用及「合法行銷行為」之拒絕權：

個資法並未針對拒絕權作出明文解釋，個資法第3條所規定之當事人不得預先拋棄或以特約限制之權利中，「請求停止蒐集、處理或利用」在概念上類似於GDPR拒絕權。拒絕權行使之情形：（1）資料當事人撤回其同意；（2）為個人資料蒐集之特定目的消失或期限屆滿時（不含因執行職務或業務所必須或經當事人書面同意者）資料當事人得行使拒絕權；（3）為違反個資法規定蒐集、處理或利用個人資料者，資料當事人得行使拒絕權。

須注意，同法第20條第2項有規定「合法行銷行為之拒絕權」，係指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。且，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。

[116] 張陳弘、莊植寧（2019）。**新時代之個人資料保護法制歐盟 GDPR 與臺灣個人資料保護法的比較說明**。臺北：新學林，133。

4、 特定目的外之處理或利用行為：

如前述，為保護當事人個人資料，機關於蒐集、處理或利用個人資料時，原則上受「目的限定原則」所拘束，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，特別是公務機關，對個人資料之利用，應於執行法定職務必要範圍內為之[117]。但為促進資料流動、保障契約效力，及增進公共利益等，個資法規定，符合下列情形之一者，得為特定目的外之利用，相關整理如**表4**：

表 4：我國個人資料保護法特定目的外之處理或利用情形

公務機關（第 16 條但書）	非公務機關（第 20 條但書）
1、 法律明文規定 2、 為維護國家安全或增進公共利益所必要 3、 為免除當事人之生命、身體、自由或財產上之危險 4、 為防止他人權益之重大危害 5、 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 6、 有利於當事人權益 7、 經當事人同意	1、 法律明文規定 2、 為增進公共利益所必要 3、 為免除當事人之生命、身體、自由或財產上之危險 4、 為防止他人權益之重大危害 5、 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 6、 經當事人同意 7、 有利於當事人權益

資料來源：個人資料保護法。

公務機關與非公務機關為特定目的外之處理或利用之例外情形差別為非公務機關無「為維護國家安全」事由。

5、 例外得蒐集、處理或利用特種資料之情形：

按我國個資法第6條規定，特種資料原則不得蒐集、處理或利用，除前述同意部分提及，經當事人同書面同意，以及符合同條第1項第6款但書規定，得例外合法蒐用特種資料外，同條第1項有其他例外情形，包含：

(1) 法律明文規定；

(2) 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事

[117] 個人資料法第 16 條規定。

前或事後有適當安全維護措施；

(3) 當事人自行公開或其他已合法公開之個人資料；

(4) 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，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；

(5) 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

符合以上情形之一者，得例外蒐集、處理或利用病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

另須注意，由於個資法並未針對特種資料區分有無特定目的外之利用，特種資料之特目的外之利用是否同樣適用於一般個資的特定目定外之利用規定（第16或第20條）有不同見解。

對此，我國有學者認為，個資法第6條僅規範特種個資之蒐集、處理、（目的內）利用，而目的外利用則與一般個資同適用同法第16條及20條，同樣當機關對特種資料為特定目的外之利用時，依個資法第6條第2項規定將「準用」同法第8條規定，即針對特種資料目的外之利用，機關不具告知資料當事人之義務[118]。實務上則持有不同意見之判決，認為：「個資法第20條僅適用在一般個人資料，特種資料之蒐集或處理，仍應依同法第6條規定為之，因其私密性程度不同，受到保護之高度與密度有異，因此在構成要件上對於可合法蒐集、利用之主體、合法蒐集後應為合目的性利用之要求、例外排除非法使用之範圍等等，自有嚴緊不同之差別規定」[119]。

(四) 其他與知情同意有關規定

1、 請求閱覽或製給複製本權：

個資法第10條規定，公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。若有以下情形之一者，機關得拒絕該請求：

(1) 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

(2) 妨害公務機關執行法定職務。

(3) 妨害該蒐集機關或第三人之重大利益。

對於是否受理當事人之請求時，機關應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求

[118] 張陳弘、莊植寧，同註 116，154。
[119] 臺灣高等法院 106 年度上訴字第 1550 號刑事判決。

人。此外，查詢或請求閱覽個人資料或製給複製本者，機關得酌收必要成本費用。

2、 資料跨境傳輸：

個資法規定個人資料跨境傳輸行為，原則允許例外禁止。公務機關為合法蒐集、處理、或利用即可將個人資料跨境傳輸。惟依個資法第21條規定，當非公務機關為國際傳輸個人資料，為防止個人資料不當國際傳輸，有下列情形之一者，中央目的事業主管機關得限制之：涉及國家重大利益、國際條約或協定有特別規定、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞、以迂迴方法向第三國（地區）傳輸個人資料規避個資法。

六、 彙整因應 GDPR 或 CBPR 體系指引手冊或工具

(一) 因應 GDPR 相關作為

1、 澳洲：

澳洲資訊委員辦公室（Office of the Australian Information Commissioner, OAIC）於2018年6月8日發布因應GDPR之指引及建議－Australian entities and the EU General Data Protection Regulation（GDPR）。

2、 西班牙：

西班牙資料保護局（Agencia Española de Protección de Datos, AEPD）於2021年6月29日推出風險管理及個資保護影響評估（DPIA）指引[120]，同時發布Evaluate-Risk GDPR評估工具[121]，該工具旨在執行DPIA並協助評估風險。

3、 英國：

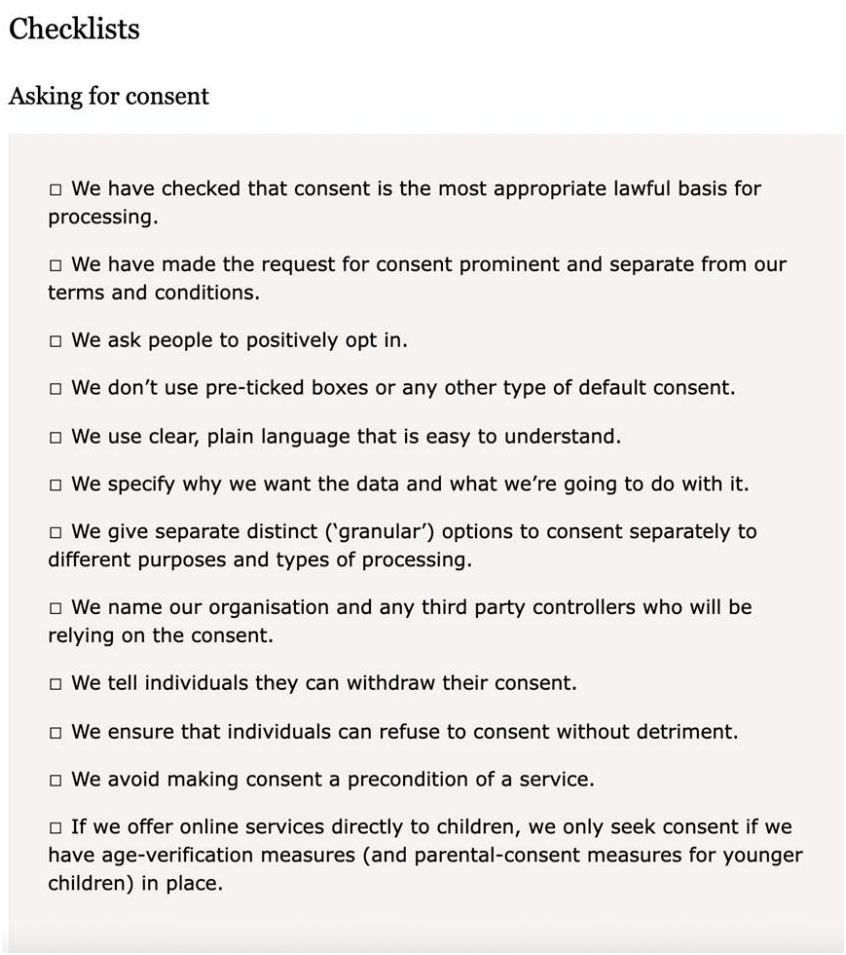
(1) 英國資訊專員辦公室（Information Commissioner's Office, ICO）於其網站上發布針對 GDPR 相關指引（Guide to the General Data Protection Regulation），該網站稱之為「英國 GDPR（UK GDPR）」指引[122]。適用於 DPO 和其他負責資料保護工作的人員，並解釋了適用於大多數英國企業和組織的一般資料保護制度。解釋了每一項資料保護原則、權利和義務，並總結了關鍵要點、回答了常見問題，以及包含可幫助企業

[120] Agencia Española de Protección de Datos, AEPD (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Retrieved May 04, 2021, from https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf.

[121] Agencia Española de Protección de Datos, AEPD (2021). Evalúa-Riesgo RGPD. Retrieved May 04, 2021, from https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd.

[122] Information Commissioner's Office, ICO (2018). Guide to the General Data Protection Regulation. Retrieved November 09, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

與組織遵守的實用檢查表（practical checklist）如**圖 20**。



Checklists

Asking for consent

□ We have checked that consent is the most appropriate lawful basis for processing.

□ We have made the request for consent prominent and separate from our terms and conditions.

□ We ask people to positively opt in.

□ We don't use pre-ticked boxes or any other type of default consent.

□ We use clear, plain language that is easy to understand.

□ We specify why we want the data and what we're going to do with it.

□ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

□ We name our organisation and any third party controllers who will be relying on the consent.

□ We tell individuals they can withdraw their consent.

□ We ensure that individuals can refuse to consent without detriment.

□ We avoid making consent a precondition of a service.

□ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

圖 20：Practical Checklist 示意圖

資料來源：英國 ICO。

(2) 英國文化媒體暨體育部（Department for Digital, Culture, Media and Sport, DCMS）於 2019 年 2 月 6 日發布歐盟一般資料保護規則（GDPR）第 36 條第 4 項之應用指引（Guidance on the application of Article 36 (4) of the General Data Protection Regulation (GDPR)），內容主要指導政府部門與相關公共部門組織，其依 GDPR 第 36 條第 4 項之規定有何職責以及須採取何種措施[123]。

[123] Department for Digital, Culture, Media and Sport, DCMS (2019). Guidance on the application of Article 36(4) of the General Data Protection Regulation (GDPR). Retrieved November 09, 2021, from https://www.gov.uk/government/publications/guidance-on-the-application-of-article-364-of-the-general-data-protection-regulation-gdpr.

4、 香港：

香港獨立隱私監督機關「個人資料私隱專員公署（私隱公署）」為提高香港機構／企業認識GDPR（香港稱為《通用數據保障條例》）新制定的資料保障監管框架對機構及組織可能帶來的影響，私隱公署出版了小冊子：「歐洲聯盟《通用數據保障條例》2016最新資訊」，該手冊於2020年5月修訂[124]。

5、 韓國：

(1) 為了因應 GDPR，韓國網路安全局（Korea Internet & Security Agency，KISA）召集專家學者共同研究，於 GDPR 實施前一年發布針對韓國企業之「歐盟一般資料保護規則（GDPR）」指引（우리 기업을 위한「유럽 일반 개인정보 보호법」안내서），以通俗易懂之方式向韓國企業說明 GDPR 之目的以及主要內容，以協助韓國企業了解 GDPR[125]。

(2) 在針對韓國企業之「歐盟一般資料保護規則（GDPR）」指引（우리 기업을 위한「유럽 일반 개인정보 보호법」안내서）發布後，歐盟陸續又公布了其他 GDPR 相關指引，故 KISA 與韓國行政安全部於 2017 年 12 月再次發布針對韓國企業之「歐盟一般資料保護規則（GDPR）」第一指引（우리 기업을 위한 EU 개인정보보호법（GDPR）1 차 가이드라인），其內容主要講解歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party, WP29）所發布之 GDPR 指引，包含資料可攜權、自動化個人決策與剖析、個資保護影響評估等，並增加隱私保護設計及預設隱私保護（Data Protection by Design and Default）、資料傳輸到第三國以及被遺忘權之相關內容，提高韓國企業對於 GDPR 之認識，並提前做好準備[126]。

(3) 為了使企業能更方便獲取 GDPR 之資料，KISA 與韓國行政安全部將上述兩個指引之內容進行整合，並新增歐盟第 29 條個資保護工作小組所發布的新指引、建議、具體案例與參考資料等內容，於 2018 年發布針對韓國企業之「歐盟一般資料保護規則（GDPR）」指引修訂版（ [개정판] 우리 기업을 위한 EU 일반 개인정보보호법（GDPR）

[124] 香港個人隱私引專員公署（2020）。「歐洲聯盟《通用數據保障條例》2016 最新資訊」，2021 年 11 月 8 日，取自：https://www.pcpd.org.hk/tc_chi/data_privacy_law/eu/files/eugdpr_c.pdf。

[125] KISA GDPR 대응지원 센터(2020).우리 기업을 위한「유럽 일반 개인정보 보호법」안내서/ p236/2017/행정안전부,한국인터넷진흥원. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

[126] KISA GDPR 대응지원 센터(2020).우리 기업을 위한 EU 개인정보보호법(GDPR) 1 차 가이드라인 / p107 / 2017 / 행정안전부,한국인터넷진흥원. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

가이드북）[127]。

(4) 隨著 GDPR 的全面實施，因違反 GDPR 而被裁罰的案例越來越多，為了給韓國企業提供確實可行的 GDPR 遵守指引，KISA 與韓國行政安全部參考了主要國家以及歐盟近期所發布的指引、報告，並加以整理，於 2020 年 5 月發布 2020 年歐盟一般資料保護規則（GDPR）指引（2020 EU 일반개인정보보호법（GDPR） 가이드북）[128]。

(5) KISA 於 2020 年 12 月發布 2020 GDPR 諮詢案例手冊（2020 GDPR 상담사례집），本手冊是根據 GDPR 響應支持中心（GDPR 대응지원센터）諮詢之案例所編寫，內容包含案例、行政處罰等，並提出 GDPR 之判斷標準，以幫助企業理解[129]。

6、 日本：

(1) 日本貿易振興機構（JETRO）於 2016 年 6 月發布歐盟一般資料保護規則（GDPR）實務手冊（入門編）（「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）），為了方便從事歐洲業務的中小企業使用，該手冊主要以實際案例的「問答格式」撰寫內容，內容包含講解 GDPR 的意義與整體結構、GDPR 的基礎知識，以及重點介紹客戶與員工相關的反應，並描述問題、對策以及具體「內部」作法[130]。

(2) 2017 年 8 月，日本貿易振興機構（JETRO）發布歐盟一般資料保護規則（GDPR）實務手冊（實踐編）（「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）），內容主要講解標準契約條款（Standard Contractual Clauses，下稱「SCC」）與拘束性企業規則（BCR）之規定，以及在 2017 年 7 月 31 日以前企業實際遵守 GDPR 之情況

[127] KISA GDPR 대응지원 센터(2020). [개정판] 우리 기업을 위한 EU 일반 개인정보보호법(GDPR) 가이드북 / p206 / 2018 / 행정안전부, 방송통신위원. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

[128] KISA GDPR 대응지원 센터(2020). 2020 EU 일반개인정보보호법（GDPR） 가이드북 / p290 / 2020 / 방송통신위원회, 한국인터넷진흥원. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

[129] KISA GDPR 대응지원 센터(2020). 2020 GDPR 상담사례집. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

[130] 日本貿易振興機構 (JETRO) (2016).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック(入門編). Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html.

[131]。

(3) 2018 年 2 月，日本貿易振興機構（JETRO）發布歐盟一般資料保護規則（GDPR）之（歐盟第 29 條個資保護工作小組）資料可攜權實務手冊（「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編)データポータビリティの権利)，主要內容為說明歐盟第 29 條個資保護工作小組所發布之資料可攜權指引[132]。

(4) 為了因應歐盟第 29 條個資保護工作小組所發布之「識別主責監管機關指引」，日本貿易振興機構（JETRO）發布歐盟一般資料保護規則（GDPR）之（歐盟第 29 條個資保護工作小組）識別主責監管機關實務手冊（「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）管理者および処理者の主導監督当局の特定)，講解並分析「識別主責監管機關指引」之規定[133]。

(5) 2018 年 2 月，日本貿易振興機構（JETRO）發布歐盟一般資料保護規則（GDPR）之（歐盟第 29 條個資保護工作小組）個資保護長實務手冊（「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）データ保護責任者)，主要內容為說明歐盟第 29 條個資保護工作小組所發布之「個資保護長指引」[134]。

7、 新加坡：

新加坡個人資料保護委員會（The Personal Data Protection Commission, PDPC）於2017年10月4日發布針對組織之歐盟一般資料保護規則（GDPR）說明資料（European Union General Data Protection Regulation Factsheet for Organisations)，內容主要向新加坡之各組織強調歐盟GDPR之關鍵內容並不

[131] 日本貿易振興機構 (JETRO) (2017).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html.

[132] 日本貿易振興機構 (JETRO) (2018).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）データポータビリティの権利. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2018/01/2d8d30044cc65583.html.

[133] 日本貿易振興機構（JETRO）(2018).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）管理者および処理者の主導監督当局の特定. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2018/01/9a90f1003bc16515.html.

[134] 日本貿易振興機構 (JETRO) (2018).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）データ保護責任者. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2018/01/28dd771ad2a2c020.html.

包含對GDPR之解釋，本資料之內容並非等同於法律、法律之聲明或其他專業建議之替代品[135]。

(二) 因應 CBPR 體系相關作為

1、 新加坡：

(1) 新加坡資訊與媒體發展管理局（Infocomm Media Development Authority, IMDA）發布 APEC 跨境隱私保護規則工具包（APEC Cross Border Privacy Rules System Information-kit），內容介紹 APEC 跨境隱私保護規則(Cross-Border Privacy Rules, CBPR)之規定，以及 CBPR 申請資格、申請流程、認證標準等，方便組織理解 CBPR 之運作[136]。

(2) 為了鼓勵組織主動申請加入 CPBR 與資料處理業隱私識別體系（Privacy Recognition for Processors system，PRP），IMDA 發布 APEC Cross Border Privacy Rules (CBPR) & Privacy Recognition for Processors (PRP) Systems，以圖表之方式介紹 CPBR 與 PRP，重點包含兩者之認證標準以及教導組織如何提出申請並參與 CPBR 以及 PRP[137]。

(3) IMDA 於 2020 年 6 月發布「如何與 APEC CBPR 以及 PRP 認證之組織輕鬆跨境傳輸個人資料介紹圖」（Easy Data Transfers To APEC CBPR /PRP Certified Organisations），主要描述新加坡承認 APEC 跨境隱私規則（CBPR）系統以及 PRP 認證，故組織得依圖表上之指示與 APEC CBPR 以及 PRP 認證之組織合法跨境傳輸個人資料[138]。

(4) 新加坡制定向 APEC CBPR 和 PRP 認證組織傳輸資料的一契約條款範例[139]，使組織組織可以將其納入與接收方的契約中。

---

135 Personal Data Protection Commission, (2017). EU GDPR Factsheet for Organisations Now Available. Retrieved November 09, 2021, from https://www.pdpc.gov.sg/news-and-events/announcements/2017/10/eu-gdpr-factsheet-for-organisations-now-available.

136 IMDA (2021). APEC Cross Border Privacy Rules System Information-kit. Retrieved November 14, 2021, from https://www.imda.gov.sg/-/media/Imda/Files/Programme/CBPR-and-PRP/CBPR-Information-Kit.pdf?la=en&hash=15C4EADE10B648D50DB026C55D701F7A.

137 IMDA (2021). APEC Cross Border Privacy Rules (CBPR) & Privacy Recognition for Processors (PRP) Systems. Retrieved November 14, 2021, from https://www.imda.gov.sg/-/media/Imda/Files/Programme/CBPR-and-PRP/CBPR-and-PRP-Brochure-150620.pdf.

138 IMDA (2021). Easy Data Transfers to APEC CBPR /PRP Certified Organisations. Retrieved November 14, 2021, from https://www.pdpc.gov.sg/help-and-resources/2020/06/easy-data-transfers-to-apec-cbpr-and-prp-certified-organisations.

139 Personal Data Protection Commission, (2021). Sample Clause for Data Transfers to APEC CBPR and PRP Certified Organisations. Retrieved November 14, 2021, from https://www.pdpc.gov.sg/Help-and-Resources/2020/06/Sample-Clause-for-Data-Transfers-to-APEC-CBPR-and-PRP-Certified-Organisations.

2、 日本：

(1) 日本情報經濟社會推進協會（Japan Information Processing Development Corporation, JIPDEC）於 2021 年 7 月發布 APEC CBPR 認證介紹（APEC CBPR 認証のご紹介），其以簡報方式介紹 APEC CBPR，並針對提出申請、申請條件、手續、費用等內容進行整理，方便企業查看[140]。

(2) JIPDEC 於 2021 年 2 月發布 APEC CBPR 認證指引第 2 版（APEC CBPR 認証申請ガイドブック），內容詳細介紹 CBPR 審查之要點、企業該如何申請加入以及申請所需之文件，此指引介紹更為詳細[141]。

第四節　知情同意各國案例介紹

一、 新加坡

新加坡以國家數位身分憑證（National Digital Identity, NDI）為基礎，逐年擴展了個人與企業的數位服務領域，並且允許個資所有者以其數位憑證，跨部門取得個資內容與授權應用，針對個人資料使用服務，新加坡政府於 2003 年啟動了驗證系統「SingPass」，只要年滿 15 歲且為新加坡公民、永久居民或是領有就業許可證的民眾，透過雙因子驗證方式，以使用者同意作為資料共享之基礎，帶動各項數位服務發展，在個資法規上，由新加坡個人資料保護委員會（Personal Data Protection Commission, PDPC）負責管理和執行《個人資料保護法》（the Personal Data Protection Act 2020, PDPA），提供一般性原則與相關的審查機制。新加坡又於 2020 年底推出 SingPass 手機 App，除了數位身分識別服務外，此 App 也提供民眾線上簽署同意書與交易確認等功能。此外，新加坡金管局也基於 SingPass 推出了「新加坡財務資料交換平臺」（Singapore Financial Data Exchange, SGFinDex）。

(一) SGFinDex

SGFinDex 是由新加坡金融管理局（Monetary Authority of Singapore）、智慧國家及數位政府工作團（Smart Nation and Digital Government Group）、新加坡政府人力部（the Ministry of Manpower）、新加坡銀行公會（the Association of Banks in Singapore）等公共部門和 7 家參與銀行合作開發的平臺，是全球首個允許使用全國數位身分驗證／電子政府密碼（SingPass）登入及取得自己在不同金融及政府機構財務資訊的公共數位基礎建設，如**圖 21**。

---

140 一般財団法人日本情報経済社会推進協会 (JIPDEC) (2021). APEC CBPR 認証のご紹介. Retrieved November 14, 2021, from https://www.jipdec.or.jp/protection_org/JIPDEC_AOP_CBPR_015.pdf.

141 一般財団法人日本情報経済社会推進協会 (JIPDEC) (2021). APEC CBPR 認証申請ガイドブック. Retrieved November 14, 2021, from https://www.jipdec.or.jp/protection_org/JIPDEC_AOP_CBPR_008.pdf.

圖 21：新加坡 SGFinDex 應用過程

資料來源：https://bfsi.economictimes.indiatimes.com/news/fintech/singapore-launches-singapore-financial-data-exchange-today/79600638。

參與的金融機構有星展銀行有限公司（DBS Bank Ltd）、華僑銀行有限公司（Oversea-Chinese Banking Corporation Ltd）、大華銀行有限公司（United Overseas Bank Ltd）、花旗新加坡銀行有限公司（Citi Singapore Ltd）、匯豐銀行新加坡有限公司（HSBC Bank Singapore Ltd）、馬來亞銀行新加坡有限公司（Maybank Singapore Ltd）及渣打銀行新加坡有限公司（Standard Chartered Bank Singapore Ltd）。

SGFinDex 平臺是透過公私協力的方式去提供民眾「金融個資聚合」的功能，對於該平臺而言，公部門及私部門都可以當作資料提供者（Data Provider, DP）及服務提供者（Service Provider, SP）。民眾可將分散於不同金融機構及政府單位的財務資訊整合至此單一平臺，以進行更有效的財務規劃。民眾透過 SingPass 登入 SGFinDex 平臺後，從平臺選擇欲連結的銀行或政府機構，即可從參與銀行獲取個人財務資訊（例如存款、信用卡、貸款和投資）以及從相關政府機構獲取個人的財務狀況（例如 HDB 房屋貸款－Housing Development Board 和 CPF 中央公積金制度－Central Provident Fund），當民眾獲得個人綜合的財務資訊之後，就可以更簡單、有效地對自己的財務做出更全面性的規劃。

整體來說，該平臺的資料集有兩個來源，第一個來源為「銀行」：（1）往來／儲蓄賬戶和定期存款（過去 4 個月的月末帳戶餘額）；（2）信用卡未結餘額（最近 4 個月的結算單）；（3）貸款餘額（上月報表餘額）；（4）單位信託（上個月的帳戶餘額）；（5）公積金投資計畫（The CPF Investment Scheme）／補充退休計畫（Supplementary Retirement Scheme）持有量（上月帳戶餘額）。第二個來源則為「政府」：（1）CPF 普通帳戶（Ordinary Account）、特別帳戶（Special Account）、保健儲蓄帳戶（MediSave Account）和退休帳戶（Retirement Account）的最新餘額；（2）新加坡國內稅務局（Inland Revenue Authority of Singapore）年度應課稅收入；（3）建屋發展局（Housing and Development Board）每月房屋貸款分期付款、房屋貸款餘額。

SGFinDex 平臺的好處在於：（1）高效標準化，採用基於共通資料格式與應用程式介面（API）標準的集中式閘道器處理；（2）安全基礎設施，該平臺之基礎設施由政府擁有及營運，並使用國家數位身分（SingPass）之身分驗證和同意框架；（3）推動數位轉型，實現了資料驅動的創新。使用 SGFinDex 可以更方便地跨實體共享資料，例如：（1）以往蒐集資料的舊方式為個人橫跨不同的資料集去手動整理財務資料，過程既繁瑣又費時；（2）新加坡 SGFinDex 平臺的方式則為個人可以在他們選擇的財務規劃應用程式上方便且安全地查看所有的個人財務資料；（3）使民眾能夠進行更好的財務規劃並實現金融福祉、財務規劃更輕鬆。

SGFinDex 平臺的資料授權時間，從第一次同意起可延續一年、中途可隨時撤銷授權。該平臺有四個重要的資訊安全機制：（1）同意驅動，只有在使用者同意後才會蒐集資料，使用者保留對他們希望與其共享資料之參與實體的控制權；（2）資料安全，資料在傳輸過程中受到保密和保護，SGFinDex 無法讀取也不儲存使用者的個人財務資料，意即該平臺僅協助傳輸但不儲存任何財務資料；（3）「SingPass」作為「身分驗證和授權」機制，使用者在連接他們的銀行帳戶和搜尋資料之前都必須透過 SingPass 進行驗證，因此，每次檢索使用者的個人財務資料時都會驗證使用者的身分；（4）資料加密，使用者的個人財務資料在透過 SGFinDex 檢索時被加密，只有使用者授權可以接收資料的財務規劃應用程式或網站才能對其進行解密。新加坡政府的未來規劃則是將 SGFinDex 的下一階段計畫納入保單與股票持有資訊。

(二) 資料保護信賴標章

資料保護信賴標章（Data Protection Trustmark Certification, DPTM Certification）是新加坡個人資料保護委員會（Personal Data Protection Commission, PDPC）所推動的企業自發性認證標章，使企業證明自身對於資料保護的實際行動，有助於組織提高競爭優勢，並與使用者（客戶）和利害關係人建立信任。

DPTM Certification 稽核表是基於 DPTM Certification 的要求所提供的簡略要點稽核，在組織申請 DPTM Certification 之前，可以利用此表衡量自身的準備情況。此稽核表共列出 4 個主要原則，每個主要原則之下又區分為各個主題，而每個主題之下則是多項稽核要點，企業透過勾選是否達成稽核要點來衡量準備情況（詳細稽核要點請參考附錄一）。另外，此表也根據稽核要點，對應到 PDPC 所提供的參考指引作為詳細的稽核依據。以下摘要出 DPTM Certification 稽核表之原則如**表 5**：

表 5：DPTM Certification 稽核表原則

DPTM Certification 稽核表	
原則	稽核項目
治理和透明度 （**governance and transparency**）	1、 制定資料保護政策與實際作法
	2、 制定查詢、投訴、爭議處理的流程
	3、 建立識別、評估、確認資料保護的流程
	4、 建立資料外洩的管理計畫
	5、 可歸責性
	6、 組織內部溝通與培訓
個人資料管理 （**management of personal data)**	1、 適當的目的
	2、 適當的同意
	3、 適當的使用與揭露
	4、 符合規範的跨境資料傳輸
個人資料保管 （**care of personal data**）	1、 適當的保護
	2、 適當的保留與刪除
	3、 正確且完整的紀錄
個人權利 （**individual's rights**）	1、 撤銷同意的權利
	2、 近用與更正資料的權利

資料來源：IMDA。

二、 法國

以法國個資保護主管機關國家資訊自由委員會（CNIL）為例，其工作大致分為三類，目標是創建符合 GDPR 規範並尊重隱私之使用者旅程。

(一) 平臺工作

1、 提供案例，作為設計使用者介面的靈感。

2、 提供讓個人資料介面能夠符合 GDPR 的工具。

3、 展示不同社群為實現 GDPR 原則所做的不同解決方案。

(二) 資訊揭露

CNIL 平臺要求與個人資料處理相關的資訊必須被簡潔、透明地告知使用者，並應使用簡短、易懂的語句呈現。針對資訊可近用性、可理解性以及簡潔性，該平臺提供之範例如下：

1、 可近用性（accessible）：

右邊視窗比左邊視窗多出「資料管理」一項（粗框標示處），方便使用者直接管理個人資料（如**圖22**所示）。

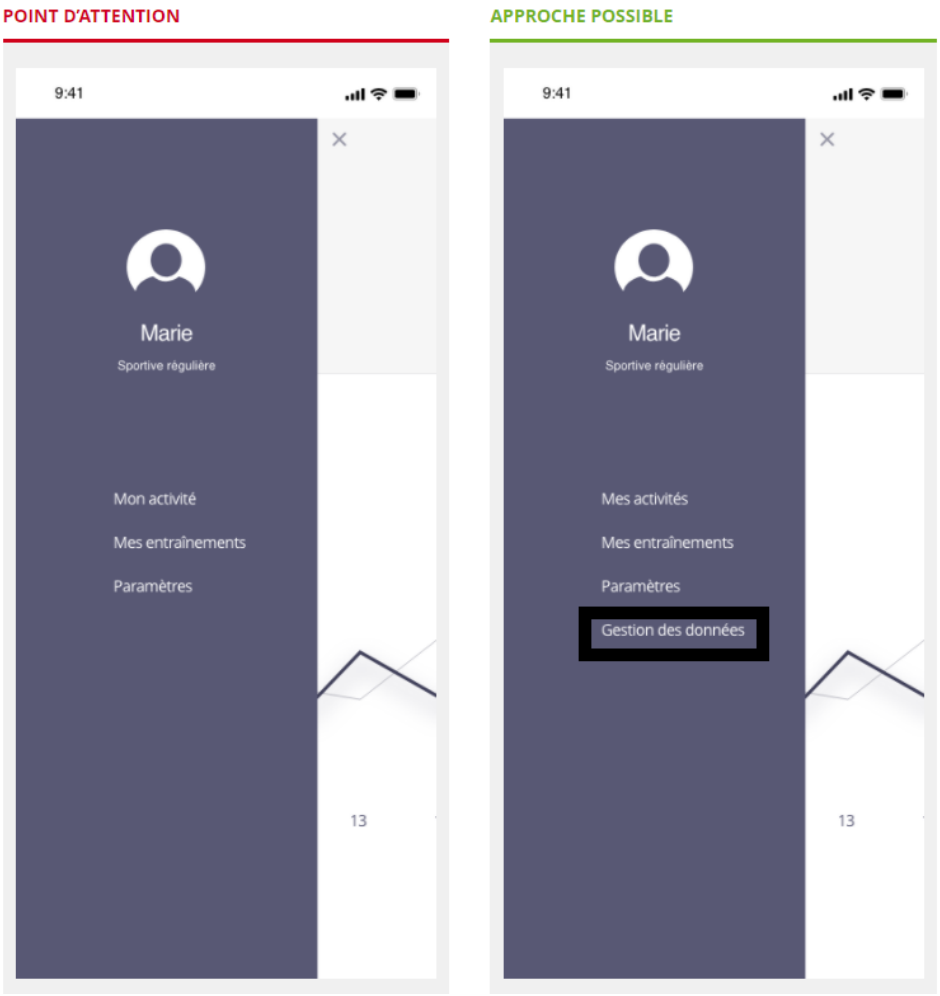


圖 22：可近用性

資料來源：CNIL。

2、 可理解性（understandable, simple and clear）：

左方視窗文字冗長，而右方敘述減少專業術語，並在敘述當中以底線突顯隱私政策之重點（如**圖23**所示）。

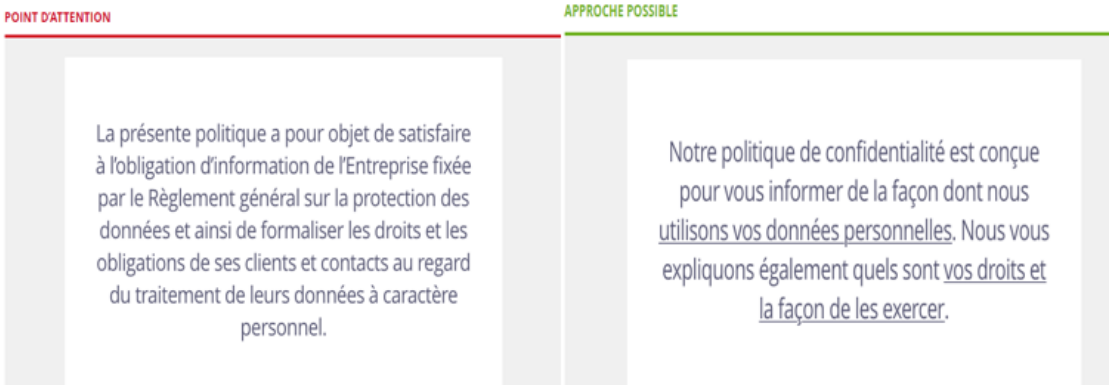


圖 23：可理解性

資料來源：CNIL。

3、 簡潔性（intelligible and concise）：

左方將個人資料蒐集的資訊放置於頁面下方，大篇幅文字容易讓使用者沒有耐心閱讀，也不易理解下方資訊與上方選項之關聯；右方採多頁呈現，每頁簡要說明個人資料被蒐集後將如何被使用，使用者必須點擊按鈕才能換頁，此設計將增進使用者與網頁互動（如**圖24**所示）。

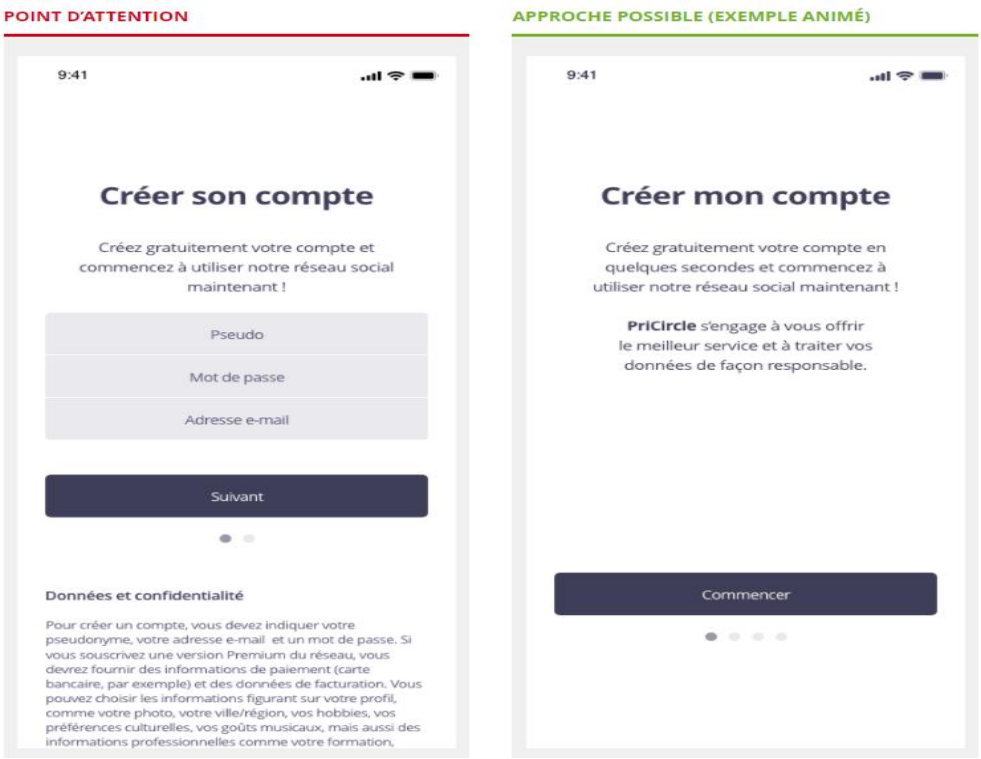


圖 24：簡潔性

資料來源：CNIL。

(三) 知情同意

CNIL 平臺要求同意書必須通過自由、特定及明確的自願行為給予同意，方能蒐集並處理其個人資料，根據以上三項原則，該平臺提供之範例如下：

1、 自由行使同意（consent must be freely given）：

如**圖25**所示，上方的使用者介面顯示使用者必須對所有選項進行勾選（包含同意該機構使用其個人資料），才能夠點選下方按鈕，並未給予使用者充分行使同意之權力；下方的使用者介面則無限制，使用者即使未勾選全部條款，仍能行使同意權。

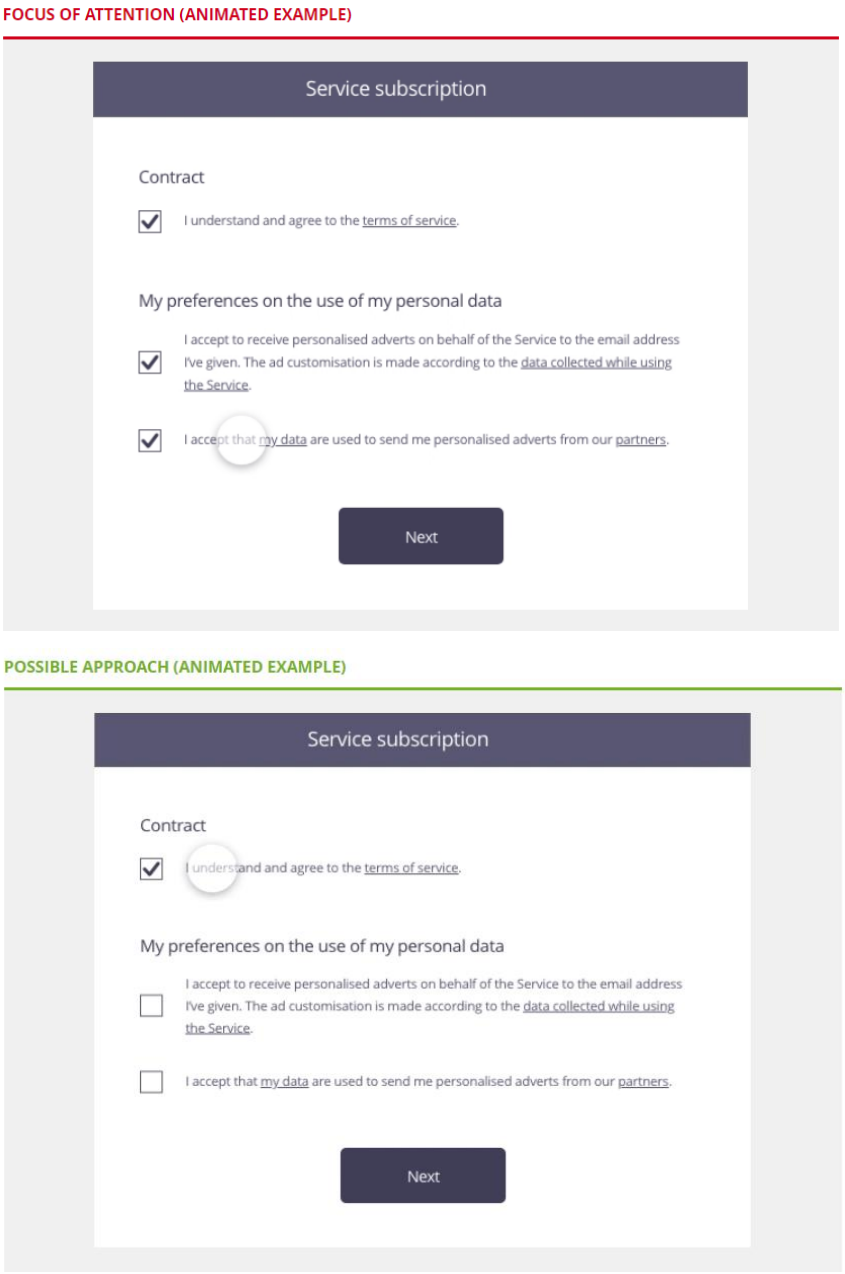


圖 25：自由行使同意

資料來源：CNIL。

2、 對特定目的行使同意（consent must be given specifically）：

如**圖26**所示，上方視窗當中的選項包含兩種用途：對E-mail地址進行商業探勘、銀行卡付款便利化，一旦勾選就必須同時同意兩案；下方視窗則將選項分開，讓使用者能夠分別勾選。

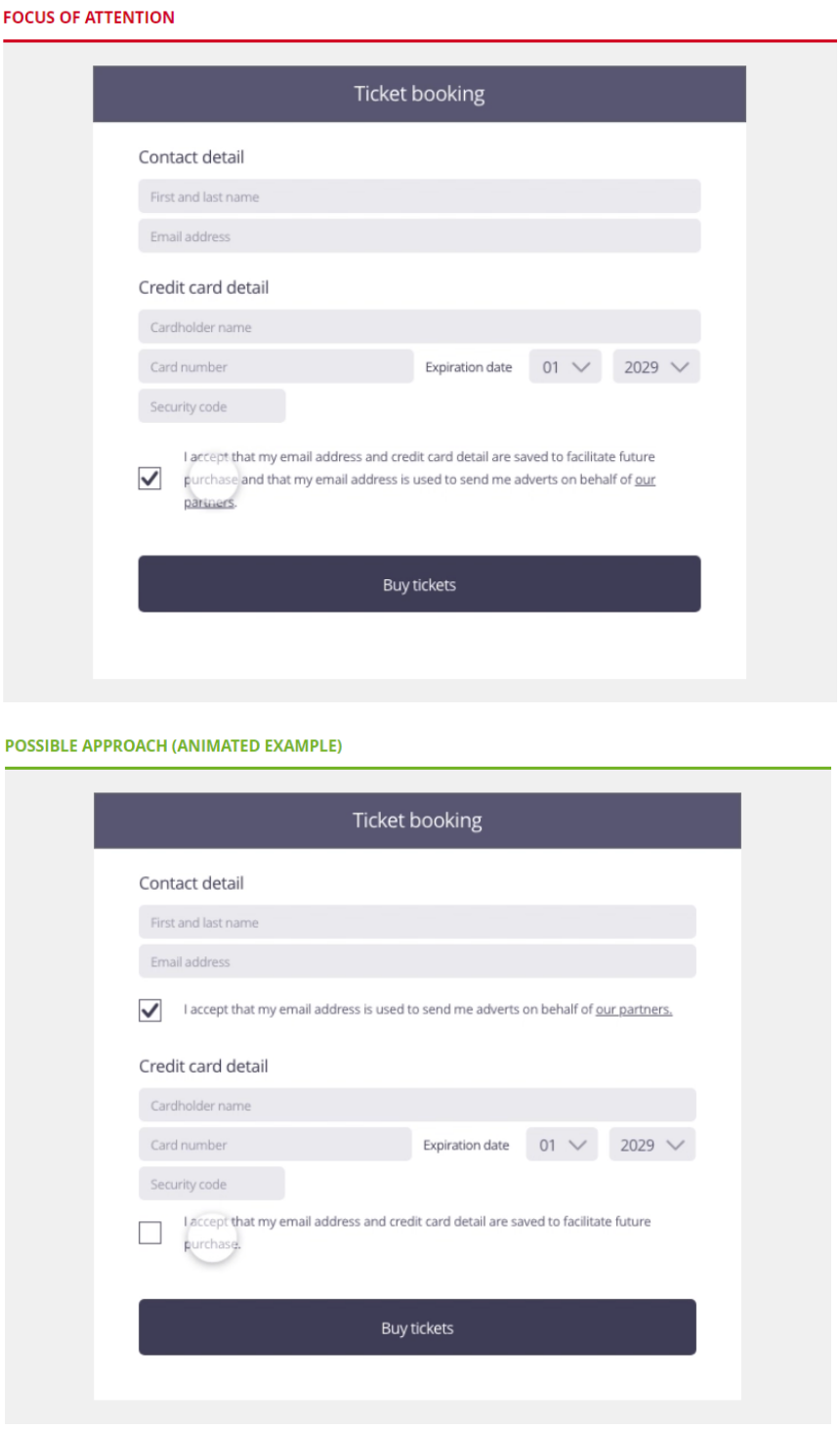


圖 26：對特定目的行使同意

資料來源：CNIL。

3、 明確行使同意（consent must be unambiguous）：

左邊視窗Chat Bot詢問使用者是否同意該機構運用其E-mail地址進行商業探勘，而使用者並未點選任一選項，但Chat Bot仍單方面宣告其E-mail將被作為商業探勘用途；右邊視窗中使用者必須明確點擊同意，Chat Bot才會進行下一步（如**圖27**所示）。

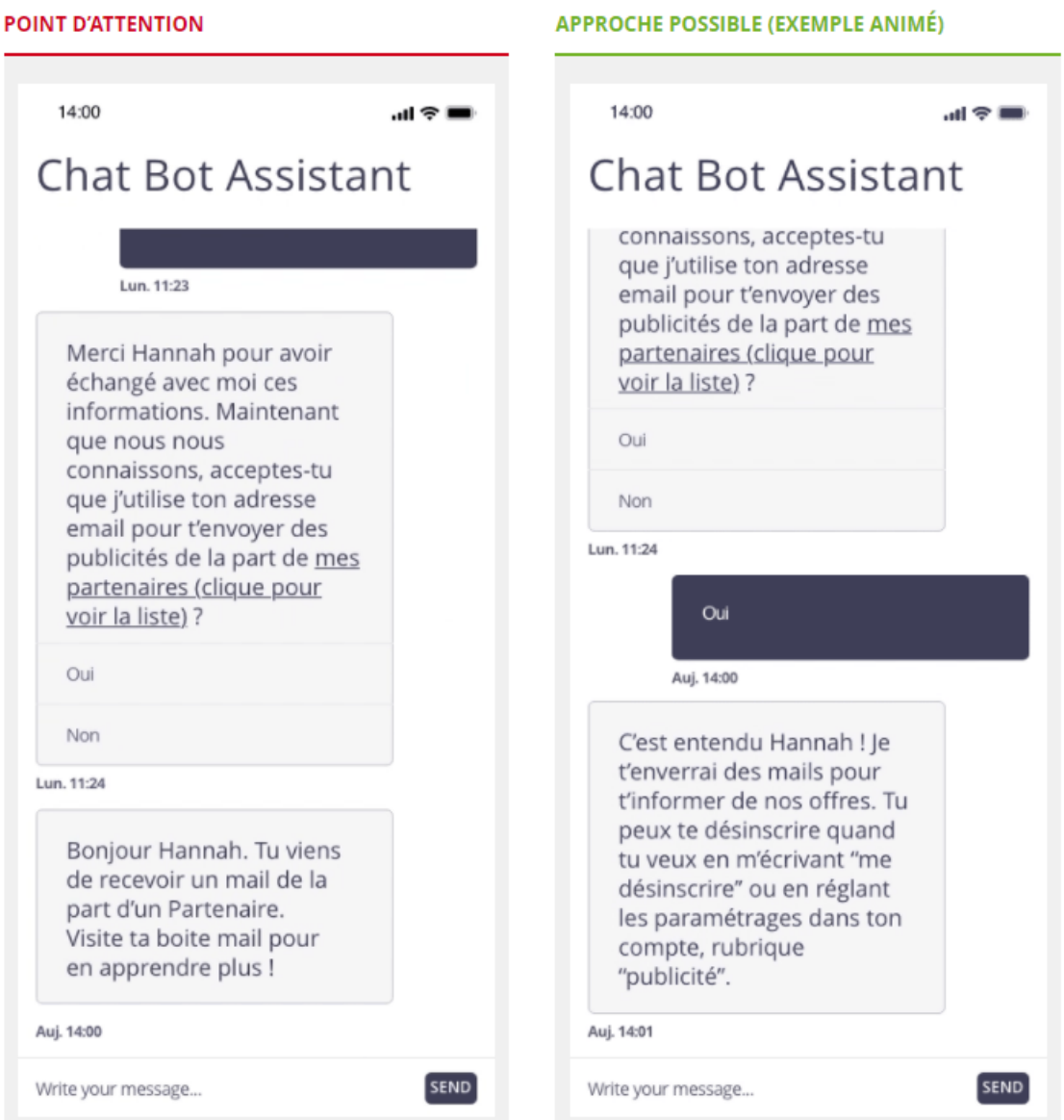


圖 27：明確行使同意

資料來源：CNIL。

(四) 實際案例

1、 Tailor-Made 服飾店：

該服飾店提供Chat Bot客服，購買過程分為三個階段，第一階段為選擇購買商品及分店。第二階段為測量包裹體積並開具發票。最後將定期通知使用者訂單的進度，直到交貨。Chat Bot會在對話中充分告知使用者與其個人資料相關之資訊，徵求使用者同意，並且在付款階段讓使用者再次確認先前同意授權之事項（如**圖28**所示）。

圖 28： Tailor-Made 服飾店付款介面

資料來源：CNIL。

2、 VODocumentaire 影片平臺：

該平臺蒐集使用者之聯絡資訊、購物車cookie，整體流程如**圖29**所示。

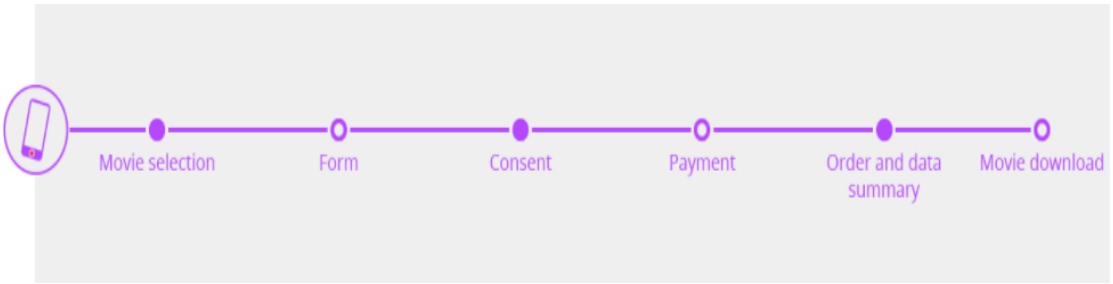


圖 29： VODocumentaire 影片平臺蒐集個資流程

資料來源：CNIL。

首先，使用者選取影片後，購物車會出現圖示，點擊後會跳出平臺方存取購物車cookie的知情同意書，以徵求使用者同意。（如**圖30**所示）

圖 30：存取購物車 cookie 之知情同意書

資料來源：CNIL。

其次，在結帳前，VODocumentaire會詢問使用者是否願意收到相同類型之影片推薦、特定品牌之商品資訊等，使用者可分項選擇（如**圖31**所示）。

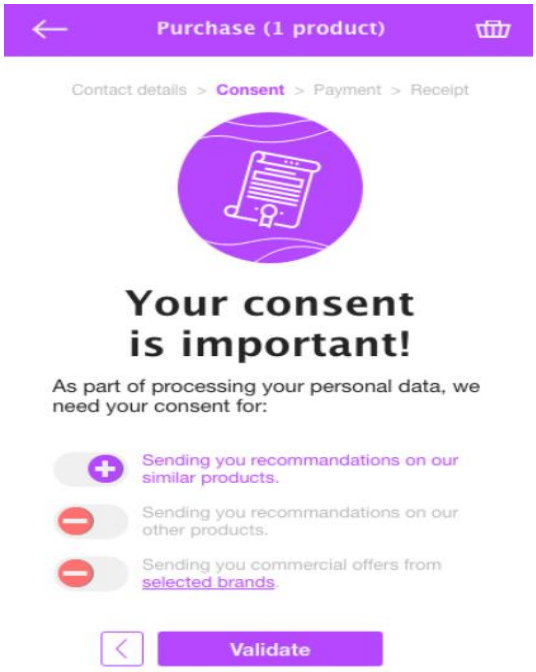


圖 31：商品推薦之知情同意

資料來源：CNIL。

最後，平臺將在結帳完成後提供發票明細，以及針對該使用者所蒐集之所有資訊（如**圖32**所示）。使用者得進行修正或要求平臺方刪除，進行最終確認。

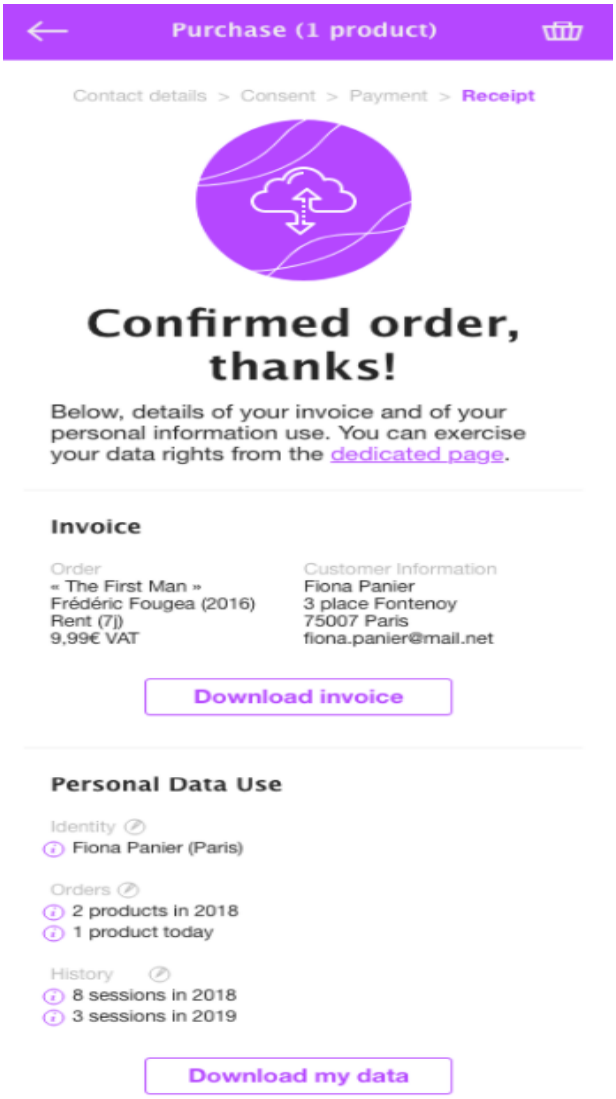


圖 32：發票和個人資料蒐集明細

資料來源：CNIL。

三、 韓國

2019 年韓國試辦 MyData 專案「Medibloc」[142]，Medibloc 是一個以病患為中心的醫療資料平臺，平臺由三星火災與海上產險（Samsung Fire & Marine Insurance）、首爾國立大學醫院（Seoul National University Hospital）、CHA 醫學院（CHA University School of Medicine）和韓國生產智慧腰帶的企業 Welt 組合而成，並開發了「區塊鏈病歷檢查資訊交流」、「參與臨床研究」以及「醫療紀錄與病歷資料為導向的健康優化指導」等服務，將醫療機構的資料和協力廠商應用程式中的健康資料整合到以患者為中心，並構建一個可直接由患者使用的資料平臺。

2021 年韓國公共管理安全部（행정안전부, MOIS）推出「Public MyData Service」[143]，允許民眾以「資料集」的形式一次性的蒐集分散在各單位的個人資料，減輕民眾在申辦政府服務過程中的不便，並避免因錯誤提交文件而延宕流程，此服務目前應用在小型企業、金融、就業等活動，進一步促進韓國的數位政府創新。韓國所推動的 Public Mydata Service 與我國 MyData 平臺的「線上服務」項目[144]很類似，目的都是使民眾可以不需要因為申辦業務所需的資料而奔波於各機關，藉以減少民眾申辦政府業務的不便及申辦時間。

此措施目前有六家機構提供八項應用服務，包括小型企業與市場服務（Small Enterprise and Market Service）、慶吉就業協會（Gyeonggi Job Foundation）、韓國信貸資訊服務（Korea Credit Information Services, KCIS）、信貸資訊與重組服務（Credit Counseling & Recovery Service）、衛生福利部（Ministry of Health and Welfare）與韓國房地產委員會（Korea Real Estate Board），分述如下：

(一) 小型企業與市場服務（Small Enterprise and Market Service）

個人申請小型企業資金時，需要提供加值稅（VAT）稅基核定證明、企業資格認定等 16 種文件，使機關在查核時十分不便。利用「Public MyData Service」提交申請，便不須再另外提供文件給小型企業資金之網站，預計有 30 萬家小型企業受惠。

(二) 慶吉就業協會（Gyeonggi Job Foundation）

申請面試補貼、青年基本收入服務等流程，需另外領取經核可之居民登記證件複印本或摘要等報送機構，手續繁雜不便。市民可以透過「Public MyData Service」中的「就業支持項目綜合申請系統」去申請這些服務，無需另外提供任何文件，預計約有 84 萬名年輕人受惠。

---

142 MEDIBLOC TEAM (2017). MediBloc Whitepaper.Retrieved July 13, 2021, from https://whitepaper.io/document/176/medibloc-whitepaper.

143 MOIS (n. d.). MOIS implements further digital government innovation with launch of Public Mydata Service. Retrieved July 11, 2021, from https://www.dgovkorea.go.kr/news/57.

144 同上，部分項目可能也需要類似 MyData 平臺的臨櫃服務模式。

(三) 韓國信貸資訊服務（Korea Credit Information Services, KCIS）

信用貸款或信用卡的申請需要向銀行和信用卡公司的各個機構申請，並提交十種類型的文件，包括收入證明和健康保險資格確認等等，透過「Public MyData Service」可加快篩選速度。KCIS 扮演 MyData 中介機構的角色，將信用、保險、金融等資料傳遞給政府機構與小型金融機構，如**圖 33** 所示，KCIS 也負責建立金融機構與 MyData 營運商「服務提供者角色共享資料」的通用標準（格式標準化、資料共享範圍、費用等）。

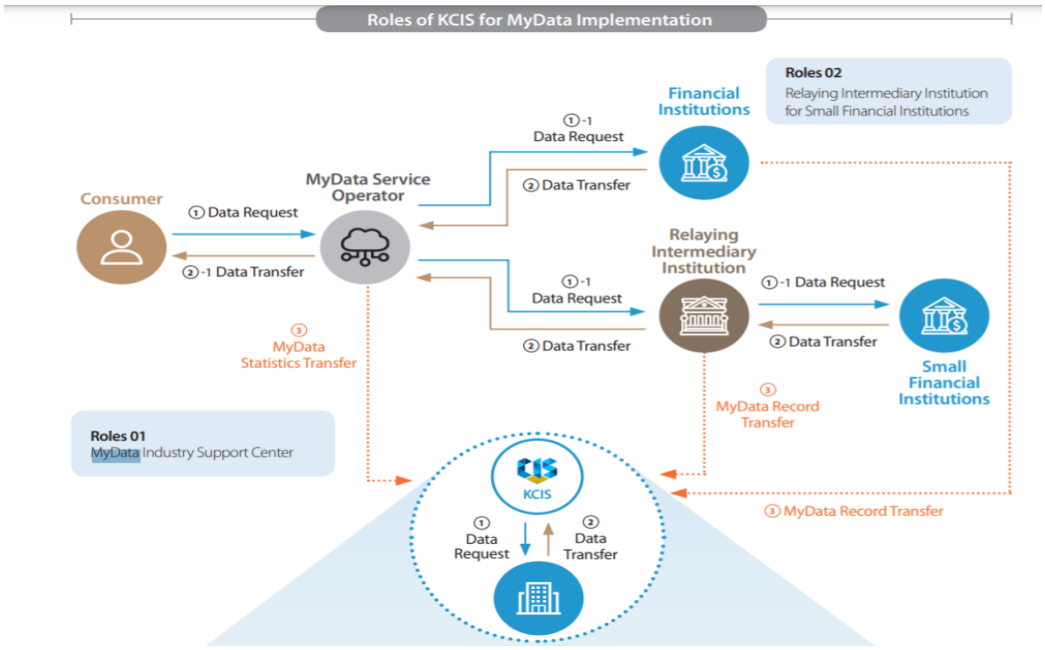


圖 33：KCIS 的 MyData 運作圖

資料來源：Korea Credit Information Services。

(四) 信貸資訊與債務重組服務（Credit Counseling & Recovery Service）

過去申請債務重組服務時，需要提供商業登記證和停業證明等 15 種文件。在個人債務重組諮詢櫃檯同意向「Public MyData Service」提供資料，即可立即申請債務重組，無需單獨提交文件。

(五) 衛生福利部（Ministry of Health and Welfare）

過去要查看健康檢查結果、治療史和用藥資訊，相關人員必須直接向相關的各個機構查詢。現在可以直接透過「Public MyData Service」中之「個人健康紀錄（Personal Health Records, PHR）」應用程式可以直接查詢用藥史、體檢紀錄、疫苗接種紀錄等。

(六) 韓國房地產委員會（Korea Real Estate Board）

過去相關機構需花費很長的時間核對申請人的居民戶口簿、收入證明、醫療保險資格證明等七類確認購房資格所需的文件。現在市民可以直接透過「Public

MyData Service」中的線上住房訂閱系統快速輕鬆地申請。公共管理安全部預計將購屋申請處理之時間由三分鐘縮短為即時，並加快行政效率。

韓國的公共管理安全部計畫預計於 2021 年 10 月前額外推出 10 項服務，包括 119 求救電話（國家消防局）、為國家提供傑出服務的傲人的就業支持（韓國就業資訊服務）和簡化公務員制度申請表（濟州特別自治道），並在此後逐步完善和擴展相關服務條款。此外，有關提供資訊之相關法規亦會一併修改，以便資料授權。

四、 臺灣

我國個人化資料自主運用（MyData）平臺是結合跨部會、跨業務之整合性資訊，以資料治理為主軸建立以資料治理為核心的數位政府服務型態，主要有三大功能：（1）資料下載，是依照個人需求提供民眾自行下載的個人資料；（2）線上服務，是透過線上服務授權方式，由民眾授權政府機關或民間業者取得其個人資料；（3）臨櫃服務，是當民眾辦理臨櫃業務時，可下載機關（構）臨櫃核驗所需資料。2019 年，各試辦單位已完成 MyData 平臺功能測試上架，上架的資料集有 18 筆（國家發展委員會，2019），2021 年 4 月正式上線，截至 2021 年 10 月底，增加至 110 筆，包含內政部 9 筆、財政部 13 筆、教育部 2 筆、衛福部 11 筆、交通部 10 筆、經濟部 11 筆、勞動部 10 筆、法務部 3 筆，其他部會也有 41 筆資料集釋出，在符合身分確認機制及安全控管措施下，可預期將陸續新增開放 MyData 平臺相關資料集，增加線上申辦之業務項目。

地方政府部分，由於過往地方政府對全國性資料取得困難、服務無法串接成一站式，以及線上申辦服務流程等問題，2018 年開始逐步試辦 MyData 平臺服務，**圖 34** 為嘉義縣政府 MyData 平臺申辦畫面。嘉義縣政府截至 2021 年 11 月，執行 62 項線上申辦示範項目，在 109 年 7 月 29 日至 110 年 11 月 23 日區間中，嘉義縣的線上服務服務提供者成功取得資料件數共有 454 件，包含社會福利及綜合服務這兩大類，社會福利：（1）老人福利，重陽節敬老禮金金融帳戶申請、敬老愛心卡、老人預防走失溫馨手鍊或項鍊、長期服務 2.0 線上申請；（2）身心障礙福利，身心障礙者生活補助、身心障礙者租賃房屋租金補助、身心障礙者輔具補助費用申請（免評估輔具）、身心障礙者職業重建服務申請轉介等。綜合服務：（1）農業相關登記申請，種苗業登記申請；（2）勞工之服務，勞資爭議調解申請；（3）一般民眾之服務，寵物登記、除戶申請、雜草叢生致影響環境衛生通報等。後續也期望能透過 MyData 平臺與一站式服務，將與「委託代理」制度相關的老人服務、身心障礙福利、偏遠地區申請服務、醫療查詢系統等服務進行改善與提供更為創新、便民之服務（曾憲立、蕭乃沂、宋同正，2020）。

圖 34：嘉義縣政府 MyData 平臺申辦畫面

資料來源：嘉義縣政府官網。

圖 35 為桃園市政府 MyData 平臺申辦畫面，「桃園市」為六都中第一個加入 MyData 平臺的直轄市，但相較嘉義縣政府而言，桃園市政府截至 2021 年 11 月底，僅執行 6 項線上申辦示範項目，在 109 年 7 月 29 日至 110 年 11 月 23 日區間中，桃園市的線上服務服務提供者成功取得資料件數共有 33 件，主要包含社會福利及綜合服務這兩大類，社會福利：（1）身心障礙者福利，專用停車位識別證；（2）婦女福利，中醫助孕養胎調理申請。綜合服務：（1）業者之服務，事業廢水處理專責單位或專責人員離職異動及因故未能執行業務之報備申請、毒性化學物質專業技術管理人員設置及變更；（2）地政士之服務，地政士開業（變更）登記申請；（3）社工師之服務，核發社會工作師執業執照。桃園市政府近年來也積極與府內機關進行深度的訪談，以掌握不同機關的需求，希望可以完成更多服務的介接。

圖 35：桃園市政府地政士開業（變更）登記申請申辦頁面

資料來源：桃園網路 e 指通官網。

圖 36 則為臺南市政府 MyData 平臺的操作畫面，臺南市是 2020 年新增的 7 個地方政府之一，包含為新竹縣、新竹市、高雄市、屏東縣、澎湖縣和宜蘭縣政府，臺南市政府截至 2021 年 11 月底，執行 41 項線上申辦示範項目，在 109 年 7 月 29 日至 110 年 11 月 23 日區間中，臺南市政府線上服務的服務提供者成功取得資料件數共有 541 件，包含社會福利及綜合服務這兩大類，社會福利：（1）老人福利，預防走失愛心手鍊申請、敬老愛心卡申請；（2）身心障礙福利，使用牌照稅身心障礙減免申請、身心障礙者專用停車位識別證申請；（3）低收入戶及中低收入戶福利，展翅高飛脫貧方案申請等。綜合服務：（1）勞工之服務，勞資爭議調解申請；（2）役男之服務，義務役在營服兵役證明書申請、役男免役證明書申請；（3）一般民眾之服務，火災證明申請、車輛行車事故鑑定申請等。

值得注意的是，臺南市政府已開始介接聯合信用卡處理中心的公務機關信用卡繳費平臺，以信用卡為繳費方式。而新竹市政府則是介接臺灣銀行系統透過四大超商、郵局、網路銀行、台灣 Pay 等繳費方式。

圖 36：臺南市政府敬老愛心卡申請頁面

資料來源：臺南市政府官網。

目前全臺各縣市當中「已推行」MyData 平臺的地方政府為 12 個；「尚未推行」的地方政府則為 10 個，顯示國發會推行的 MyData 平臺服務，目前並無遍及全臺各縣市，如**表 6** 所示。

表 6：目前臺灣地方政府執行 MyData 平臺之現況

是否推行 MyData 平臺	是否為直轄市	地方政府
已推行	直轄市	桃園市、臺南市、高雄市
	非直轄市	新竹市、新竹縣、雲林縣、嘉義縣、宜蘭縣、花蓮縣、屏東縣、澎湖縣、嘉義市
尚未推行	直轄市	臺北市、新北市、臺中市
	非直轄市	基隆市、苗栗縣、南投縣、彰化縣 臺東縣、金門縣、連江縣

資料來源：本計畫自行整理。

而在當前「已推行」之地方政府，「桃園市」為六都中第一個加入 MyData 平臺的直轄市[145]；「嘉義縣」則為非直轄市推行 MyData 平臺數量最多的縣轄市[146]。這兩個縣市透過串連原先散佈在各機關的資料，使機關之間資料取得複雜度下降，讓兩縣市民眾藉由 MyData 平臺獲得更便利的服務。惜目前民眾僅能進行

[145] 蘇文彬（2020）。MyData 地方政府實例：桃園市政府，中央與地方跨機關資料交換新作法，臨櫃申辦不只簡化更能無紙化，2021 年 3 月 10 日，取自：https://www.ithome.com.tw/news/139398。

[146] 呂妍庭（2020）。嘉縣打造全國最大 MyData 網站 一站式服務超便民，2021 年 3 月 10 日，取自：https://www.chinatimes.com/realtimenews/20201230006344-260421?chdtv。

一次性的同意授權使用，無法設定同意授權期限；當涉及第三方服務（如金融服務）須同時在平臺與服務提供端進行同意授權；部分服務需由服務提供端到 MyData 平臺下載檔案，無法直接向資料提供機關介接民眾的資料，若因個別服務需要，未能於八小時內下載檔案，則無法順利介接民眾同意提供之資料。

第三章　調查分析方法

為回答本計畫之研究目的：（1）優化現行 MyData 平臺數位服務流程，包含業務主管機關或個資稽核的行動指引等；（2）研提包含（但不限於）授權的時間區間、單次授權方式、知情同意查閱與存取等機制改進模式與方法；（3）研提知情同意操作介面或管理平臺架構供政府及第三方服務業者參考之規範指引；（4）彙整政府應該如何輔導廠商符合 GDPR 或 CBPR 體系之知情同意指引。本計畫彙整各國案例，如歐盟一般資料保護規則、美國加州消費者隱私保護法、新加坡個人資料保護法、以及亞太經濟合作會議的跨境隱私保護規則體系之隱私綱領對個人資料保護機制與法令，並透過 4 項研究方式回應上述研究目的，包含（1）文獻蒐集，文獻蒐集之成果如第二章所整理；（2）使用者體驗（User Experience, UX）問題診斷（下稱 UX 診斷），UX 診斷則針對優化現行 MyData 平臺數位服務流程，並以 3A 的架構分析之，聚焦於授權方式的簡化；（3）實驗法，針對知情同意文件的長度與呈現方式進行實驗設計；（4）專家訪談及座談，針對平臺現有與未來可能加入的服務提供者，訪談其對平臺及現行資料交換相關規範的建議，並舉辦專家座談會邀請各法學及資安學者、業務主管機關，提供資料釋出與授權機制之規劃建議。

研究目的與方法及相關資料來源的對照如**表 7**，各方法的操作說明與目前研究成果則見下節內容。

表 7：研究設計摘要

研究目的	研究方法與對象
1、MyData 平臺對個人資料保護、知情同意機制、線上授權流程簡化等管理模式的改善建議與改進方向	
1-1 業務主管機關或個資稽核的行動指引	整理蒐集國內外業務主管機關或稽核行動指引的文獻等
1-2 預先因應可能之跨領域、跨部門加值服務生態體系，發展所需之知情同意管理機制架構	整理蒐集國內外類似生態系，例如：衛福部 108 年委託研究案「強化電子病歷交換資訊安全及建立公私合營機制之評估研究」（醫療與保險業）；新加坡的 SGFinDex（政府與銀行業）
1-3 資料提供端—使用者—服務提供端間資料轉拋、介接之服務流程簡化	UX 診斷

研究目的	研究方法與對象
2、研提包含(但不限於)授權的時間區間、單次授權方式、知情同意查閱與存取等機制改進模式與方法	文獻回顧與訪談／資料需求端為主，如服務提供者的銀行
3、規劃並實驗可行之知情同意操作介面或管理平臺架構，提出精進 MyData 平臺設計原則，及可供政府及第三方服務業者參考之規範指引	1、實驗：設計原則與流程簡化圖，輔以系統實驗 2、訪談：預計訪談資料提供者、服務提供者、主管機關與平臺廠商 3、專家座談會：邀集相關法學及資安學者提供資料釋出與授權機制之規劃建議。
4、研議政府應該如何輔導廠商符合 GDPR 或 CBPR 體系之知情同意指引。(政府可以採取的措施，例如提供手冊、諮詢服務，技術指導之政策建議)	彙整各國指引手冊，瞭解其他國家知情同意機制，著重於檢視其國家是如何遵循 GDPR 及 CBPR 體系

資料來源：本計畫自行整理。

第一節　使用者體驗（UX）診斷

根據 ISO 9241-210 規範，使用者體驗的定義如下：「當使用者在接觸產品、系統、服務後，所產生的感知反應與回饋。使用者體驗包含使用者的情緒、信念、偏好、認知、生理及心理反應、行為及成就來源，其發生在產品系統服務使用的前期、中期以及後期。」簡而言之，使用者體驗強調的就是「使用者體驗的過程」，根據使用者的習慣去優化、安排整個頁面的內容規劃，讓使用者體驗的好感度及滿意度增加。本計畫透過研究助理真人實測 MyData 平臺與服務提供者兩方申辦服務的操作流程，彙整使用者體驗的表格及泳道圖並以此進行診斷。

MyData 平臺服務有三項功能，線上申辦，資料下載與臨櫃服務，本計畫聚焦在線上申辦業務，線上申辦業務又可分為政府間資料傳遞，以及民眾授權第三方介接政府資料以取得個人化服務（如申辦信用卡），本計畫依政府間資料傳遞服務，所涉及的機關單位數量以及層級（是否跨中央地方政府），選取了三個線上申辦服務做為測試標的，分別是**圖 37** 客家委員會—客家文化發展中心線上場地租借（單一機關）、**圖 38** 高雄市—申請地價稅自用住宅用地稅率（單一機關、地方政府）、以及**圖 39** 教育部—中低收入戶學生學雜費減免線上申請（跨機關、中央與地方政府）；在民眾授權第三方介接政府資料以取得個人化服務部分，選擇了信用卡線上申辦業務（包含台新銀行、臺灣銀行及彰化商業銀行），每個申辦業務先都由本計畫協同主持人向研究助理做診斷項目之說明，再由助理做線上

業務的申辦，全程側錄申辦過程，以了解在哪個申辦環節卡關或不順暢，並繪製作業流程圖，再透過申辦影片之檢討，提出流程簡化的建議。

圖 37：客家委員會—客家文化發展中心線上場地租借申辦頁面

資料來源：https://thcdc.hakka.gov.tw/#。

圖 38：高雄市—申請地價稅自用住宅用地稅率申辦頁面

資料來源：https://www.kctax.gov.tw/module/main.aspx?id=1&MenuID=1060。

圖 39：教育部—中低收入戶學生學雜費減免線上申請申辦頁面

資料來源：https://www.gov.tw/News3_Content.aspx?n=2&s=393138。

一、 作業流程圖介紹

作業流程圖是「統一塑模語言」（Unified Modeling Language, UML）的一種圖形，UML 圖是為了能夠更好理解、更改、維護或記錄訊息及資訊，其用視覺化的方式表現出系統及其主角色、動作、元素、要件或概念間的關係。UML 是由物件塑模技術（Object Modeling Technique）、物件導向的軟體工程（Object-Oriented Software Engineering）統一而來的符號。Visual Paradigm（2021）認為是這兩種主流方法的創辦人加入了「用例」（use cases）的概念而形成現今的 UML。1996 年，物件管理組織（Object Management Group）號召一些組織以 UML 1.0 的規範定義去建立了 UML 合作夥伴聯盟，發展歷程如**圖 40** 示。

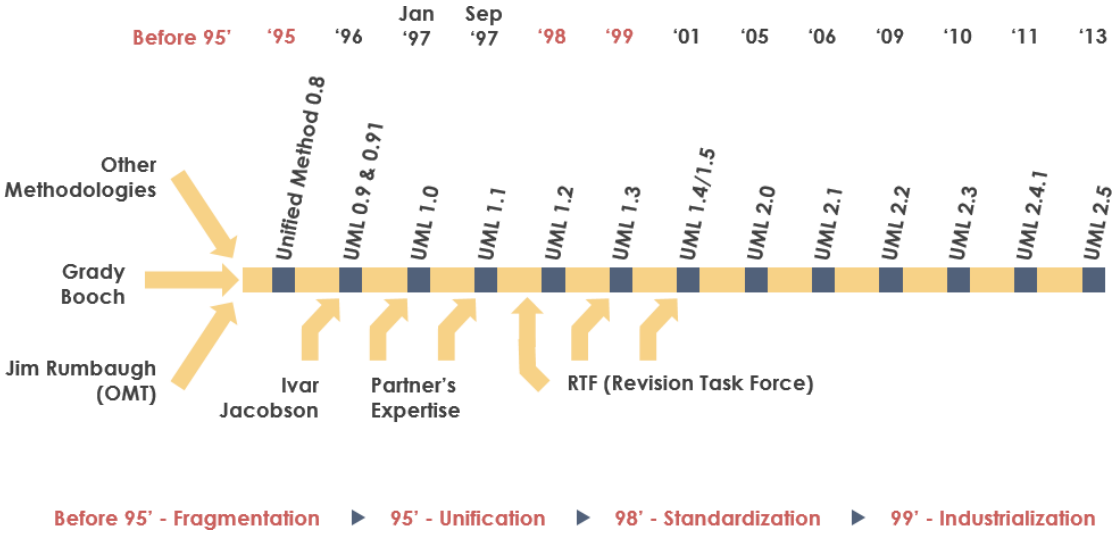


圖 40：UML 規範發展時程

資料來源：https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-uml/。

UML 圖分為「結構 UML 圖」及「行為 UML 圖」兩大類。

(一) 結構 UML 圖

結構 UML 圖顯示了系統的靜態結構及其在不同抽象和實現級別上的部分以及它們如何相互關聯，嘗試去分析和描述系統或過程的結構，此類型也有七種不同種類的圖（Visual Paradigm, n.d.）。

1、 類圖（class diagram）；

2、 組件圖（component diagram）；

3、 部署圖（deployment diagram）；

4、 物件圖（object diagram）；

5、 封裝圖（package diagram）；

6、 複合結構圖（composite structure diagram）；

7、 輪廓/剖面圖（profile diagram）。

(二) 行為 UML 圖

行為圖 UML 顯示了系統中對象的動態行為，可以描述為系統隨時間發生的一系列變化，描述系統的參與者及其建構組件的行為，有七種不同種類的圖（Visual Paradigm, n.d.）。

1、 用例圖（use case diagram）；

2、 活動圖（activity diagram）：「作業流程圖」為活動圖當中的一種呈現方式，詳細說明如後；

3、 狀態機圖（state machine diagram）；

4、 序列圖（sequence diagram）；

5、 通訊圖（communication diagram）；

6、 交互概述圖（interaction overview diagram）；

7、 時序圖（timing diagram）。

「作業流程圖」可以說是 UML 圖當中進行「業務流程塑模」最重要的「行為圖」，其用於描述系統的「動態」方面。活動圖本質上是流程圖的高級版本，在軟體開發中，它通常用於描述不同活動和行為的流程，既可以是單一順序的也可以是並行。它對從一個活動到另一個活動的流程進行模型構建，也描述一項活動當中所使用的消費或生產的物品以及不同活動之間的關係。活動圖關注的是「過程」，集中在導致彼此相互關聯的一系列活動上，所以開始和結束都是被清楚顯現出來。活動圖在商業當中很常被用來進行業務流程的建構，因為其將工作流的逐步活動及各項工作用圖形表示，可簡化複雜的業務規則及操作。在統一塑模語言當中，活動圖旨在對計算和組織過程（即工作流）進行模型建構。活動圖即為顯示流程（例如算法或業務流程）中的步驟和決策以及並行操作的美化流程圖。

活動圖是用來顯示軟體系統中特定的活動情形，和其他圖型最大的差異，就是它專注在「活動」上面，不會去理會物件、類別相關的問題。因此，活動圖型只關心活動的開始、過程、與結束。John（2013）認為活動圖由以下五個基本元素而組成：狀態與活動（state and activity）、轉換（transition）、分支（branch）、分歧與結合（fork and join）以及泳道（swimlane）。

(三) 使用時機

1、 透過檢查業務工作流以確定候選用例（candidate use cases）；

2、 確定用例的前置和後置條件（上下文）；

3、 用例之間／內部的模型工作流；

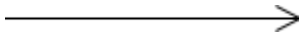
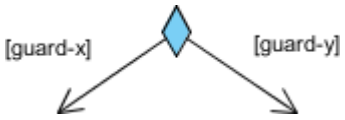
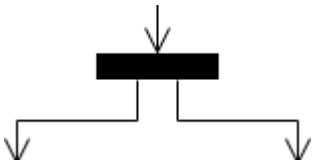
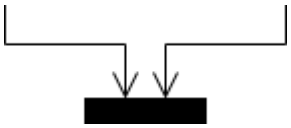
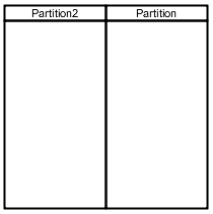
4、 對物件操作中的複雜工作流進行模型建構；

5、 在高級活動圖中對複雜活動進行詳細建模。

(四) 符號

UML 圖為一種圖像化的統一程式語言，活動圖（activity diagram）則是主要將活動的流程進行圖像化的呈現。因此，UML 圖有固定的符號，以**表 8** 簡要呈現出活動圖常會用到的 UML 符號以及符號的摘要說明。

表 8：活動圖符號彙整表

符號名稱	符號說明	UML 符號
控制流	顯示執行順序。	
對象流	顯示對象從一個活動（或動作）到另一個活動（或動作）的流程。	
活動	用於表示一組動作。	
行動	要執行的任務。	
活動最終節點	停止活動（或動作）中的所有控制流和對象流。	
對象節點	表示連接到一組對象流的對象。	
決策節點	表示一種測試條件，以確保控制流或對象流只沿著一條路徑走。	
合併節點	將使用決策節點創建的不同決策路徑重新組合在一起。	
分叉節點	將行為拆分為一組並行或併發的活動（或操作）流。	
加入節點	將一組並行或併發的活動（或動作）流重新組合在一起。	
泳道和隔斷	一種在活動圖上對同一參與者執行的活動進行分組或在單個線程中對活動進行分組的方法。	

資料來源：https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-activity-diagram/。

另一種「作業流程圖」，稱為泳道圖（swimlane）是「跨職能流程圖」，與普通的流程圖不同，泳道圖在原來的流程圖基礎上，能夠按照整個過程中設計到的人員、部門和功能範圍，旨在展示工作流中每個步驟涉及的流程和職能部門，將涉及的步驟、負責人、任務交接次數等資訊及過程更直觀地展現出來，泳道圖的樣式如**圖 41**。泳道圖的排版可以分為能夠凸顯「過程」的「水平跨職能流程圖」以及更強調「職能單位」的「垂直跨職能流程圖」，製圖者可以視不同情況而決定要使用哪一種排版方式。

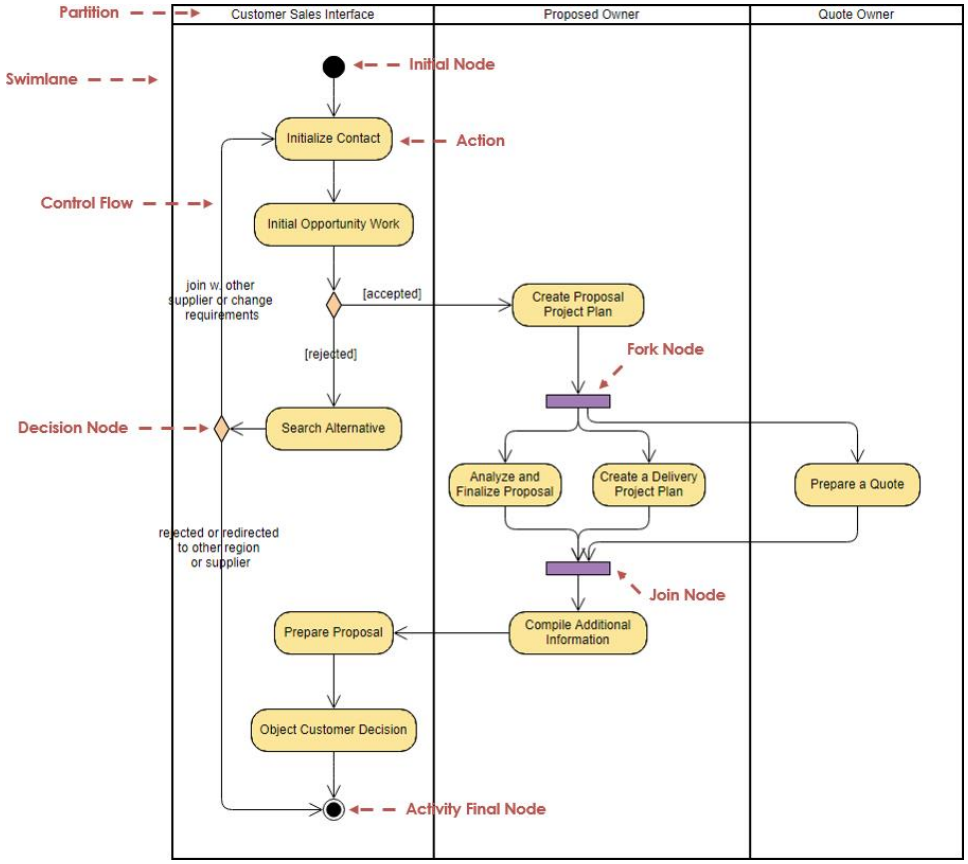


圖 41：泳道圖示例

資料來源：https://dotblogs.com.tw/Unified_Modeling_Language/2018/05/25/164538。

二、 泳道圖介紹

泳道圖是活動圖當中的一種特殊呈現方式，將流程畫成游泳道一般，主要是要「強調不同的角色之間的多方互動」，各有各的流程但彼此之間又會有互動的關係存在，泳道圖的最上面一列是參與作業的角色（人或系統），以我們的計畫案來舉例，泳道圖最上列當中涵蓋的角色有使用者、MyData 平臺以及不同的服務提供者。

(一) 泳道圖必須包含的重點（張國洋，2014）

1、 工作的流程與順序：

2、 哪一個工作先做、哪一個工作後做，呈現工作之間接續的先後順序。

3、 工作的分工方式：

4、 每一個工作分別由哪一個部門進行的。

5、 工作的分支狀況：

某些工作達成接續哪些工作事項，以及某些工作沒有達成又該如何處理。

(二) 泳道圖的作用（萬興科技，無日期）

1、 透過簡單且職務分配明確的泳道圖，將繁雜的資訊解釋清楚。

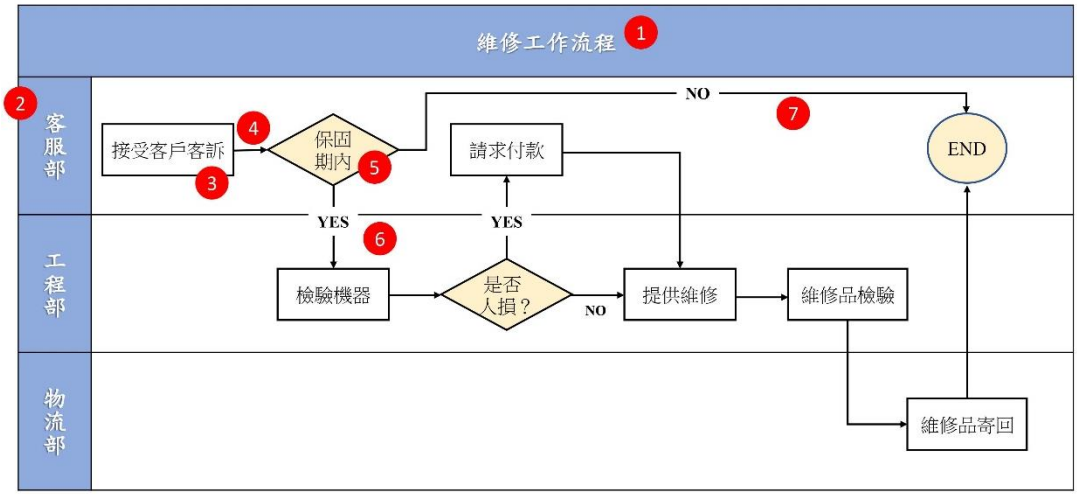
2、 對於企業而言，泳道圖能夠讓工作部署更加流程，提升工作效率。

3、 有助於研究整個流程中，人與人，或者是工作小組和工作小組之間交接的動作。

(三) 操作說明

張國洋（2014）認為泳道圖的架構其實可以拆解成兩張圖（如**圖 42**）。第 1 張圖是「流程圖」，包含了工作的流程、順序以及工作的分支狀況；第 2 張圖是「分工的結構」，每一個橫格子代表分工的狀況。實際使用上，這個欄目也可以劃分成組別、工作負責人等。而劃分的每個格子，結合在一起就像是游泳池的水道，這也是被稱為泳道圖的原因。

透過上一段的說明可以得出，泳道圖的繪製可以分為兩個部分，因此在繪製泳道圖的時候可以拆解成兩個步驟，第一步驟是先「繪製工作流程與順序」，第二步驟再進行「工作事項的分工」。



編號	項目	內容
1	名稱	說明這個流程是做什麼的，確保讀的人不用細看內容就能理解。
2	分工	說明這張泳道圖的工作事項分屬於哪一個單位或個人。
3	工作	方形圖案，嚴格講是流程圖。實際上就是一項必須要達成的工作。
4	工作順序	這條帶有箭頭的線，顯示工作跟工作接續的順序。有箭頭的那一端代表下一項要開始的工作。
5	決策點	菱形圖案，通常會有 YES 及 NO 兩個分歧路線。
6	YES 路線	當決策點的要素滿足時，工作往 YES 的路徑繼續。
7	NO 路線	當決策點的要素沒被滿足時，工作往 NO 的路徑繼續。

圖 42：泳道圖拆解說明

資料來源：
https://www.businesstoday.com.tw/article/category/80407/post/201805040057/%E6%8A%8A%E8%8A%B1%E5%9C%A8%E8%A7%A3%E9%87%8B%E6%B5%81%E7%A8%8B%E7%9A%84%E6%99%82%E9%96%93%E7%9C%81%E4%B8%8B%E4%BE%86%20%20%E2%80%94%E8%A4%87%E9%9B%9C%E7%9A%84%E5%B7%A5%E4%BD%9C%E5%88%86%E6%B4%BE%20%E8%AE%93%E3%80%8C%E6%B3%B3%E9%81%93%E5%9C%96%E3%80%8D%E6%B8%85%E6%A5%9A%E8%AA%AA%E6%98%8E%E7%99%BD。

圖 43 為本計畫操作「客家委員會—客家文化發展中心線上場地租借」線上申辦之錄影畫面，操作過程如下，先從 MyData 平臺搜尋想申辦的服務內容、閱讀平臺告知事項，系統會自動連結至服務提供者網站閱讀服務提供者的使用須知，行使同意後，系統會自動跳轉回 MyData 平臺進行身分驗證並閱讀服務條款，完成後 MyData 平臺會將資料傳給服務提供者並連結至服務網站，使用者繼續填寫資料後即申請完畢。

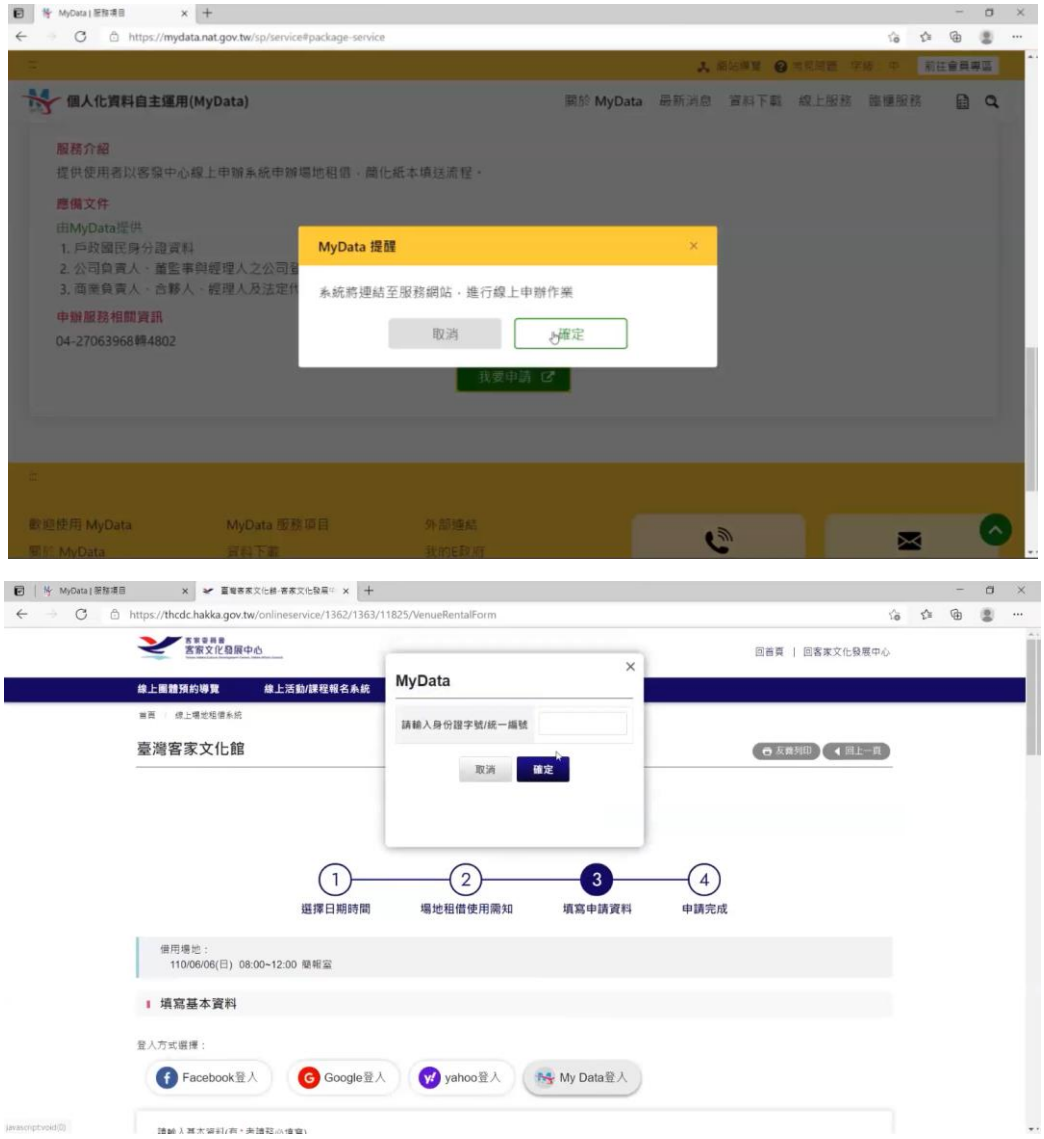


圖 43：UX 診斷錄影畫面

資料來源：MyData 平臺與客家委員會客家文化發展中心。

本計畫所使用之作業流程圖，其特色是把參與多方都納入考量，圖中呈現各自的活動，以及彼此之間的互動，比較能夠快速掌握全局，**圖 44** 為本計畫所產生之作業流程圖，以「客家委員會—客家文化發展中心線上場地租借」作業流程圖為例，圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站。

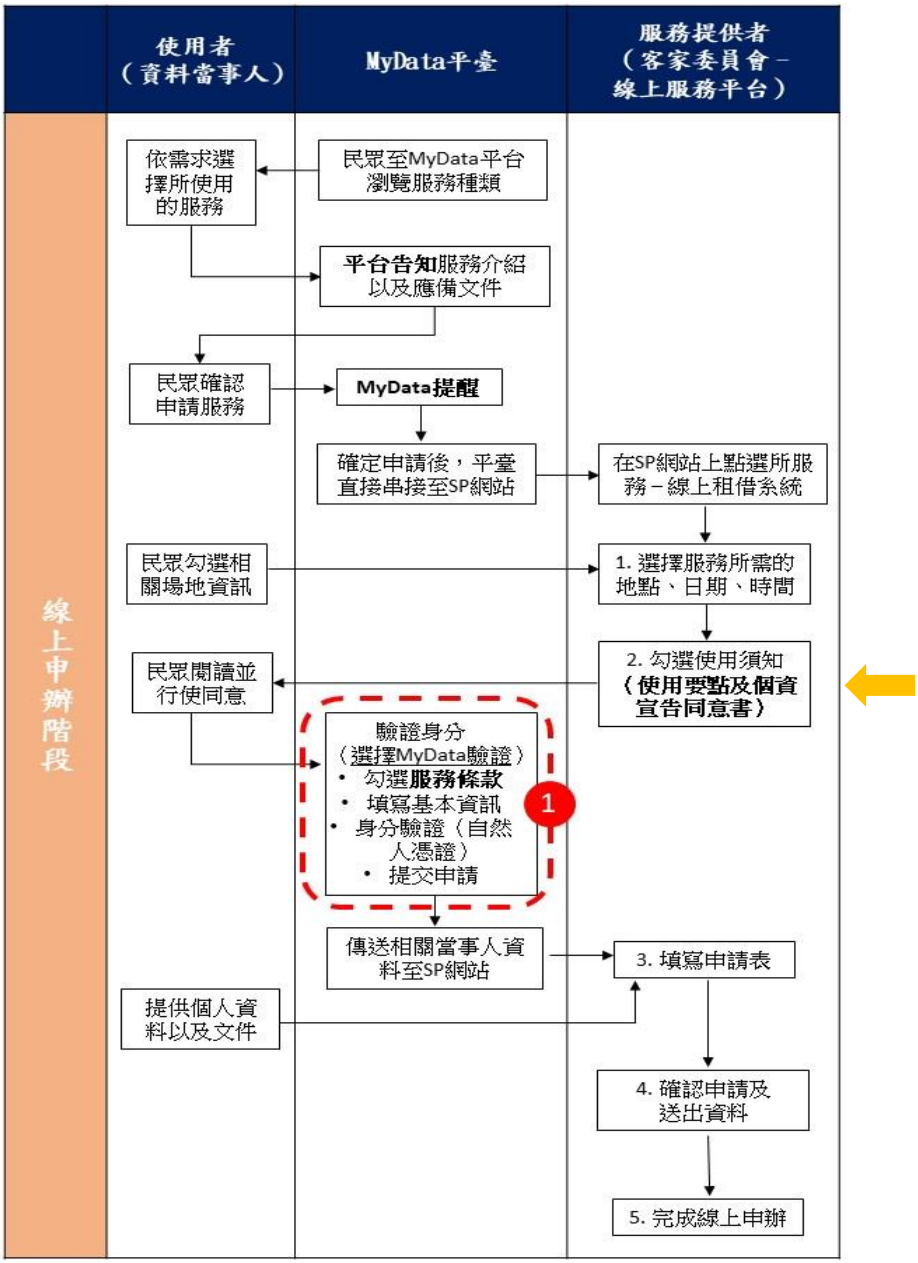


圖 44：線上申辦「客家委員會—客家文化發展中心線上場地租借」作業流程圖

資料來源: 本計畫自行整理。

（註：底線處為驗證方式，字體加粗處為使用者須按下同意按鈕的步驟）

第二節　實驗設計

本實驗有關知情同意呈現方式，以及如何避免第二章所談到知情同意內容過度冗長及繁瑣，內容多為純文字，使用者易有視覺上的比重差異，以及用語過於專業等問題進行小規模實驗。

本計畫首先針對相關研究進行文獻整理，例如 Sakshaung、Schmucker、Kreuter、Couper 與 Singer（2019）透過完全交叉 2×2 因子實驗設計（fully crossed 2×2 factorial design），探討知情同意所置放位置以及陳述方式對同意率的影響，該研究結果發現位置因素影響大於框架因素，研究還發現知情同意放在使用者一進入的開始位置時，知情同意率較高，這和過去問卷設計指引建議問卷結束時才問一些敏感或個資問題相左，此外，只有在將同意問題置於問卷的末尾時，框架因素在網路問卷中才有顯著影響，顯見知情同意的位置及陳述方式會造成同意率的顯著差異。Kodapanakkal、Brandit、Kogler 與 Beest（2020）針對六個領域（刑事調查、預防犯罪、公民分數、銀行、就業、醫療保健），在控制技術現況下（全新技術、他地已使用此技術、本地已使用此技術多年），設計一 2×3×2 的聯合實驗，探討結果有利性（outcome favorability，分正負面效果）、資料共享（data sharing，分不與第三方、與信任程度低、信任程度高第三方分享資料）和資料保護（data protection，有無加密安全儲存），對民眾 AI 巨量資料之科技採行（adoption）以及道德接受（moral acceptability）的影響，如**圖 45**。該研究結果發現，當資料受到安全保護、結果有利性下，民眾願意採行且道德上也接受巨量資料技術，特別的是在醫療保健領域，結果有利性對採行意願以及道德接受度的影響程度較大。此外，資料共享會微幅降低對巨量資料技術的偏好；科技使用現況在公民評分領域會影響道德接受程度，但對技術接受則不具影響力。

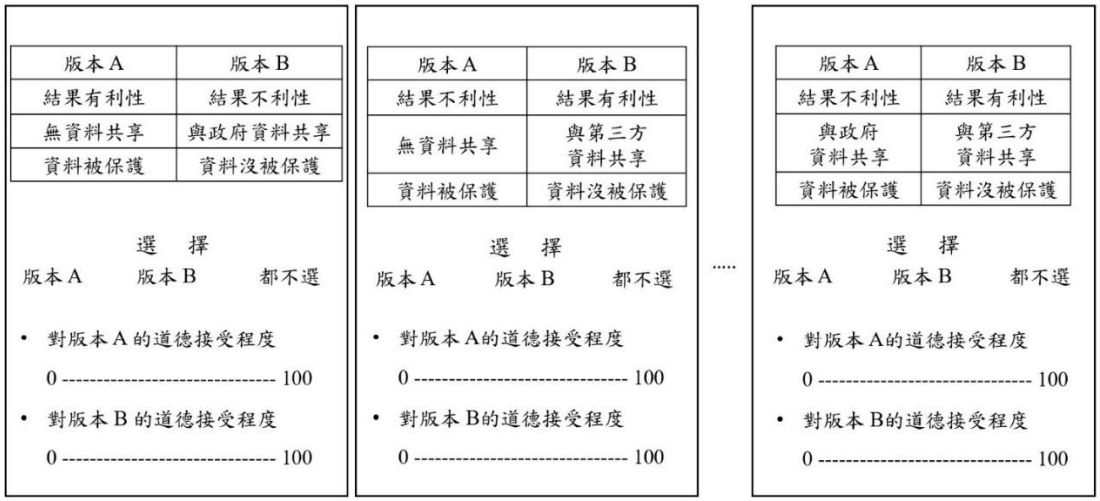


圖 45：Kodapanakkal et al.（2020）實驗設計

資料來源：Kodapanakkal, R. I, M. J. Brandit, C. Kogler, & I. V. Beest (2020). Self-interest and data protection drive the adoption and moral acceptability of big data technologies: A conjoint analysis approach. ***Computers in Human Behavior***, (108), 1–13.。

一、 實驗變數

由前述文獻可發現，知情同意的描述方式、位置（placement）、內容、是否有助推（nudging）、視覺化（visual effect）、乃至於載具（carrier）等因素都會影響同意率。考量 MyData 平臺線上申辦業務的屬性與流程，實驗的線上申辦項目為客家委員會—客家文化發展中心線上場地租借和高雄市—申請地價稅自用住宅用地稅率。以客家文化發展中心線上場地租借服務來說，在確認過所需要租借的場地之日期後，需同意場地使用須知與驗證身分，服務提供者平臺的「驗證方式」有四種，助理測試時選擇 MyData 平臺驗證（如**圖 44** 之 1 號虛線框），驗證成功後便可繼續填寫申請資料，送出申請即完成線上申辦業務。實驗的範圍為**圖 44** 粗箭頭所示之勾選使用須知。

本計畫藉由比較文本的不同呈現方式（文件式或圖像式、長版或短版）、地域不同之公私立學校（政治大學、臺南大學）、對隱私保護的態度（意識高低），以實驗方式了解民眾對知情同意文本閱讀的「花費時間」以及對文本的呈現方式，對文本內容的「正確理解」是否有所不同，具體而言，對文本內容的正確理解可能存在呈現方式、對隱私保護的態度、甚至地域不同的差異可能。

本計畫觀察的變項為對文本內容的正確理解，包含知情同意文本閱讀的花費、時間文本的呈現方式、對隱私保護的態度、地域差異等。

二、 研究設計

本實驗的研究問題牽涉知情同意文本的不同呈現方式，對民眾閱讀文本的花費時間與解讀正確性的影響。須以不同文本的設計方式驗證，故採用實驗法，希冀控制外來干擾變項以操縱一些自變項並觀察依變項變化，藉此測自變項間的關聯與交互作用。此外，我們也透過統計控制方式，觀察受試學生對隱私保護的態度（意識高低）的影響力。

故本計畫採用 4（知情同意文本）×2（地區）×2（意識高低）16 個實驗組別的三因子實驗設計。

三、 研究對象

為了增加實驗的內在效度以利對自變項的操縱與對依變項的觀察，以及受試者聯繫和參與實驗的便利性，本計畫招募對象以同質性高、年齡與教育程度相當的年輕族群為主。本計畫原預計招收 400 名受試者參與，進行時間為 2021 年 10 月間，受試者須為國立政治大學與國立臺南大學年滿 20 歲的學生。正式實驗以小團體（每次約 30-40 人）施測為主，每場實驗過程約為 30-40 分鐘，完整參與實驗者，將會給予超商提貨券 300 元以茲感謝，實驗所蒐集之資料不會辨識出個別的填答者，也不會對受試者有心理上的負擔，如果中途退出，則該筆資料不計入實驗統計結果，並會另外招募受試者補足樣本數。

四、 知情同意文本

本計畫針對民眾瀏覽知情同意文件的「花費時間」與「了解程度」，就「知情同意文件長度」與「知情同意文件視覺」做實驗設計，使用 Figma 軟體產出 4 個版本的知情同意呈現方式，如**表 9**。

表 9：本計畫實驗之情境

		知情同意文件長度	
		長	短
知情同意文件視覺	**非圖像化**	原版[147]	B 版[148]
	圖像化	A 版[149]	C 版[150]

資料來源：本計畫自行整理。

知情同意文件視覺化處裡部分，舉例來說，根據 GDPR 對「知情同意」的要求，同意書應使用容易理解的文字或形式。本計畫實驗設計將 MyData 平臺的資料下載及線上服務條款試改成以下形式，在主要頁面僅顯示服務條款的圖示及條款的小標題（如**圖 46**）。

147 原版知情同意文本 https://www.figma.com/proto/TsZZzsHaVoVNqL4hH91pNC/%E9%95%B7%E7%89%88%2B%E6%96%87%E5%AD%97?node-id=11%3A3&scaling=scale-down-width。

148 短版文字知情同意文本 https://www.figma.com/proto/Tn71q2O3RMQ9S9xensctw/短版%2B 文字?node-id=11%3A3&scaling=scale-down-width。

149 長版圖像知情同意文本 https://www.figma.com/proto/cXXCp5iBT9CrHpIy80VLpt/長版%2B 圖像_test?node-id=11%3A3&scaling=scale-down-width。

150 短版圖像知情同意文本 https://www.figma.com/proto/iTDzD7WO26dfQe70eJYToi/短版%2B 圖像_test?node-id=11%3A3&scaling=scale-down-width。

圖 46：MyData 平臺「資料下載及線上服務條款」模擬介面

資料來源：本計畫自行繪製。

除了圖像化外，實驗也加入階層化設計，使用者在主要頁面（第一階層）可以先閱讀較接近口語的簡短說明，以了解以了解此部分條約在規範哪些項目，而後，使用者須依序點擊各圖像（第二階層），閱讀條約內容（如**圖 47**）。

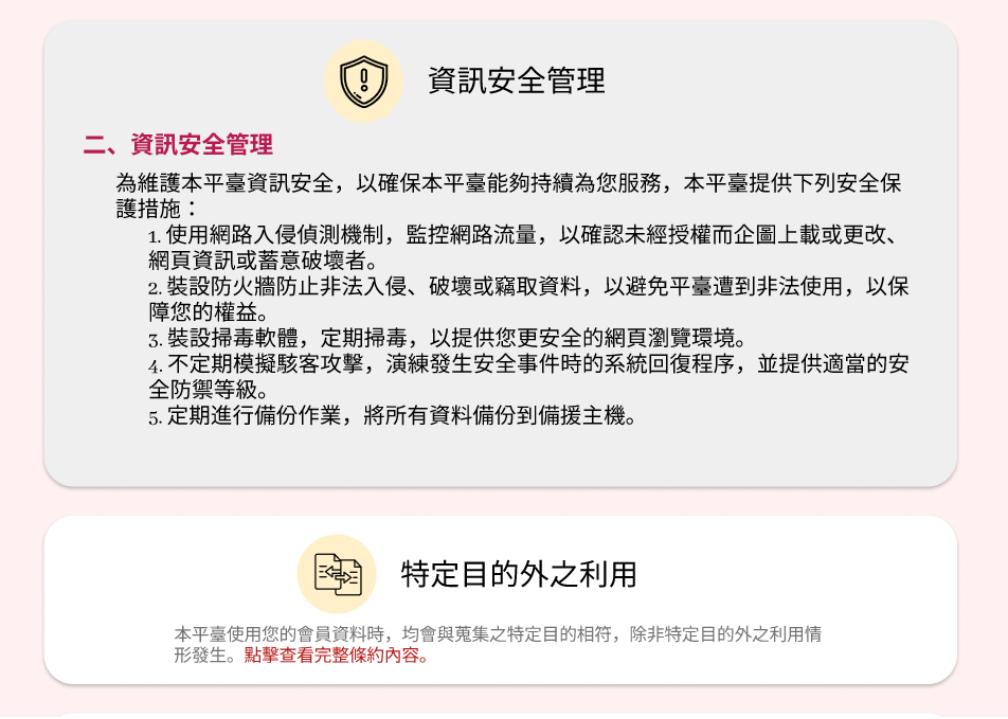


圖 47：點擊區塊後介面

資料來源：本計畫自行繪製。

五、 實驗問卷

為符合研究倫理的要求，本計畫於 110 年 9 月 24 日向國立政治大學研發處申請簡易倫理審查申請，並於 110 年 10 月 8 日通過，所有參與本計畫的受試者均會簽署一式兩份之研究知情同意書，同意書留存於計畫主持人的辦公室，此外，受試者實驗資料以代碼標示，並與受試者的身分資料分開存放於計畫主持人之電腦，若有紙本問卷，受試者知情同意書、紙本問卷皆另儲存於上鎖之櫃子，知情同意書與實驗資料有效期限皆為 3 年，到期後會刪除電子資料，紙本資料則另使用碎紙機銷毀。

本次實驗之招募問卷如**表 10**，共有三大構面，第一題到第三題為個人現況面，用以了解受試者平時習慣，並剔除有使用過「個人化資料自主運用（MyData）」平臺的受試者，避免影響實驗結果，第四題至第十三題為隱私保護的態度（意識）面，透過受試者填答隱私保護相關的問題，去了解該名受試者在隱私保護態度上的意識高低以進行實驗分組。第十三題到第十八題為個人基本資料，用以核對身分及後續聯繫。

表 10：招募問卷

構面	問題	選項
個人現況面	1、 請問您是否使用過「個人化資料自主運用（MyData）」平臺？	● 是 ● 否
	2、 過去一個月內，您是否曾同意任何網路服務條款或個人資料隱私保護文件？	● 有，是什麼樣的服務條款或隱私保護文件_____ ● 無
	3、 會讓你安心分享個人資料的原因？（例如分享手機內資料給 App）	● 顯示資料使用的情況 ● 通知我何時使用資料 ● 社交網絡中有人分享或使用 ● 讓服務更易於使用 ● 對隱私保護有更嚴格規範 ● 其他
隱私保護的態度（意識）面	4、 依《個資法》規定，公務機關對非敏感性個人資料之蒐集或處理，應有特定目的，並且符合下列何種情形之一，才可以為之？	● 執行法定職務必要範圍內 ● 對當事人權益無侵害 ● 經當事人同意 ● 以上皆是 ● 我看不懂這一題的題目或不知道答案
	5、 阿堯很喜歡上網，大美常常提醒他在網路上要好好保護自己的個人	● I & II ● I, II & III ● I, II & IV

構面	問題	選項
	資料。你能分辨以下資訊中哪些屬於個人資料嗎？ I. 聯絡方式 II. 財務情況 III. 社會活動 IV. 犯罪前科	● I, II, III & IV ● 我看不懂這一題的題目或不知道答案
	6、 以下何者是安裝行動裝置的應用程式（App）時，條款上不合理的權限要求？	● 直播視訊 app 使用裝置上的相機進行拍照或攝影 ● 地圖導航 app 要求精確位置(利用 GPS 和網路定位) ● 遊戲 app 要求讀取手機上的聯絡人 ● 網路社群 app 查看手機的 WiFi 或行動網路連線資訊 ● 我看不懂這一題的題目或不知道答案
	7、 下列四種資料中，何者不是《個資法》要保護的個人資料？	● 員工非匿名填寫的旅遊史 ● 已死亡人士的姓名與特徵 ● 人事室彙整的員工通訊錄 ● 打掃人員的健康檢查紀錄 ● 我看不懂這一題的題目或不知道答案
	8、 何者是《個資法》規定原則上不得蒐集、處理或利用之個人資料？	● 國民身分證統一編號 ● 出生年月日 ● 健康檢查 ● 指紋 ● 我看不懂這一題的題目或不知道答案
	9、 相較於其他人，我更不會輕易地提供我的個人資料。	7 點量表 ● 完全不同意 1 ● 完全同意 7
	10、相較於其他人，我對於註冊時要我填寫一堆個人資料的機關，會格外小心。	
	11、相較於其他人，我更在意其他人或機關如何處理或利用我的個人資料。	
	12、相較於其他人，我將「保有我個人資料的機密性」看得更重要。	

構面	問題	選項
	13、相較於其他人，我更擔心我的個人隱私受侵害的潛在威脅。	
個人基本資料	14、姓名 15、性別 16、年齡 17、學校/學院/系所 18、電子信箱/手機	自填

資料來源：本計畫自行整理。

本次實驗問卷如**表 11**，共有三大構面，第一題為個人基本資料，透過受試者的手機號碼核對身分及後臺資料，第二題到第四題為知情面，用以了解受試者閱讀文件後的信心、清楚程度及閱讀方式，第五題至第八題為測試題，用以測試受試者是否真的有閱讀並理解知情同意文本（MyData 平臺隱私權保護政策），第九題為呈現面，用以了解受試者的閱讀喜好。

表 11：實驗問卷

構面	問題	選項
個人基本資料	1、 手機	自填
知情面	2、 請問您，閱讀完個人資料隱私保護文件，是否清楚文件的內容？	7 點量表 ● 完全不清楚 1 ● 完全清楚 7
	3、 請問您，閱讀完個人資料隱私保護文件，對文件內容的解讀，覺得有多少的信心？	7 點量表 ● 完全沒信心 1 ● 完全有信心 7
	4、 請問您，剛剛閱讀個人資料隱私保護文件時，您的閱讀方式是？	● 仔細閱讀字句 ● 大略瀏覽 ● 僅閱讀特定部分
測試題（了解填答者對 MyData 平臺隱私權保護政策	5、 在 MyData 平臺下載資料，平臺僅留存個人資料八小時，之後會自動刪除。	
	6、 您使用 MyData 時，可以拒絕接受網站的 cookie 運用，而不影響使用權益。	● 是 ● 否 ● 不確定
	7、 MyData 服務會在服務條款更改時通知您，並讓您先瀏覽過條款後再行使同意。	

構面	問題	選項
是否知情）	8、 如果您改變主意，不再同意隱私條款，您認為應該怎麼做？	● 聯繫客服 ● 刪除會員帳戶 ● 其他（請註明）
呈現面	9、 請按照優先順序排列您希望在隱私條款聲明中看到的內容。	● 語言使用簡單，技術術語較少 ● 整體文長短 ● 一個區塊中只放少量文字 ● 通過問問題來確認用戶是否理解 ● 在條款頂部重點標示主要功能 ● 在條款頂部強調潛在的風險

資料來源：本計畫自行整理。

第三節　專家訪談與座談

為了解不同政府與組織應如何考量與調適 MyData 平臺在服務便利、身分驗證、個資隱私保護、與資訊安全等多方面的權衡，並發展個人資料保護、知情同意機制及線上授權流程簡化等管理模式的改善建議與改進方向及資料釋出與授權機制之規劃建議。本計畫規劃專家訪談與專家座談，說明如後。

一、　專家訪談大綱與出席人員

個別訪談約 40 至 60 分鐘不等，訪談對象有業務主管機關、服務提供者、資料提供者、第三方服務提供者這四個類別。本計畫訪談會在取得受訪者同意之後，以錄音、筆記等方式記錄訪談內容，並於整理訪談摘要與逐字稿後，與受訪者確認訪談內容。本計畫訪談名單與服務機關如**表 12**。

訪談大綱有四個構面，分別為策略面、法規面（側重知情同意事項）、風險效益構面及推廣應用面，訪談大綱並依這些構面延伸訪談問題，同時針對受訪機關在 MyData 平臺中不同角色，提供不同的訪談題目（**表 13** 中粗體部分）。

表 12：個別訪談名單

類別	機關單位
業務主管機關	國家發展委員會
	金融監督管理委員會
服務提供者	地方政府－嘉義縣
資料提供者	衛生福利部中央健康保險署 （針對健康存摺訪談）
第三方服務提供者	臺灣銀行
	中國信託銀行

資料來源：本計畫自行整理。

表 13：訪談大綱

	國發會	金管會	銀行	地方政府	健保署
構面	**訪談提問**				
策略面	請問您，貴單位推動 MyData 平臺的策略與目標為何？（組織內、外或第三方）				
			根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，銀行除擔任 MyData 平臺服務提供者外，也可申請成為平臺的資料提供者。基於資料雙向共享互惠的原則，想請教貴行對成為 MyData 平臺資料提供者的看法？	請問您，貴單位加入 MyData 平臺服務，考量的因素是什麼？（如接取中央資料、提供更快速的線上申辦服務、有效的資安防護等）	**根據「健康存摺系統軟體開發套件使用管理要點」，貴單位除擔任健康存摺 App 的服務提供者，也是 SDK 資料提供者。基於資料雙向共享互惠的原則，想請教貴單位推動第三方開發者的規範與想法。**
法規面	請問您，MyData 平臺在知情同意流程與呈現方式該如何精進以達成民眾資料自主管理的目標？				請問您，健康存摺在知情同意流程與呈現方式該如何精進以達成民眾資料自主管理的目標？
		請問貴會針對所轄管之金融機構及周邊單位，	**根據國發會「個人化資料自主運用（MyData）**	對於民眾申辦資料的保存或分析，依照什	**根據「健康存摺系統軟體開發套件使**

	國發會	金管會	銀行	地方政府	健保署
構面	訪談提問				
		申請成為 **MyData** 平臺的服務提供者，是否已經制訂了「審查作業要點」之類的規範，據以對其申請進行審查？若還在制定中，請問預計完成的期程是？	平臺介接作業要點」，貴行擔任服務提供者，如何確保介接 **MyData** 平臺提供當事人個人資料時，能確保個人資料之蒐集以最小化原則？其次在當事人同意提供其下載之個人資料前，以何種機制確保當事人對服務條款知情瞭解？	麼樣的個資保護規範？是否有稽查機制？	用管理要點」，貴單位如何確保介接提供當事人個人資料時，能確保個人資料之蒐集以最小化原則？其次在當事人同意提供其下載之個人資料前，以何種機制確保當事人對服務條款知情瞭解？
			根據國發會「個人化資料自主運用（**MyData**）平臺服務條款暨隱私權保護政策」中規範：「若您為未滿二十歲之未成年人，……當您使用本平臺時，即推定您的父母或監護人已閱讀、瞭解並同意接受本條款之		

	國發會	金管會	銀行	地方政府	健保署
構面	訪談提問				
			所有內容」。貴行目前是否將未成年線上開戶（數位存款帳戶）的服務與數位化個人資料自主運用平臺服務機關連結？倘若欲準備連結，如何確保線上申請並非未成年人自行操作？		
風險效益面	請問您，貴單位推動 MyData 平臺於線上申辦是否評估過個資保護或資料傳遞時的資安風險？				請問您，貴單位推動健康存摺時，是否評估過個資保護或資料傳遞時的資安風險？
	請問您，貴單位推動 MyData 平臺於線上申辦是否有效加快行政效率或民眾（使用者）滿意度？				請問您，貴單位推動健康存摺時，是否評估過有效加快行政效率或民眾（使用者）滿意度？

	國發會	金管會	銀行	地方政府	健保署
構面	訪談提問				
	有關資料提供者（DP）在MyData平臺上的使用情況，貴單位預計會在8月底於後臺提供機關查詢資料與服務，請問您，目前的發展進度？				
推廣應用面	請問您認為MyData平臺開發上的服務缺口為何？（如資訊素養、人員抗拒）				請問您認為健康存摺開發上的服務缺口為何？（如資訊素養、人員抗拒）
	銀行局是國發會最早接觸的示範單位，請問他們當初有提出哪些服務缺口？	請問您，希望MyData平臺未來還增加哪些資料集或服務？	貴行是參與國發會MyData平臺、擔任服務提供者的銀行業者之一。想請貴行就MyData平臺未來的發展提出一些建議。	請問您，希望MyData平臺未來還增加哪些資料集或服務？	想請貴單位就健康存摺服務，以及如何保障民眾知情同意、及資料利用的未來發展提出一些建議。
	請問您，希望MyData平臺未來還增加哪些資料集或服務？	**根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，貴會所轄管之金融機構**			

	國發會	金管會	銀行	地方政府	健保署
構面	訪談提問				
		及周邊單位，除服務提供者外，也可申請成為 **MyData** 平臺的資料提供者。故想請教貴會對於所轄管之金融機構及周邊單位，申請成為資料提供者的看法。			

資料來源：本計畫自行整理。

（註：字體加粗處為針對該機關的個別提問）

二、 座談會大綱與出席人員

本計畫另於 110 年 11 月 8 日舉辦線上專家座談，座談會邀請各法學及資安學者、業務主管機關，提供資料釋出與授權機制之規劃建議。會議時間為 100 分鐘，在取得與會專家同意後，以錄音、筆記等方式記錄訪談內容，並於整理摘要與逐字稿後，向與會專家確認訪談內容。專家座談的名單與服務機關如**表 14**。

- 議題一：請您就所知（或業務主管之經驗），分享國內外對知情同意授權機制的優化方式與挑戰（如資訊安全、資料保護、資料傳輸等）。
- 議題二：請您就本計畫目前執行成果，提供對個人化資料自主運用平臺（MyData）資料釋出或知情同意授權機制的優化建議，以及未來平臺精進方式的建議。

表 14：專家座談名單

類別	機關單位
業務主管機關	勞動部資訊處
法學專家	理律法律事務所
	世新大學法律學院
	國立成功大學法律學系
資訊/資安專家	中央研究院資訊科學研究所
	國立中山大學資訊工程學系

第四章　調查分析發現

為回答本計畫之四項研究目的，本計畫透過文獻蒐集、專家訪談及座談、使用者問題診斷與實驗法蒐集並彙整國內外業務主管機關或稽核行動指引的文獻，本計畫之調查分析發現，茲說明如後：

第一節　流程簡化

一、 3A 診斷

本計畫以 3A 面向對 MyData 平臺線上申辦流程進行問題診斷（如**表 15**），結果發現：（1）在驗證（Authentication）部分，服務提供者網站與 MyData 平臺兩者的驗證方式略有不同，MyData 平臺較為嚴格；（2）在授權（Authorization）部分，依民眾所選擇的服務項目，服務提供者間知情同意文件的呈現方式未一致（如同樣是信用卡申辦，不同服務提供者的知情同意文件內容與呈現方式均略有差異），由於平臺對知情同意文件的態度，目前採尊重服務提供者主管機關的審核，因此造成同樣是線上申辦業務，但不同的服務提供者對知情同意文件的內容與呈現方式均有所差異，若進一步考量知情同意文件的要式行為及呈現方式，可考慮階層化與圖像化呈現；（3）在紀錄（Accounting）部分，平臺前臺民眾可查詢所申辦業務的時間，後臺部分本計畫則沒有涉及。

表 15：3A 問題診斷表

申辦業務	客家委員會—客家文化發展中心 線上場地租借	高雄市—申請地價稅自用住宅用地稅率	教育部—中低收入戶學生學雜費減免線上申請
驗證	MyData 平臺： 自然人憑證、晶片金融卡、硬體金融憑證、TW Fido	MyData 平臺： 自然人憑證、晶片金融卡、硬體金融憑證、TW Fido	MyData 平臺： 自然人憑證、晶片金融卡、硬體金融憑證、TW Fido、健保卡、軟體金融憑證、雙證件驗證
	SP 網站： Facebook 、 Google 、 Yahoo、MyData	SP 網站： 跳轉至高雄市單一認證平臺，僅能選擇「自然人憑證」進行身分驗證	SP 網站： 測試流程中斷，無到此步驟
授權	1、會議場地使用管理要點及個資宣告； 2、MyData 平臺資料	1、自用住宅用地稅率申請說明； 2、高雄市民服務平臺	1、學雜費減免服務告知事項； 2、MyData 平臺資料

申辦業務	客家委員會—客家文化發展中心 線上場地租借	高雄市—申請地價稅自用住宅用地稅率	教育部—中低收入戶學生學雜費減免線上申請
	下載及線上服務條款	網路服務規定； 3、個人資料授權同意書	下載及線上服務條款
紀錄	民眾可透過會員專區，查詢個人申辦紀錄		
流程簡化	建議「統一讀卡元件」、可簡化身分驗證流程：用不同的驗證方式就需要下載不同的讀卡元件，例如：欲用健保卡驗證就需下載健保卡元件	建議「統一平臺元件」：從MyData平臺轉至高雄市的平臺，身分驗證時還需再下載高雄市平臺的安裝元件才能使用	因身分關係無法測試完整流程，因此無法提供流程簡化之建議
備註	1、使用者測試時發現Chrome瀏覽器有時無法操作，只要轉換成IE即可 2、SP網站的「驗證方式」有四種，助理測試時選擇MyData平臺驗證→如1號虛線框* 3、在109年07月29日至110年11月23日區間中，此線上服務服務提供者成功取得資料件數共有12件	1、「個人資料授權同意書」需要使用者點入才能觀看內容→如2號虛線框** 2、內部伺服器問題：助理測試時，有時可以進入高雄市平臺進行申辦、有時卻出現502 error而無法進入高雄市平臺 3、在109年07月29日至110年11月23日區間中，此線上服務服務提供者成功取得資料件數共有11件	1、使用者無中低收入戶身分，因此測試流程中斷→如5號虛線框* 2、在109年07月29日至110年11月23日區間中，此線上服務服務提供者成功取得資料件數共有573件

資料來源：本計畫自行整理。

*1號等虛線框請見**圖48。**

**2號、5號等虛線框請見附錄二，各UX診斷之作業流程圖所示。

二、 使用者體驗（UX）診斷

本計畫以使用者體驗診斷，測試 MyData 平臺的 6 個線上申辦業務，分別為：客家文化發展中心線上場地租借、高雄市—申請地價稅自用住宅用地稅率、教育部—中低收入戶學生學雜費減免線上申請（如**表 15**）、台新銀行、臺灣銀行與彰化商業銀行的信用卡線上申辦業務（如**表 16**）。結果發現：若為初次使用，由於憑證安裝與驗證步驟較繁瑣，極有可能降低使用者的使用意願，加上認證方式多為實體卡片、不同瀏覽器也會影響使用者體驗、尚未有能以行動裝置完成的線上申辦服務、甚至原本服務提供者的流程更為簡便。

表 16：台新銀行、臺灣銀行與彰化商業銀行信用卡線上申辦比較問題診斷

申辦業務	台新銀行信用卡 線上申辦	臺灣銀行信用卡 線上申辦	彰化商業銀行 線上申辦
驗證	MyData 平臺： 自然人憑證、TW Fido	MyData 平臺： 自然人憑證、健保卡、TW Fido	MyData 平臺： 自然人憑證、TW Fido
	SP 網站： 自然人憑證	SP 網站： 自然人憑證	SP 網站： 自然人憑證
授權	1、台新銀行使用 MyData 服務告知事項 2、MyData 資料下載及線上服務條款 3、信用卡相關功能告知事項	1、 個人網路銀行信用卡業務服務契約 2、 臺灣銀行股份有限公司履行個人資料保護法告知義務內容 3、 臺灣銀行信用卡重要告知事項 4、 信用卡申請書聲明及同意事項 5、 臺灣銀行信用卡/達人金融卡電子帳單服務契約約定條款 6、 臺灣銀行一卡通聯名卡特別約定條款 7、 臺灣銀行信用卡約定條款 8、 申辦臺灣銀行股份有限公司信用卡介接 MyData 平臺服務告知事項 9、 一卡通使用服務條款	1、彰化銀行信用卡申請線上服務使用條款 2、蒐集、處理及利用個人資料告知事項 3、MyData 平臺資料下載及線上服務條款 4、使用 MyData 平臺服務應注意事項 5、申請人聲明及同意事項 6、彰化銀行信用卡用卡須知 7、電子帳單服務約定事項

申辦業務	台新銀行信用卡 線上申辦	臺灣銀行信用卡 線上申辦	彰化商業銀行 線上申辦
紀錄	民眾可透過會員專區，查詢個人申辦紀錄		
流程簡化	建議「統一平臺元件」:從 MyData 平臺轉至台新銀行時須再下載台新銀行的安裝元件才能繼續使用	建議「統一平臺元件」：從 MyData 平臺轉至臺灣銀行雲端銀行時須再下載臺灣銀行的安裝元件才能繼續使用	建議「增加 MyData 平臺提供文件」：從 MyData 平臺轉至彰化銀行時需填的基本資料繁多，且內容多為可從 MyData 平臺取得的
備註	1、使用者測試時發現 Chrome 瀏覽器有時無法操作，只要轉換成 IE 即可； 2、「台新銀行使用 MyData 服務告知事項」無須使用者點選「同意」按鈕→如 3 號虛線框*； 3、從 MyData 平臺進行線上申辦僅有自然人憑證一個選項可以進身分驗證，但從官網直接申辦卻有三個選項（其他銀行信用卡、自然人憑證、紙本列印填寫）→如 4 號虛線框* 4、在 109 年 07 月 29 日至 110 年 11 月 23 日區間中，此線上服務服務提供者成功取得資料件數共有 556 件	1、使用者測試時發現 Chrome 瀏覽器無法操作，轉換成 IE 瀏覽器即可操作； 2、臺灣銀行線上辦卡條文審閱，有強制使用者須皆看完條款才能勾選同意→如 6 號虛線框*； 3、從 MyData 平臺進行線上申辦僅有自然人憑證一個選項可以進身分驗證。然而，從官網直接申辦信用卡時，在身分驗證的部分會跳轉至 MyData 平臺進行身分驗證，但僅能選擇「TW Fido」進行驗證； 4、有「第二次驗證」機制，但僅能選擇自然人憑證進行驗證； 5、完成申請時，有告知使用者其申辦過程中同意的條款細項有哪些，也可以去查詢案件的申辦進度→如 7 號虛線框* 6、在 109 年 07 月 29 日至 110 年 11 月 23 日區間中，此線上服務服務提	1、使用者測試時發現 Chrome 瀏覽器無法操作，轉換成 IE 瀏覽器即可操作； 2、點選「信用卡申請線上服務使用條款」前的文字說明有明確寫出將從 MyData 平臺拿取的資料→如附錄二 8 號虛線框* 3、在 109 年 07 月 29 日至 110 年 11 月 23 日區間中，此線上服務服務提供者成功取得資料件數共有 3946 件

申辦業務	台新銀行信用卡線上申辦	臺灣銀行信用卡線上申辦	彰化商業銀行線上申辦
		供者成功取得資料件數共有 1580 件	

資料來源：本計畫自行整理。

*3 號、4 號虛線框請見**圖 49**。

**6-8 號虛線框請見附錄二，各 UX 診斷之泳道圖所示。

診斷過程中，本計畫發現 MyData 平臺各服務的知情同意呈現方式不盡相同，當身分驗證方式（身分驗證）太過複雜時會影響到 MyData 平臺的使用意願及績效，因此在表格中增加「流程簡化」的建議欄位，希望透過流程的精簡、統一的平臺元件及統一的讀卡元件讓使用者的申辦感受更佳，進而增加使用意願。以**圖 48**「客家委員會—客家文化發展中心線上場地租借」作業流程圖為例（另外兩項診斷請見附錄一），圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站。以客家文化發展中心線上場地租借服務來說，在確認過所需要租借的場地之日期後，需同意場地使用須知與驗證身分，服務提供者平臺的「驗證方式」有四種，助理測試時選擇 MyData 平臺驗證（如**圖 48** 之 1 號虛線框），驗證成功後便可繼續填寫申請資料，送出申請即完成線上申辦業務。

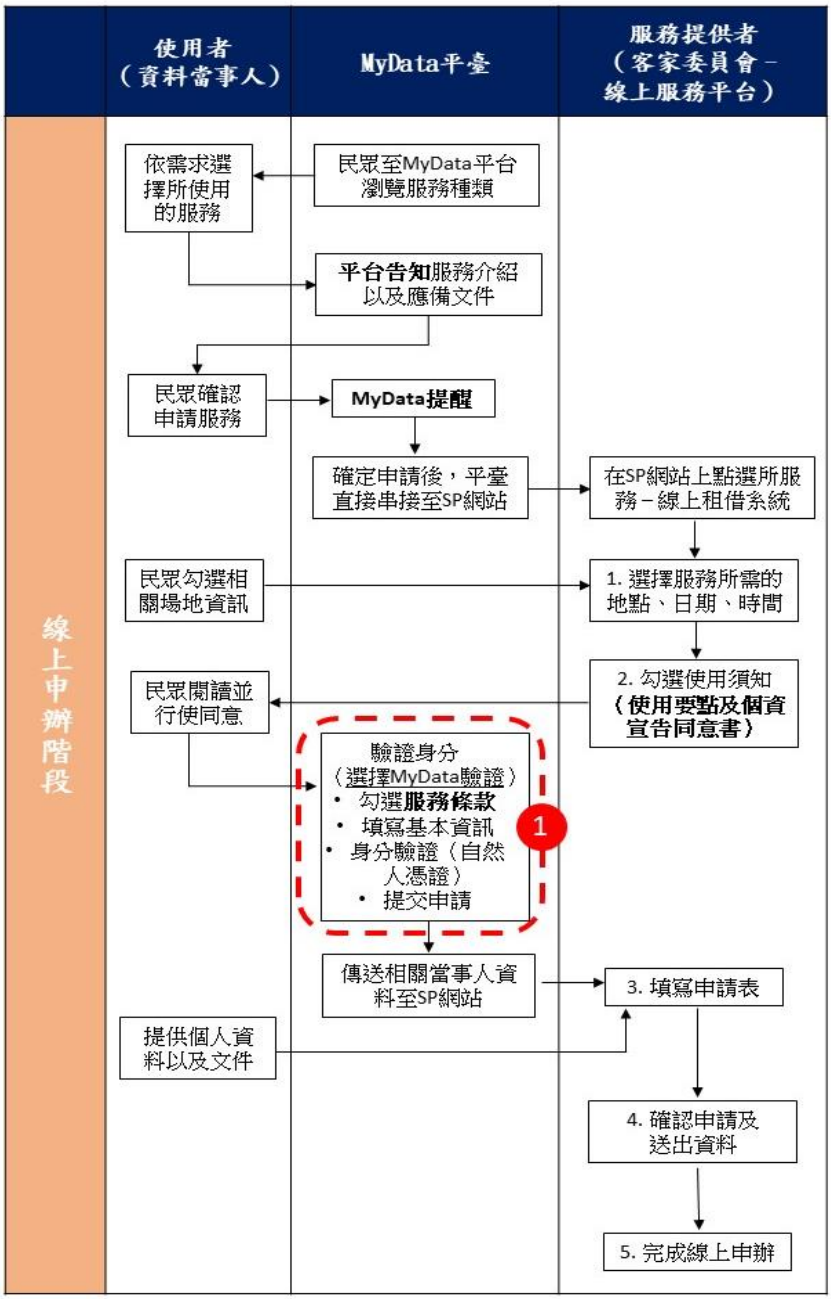


圖 48：線上申辦「客家委員會—客家文化發展中心線上場地租借」作業流程圖

資料來源：本計畫自行整理。

（註：底線處為驗證方式，字體加粗處為使用者須按下同意按鈕的步驟）

圖 49 為線上申辦「台新銀行信用卡」作業流程圖，圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站。以台新銀行申辦信用卡服務來說，需閱讀「台新銀行使用 MyData 服務告知事項」，此文件無須使用者點選「同意」按鈕（3 號虛線框），填寫身分證字號、生日、選擇卡片，並在 MyData 平臺進行第一次驗證身分，驗證成功後後會跳轉到服務提供者的網站，再次身分驗證，成功後便可繼續填寫申請資料，送出申請即完成線上申辦業務。

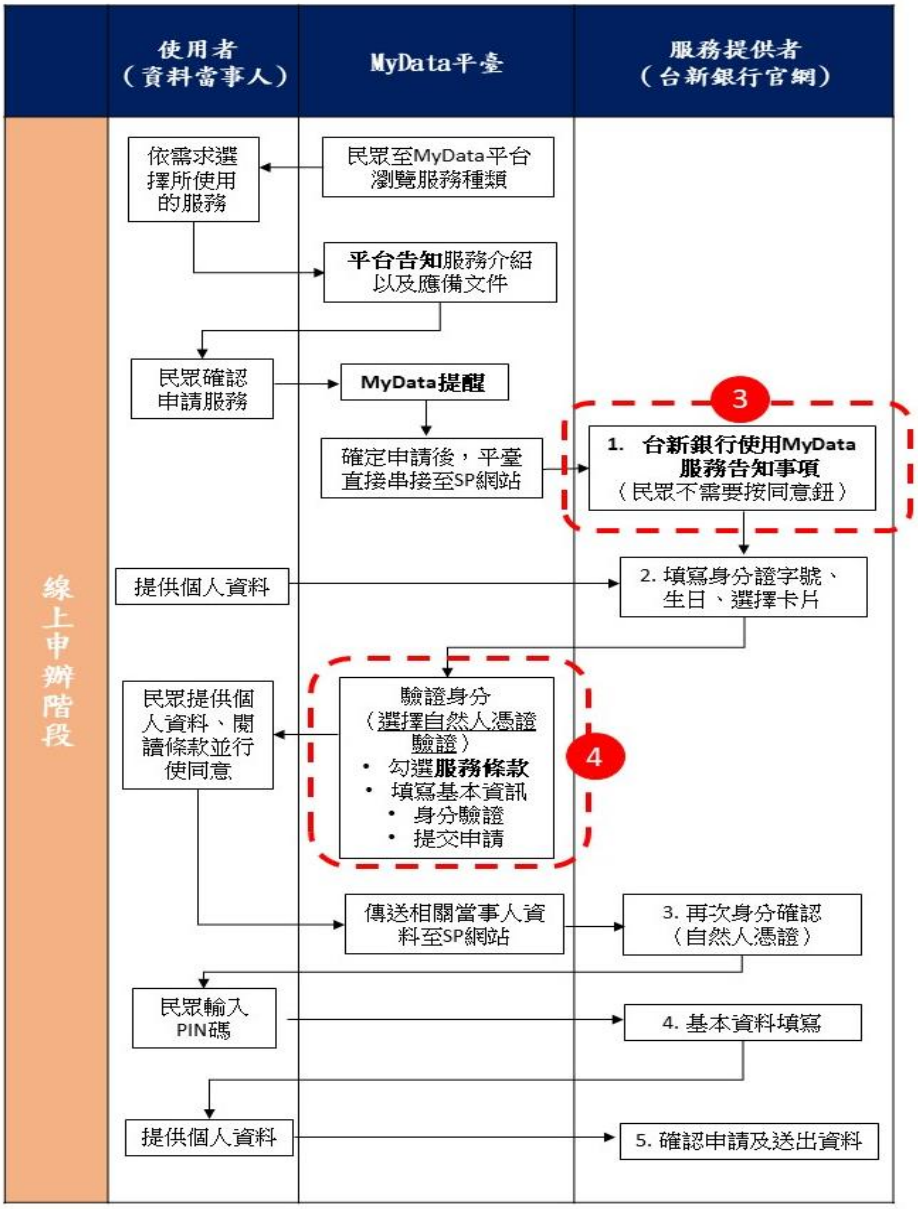


圖 49：線上申辦「台新銀行信用卡」作業流程圖

資料來源：本計畫自行整理。

（註：底線處為驗證方式，字體加粗處為使用者須按下同意按鈕的步驟）

第二節　知情同意實驗結果

本計畫於 10 月 26 日至 12 月 23 日間分別在政治大學與臺南大學招收實驗受試者，其中政治大學共 184 位受試者，臺南大學共 227 位受試者（已扣除一份無效樣本）。為了平衡受試者對法律知識的了解，實驗排除了法律相關系所的學生。關於兩校知情同意統計資料，茲說明如後。

總的來說，知情同意文件閱讀時間以長版圖像最高，達 139.11 秒；最短的是短版文字，僅需 72.02 秒。這點發現和原本假設圖像會減少閱讀時間不同，本計畫認為可能是因為是受試者在閱讀網頁時需要開合圖像中的文字，因而增加了其閱讀網頁的時間。

表 17 為受試者閱讀個人資料隱私保護文件所花費時間的統整。政治大學受試者閱讀知情同意文件的平均時間，長版圖像的花費時間最長，達 154.56 秒；其次為長版文字，達 134.67 秒；再來是短版圖像 117.71 秒；花費時間最短的則是短版文字，僅 75.55 秒。臺南大學受試者知情同意文件閱讀時間平均來說以長版圖像最高，達 123.66 秒；其次為長版文字，達 94.43 秒；最短的是短版文字，僅 69.18 秒。

表 17：知情同意文件閱讀時間一覽

	政治大學		臺南大學	
	平均數	中位數	平均數	中位數
長版文字	134.67	120.59	94.43	83.38
短版文字	75.55	69.12	69.18	46.56
長版圖像	154.56	147.48	123.66	88.61
短版圖像	117.71	115.11	89.14	83.15

資料來源：本計畫自行整理。

（註：單位：秒）

表 18 為受試者閱讀個人資料隱私保護文件的方式及了解程度的整理，閱讀完個人資料隱私保護文件之後的結果如下。政治大學約有 30.5%的受試者仍不太清楚文件內容、有 35.4%的受試者對於隱私保護文件的解讀不具信心；另外在 184 位受試者當中，有 114 位受試者在閱讀個人資料隱私保護文件的方式為大略瀏覽，比例高達 61.96%。臺南大學則是有 39.6%的受試者仍不太清楚文件內容，有 49.8%的受試者仍對於文件的解讀不具信心，此外，在 227 位受試者中，有 181 位受試者閱讀個人資料隱私保護文件的方式為大略瀏覽，比例高達 79.74%。

表 18：文件閱讀方式

題目	資料來源	完全清楚	清楚	有點清楚	普通	有點不清楚	不清楚	完全不清楚
1. 請問您，閱讀完個人資料隱私保護文件，是否清楚文件的內容？	政大	14	66	48	29	18	7	2
		7.6%	35.9%	26.1%	15.8%	9.8%	3.8%	1.1%
	南大	12	59	66	53	28	5	4
		5.3%	26%	29.1%	23.3%	12.3%	2.2%	1.8%
2. 請問您，閱讀完個人資料隱私保護文件，對文件內容的解讀，覺得有多少的信心？	政大	4	46	69	30	22	11	2
		2.2%	25%	37.5%	16.3%	12%	6%	1.1%
	南大	6	47	61	77	27	7	2
		2.6%	20.7%	26.9%	33.9%	11.9%	3.1%	0.9%
		仔細閱讀字句			**大略瀏覽**		**僅閱讀特定部分**	
3. 請問您，剛剛閱讀個人資料隱私保護文件時，您的閱讀方式是？	政大	41			114		29	
		22.28%			**61.96%**		15.76%	
	南大	20			181		26	
		8.81%			**79.74%**		11.45%	

資料來源：本計畫自行整理。

表 19 為受試者閱讀個人資料隱私保護文件後的理解正確性整理。可以發現三題測試題的錯誤率，政治大學分別為 47.28%、40.76%、89.67%；然而臺南大學則分別為 51.54%，36.12%，98.24%。錯誤率最高的是第三題「MyData 服務會在服務條款更改時通知您，並讓您先瀏覽過條款後再行使同意」。

表 19：理解正確性

題目	資料來源	正確	錯誤 / 不確定
1. 在 MyData 平臺下載資料，平臺僅留存個人資料八小時，之後會自動刪除。	政大	97	87
		52.72%	47.28%
	南大	110	117
		48.46%	51.54%
2. 您使用 MyData 平臺時，可以拒絕接受網站的 cookie 運用，而不影響使用權益。	政大	109	75
		59.24%	40.76%
	南大	145	82
		63.88%	36.12%
3. MyData 服務會在服務條款更改時通知您，並讓您先瀏覽過條款後再行使同意。	政大	19	**165**
		10.33%	**89.67**%
	南大	4	**223**
		1.76%	**98.24**%

資料來源：本計畫自行整理。

表 20 及**表 21** 為受試者希望在隱私條款聲明中看到的內容，問卷當中讓受試者以「排列該六個選項優先順序」的方式做提問。在政治大學的 184 位受試者當中，「語言使用簡單，技術術語較少」是被認為最想要在隱私條款當中所看到的，有 51 位受試者將該選項選為第一重要；而「通過問問題來確認用戶是否理解」則是被認為最不想要在隱私條款當中看到，有 101 位受試者將該選項選為最不重要。

表 20：希望在隱私條款聲明中看到的內容_政大

選項	被認為最重要的次數	被認為最不重要的次數
1. 語言使用簡單，技術術語較少	51	7
2. 整體文長短	23	31
3. 一個區塊中只放少量文字	27	26
4. 在條款頂部重點標示主要功能	42	6
5. 在條款頂部強調潛在的風險	35	13
6. 通過問問題來確認用戶是否理解	6	101

資料來源：本計畫自行整理。

在臺南大學的 227 位受試者當中，「語言使用簡單，技術術語較少」是被認為最想要在隱私條款當中所看到的，有 84 位受試者將該選項選為第一重要；而「通過問問題來確認用戶是否理解」則是被認為最不想要在隱私條款當中看到，有 131 位受試者將該選項選為最不重要。

表 21：希望在隱私條款聲明中看到的內容_南大

選項	被認為最重要的次數	被認為最不重要的次數
1. 語言使用簡單，技術術語較少	84	9
2. 整體文長短	35	28
3. 一個區塊中只放少量文字	18	28
4. 在條款頂部重點標示主要功能	48	16
5. 在條款頂部強調潛在的風險	37	15
6. 通過問問題來確認用戶是否理解	5	131

資料來源：本計畫自行整理。

第三節　國內外隱私法提要分析

本計畫彙整歐盟一般資料保護規則（GDPR）、美國加州消費者隱私保護法（CCPA）、新加坡個人資料保護法（PDPA）、亞太經濟合作會議的跨境隱私保護規則（CBPR 體系）之隱私綱領（APEC 隱私綱領）及我國對個人資料之蒐集、處理等行為的知情同意制度。以下分別針對國內外隱私法規適用範圍、一般個人資料、特種／敏感個人之料、知情權、及同意方式之作扼要比較。

首先在**表 22** 適用範圍中，歐盟 GDPR、APEC 隱私架及我國個資法構皆適用於公私部門，加州 CCPA 及新加坡 PDPA 原則上不適用於政府機構。且非如 PDPA 規範所有在依據新加坡法律或在新加坡設有辦事處或營業地點之私人組織，僅有在加州境內有營業行為且符合 CCPA 三項要件之企業才受到 CCPA 管轄。

表 22：國內外隱私法規適用範圍概覽

	GDPR	CCPA/CPRA	PDPA	APEC	我國
受規範主體	公私部門	企業	私人組織	公務機關、非公務機關	公務機關、非公務機關
規範境內	在歐盟境內設置據點之企業： ● 設立公司、子公司、分公司、事務所、辦事處等據點的企業 ● 派駐本國或非歐盟員工到歐盟境內的企業	於加州進行業務活動之企業	私人組織： 包含任何個人、公司、協會或個人團體、公司或未註冊公司，無論是否依據新加坡法律所設立，或在新加坡設有辦事處或營業地點	無規定	● 依法行使公權力之中央或地方機關或行政法人 ● 自然人、法人或其他團體
規範境外	● 對歐盟境內資料主體提供商品 或服務的企業 ● 在歐盟境內監控資料主體於歐盟境內行動的企業	無	區域外效力，PDPA 並無具體規定	無規定	公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法
受保護者	● 在歐盟境內的任何個人資料 ● 在歐盟設立的機構所處理的個人資料	加州居民： ● 非臨時或臨時目的而在該州者	新加坡自然人與死者	自然人	自然人

	GDPR	CCPA/CPRA	PDPA	APEC	我國
	（不限於歐盟境內的自然人）	● 居住在該州但臨時或因暫時目的而在該州外者			

資料來源：本計畫自行整理。

國內外隱私法規對於個人資料之概括定義皆包含任何能直接或間接識別特定個人（消費者）之資料，並對一般個人資料有例示規定如**表 23**。

表 23：國內外隱私法規定之一般個人資料

	一般個人資料	
	概括定義	**例示**
GDPR	● 關聯於一個已識別或可識別的資料主體的任何資料； ● 可直接或間接識別個人（自然人）之身體的、生理學的、遺傳基因的、精神的、經濟的、文化的、社會的固有性之相關因素	● 姓名、識別號碼（如社會安碼）、電話號碼、所在地資料、線上識別符號； ● 實務案例： 線上文件交換平台的使用者名稱與密碼認定為個人資料、有關安裝防止盜版文件分享之過濾軟體，認定 IP 位址是個人資料
CCPA	直接或間接地識別、關聯、描述、能夠合理地與某一特定消費者或家庭相關聯或可以合理地與之相關聯的資訊	聯絡資訊、社會安全碼、生物識別資料、商業資訊、地理位置資料、帳戶資料、學歷、商業資訊、網路或裝置識別碼，以及網路搜尋瀏覽及其他活動之紀錄
PDPA	無論真實與否，僅需為足以個人可識別之資料，其中識別分為直接識別及間接識別	PDPA 關鍵諮詢指引說明以下資料集屬於個人資料：涉及個人病例的電子郵件；私人通訊內容；客戶資料庫；將特定個人列入黑名單的通訊內容。以上 4 點可能被列為個人資料
APEC 隱私綱領	個人資料指任何關於可識別個人或足資識別該個人之資料	無例示規定
我國	直接或間接方式識別該個人之資料	自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動

資料來源：本計畫自行整理。

新加坡 PDPA 及 APEC 隱私綱領中尚無對特種／敏感個人資料定義，而歐盟 GDPR、加州隱私法規（CCPA 新修正法案及 CPRA）及我國個資法明文規定特種／敏感個人資料如**表 24**，且原則禁止蒐集和處理。

表 24：國內外隱私法規定之特種／敏感個人資料個人資料

	特種／敏感個人資料
GDPR	種族、政治觀點、宗教、哲學信仰、工會會員、基因、生物特徵資料、健康資料、性生活或性取向
CCPA	種族、宗教信仰、工會會員、駕駛執照或護照號碼、個人通訊、財務資料、基因、生物特徵資料、健康資料、性生活或性取向、精確地理位置
PDPA	無規定，惟新加坡衛生主管機關「健康科學局」，得針對醫療院（所）自行制訂法規命令，將病歷、個人健康資料等特別加以保護與管制
APEC 隱私綱領	無規定
我國	病歷、醫療、基因、性生活、健康檢查及犯罪前科

資料來源：本計畫自行整理。

其次，有關知情同意方式，歐盟 GDPR 要求當事人明確而肯定的同意，資料控管者須充分告知法定資訊、資料主體須出於自願同意且該同意者能力健全（選擇同意），換句話說，資料主體須先知情才能有效同意；加州 CCPA 同樣規定企業應於蒐集個人資料時或前，告知消費者法定資訊，有別於歐盟須告知後明確同意才能蒐集和處理個資，加州 CCPA 採取選擇退出制度，企業在合法告知後即可銷售當事人個資，當事人則有權於任何時間指示企業不得銷售其個人資料，同時 CCPA 針對選擇退出制度要求企業應提供「不要銷售我的個人資料」連結，並於施行細則推出選擇退出標誌；新加坡 PDPA 知情權規定組織應於蒐集個資前等情狀告知當事人法定資訊，並制定包含選擇同意、視為同意、選擇退出及同意之例外供各情狀使用；最後 APEC 隱私綱領，雖有明確規定資料控管者應盡到告知義務，並列舉告知事項，然而 APEC 隱私綱領以規定當事人自主原則，要求資料控管者應提供適當的機制，供當事人就其蒐集、利用和揭露個人資料方面做出選擇。有關國內外隱私法規應告知事項如**表 25**。

表 25：國內外隱私法規應告知事項及免為告知之事項

	GDPR	CCPA	PDPA	APEC 隱私綱領	我國個資法
應告知之事項	● 一般個人資料： 1、 控管者及其代表人身分及聯繫方式、資料保護專員之聯繫方式 2、 處理之個人資料之處理目的及該處理之法律依據、處理係依據 3、 第 6 條第 1 項第 f 點者，該控管者或第三人所追求之正當利益 4、 個人資料之接收者或接收者類型 5、 控管者欲將個人資料移轉至第三國或國際組織，及執委會是否 6、 提供適足性之決定等相關事宜 ● 進階資訊：	1、 企業蒐集之個人資料及類別和具體內容、 2、 蒐集的企業或商業用途、個人資料為「分享」之第三方（third parties）類別 3、 「已銷售」的個人資料類別 4、 銷售的每一類個資之「第三方」類別 5、 已因商業目的而揭露的個資類別 6、 已轉接的第三方類別	1、 於蒐集個人資料時或之前，告知蒐集、利用或揭露個人資料之目的 2、 在利用或揭露先前未告知目的的個人資料之前，對個人告知此額外之目的 3、 代表組織之聯繫人所提供的資訊，能滿足當事人有關其個資被蒐集、利用或揭露的問題 4、 當事人撤回同意方式	1、 個人資料正在被蒐集的事實 2、 蒐集個人資料之目的 3、 可能向其揭露個人資料之個人或組織的類型 4、 個人資料控管者的身分及位址，包括如何和個人資料控管者就其實踐和個人資料利用的聯絡資料 5、 個人資料控管者為限制個人資料的利用和揭露以及近用	1、 公務機關或非公務機關名稱 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

	GDPR	CCPA	PDPA	APEC 隱私綱領	我國個資法
	1、 個人資料被儲存期間、向控管者請求近用及更正或刪除或限制處理或拒絕處理與資料主體相關個人資料之權利，以及資料可攜權、向主管機關申訴之權利等 2、 就第 22 條第 1 項及第 4 項自動化決策（包括剖繪）者，為資料主體之處理涉及邏輯性有意義資訊、重要性與預設結果		5、 當事人近用或更正其個資方式以及組織的保留政策等	和更正個人資料提供的選擇和方法	
免為告知之情形	● 資料主體已有該資訊相關內容及範圍 ● 在第 13 條第 4 項中使用「就其範圍」一詞清楚表示，即使當事人先前已從第 13 條規定之資訊清單中取得某些類別之資訊，資料控管者仍有義務補充該資訊，以確保當事人擁有第 13 條第 1 項和 13 條第 2 項所列舉之完整資訊	1、 企業無義務在 12 個月內向同一消費者揭露兩次以上關於加州民法第 1798.110 和 1798.115 條所蒐集之個人資料類別及其使用目的	1、 個人被視為已根據 PDPA 第 15 或第 15A 條而同意企業蒐集、使用或揭露其個人資料 2、 根據 PDPA 第 17 條，企業在未經個人同意的情況下蒐集、	1、 蒐集及利用公開可獲的資料 2、 基於商業關係而取得的資料，或是關於當事人之專業能力的資料	1、 依法律規定得免告知 2、 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要 3、 告知將妨害

	GDPR	CCPA	PDPA	APEC 隱私綱領	我國個資法
			使用或揭露個人資料		公務機關執行法定職務 4、 告知將妨害公共利益 5、 當事人明知應告知之內容 6、 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響

資料來源：本計畫自行整理。

第四節　訪談與座談結果

本計畫於 110 年 7 月至 9 月間以視訊方式進行訪談，共 6 位，如**表 12** 個別訪談名單所列，專家訪談的目的是為了解不同政府與組織應如何考量與調適 MyData 平臺在服務便利、身分驗證、個資隱私保護、與資訊安全等多方面的權衡，並發展個人資料保護、知情同意機制及線上授權流程簡化等管理模式的改善建議與改進方向，訪談大綱有四個構面，分別為策略面、法規面（側重知情同意事項）、風險效益構面及推廣應用面，訪談大綱並依這些構面延伸訪談問題。個別訪談約 40 至 60 分鐘不等。在取得受訪者同意之後，以錄音、筆記等方式記錄訪談內容，並於整理訪談摘要後，與受訪者確認訪談內容紀錄之正確性（詳見附錄三）。

本計畫另於 110 年 11 月 8 日舉辦線上專家座談，座談會邀請各法學及資安學者、業務主管機關，提供資料釋出與授權機制之規劃建議，共 6 位，如**表 14** 專家座談名單所列。會議時間為 100 分鐘，同樣以錄音、筆記等方式記錄訪談內容，並於整理訪談摘要後，與受訪者確認訪談內容紀錄之正確性（詳見附錄四）。

以下簡要整理附錄三與附錄四各受訪者對 MyData 平臺在策略面、法規面（側重知情同意事項）、風險效益構面及推廣應用等面向，以及資料釋出與授權機制之規劃建議的綜合意見。

一、　推動策略

(一) 優化會員專區

目前 MyData 平臺會員專區，已含完整使用、下載紀錄，在推動策略上，可配合資安保護需求增加文字敘明（如平臺為單次授權、不保存資料等），並持續優化使用者介面與呈現方式，讓會員專區成為民眾使用資料的儀表板，從社會信任的角度來說，也可以累積民眾對於平臺的信心。

(二) 給予民眾近用權

為簡化知情同意內容與同意之設計，平臺可考量提供民眾近用權（right of access control），由民眾自己選擇是否要更深入了解知情同意內容，讓不同取向的民眾各自擁有適合的知情同意機制。未來或許可以朝定型化契約發展，知情同意書可刪減「共通素養」（社會中已形成共識）的內容篇幅，或以階層化方式呈現，將蒐集目的及法規重點放在首頁，其他細節（GDPR 要求告知事項）整理成文件放置於第二頁。

(三) 介接線上化

受訪單位也對申請方式提出建議，若要申請介接 MyData 平臺，仍須透過紙本申請書與發文程序，公文往返、紙本文件修訂，介接程序繁瑣且耗時，建議能提供線上同意書，以加速行政程序。

二、 特種資料之蒐集、處理或利用

截至目前，MyData 平臺僅蒐集、處理或利用一般個人資料，並未有蒐用特種個人資料之情形。衛福部訪談中也提及其服務項目有健康保險資料，而保險資料並非我個個資法所規定之特種資料。

雖個資法第六條第 1 項原則規定，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。惟上述特種資料並非完全禁止蒐集、處理或利用，依同項但書規定，有法定例外適用之情形，包含：

(一) 法律明文規定。
(二) 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
(三) 當事人自行公開或其他已合法公開之個人資料。
(四) 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，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) 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
(六) 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

應得以經當事人書面或電子方式所為同意，作爲合法蒐集、處理或利用特種資料要件之一，故 MyData 平臺未來可評估是否將特種資料，納入服務項目內，確保平臺隱私保護權政策及相關文件將特種資料法規定列入，並盡告知義務。

三、 資安風險與效益

民眾使用的滿意度和授權方式直接相關，受訪者提出插卡驗證會增加推動的難度，但簡易（便）的授權方式會提高風險，在合規與便利使用的平衡上，服務提供者可以理解與配合，以銀行端的角度而言，若可取得民眾在政府端的資料，資料品質與正確度比民眾自行提供更為可信，因此服務優化的關鍵還是在於流程簡化。

從民眾第一次透過 MyData 平臺進行線上申辦時需要雙重驗證，加上服務提供者端驗證完，還需要到 MyData 平臺再進行一次身分驗證，多道流程產生斷點及不便利性會增加民眾放棄的可能，金融業者就希望可以在服務提供者端做驗證

或改以軟體開發套件（Software Development Kit, SDK）提供銀行嵌入服務流程中，並搭配文字說明來進行，以確保民眾知道該個人化資料自主化運用是由MyData 提供服務，並可兼顧服務體驗。

雖然第二次之後的使用簡化了驗證方式，但不同資料主管機關所要求的認證方式略有差異，以自然人憑證最為廣泛，但仍須考量需要下載多種類別資料的申辦服務時，驗證方式的強弱程度。另外，由於平臺的服務大多都是非經常性服務，很多民眾只使用過一次 MyData 平臺或使用間隔非常長，或可考慮調整授權方式，如期間授權，如同開放銀行（open banking）對第三方服務提供者的授權方式，以提升資料運用價值。

四、 以整合平臺為目標

現行 MyData 平臺無法以請求製給複製本權來縮減蒐用資料當事人知情同意流程。若 MyData 平臺作一整合平臺，為便於民眾取得其個資，於個資法第 15 條範圍內，限於資料當事人向政府機關請求將其存於資料庫（database）中之個資提供給資料當事人時，僅需盡法定告知義務，無需同意。即各政府機關得委託國發會 MyData 平臺進行資料當事人的資料處理或利用，作第一層告知同意，降低須多次取得同意之不便；至於平臺對接銀行和國營企業則或回溯個資法第 7 條第 2 項，僅需提及特定目的外之同意為何，再取得一單獨同意，換言之，此設計應可縮減目前 MyData 平臺隱私權政策篇幅。

前述「資料當事人向政府機關請求將其存於資料庫（database）中之個資提供給資料當事人，僅需盡法定告知義務，而無需同意」，該情狀係指當公務（或非公務）機關蒐集個資時，需告知後取得資料當事人同意。而該筆資料存放於機關資料庫中，此時資料當事人想藉由 MyData 平臺（使用平臺服務前須先知情同意服務條款及隱私保護政策）取得資料庫中其個資，相當行使個資法第 3 條請求製給複製本權，無需再行同意。

第五章　結論與政策建議

第一節　研析結論

本計畫主題為個人資料授權應用與知情同意管理機制之研析，針對彙整國內外法規研提 MyData 平臺對個人資料保護、知情同意機制、線上授權流程簡化等管理模式的改善建議與改進方向之研究目的有以下結論：

一、　知情同意文件之呈現方式可採圖像化與階層化方式呈現

由本計畫文獻、實驗與專家座談之結果發現，知情同意文件之呈現方式可採圖像化與階層化方式呈現，以利民眾閱讀，圖像化標記可由主管單位統一訂定，而階層的設計部分，階層不宜過多，以三層為限。

本計畫於實驗發現，希望在隱私條款聲明中看到「語言使用簡單，技術術語較少」，為政治大學與臺南大學受試者認為「最重要」次數最多的內容；以「大略瀏覽」的方式閱覽文件中，政治大學受試者比例佔 6 成左右，臺南大學則高達 8 成，且僅有政治大學 8%及臺南大學 5%的受試者表示其完全清楚個人資料隱私保護政策內容。實驗結果顯現受試者在面對篇幅不短、深澀且較難理解的法律或技術專業用語告知文件時，以大略瀏覽方式為多數。事實上，於應用服務授權同意時，同樣常見使用者直接勾選同意省略閱讀服務條款及隱私權保護政策等情狀發生。考量到僅有少數資料當事人對資料控管者所發布的條款及政策全程仔細閱讀字句，且無論仔細閱讀、大略閱覽，或僅閱讀特定部分，資料當事人是否正確清楚告知事項，無法探查得知。以上情狀將導致告知效果不明，進而對於民眾知情權益產生負面影響。

回顧我國個資法有關知情相關規定，僅規定資料當事人有知情權、資料控管者有告知義務及法定應告知事項，為落實及確保資料當事人充分知情，以保障資料當事人之資料自主權行使。建議 MyData 平臺服務條款、隱私權政策聲明等於網頁介面上以分層化（layered approach）與圖像化之設計，降低平臺使用者閱讀理解門檻，設計分別可參考國外法規規定：

(一) GDPR 所規定之分層化資訊通知

歐盟 GDPR 與支付服務指令相互運用指引 2.0 版[151]第 78 點提到，關於線上支付服務，資料控管者可採用分層方法，可選擇結合多種使用方法來確保透明度。特別建議使用分層的隱私聲明／通知來連結到必須提供給資料主體的各種類別

[151] Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0 Adopted on 15 December 2020.

的資訊，而非僅在螢幕上單一通知中顯示所有相關資訊，以避免資訊疲勞（information fatigue），同時確保資訊的有效性。

以及，歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party, WP29）發布 GDPR 透明化指引（Guidelines on Transparency under Regulation 2016/679）中第 8 點提到，為避免資訊疲勞（information fatigue），資料控管者應該有效率地和簡潔地提供資訊／溝通。此類資訊應和其他非隱私相關資訊（如契約條款或一般使用條款）做出明確之區分。在網路環境中，使用階層隱私聲明／通知將能夠引導當事人至其想要立即取得隱私聲明/通知之特定部分，而不需瀏覽大量文本以搜尋特定之項目[152]。其中，GDPR 透明化指引與 GDPR 與支付服務指令相互運用指引 2.0 版同樣提到，分層隱私聲明／通知應使用連結方式，至須提供給當事人之各類資訊，而非僅在螢幕上單一通知中顯示所有相關資訊。另外應注意，分層隱私聲明／通知並非須經多次點擊始能獲得相關資訊之嵌套頁面（nested pages）。隱私聲明/通知的第一層設計和版面，應使當事人能就處理其個人資料可取得之相關資訊有清楚之概觀，以及在何處／如何於隱私聲明/通知的各個階層中找到詳細資訊[153]。

對於分層式隱私聲明／通知之內容設計，WP29 於 Opinion 10/2004 on More Harmonised Information Provisions [154]中建議：

1、 第一層「簡短告知（the short notice）」：

第一層形式應包含處理目的之詳細資訊、控管者之身分和資料主體權利之描述，亦應包含對當事人產生重大影響或使其感到意外之處理的相關資訊，使當事人得以理解該資料處理將產生之後果[155]。另外，當使用手機等行動裝置時，由於螢幕畫面有限、較為窄小之情形，可「使用非常簡短告知（use very short notice）」的方式[156]。

2、 第二層「濃縮告知（the condensed notice）」[157]：

此層告知資訊包含公司名稱、資料處理目的、資料收受者（data rerecipients）或資料接受者類別、對問題的答覆是否為強制性或自願性，

[152] 國家發展委員會（n.d.）。GDPR 透明化指引文件中英翻譯對照，2021 年 11 月 8 日，取自：https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS8wY2MxN2RhMC01NGI3LTQ1ZjMtODRiOC03OWQzN2JmMmJkYzUucGRm&n=6YCP5piO5YyWLeWIiueZu%2bWumOe2sueJiC5wZGY%3d&icon=..pdf。

[153] GDPR 透明化指引第 35 點。

[154] ARTICLE 29 Data Protection Working Party (2004). ***Opinion 10/2004 on More Harmonised Information Provisions***. Brussels: European Commission.

[155] GDPR 透明化指引第 36 點。

[156] ARTICLE 29 Data Protection Working Party, *supra note* 141, at 8.

[157] ARTICLE 29 Data Protection Working Party, *supra note* 141, at 9.

及不回覆可能產生的後果、個資移轉第三人的可能性、個人得選擇，以及近用、更正及拒絕的權利。

3、 第三層「完整告知（the full notice）」[158]:

此層告知內容必須包括所有國家的法律要求與特定性（specificities）。告知方式可包含一份完整的隱私聲明，並附上指向各國聯繫資訊的連結。

(二) GDPR 透明化指引所規定之標準化圖示

GDPR 規定在適當情況下可提供視覺化之工具（特別是圖示、認證機制和資料保護標章和標誌）[159]。有關圖示之規定依 GDPR 第 12 條第 7 項規定：「根據第 13 條和第 14 條提供予當事人之資訊，可與標準化圖示（standardised icons）組合使用，以便提供易見、易懂且清晰易讀之方式，並就預計之處理提出有意義之概述。當圖示係以電子方式呈現時，應使用機器可讀取之方式」。然而，WP29 也提出圖示能否有效地將第 13 條和第 14 條所要求之資訊傳達予當事人，取決於該符號／圖像之標準化，是否在歐盟境內被普遍使用和承認。

二、 現行個資稽核方式宜再優化

以 3A 模式來說，紀錄（accounting）包括量測（measuring）、監控（monitoring）、報告（reporting）各種資源使用量及事件紀錄（log），以提供後續的稽核（audit）、計費（billing）、分析（analysis）與規則管理，因此紀錄的主要精神在於蒐集必要的使用者與系統之間互動的資料，考量民眾個資數位化傳遞過程，應符合資通安全管理法，甚至 ISO 27001、27701 等規範，針對健康與醫療產業的資訊安全管理需求，國際標準組織另提供了 ISO 27799:2016，指引如何保護個人健康的資訊，規範健康資訊的儲存、傳輸與防護要求，確保達成機密性、完整性、可稽核性、可用性，與隱私保護，應至少考慮三個層面的紀錄與呈現方式，民眾端（透過會員專區），主管機關（包含資料提供者與平臺營運者），和服務提供者。

三、 同意管理平臺架構之規劃，仍可精進

現行 MyData 平臺使用者需登入網站會員專區，才能瀏覽自己過去的申辦紀錄，若考慮發展線下或離線瀏覽方式，並提供同意收執聯（consent receipt），同意收執聯是個人每次同意或撤回同意處理其個人資料時，將收到之證明文件。如同超市給予顧客購物的交易明細，上面會記錄購買商品、價格等資訊，使用個人資料之機構也可以給予同意收執聯作為證據，確保個人資料將被妥善處理。同意收執聯中會詳實記載個人行使同意的要件，包含蒐集個人資料之目的、日期、個人資訊、機構資訊等，如**圖 50** 所示，在使用者完成申辦服務後，MyData 平臺提供收執聯，以手機簡訊方式或者建置同意管理平臺，爾後使用者無需登入 MyData

[158] *Id*.
[159] GDPR 透明化指引第 49 點。

平臺會員，即可查詢申辦過的業務內容及紀錄等資料，同意管理平臺未來也可擴充，可查詢民眾在不同機關單位的申辦紀錄與同意事項。

參考 GDPR 規定，根據第 13 條之規定，如果從資料主體蒐集與其有關之個人資料，則蒐集者應在獲取其個人資料時，主動向資料主體告知蒐集者的身分、蒐集資料之目的、資料共享等詳細資訊。由於目前個人在知情同意事項上無法留存憑證，因此無法記錄其提供哪些資料、將資料給誰、出於何種目的。上述紀錄僅儲存在資料庫中，行使同意或變更同意的使用者無法取得該紀錄，亦難以得知服務提供者將如何處理其個人資料，導致服務使用者與服務提供者之間產生資料使用之認知差距，也不易對資料使用等問題究責。

此外，根據 GDPR 第 7 條之規定，如果在授權同意後進行資料處理，處理程序必須可被驗證，且資料蒐集者必須證明該行為係經過資料主體授權。然而，GDPR 當中並未明文規定資料蒐集者應以何種方式證明，因此以 Kantara Initiative 為首等非營利組織研擬出「Consent Receipt Specification」，期望藉由同意收執聯的方式，提供一種通用、結構化、開放的格式，讓資料蒐集者能夠提供類似「收據」的憑證，弭平雙方的認知落差，同時符合 GDPR 之規範。

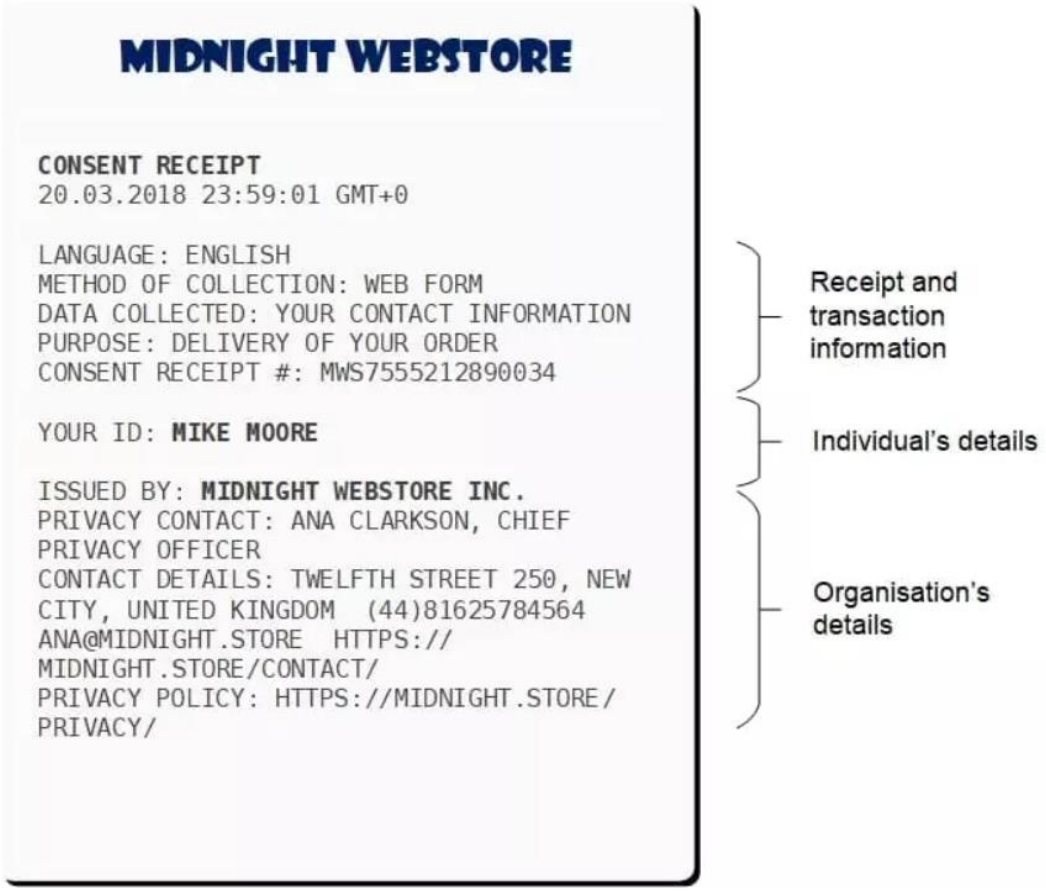


圖 50：consent receipt 示意圖

資料來源：https://www.ubisecure.com/data-protection/what-is-consent-receipt/。

四、 平臺服務流程再簡化，應朝資料營運者之目標

服務流程的簡化，受到授權方式、資料主管機關對個資保護之規範、服務提供者依服務所提供之知情同意文件等因素牽連，較難一致性提出簡化建議，但仍有三個方向可以考量：第一，多元授權方式與便利性的提升，包含授權區間的放寬、朝免插卡的方式規劃、相容於行動裝置與更簡潔的使用者介面。第二，服務提供者蒐集的設計。第三，由於 MyData 平臺和服務提供者都有身分驗證機制，流程設計上應將平臺間的互通性（interoperability）列入規劃，例如芬蘭資料系統管理者（MyData operator）與歐盟資料治理法草案之資料中介者（data intermediary）角色之可能。

特別是，歐盟於 2020 年提出歐洲資料治理規則草案（Proposal for a Regulation of The European Parliament and of The Council on European data governance, Data Governance Act）[160]，其制訂的主要目的在於透過強化資料中介機構（data intermediary）的公信力、以及優化歐盟整體的資料共享機制，來提升資料的可取得性[161]。中介服務在於當事人及資料持有者與潛在資料使用者之間建立業務、法律或技術關係[162]，其中，資料共享服務提供者為專門提供技術、平臺、資料庫等服務以協助交易雙方、多方交換或聯合利用（joint exploitation）之業者[163]。

未來若我國 MyData 平臺又或有其他業者發展為資料中介者，為因應資料治理需求，應納入類似歐盟資料治理規則草案之資料治理機制，促進資料的流通與交換並規範資料中介者，使其成為可信任的資料共享服務提供者。

然，特別說明的是，由於 My Data 平臺仍著重在個人資料的提供，故本計畫缺少進行個人資料授權應用之研析，為本計畫在研究對象及方法上的限制。

五、 為因應個資生態系，個資目的外使用應完備

就 MyData 平臺隱私權保護政策第三點有關特定目的外之利用，內容列以：本平臺絕不會任意出售、交換、或出租任何您的會員基本資料給其他團體、個人或私人企業，於利用您的會員基本資料時，均與蒐集之特定目的相符，但有下列情形之一者，得為特定目的外之利用：

---

[160] Proposal for a Regulation of The European Parliament and of The Council on European data governance (Data Governance Act), COM/2020/767 final.

[161] 劉純妤（2021）。歐盟發布《歐洲資料治理規則》草案。**科技法律透析，33**（3），8。

[162] Data Governance Act, Article 9 (1) (b).

[163] 戴豪君、賴芃聿（2021）。從歐美開放資料法制看我國開放資料專法之挑戰。**臺灣科技法學叢刊**，（2），125。

(一) 法律明文規定。
(二) 為維護國家安全或增進公共利益之必要。
(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蒐集者依其揭露方式無從識別特定之當事人。
(六) 有利於當事人權益。
(七) 經當事人同意。

該隱私權保護政策第三點係將個資法第 16 條第 1 項第 1 款至第 7 款之條文文字予以納入。但觀察隱私權保護政策第三點前段文字，MyData 平臺應無「特定目的外之利用」之意圖。若 MyData 平臺有進行「特定目的外之利用」之需求，應考量根據我國個人資料保護法第 7 條第 2 項規定：「第 16 條第 7 款、第 20 條第 1 項第 6 款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示」。即平臺不得僅以當事人已同意服務條款為由，將其個資作特定目的外之利用，應向當事人單獨另行取得同意。有關「單獨所為之意思表示」之內涵，依個資法施行細則第 15 條之規定:「本法第 7 條第 2 項所定單獨所為之意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意」。實務上，就是在書面另就「特定目的外利用之同意」，單獨另設一處進行簽名。若採網路服務模式，網頁上則需另行設計「特定目的外利用之同意」之同意機制。

就目前而言，MyData 平臺並未將使用者個資做特定目的外之利用，且考慮到 MyData 平臺由國家發展委員會建置，定性屬於公務機關。依個資法第 16 條規定，公務機關對個人資料之利用，有該條第 1 款至第 6 款情形時，無須當事人同意，得為特定目的外之利用。簡而言之，於法定情形下，平臺無須另行通知及取得當事人知情後之同意，即可依個資法之規範進行特定目的外之利用，亦無須於服務條款中列出。須注意，若不符合該法第 16 條第 1 至第 6 項情形時，則如前述，按同法第 7 條第 2 項規定，公務機關應明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，取得當事人單獨所為之意思表示後，方得將其個資為特定目的外之利用。

MyData 平臺隱私權保護政策中第三點有關特定目的外之利用，其中列出「經當事人同意」之情形。將令使用者在同意 MyData 平臺之隱私權保護政策時，可能發生「同時同意」MyData 平臺得為特定目的外之利用之情形，恐與同法第 7 條第 2 項規定相違[164]。以目前所見，MyData 平臺無意為特定目的外之利用，但前述問題將產生平臺隱私權保護政策與個資法有衝突之虞。

[164] 法務部法律字第 10603503880 號函略以：「...惟若欲將所蒐集個人資料為特定目的外利用（例如：作為其他行銷之用），則應依個資法第 7 條第 2 項規定，另行取得當事

依照本節研析結論，本計畫具體提供以下政策面之短中長期建議。

第二節　政策短期建議

一、 主管機關管理者層面－知情同意管理建議

(一) 知情同意管理建議

1、 階層化與圖像化的知情同意介面

由本計畫文獻、實驗與專家座談之結果，建議MyData平臺的服務條款與隱私保護政策可考慮以圖像化與階層化方式呈現，圖像化的標記可參考IOS App下載軟體App Store，或由主管機關統一訂定，階層不宜過多，一般以三個階層為限。

2、 減少同意疲勞（consent fatigue）

現行MyData平臺採單次授權，使用者申辦每個業務都需閱讀相同的同意內容，就算在短期間內重新申辦一樣的業務也需再次閱讀，反覆多次後，容易造成使用者的同意疲勞，不願意再閱讀知情同意書。本計畫建議未來的優化可以朝向將驗證及授權改為「特定期間」或「依年度更新會員制」，同時調整隱私權保護政策、個人化資料自主運用平臺介接作業要點等「單次同意」之內容，讓使用者在短期內申請一樣的業務可以不必重複閱讀知情同意書，以減少同意疲勞。

未來如有其他機關單位需參考對知情同意管理之相關做法，建議參考本研析所提之知情同意管理建議之原則：階層化與圖像化界面，及減少使用者的同意疲勞。

(二) 優化會員專區功能

1、 知情同意授權方式

考量未來開放企業相關服務（以工商憑證登入），以及第三方服務業者，如保險、證券業者，會員專區的功能勢必需要調整及優化，如批次同意或期間內同意之機制設計。另建議各資料提供者、服務提供者盤點個各自於MyData平臺的現行服務，以民眾申辦業務中資料變動性較低者，以年份為切點，提供期間性的授權，如：各類證照換證服務。

人同意（個資法第 20 條第 1 項第 6 款），而不得僅以一概括之特別聲明，即將所蒐集之個人資料逕為特定目的外利用」。

2、 「同意收執聯（consent receipt）」

MyData平臺的會員專區需驗證登入，查詢使用者基本資料、上次登入時間、使用紀錄、資料條碼等三大項服務，未來應可考慮同意收執聯（consent receipt）機制，可線下提供個人每次同意或撤回同意處理其個人資料時，收到之證明，包含蒐集個人資料之目的、日期、個人資訊、機構資訊等。同意收執聯或可解釋為資料複製本，依我國個資法第3條規定，資料當事人有請求製給複製本之權利，惟製給複製本為請求權基礎，即當資料當事人主動請求才可獲得，而回執係指當資料當事人同意完後，平臺主動提供給資料當事人回執。

本計畫案為確保個人資料將被妥善處理，參考國外同意收執聯之機制提供同意收執聯，使資料當事人能明確瞭解其最後同意內容為何，作為同意之證據；若無提供資料當事人同意紀錄，此時資料當事人或得主張個資法第3條請求製給複製本之權利，要求MyData平臺提供。

(三) 個資稽核建議–持續稽核方式的精進

建議 MyData 平臺主管機關應對服務提供者落實稽核或民眾發生個資危害事件的兵棋推演或處置 SOP，如發生人民向主管機關請求作出具體個案解釋時，主管機關應積極為行政函釋，為人民釐清爭議。

對於現行稽核表單之建議：（1）「作業程序」類別下，增加「不」提供資料之影響，以確保資料當事者知情瞭解。（2）除填表聯絡人，建議各單位留有「個資保護聯絡窗口」，協調聯繫個資相關事宜。（3）增加「認知宣導與教育訓練」相關內容，以確保資安意識，如：服務提供單位是否已清楚了解單位儲存個資檔案之媒體宜有攜出、拷貝或複製的管控機制、當年度是否派員參加個資相關教育課程、是否指定相關人員負責管理儲存個資檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等。

(四) MyData 平臺隱私政策聲明修訂方向建議

1、 增加特種資料之合法蒐集、處理或利用

目前MyData平臺僅蒐集、處理或利用一般個人資料，並未有蒐用特種個人資料之情形。本計畫建議後續平臺將來考量是否將特種資料納入服務時，應確保隱私權保護政策中有關特種資料之蒐集、處理或利用行為內容，盡應告知之法定事項義務，並取得資料當事人書面或電子方式之同意。

2、 特定目的外之利用

以目前所見，MyData平臺無意為特定目的外之利用，惟如於研析結論第五點所述，現平臺隱私保護政策之設計有與個資法相衝突之風險。因此建議如下：

(1) 須先確定國發會是否有意在 MyData 平臺為個資法第 16 條第 1 款至第

6 款以外之特定目的外之利用情形。若無，可考量無須於隱私權保護政策設定特定目的外之利用規定；若有此需求，則須符合個資法規定，採作另行通知及取得當事人同意之設計。

(2) 前述設計，例如建議國發會在 MyData 平臺會員專區，應有個人資料為特定目的外之利用同意文件或其他形式，單獨點選同意之機制。

二、 平臺使用者層面－使用者體驗（UX）優化建議

身分驗證之方式，應由實體卡片放寬，並與各業務主管機關協商，持續精進或放寬資訊委託人或代理人制度。

(一)「告知＞同意＞驗證」

由服務提供者轉跳至 MyData 平臺進行知情同意時，MyData 平臺的知情同意（MyData 資料下載及線上服務條款）皆為統一模板，並未根據不同服務有所客制化、也未在事前告知使用者 MyData 平臺將傳送哪些資料到服務提供者網站，MyData 平臺將資料詳細內容擺在流程完成的最後步驟，導致使用者操作到最後才知道自己被服務提供者拿了什麼資料。本計畫建議 MyData 平臺應以「告知＞同意＞驗證」作為步驟順序，再轉跳回 MyData 平臺的第一步驟就明確嵌入要拿取的資料並尋求民眾同意。

1、 簡化再次造訪民眾之業務申辦流程

首次申辦服務時須同意資料下載及線上服務條款（包含服務條款與隱私權保護政策）、服務條款與隱私權保護政策。對於再次造訪之民眾，若已登入會員專區，建議可簡化資料下載及線上服務條款，僅保留單次需要提醒及同意的事項。

2、 降低個人資料重複填寫

民眾個人資料需多次提供。**圖51**為嘉義縣政府申辦「特定寵物兔絕育」服務頁面，可以發現即使在MyData平臺已輸入過身分證字號，連結回服務提供者的網站仍需重新填寫一次，同樣的，**圖52**為桃園市政府申辦「中醫助孕養胎調理」服務頁面，也可以發現即使輸入身分證字號，回傳的資料只有身分證正反面影本，沒有包含簡單的個人資訊（姓名、戶籍地址等）。由於服務提供者拿取使用者的資料集項目是經由主管機關審核，導致MyData平臺上不同服務提供者的知情同意與授權方式皆不同，也因此使用者在申辦大部分服務時，都需要重新填寫個人戶籍資料，使整體流程變的繁瑣。

可參考新加坡SingPass的做法，以提高公部門、使用者及第三方服務的操作便利性與使用意願。舉例而言，使用SingPass App，就醫時就不需手寫個人資料，只要掃瞄醫院提供的QR Code，並用上述任一方式驗證身分，即可查看該服務所需之個人資料，點選同意後即完成掛號手續（操作流程如**圖53**）。

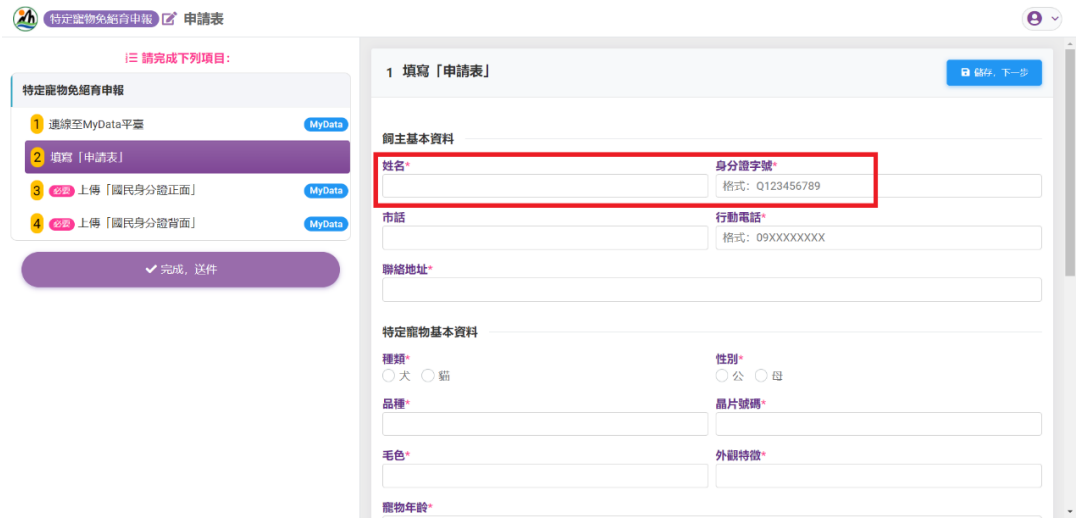


圖 51：嘉義縣政府申辦特定寵物兔絕育頁面

資料來源：嘉義一站式便民服務平臺。

圖 52：桃園市政府申辦中醫助孕養胎調理頁面

資料來源：桃園網路 e 指通。

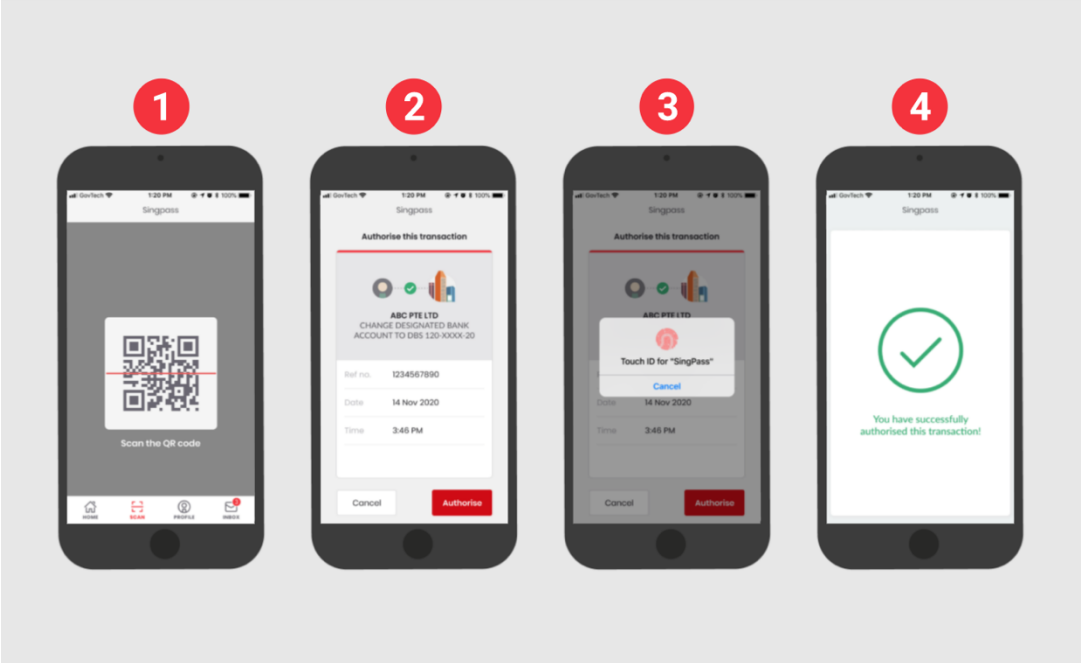


圖 53：SingPass 操作流程

資料來源：SingPass 官網。

(二) 減少服務斷點

依照國際標準以應用程式介面（API）對接，避免如資料傳遞過程的服務斷點，同時優化 MyData 平臺客服與各資料提供者、服務提供者間的聯繫管道與聯繫方式。

第三節　政策中長程建議

一、 主管機關管理者層面－知情同意管理建議

MyData 平臺應可朝向同意管理平臺角色如**圖 54** 及**圖 55**，提供標準化的應用程式介面（API）與操作指引給服務提供者，集中管理民眾對服務提供者使用資料提供者個資所進行的知情同意。

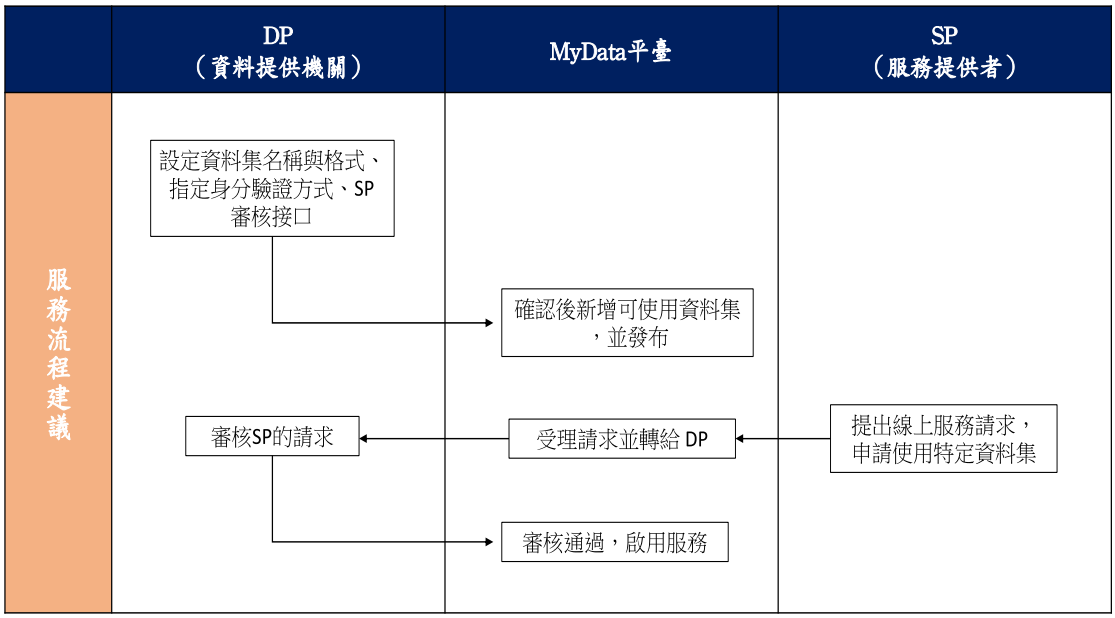


圖 54：DP 註冊與啟用 SP 線上服務之游泳道圖

資料來源：本計畫自行整理。

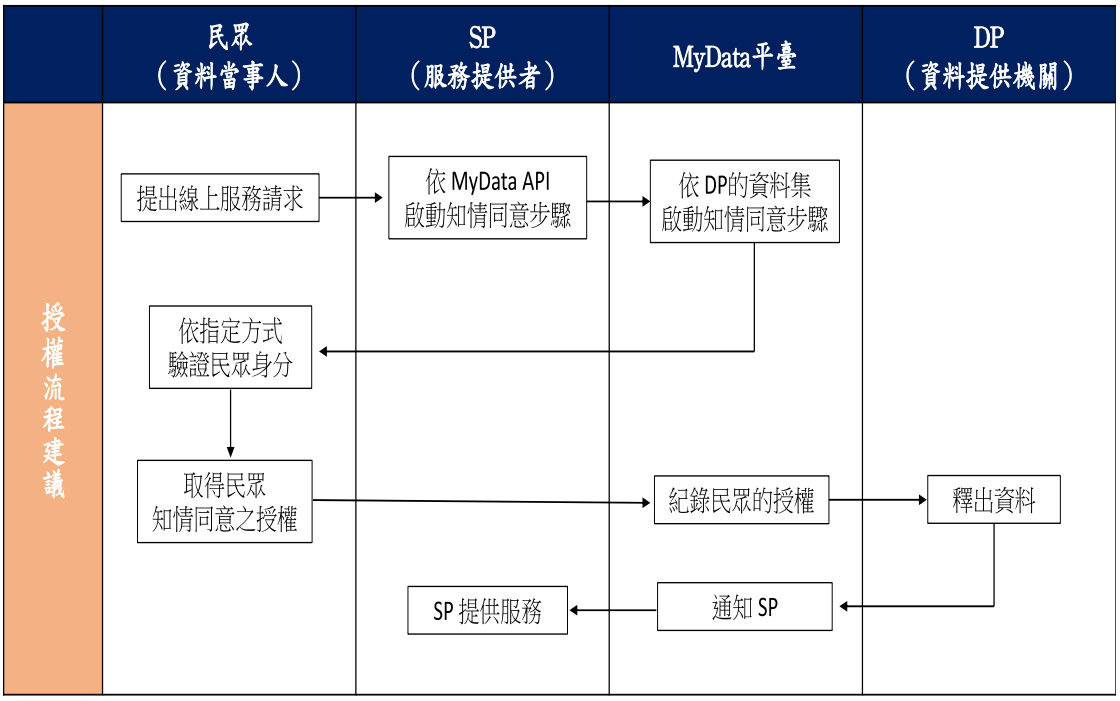


圖 55：SP 取得民眾授權之游泳道圖

資料來源：本計畫自行整理。

二、 建議未來法規增修方向及增修後平臺發展建議

(一) 標準化圖示

本計畫於短程建議部分，建議 MyData 平臺的服務條款與隱私保護政策可考慮以圖像化與階層化方式呈現。惟圖示告知之有效性取決於該圖示是否被普遍使用和被承認作為相關資訊之簡化圖示。故建議 MyData 平臺將來若有設計相關圖示，應朝向將圖示推廣為標準化圖示方向邁進，提供易見、易懂且清晰易讀之圖示，參考諸如創用 CC 與歐盟 GDPR 所提標準化圖示，以加速使用者閱覽，並降低理解門檻。

(二) 撤回同意之規定

我國個資法第 3 條規定資料當事人有請求資料控管者停止蒐集、處理或利用其個資之權利。未來個資法修法，建議可參考 GDPR 第 7 條第 3 項規定：「資料主體有權隨時撤回其同意。同意之撤回不影響撤回前基於該同意所為處理之合法性。資料主體為同意前，資料主體應受告知其得隨時撤回該同意。同意之撤回應與給予同意一樣容易」。強調資料當事人請求停止蒐用其個資時，該權利之行使應如授權同意同樣容易程度。對此，建議 MyData 平臺未來因應相關修法，應確保使用者撤回同意的方式與取得使用者同意之容易程度相等。

(三) 資料可攜權

資料當事人藉由 MyData 平臺請求索取存於其他機關（資料提供端）資料庫中之個資，該行為得基於個資法第 3 條請求製給複製本之權利。而 MyData 平臺（公務機關）傳輸資料當事人之個資至服務提供方，雖我國個資法並未規定資料可攜權，惟此傳輸行為基於給付行政無違法之疑慮。未來若個資法修法將資料可攜權明文化，此時 MyData 平臺在某些情境下將從給付行政措施更改為當資料當事人請求傳輸時，負有傳輸義務。未來研析方向建議有二，一是針對 MyData 平臺服務，擴展平臺服務功能；其次為結合技術層面，探討知情同意之資料提供與第三方服務串接的適法性。

(四) 接軌國際認證方式與標準

MyData 平臺朝向芬蘭資料系統管理者（MyData operator）與歐盟資料治理法草案中資料中介服務（data intermediary）角色，並考慮未來可能有多個類似 MyData 平臺並存的需求，應將平臺間的互通性（interoperability）列入規劃，及納入資料治理機制規定用以規範資料中介者服務。

(五) 個資稽核

國內應發展有關個資稽核之規範，與國外政府或研究機構所公布因應 GDPR 或 CBPR 體系指引手冊或工具，如法規遵循、個資保護技術等方向，以利指引國內業者。

參考文獻

一、 中文文獻

John（2013）。UML 之 Activity Diagram 的簡介，2021 年 7 月 28 日，取自：http://puremonkey2010.blogspot.com/2013/11/uml-uml.html。

TW511 教學網（2020）。UML 教學，2021 年 7 月 29 日，取自：http://www.tw511.com/6/78/2361.html。

王君善（2018）。UML 活動圖表（Activity Diagram），2021 年 7 月 28 日，取自：https://studentcodebank.wordpress.com/2017/11/21/uml-%E6%B4%BB%E5%8B%95%E5%9C%96%E8%A1%A8-activity-diagram/。

王慕民（2019）。跨境隱私管理機制—GDPR 下的透明與同意，2021 年 4 月 6 日，取自：https://www.ncc.gov.tw/chinese/files/19120/5162_42306_191202_3.pdf。

王德瀛（2020）。簡評加州消費者隱私保護法—規範重點與其對美國隱私保護的影響。**科技法律透析**，**32**（03），21。

王儷玲、陳恭、劉建良、吳麥斯、黃遵誠、陳仁偉、葉雨婷（2019）。**強化電子病歷交換資訊安全及建立公私合營機制之評估研究**。衛生福利部 108 年度委託科技研究計畫，未出版。

李沛宸（2019）。GDPR 當事人同意之實務採行建議。**商業法律與財金期刊**，**2**（1），67-96。

李世德（2018）。GDPR 與我國個人資料保護法之比較分析。**台灣經濟論衡**，**16**（3），69-93。

呂妍庭（2020）。嘉縣打造全國最大 MyData 網站一站式服務超便民，2021 年 3 月 10 日，取自：https://www.chinatimes.com/realtimenews/20201230006344-260421?chdtv。

我的 E 政府（n.d.）。教育部國民及學前教育署主管高級中等學校特殊身分學生學雜費減免及就學費用補助，2021 年 3 月 10 日，取自：https://www.gov.tw/News3_Content.aspx?n=2&s=393138。

吳統雄（2017）。UML：統一塑模語言/開發圖神掌，2021 年 7 月 28 日，取自：http://tx.liberal.ntu.edu.tw/InfoMgt/Jx/IS_IM/UML.htm。

客家委員會客家文化發展中心（2020）。客家文化發展中心全球資訊網，2021 年 7 月 28 日，取自：https://thcdc.hakka.gov.tw/#。

香港個人隱私引專員公署（2020）。歐洲聯盟《通用數據保障條例》2016 最新資訊，2021 年 11 月 8 日，取自：https://www.pcpd.org.hk/tc_chi/data_privacy_law/eu/files/eugdpr_c.pdf。

翁逸泓、李寧修（2020）。**歐盟國家個人資料保護法制因應 GDPR 施行之調適—以德國與英國為例**。國家發展委員會 109 年度委託研究報告，未出版。

財團法人資訊工業策進會科技法律研究所 TPIPAS 制度維運小組（2014）。新加坡個人資料保護法之現況與比較。**集保結算所雙月刊 TDCC BIMONTHLY**，(213)，46-61。

財團法人資訊工業策進會科技法律研究所（2020）。新加坡國會於 2020 年 11 月通過個人資料保護法之修正案，2021 年 5 月 19 日，取自：https://stli.iii.org.tw/article-detail.aspx?tp=1&i=180&d=8580&no=64。

高雄市稅捐稽徵處（n.d.）。地價稅自用住宅用地資料，2021 年 7 月 22 日，取自：https://www.kctax.gov.tw/module/main.aspx?id=1&MenuID=1060。

桃園市政府（2021）。桃園網路 e 指通，2021 年 7 月 7 日，取自：https://e-services.tycg.gov.tw/TycgOnline/tycgOnline.action。

翁清坤（2013）。告知後同意與消費者個人資料之保護。**臺北大學法學論叢**，(87)，217-322。

國家發展委員會。EDPB 同意指引文件中英翻譯對照：Guidelines 05/2020 on consent under Regulation 2016/679 關於第 2016/679 號規則（GDPR）中的同意之指引，2021 年 11 月 19 日，取自：https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9hNTI2ZmUyYy0wZjNlLTQ1NzAtOTFiYS1jYzkzZTExNTc0NDgucGRm&n=44CQ5paw44CRMeWQjOaEjyBHdWlkZWxpbmVzIG9uIGNvbnNlbnQgKEFkb3B0ZWQgb24gNCBNYXkgMjAyMCkucGRm&icon=..pdf。

國家發展委員會（n.d.）。GDPR 透明化指引文件中英翻譯對照，2021 年 11 月 8 日，取自：https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS8wY2MxN2RhMC01NGI3LTQ1ZjMtODRiOC03OWQzN2JmMmJkYzUucGRm&n=6YCP5piO5YyWLeWIueZu%2bWumOe2sueJiC5wZGY%3d&icon=..pdf。

國家發展委員會（2019）。加州消費者隱私保護法（CCPA）規範重點說明，2019 年 10 月 11 日，取自：https://www.ndc.gov.tw/Content_List.aspx?n=48BEF57F071432E0。

國家發展委員會（2020）。個人化資料自主運用（MyData）平臺，2021 年 4 月 5 日，取自：https://mydata.nat.gov.tw/。

張瑞星（2019）。臺灣個人資料保護與管理制度（TPIPAS）之現況與挑戰，2019 年 11 月 26 日，取自：https://www.ncc.gov.tw/chinese/files/20011/5162_42529_200110_5.pdf。

張陳弘（2020）。**GDPR 施行兩周年評估報告之分析及相關議題研析計畫規劃**。國家發展委員會 110 年度委託研究報告，未出版。

張陳弘（2019）。新興科技下的資訊隱私保護—「告知後同意原則」的侷限性與修正方法之提出。**臺灣大學法學論叢**，**47**（1），201-297。

張陳弘、莊植寧（2019）。**新時代之個人資料保護法制歐盟 GDPR 與臺灣個人資料保護法的比較說明**。臺北：新學林。

張國洋（2014）。把花在解釋流程的時間省下來 —複雜的工作分派 讓「泳道圖」清楚說明白，2021 年 7 月 28 日，取自：https://www.businesstoday.com.tw/article/category/80407/post/201805040057/%E6%8A%8A%E8%8A%B1%E5%9C%A8%E8%A7%A3%E9%87%8B%E6%B5%81%E7%A8%8B%E7%9A%84%E6%99%82%E9%96%93%E7%9C%81%E4%B8%8B%E4%BE%86%20%20%E2%80%94%E8%A4%87%E9%9B%9C%E7%9A%84%E5%B7%A5%E4%BD%9C%E5%88%86%E6%B4%BE%20%E8%AE%93%E3%80%8C%E6%B3%B3%E9%81%93%E5%9C%96%E3%80%8D%E6%B8%85%E6%A5%9A%E8%AA%AA%E6%98%8E%E7%99%BD。

陳宏志（2017）。網路無國界，跨境個資傳輸如何管—以 APEC CBPRs 為例，**科技法律透析**，**29**（8），30-50。

陳恭（2013）。從應用系統的權限控管到隱私保護。**叡揚 e 論壇**，（71），44-47。

集客數據行銷（2021）。【2021 最新】做網路行銷還沒聽過 UI UX？Google 給企業的 UI UX 操作建議，2021 年 8 月 4 日，取自：https://inboundmarketing.com.tw/websites-optimization/uiux-design.html。

萬興科技（n.d.）。泳道流程圖原來這麼簡單！為你詳解泳道跨職能流程圖，2021 年 7 月 28 日，取自：https://www.edrawsoft.cn/flowchart/yongdaotu/。

葉奇鑫（2020）。**韓國個人資料保護法制因應 GDPR 施行之調適**。國家發展委員會 109 年度委託研究報告，未出版。

達文西個資暨高科技法律事務所（2020）。【快訊】CCPA 或將面臨大改？—美國加州消費者隱私保護法規最新動，2021 年 7 月 13 日，取自：https://www.davinci.idv.tw/news/787。

嘉義縣政府（2021）。一站式便民服務平臺，2021 年 7 月 7 日，取自：https://eservice.cyhg.gov.tw/。

臺南市政府（2021）。一站式整合服務平臺，2021 年 7 月 7 日，取自：https://e-services.tainan.gov.tw/。

劉純妤（2021）。歐盟發布《歐洲資料治理規則》草案。**科技法律透析，33**（3），8-9。

蔡柏毅（2019）。你的同意不是我的同意-淺介個資法上的「同意」。**金融聯合徵信法規**，（35），75。

衛生福利部中央健康保險署（2021）。SDK 健康服務連結，2021 年 9 月 6 日，取自：https://www.nhi.gov.tw/Content_List.aspx?n=A5407A276376FECC&topn=5FE8C9FEAE863B46。

戴豪君、賴芃聿（2021）。從歐美開放資料法制看我國開放資料專法之挑戰。**臺灣科技法學叢刊**，（2），95-144。

環球生技（2020）。突破智慧健康科技資料蒐集挑戰資策會邀醫電跨界對談共尋解方，2021 年 8 月 5 日，取自：https://store.gbimonthly.com/Article/Detail/46079?lang=zh-TW。

醫學空間（2017）。臨床試驗受試者：知情同意書你真的讀懂了嗎？，2021 年 3 月 10 日，取自：https://kknews.cc/health/3j2r5qy.html。

蘇文彬（2020）。MyData 地方政府實例：桃園市政府中央與地方跨機關資料交換新作法，臨櫃申辦不只簡化更能無紙化，2021 年 3 月 10 日，取自：https://www.ithome.com.tw/news/139398。

二、 英文文獻

ARTICLE 29 Data Protection Working Party (2004). ***Opinion 10/2004 on More Harmonised Information Provisions***. Brussels: European Commission.

CBPRs (2011). Cross-border data flows are a vital part of our vibrant and growing digital economy in the Asia-Pacific region. Retrieved May 25, 2021, from http://cbprs.org/consumers/.

Data & Design by LINC (n.d.). Co-building user journeys compliant with the GDPR and respectful of privacy. Retrieved April 23, 2021, from https://design.cnil.fr/en/concepts/consent/ .

Data & Design by LINC (n.d.). Case studies. Retrieved April 23, 2021, from https://design.cnil.fr/en/case-studies/ .

Department for Digital, Culture, Media and Sport, DCMS (2019). Guidance on the application of Article 36(4) of the General Data Protection Regulation (GDPR). Retrieved November 09, 2021, from https://www.gov.uk/government/publications/guidance-on-the-application-of-article-364-of-the-general-data-protection-regulation-gdpr.

EU Press Release Database (2016). Building on modern and unified rules to strengthen fundamental rights and create a Digital Single Market - Joint statement by Vice-President Ansip and Commissioner Jourová on the occasion of the 2016 Data Protection Day. Retrieved April 28, 2021, from http://europa.eu/rapid/press-release_STATEMENT-16-181_en.htm.

EUR-Lex (2016). Regulation (EU)2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Retrieved April 05, 2021, from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

ForgeRock (2010). Manage consent and give consumers control over their data. Retrieved April 09, 2021, from Privacy and Consent Management Solutions | ForgeRock.

Feeley, M. (2018). Research reveals what online value exchange means for millennials and Gen Z. Retrieved July 15, 2021, from https://www.thedrum.com/news/2018/10/05/research-reveals-what-online-value-exchange-means-millennials-and-gen-z.

GOV.UK (n.d.). Digital marketplace consent kit. Retrieved April 07, 2021, from https://www.digitalmarketplace.service.gov.uk/g-cloud/services/718520047914828.

Information Commissioner's Office, ICO (2018). What methods can we use to provide privacy information? Retrieved May 19, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/.

ICO (n.d.). Guide to the General Data Protection Regulation. Retrieved November 09, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

IMDA (2021). APEC Cross Border Privacy Rules (CBPR) & Privacy Recognition for Processors (PRP) systems. Retrieved November 14, 2021, from https://www.imda.gov.sg/-/media/Imda/Files/Programme/CBPR-and-PRP/CBPR-and-PRP-Brochure-150620.pdf.

IMDA (2021). APEC Cross Border Privacy Rules System Information-kit. Retrieved November 14, 2021, from https://www.imda.gov.sg/-/media/Imda/Files/Programme/CBPR-and-PRP/CBPR-Information-Kit.pdf?la=en&hash=15C4EADE10B648D50DB026C55D701F7A.

IMDA (2021). Easy data transfers to APEC CBPR /PRP Certified Organisations. Retrieved November 14, 2021, from https://www.pdpc.gov.sg/help-and-resources/2020/06/easy-data-transfers-to-apec-cbpr-and-prp-certified-organisations.

Infocomm Media Development Authority (2021). DPTM certification checklist. Retrieved November 14, 2021, from https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Checklist-220321.pdf?la=en.

Information Commissioner's Office, ICO (2018). What methods can we use to provide privacy information? Retrieved May 19, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/.

Iubenda (n.d.). A360° solution to make your sites and apps compliant with the law.Retrieved April 17, 2021, from https://www.iubenda.com/en/overview.

Kettles, G. (2020). The CCPA's impact on public agencies. Retrieved July 13, 2021, from https://www.jdsupra.com/legalnews/the-ccpa-s-impact-on-public-agencies-40892/.

Kodapanakkal, R. I., M. J. Brandit, C. Kogler, & I. V. Beest (2020). Self-interest and data protection drive the adoption and moral acceptability of big data

technologies: A conjoint analysis approach. ***Computers in Human Behavior,*** (108), 1–13.

Korea Credit Information Service (n.d.). The new future of finance. Retrieved July 15, 2021, from https://www.kcredit.or.kr:1441/download/KCIS_Brochure.pdf .

Kantara Initiative (2019). Consent Receipt Specification. Retrieved May 03, 2021, from https://kantarainitiative.org/download/7902/ .

Luger, E., S. Moran, & T. Rodden (2013). Consent for all: revealing the hidden complexity of terms and conditions. ***CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*** (pp. 2687–2696). NY: Association for Computing Machinery.

Langford, J., A. J. Poikola, & W. Janssen. & V. Lähteenoja, & M. Rikken (Ed.). (2020). Understanding MyData operators. Retrieved November 12, 2021, from https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf.

MAS (n.d.). Singapore financial data exchange. Retrieved July 11, 2021, from https://www.mas.gov.sg/development/fintech/sgfindex#_about-sgfindex.

MOIS (n. d.). MOIS implements further digital government innovation with launch of Public Mydata Service. Retrieved July 11, 2021, from https://www.dgovkorea.go.kr/news/57.

MEDIBLOC TEAM (2017). MediBloc whitepaper. Retrieved July 13, 2021, from https://whitepaper.io/document/176/medibloc-whitepaper.

MyData Global (2020). MyData Operators. Retrieved May 19, 2021, from https://mydata.org/mydata-operators/.

Personal Data Protection Commission (2021). ***Advisory Guidelines on Key Concepts in the Personal Data Protection Ac***t. Singapore: Personal Data Protection Commission, 1-164.

Personal Data Protection Commission (n.d.). Data Protection Obligations. Retrieved July 13, 2021, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act/Data-Protection-Obligations.

Personal Data Protection Commission (n.d.). Data Protection Officers. Retrieved November 27, 2021, from https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers.

Personal Data Protection Commission (2017). EU GDPR Factsheet for Organisations Now Available. Retrieved November 09, 2021, from

https://www.pdpc.gov.sg/news-and-events/announcements/2017/10/eu-gdpr-factsheet-for-organisations-now-available.

Personal Data Protection Commission (n.d.). PDPA overview. Retrieved July 13, 2021, from https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.

Personal Data Protection Commission (2021). Sample Clause for Data Transfers to APEC CBPR and PRP Certified Organisations. Retrieved November 14, 2021, from https://www.pdpc.gov.sg/Help-and-Resources/2020/06/Sample-Clause-for-Data-Transfers-to-APEC-CBPR-and-PRP-Certified-Organisations.

PwC (2019). A blueprint for robust consent management. Retrieved May 05, 2021, from https://www.pwc.in/consulting/technology/data-and-analytics/govern-your-data/insights/a-blueprint-for-robust-consent-management.html.

Poikola, A., J. Langford, M. Huhtamäki, M. Sierla, & W. Janssen (2019). Discussion Paper–What is the MyData Operator? Retrieved November 12, 2021, from https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf.

Sakshaung, J. W., A. Schmucker, F. Kreuter, M. P. Couper, & E. Singer (2019). The effect of framing and placement on linkage consent. ***Public opinion quarterly, 83***(1), 289-308.

Santos, C., M. Nouwens, M. Toth, N. Bielova, & V. Roca (2021). What are Consent Management Platforms under the GDPR: processors or controllers? Retrieved November 14, 2021, from https://www.ieee-security.org/TC/SPW2021/ConPro/papers/santos-conpro21.pdf.

SingPass App (2018). What can I do with Singpass app? Retrieved April 01, 2021, from https://app.singpass.gov.sg/.

Singapore Government Agency Website (n. d.). MyMoneySence. Retrieved July 15, 2021, from https://www.moneysense.gov.sg/.

Ubisecure (2018). What is Consent Receipt? Retrieved May 05, 2021, from https://www.ubisecure.com/data-protection/what-is-consent-receipt/.

Visual Paradigm (n. d.). What is Activity Diagram? Retrieved July 28, 2021, from https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-activity-diagram/.

Visual Paradigm (n. d.). What is Unified Modeling Language (UML)? Retrieved July 28, 2021, from https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-uml/.

Wagner, R. A. (2020). Informed consent form and important. Retrieved July 15, 2021, from_ https://www.emedicinehealth.com/informed_consent/article_em.htm.

Whitley, E. A., & R. Pujadas (2018). ***Report on a study of how consumers currently consent to share their financial data with a third party***. Unpublished doctoral dissertation, London School of Economics and Political Science.

World Economic Forum (2020). Redesigning data privacy: Reimagining Notice & Consent for humantechnology interaction. Retrieved August 23, 2021, from http://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

Zawadziński, M., & M. Wlosik (2020). What is a Consent-Management Platform (CMP) and how does it work? Retrieved November 14, 2021, from https://clearcode.cc/blog/consent-management-platform/.

Zawadziński, M., & M. Wlosik (2021). How the IAB's GDPR transparency and consent framework works from a technical perspective (TCF 1.0 and TCF 2.0). Retrieved November 14, 2021, from https://clearcode.cc/blog/iab-gdpr-transparency-consent-framework/.

三、 其他外文文獻

Agencia Española de Protección de Datos, AEPD (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Retrieved May 04, 2021, from https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf.

Agencia Española de Protección de Datos, AEPD (2021). Evalúa-Riesgo RGPD. Retrieved May 04, 2021, from https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd.

一般財団法人日本情報経済社会推進協会 (JIPDEC) (2021). APEC CBPR 認証のご紹介. Retrieved November 14, 2021, from https://www.jipdec.or.jp/protection_org/JIPDEC_AOP_CBPR_015.pdf.

一般財団法人日本情報経済社会推進協会 (JIPDEC) (2021). APEC CBPR 認証申請ガイドブック. Retrieved November 14, 2021, from https://www.jipdec.or.jp/protection_org/JIPDEC_AOP_CBPR_008.pdf.

日本貿易振興機構 (JETRO) (2016).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック(入門編). Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html.

日本貿易振興機構 (JETRO) (2017).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html.

日本貿易振興機構 (JETRO) (2018).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）データポータビリティの権利. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2018/01/2d8d30044cc65583.html.

日本貿易振興機構（JETRO）(2018).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）管理者および処理者の主導監督当局の特定. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2018/01/9a90f1003bc16515.html.

日本貿易振興機構 (JETRO) (2018).「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（第 29 条作業部会ガイドライン編）データ保護責任者. Retrieved November 08, 2021, from https://www.jetro.go.jp/world/reports/2018/01/28dd771ad2a2c020.html.

KISA GDPR 대응지원 센터(2020).우리 기업을 위한「유럽 일반 개인정보보호법 」안내서/ p236/2017/행정안전부,한국인터넷진흥원. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

KISA GDPR 대응지원 센터(2020).우리 기업을 위한 EU 개인정보보호법(GDPR) 1 차 가이드라인 / p107 / 2017 / 행정안전부,한국인터넷진흥원. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

KISA GDPR 대응지원 센터(2020). [개정판] 우리 기업을 위한 EU 일반 개인정보보호법(GDPR) 가이드북 / p206 / 2018 / 행정안전부, 방송통신위원. Retrieved November 08, 2021, from

https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

KISA GDPR 대응지원 센터(2020). 2020 EU 일반개인정보보호법（GDPR）가이드북 / p290 / 2020 / 방송통신위원회, 한국인터넷진흥원, Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

KISA GDPR 대응지원 센터(2020). 2020 GDPR 상담사례집. Retrieved November 08, 2021, from https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101.

附錄

附錄一、DPTM Certification checklist

DPTM Certification 稽核表是基於 DPTM Certification 的要求所提供的簡略要點稽核，在組織申請 DPTM Certification 之前，可以利用此表衡量自身的準備情況。

此稽核表共列出 4 個主要原則，每個主要原則之下又區分為各個主題，而每個主題之下則是多項稽核要點，企業透過勾選是否達成稽核要點來衡量準備情況。另外，此表也根據稽核要點，對應到 PDPC 所提供的參考指引作為詳細的稽核依據。

	Checklist	Yes	PDPC's Reference Advisory Guides/Guides/Templates
Principle 1: Governance and Transparency			
A: Establish data protection policies and practices			
1	Organisation shall have data protection policies and practices approved by management, setting out the organisation's approach to managing personal data (include management of special categories of personal data such as personal data of a sensitive nature) for various stakeholders such as:		• Advisory Guidelines on Key Concepts in the Personal Data Protection Act • Guide to Accountability under the Personal Data Protection Act
	• Employees - Internal data protection policy and notice	☐	• Data Protection Notice Generator (https://apps.pdpc.gov.sg/dp-notice-generator/introduction)
	• Customers, Job applicants, visitors etc - External data protection notices	☐	

	• Third party vendors - Third party agreement for management of the organisation's personal data	☐	• Guide to Managing Data Intermediaries • Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data

資料來源：IMDA。

附錄二、作業流程圖

圖 56 為線上申辦「高雄市—申請地價稅自用住宅用地稅率」作業流程圖，圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」、「高雄市單一認證平臺」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站。以高雄市—申請地價稅自用住宅用地稅率服務來說，需同意地價稅自用住宅用地稅率申請說明並驗證身分，其中「個人資料授權同意書」這份文件需要使用者點入才能觀看內容（如 2 號虛線框），驗證成功後便可繼續填寫申請資料，送出申請即完成線上申辦業務。

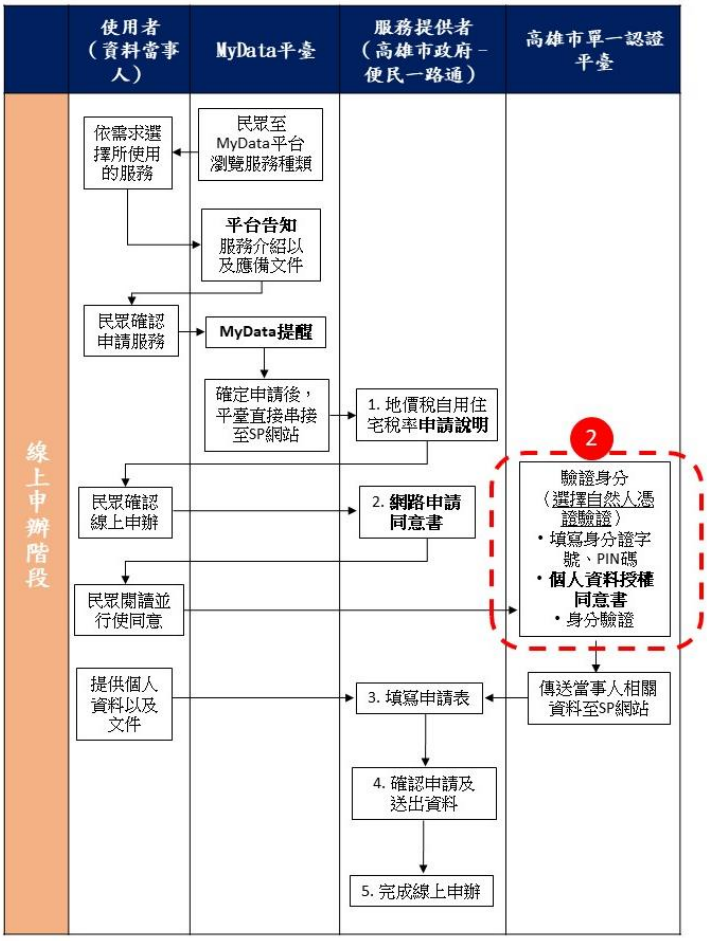


圖 56：線上申辦「高雄市—申請地價稅自用住宅用地稅率」作業流程圖

資料來源：本計畫自行整理。

（註：底線處為驗證方式，字體加粗處為使用者須按下同意按鈕的步驟）

圖 57 為線上申辦「教育部—中低收入戶學生學雜費減免線上申請」作業流程圖，圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的

服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站，但因使用者無中低收入戶身分，因此測試流程中斷（如 5 號虛線框）。

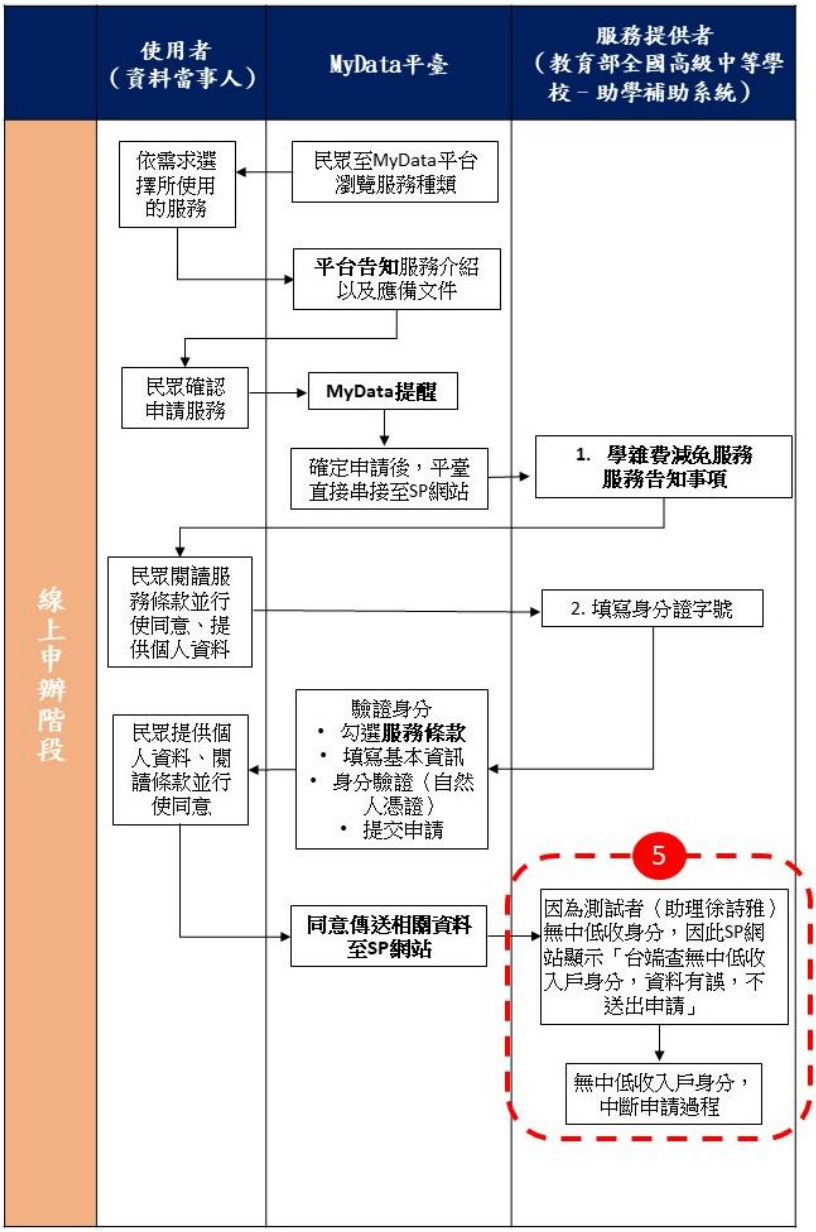


圖 57：線上申辦「教育部—中低收入戶學生學雜費減免線上申請」作業流程圖

資料來源：本計畫自行整理。

（註：底線處為驗證方式，字體加粗處為使用者須按下同意按鈕的步驟）

圖 58 為線上申辦「臺灣銀行信用卡」作業流程圖，圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站。以臺灣銀行申辦信用卡服務來說，需同意網站說明及線上辦卡條文，其中線上辦卡條文審閱，有強制使用者須皆看完條款才能勾選同意（如 6 號虛線框），並在服務提供者網站進行第一次驗證身分。驗證成功後會跳轉到 MyData 平臺，再次身分驗證，成功後便可繼續填寫申請資料，確認資料無誤後，需在服務提供者網站進行第二次驗證身分，驗證完畢即完成線上申辦業務。與其他服務不同的是，臺灣銀行在使用者完成申請時，會告知使用者申辦過程中同意條款的細項，也可以去查詢案件的申辦進度（如 7 號虛線框）。

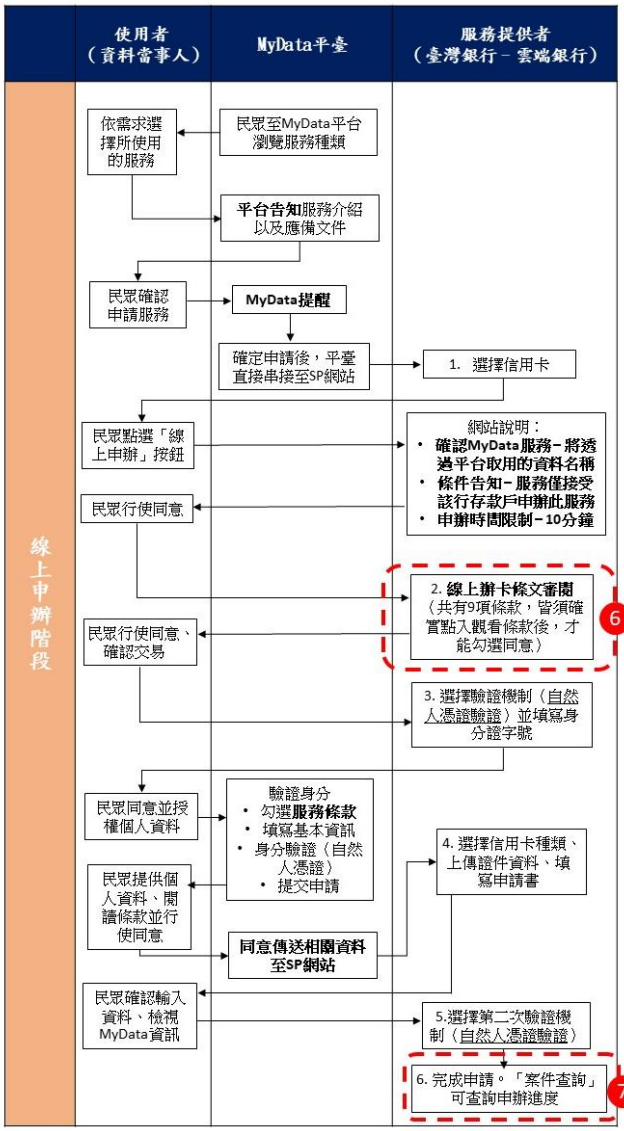


圖 58：線上申辦「臺灣銀行信用卡」作業流程圖

資料來源：本計畫自行整理。

（註：底線處為驗證方式，字體加粗處為使用者須按下同意按鈕的步驟）

圖 59 為線上申辦「彰化商業銀行信用卡」作業流程圖，圖上方從左到右依序為「使用者」、「MyData 平臺」、「服務提供者」，當使用者（民眾）從 MyData 平臺瀏覽服務種類之後，便可依需求選擇所使用的服務，透過同意平臺告知服務介紹及應備文件的說明，讓民眾進行所需服務的確認，並轉跳到服務提供者的網站。以彰化商業銀行申辦信用卡服務來說，需填寫身分證字號、勾選線上申請事項、同意信用卡線上服務使用條款及蒐集、處理及利用個人資料告知事項。與其他服務不同的是，在點選「信用卡申請線上服務使用條款」前的文字說明有明確寫出將從 MyData 平臺拿取的資料（如 8 號虛線框）。行使同意後，會跳轉到 MyData 平臺驗證身分，驗證成功後後便可繼續填寫申請資料，填寫完畢，使用者需再同意信用卡申請相關須知，確認資料無誤後送出，即完成線上申辦業務。

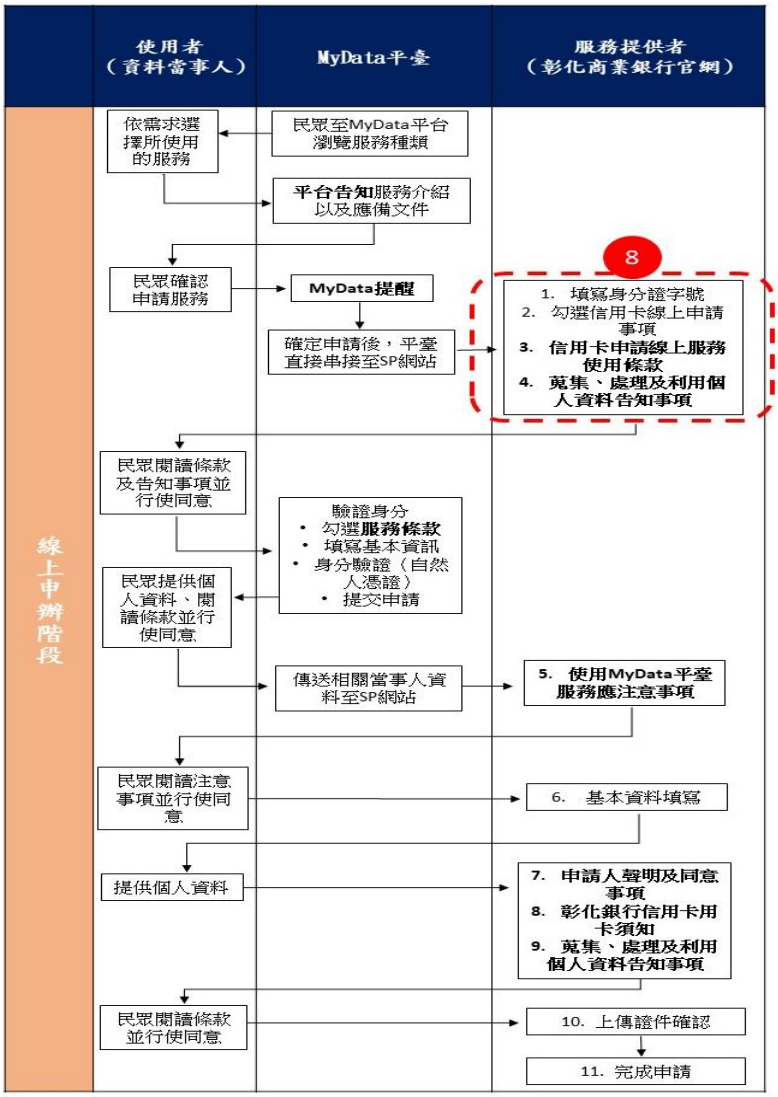


圖 59：線上申辦「彰化商業銀行信用卡」作業流程圖

資料來源：本計畫自行整理。

（註：字體加粗處為使用者須按下同意按鈕的步驟）

附錄三、訪談摘要

一、 國家發展委員會訪談摘要

- 時間：110 年 9 月 1 日（星期三） 下午 1 時 30 分
- 形式：線上會議（Google Meet）
- 摘要：

(一) 策略面

1、 請問您，貴單位推動 MyData 平臺的策略與目標為何？（對部會、地方政府、國營事業或第三方服務提供者）

當初會有 MyData 平臺的計畫是因為第五階電子化政府的計畫提及資料利用的方式，國發會規劃的方向也根據其衍生出 Open Data「依政府資訊公開法為基礎開放政府資料，供外界加值使用」、Big Data「個資去識別化後開放給第三方使用」、My Data「個人資料開放民眾自主運用」三個部分去做探討，目前已邁進第六階段電子化政府計畫，在服務型智慧政府 2.0 的計畫上仍然持續在推動並打造賦權個人的自主應用平臺，希望透過個人資料的自主運用在 MyData 平臺能夠創造更多加值服務，未來也會再持續納入中央、地方、國營事業等服務，並參考 MyData 在其他國家的發展，若有更好的方式或方向，可以做更多突破。

(1) 請問您，未來數位發展部成立後，MyData 平臺的主責機關會有變動嗎？另外，「T-Road 跨機關資料傳輸服務」目前已在多的部會營運，未來 MyData 平臺資料傳遞的部分是不是也會透過 T-Road？

數位發展部成立後，目前規劃有數位政府司及資料治理司，資訊管理處 MyData 的相關業務預期會移至資料治理司。另外，在未來，MyData 平臺取得資料提供者（Data Provider , DP）的資料都會透過機關資料傳輸專屬通道（T-Road），目前勞動部、健保署的資料皆是透過 T-Road 介接，未來也會有更多機關加入。

(二) 法規面 /知情同意

1、 請問您，MyData 平臺在知情同意流程與呈現方式，貴單位考慮如何精進（或簡化）以達成並落實民眾資料自主管理的目標？

符合個資法是達到民眾資料自主管理目標的基礎，除此之外，也需要注意操作流程的介面，除了要搭配法規告知民眾

個資蒐集目的、資料類別等法定事項外，同時也讓民眾檢閱個人資料的完整性，確定民眾知情後，由其自行選擇同意或不同意此服務，以落實個人資料自主管理的目標。

(三) 風險效益面

1、 請問您，貴單位推動 MyData 平臺於線上申辦對於個資保護或資料傳遞時的資安風險，有哪些保護措施或考量？

資料傳遞涉及技術面，不論是在與第三方業者進行座談時、或是進行內部規劃時、又或是對開發廠商公開說明的時候，都是經過測試、請廠商進行示範，並在技術、隱私權上進行充分的討論。技術面我們做了許多調整，像是我們的資料檔案加密演算法 AES[165]原本是採用 ECB 模式，有一些技術上面的先進，建議要改成 CBC 模式，或者陳恭老師提到的，原來是 JWT 資料傳輸的方式，後來也調整成 JWE 資料封裝格式去做資料傳輸加密，另外像是銀行端也提出雙向認證的問題，針對技術規範，我們是與各單位去進行討論協調，這些技術都會不斷地進行調整，最重要的目標還是在資料傳遞的安全性，希望在資安保護上可以降低風險及疑慮。

2、 為了簡政便民、流程簡化，貴單位推動 MyData 平臺線上申辦的服務，請問您認為是否有效加快行政效率或民眾（使用者）滿意度？

以銀行的回饋為例，他們認為透過平臺申請服務不管在資料的正確性還是完整性上都可以大幅提高，正確性高的原因是由於民眾的資料是由公部門提供，不易有誤；而完整性高的原因是因為當初在介接時就是由資料提供者（DP）設定要拿取哪些資料集，與 MyData 平臺介接有利於後續資料審核，審核通過率也大幅提升。因此不論在第三方的行政或成本方面，效率都有提升，對民眾來說，有了 MyData 平臺，他們只需在家線上操作，透過身分驗證就可以申辦服務，能免去以前舟車勞頓的情況。

3、 有關資料提供者（DP）在 MyData 平臺上的使用情況，貴單位預計會在 8 月底於後臺提供機關查詢資料與服務，請問您，目前的發展進度？

目前資料下載有 168 項，服務有 210 項，臨櫃服務 73 項，同時也在開發臨櫃代辦人的機制，現已接近尾聲，正委託嘉義縣政府試辦。

[165] AES 有多種加密方式和填充方式，加密方式主要有 ECB，CBC，CFB，OFB 和 CTR 等 5 種模式。

(1) 臨櫃代辦人由嘉義縣政府試辦，想請問您代辦人需要出示哪些文件？另外，臨櫃代辦人是否有身分上的限制？

在操作流程上，委託人進行身分驗證後下載資料，並設定給代辦人，代辦人收到簡訊後可進到平臺以接受委託，完成後，系統會自動產生委託書（包含委託人、代辦人、委託服務等等），代辦人只需攜帶資料條碼到臨櫃辦理即可。

(2) 臨櫃代辦人是否有身分上的限制？另外，現在需要臨櫃服務者大多為年長者，對於網路操作較不熟悉，請問您是否有相關的應對措施？

臨櫃代理的服務採「意定代理」，並由服務提供者（SP）決定是否開放「意定代理」。針對年長者身分驗證的部分，由於目前驗證方式多元，晶片金融卡也可以使用（目前有20家金融機構左右，預計明年第一季會與郵局介接完成），對年長者應該有一定的幫助，內政部也正積極研發相關免插卡身分識別的APP，待 APP 完成後能更加簡政便民。

(3) 請問您，資料提供者（DP）需不需要針對其提供 MyData 平臺使用的資料是否有被善加利用、保存、分享等問題去進行稽核？

現在的稽核流程是平臺稽核服務提供者（SP），由於稽核能量不夠，我們採取先提供自評表給服務提供者（SP）填寫（自評表包含風險面、技術面、體制面等等），後續再由我們進行抽查的方式。

目前尚未有資料提供者（DP）對平臺進行稽核，但當初向 DP 申請介接時就是依據 DP 作業規定（需取得當事人同意並進行身分驗證）去申請，並配合資料提供者（DP）的規範要求，像是內部稽核等等。

(4) 基於「目前身分驗證是由 MyData 平臺間接（或直接）協助 DP 進行處理」、「資料某種程度上暫存在 MyData 平臺上」這兩點原因，我們認為資料提供者（DP）與國發會 MyData 平臺為「委託」關係，想請問您的看法？或許未來能與各機關簽行政契約，將此關係明朗化？

MyData 平臺是中介機構，經身分驗證及個人同意後，平臺提供民眾個人資料下載及線上介接服務。以另一個角度解讀，MyData 平臺代替資料提供者（DP）處理身分驗證，資料提供者（DP）是相信 MyData 平臺並「委託」其處理身分驗證的問題，這個部分需要再討論。

在介接時，每個單位的做法（畫面跳轉）都不一樣，有些單位甚至沒有身分驗證，也造成界定關係上的困難，所以才會由 MyData 平臺統一處理。早期在規劃時，也考慮過不要將資料暫存在平臺上，但這就需要服務提供者（SP）提供公鑰給國發會，國發會將公鑰轉給資料提供者（DP），資料提供者（DP）用服務提供者（SP）的公鑰加密傳給服務提供者（SP），服務提供者（SP）再解密得到資料，一來一往對資料提供者（DP）來說過程過於冗長，經過評估後，還是現行模式較為恰當。

(四) 推廣應用面

1、 請問您認為 MyData 平臺開發上可能的服務缺口為何？（如資訊素養、人員抗拒、經費來源、技術門檻等）

我們發現，在與服務提供者（SP）介接的過程，比較常出現的缺口是「技術門檻」，開發過程中，有些單位較不了解服務過程，因此，第一步驟，就是需要讓服務提供者（SP）知道服務流程，通常我們會舉辦應用及技術開發說明會加以說明整個流程，緊接著，第二步驟就是技術人員開發，包含資訊要加密、畫面跳轉等等，技術人員須對憑證及加密等有所認知。不過此類情況通常出現在首次開發，首次介接需開發 3 到 4 個月不等，在測試過程中反覆進行調整外，也需要找內部員工比照真實環境操作以進行試辦，通常服務提供者（SP）在增加後續服務時，所需花費的時間都會縮短許多。

2、 銀行局是國發會最早接觸的示範單位，請問他們當初有提出哪些服務缺口？

銀行局作為事業主管機關，反而比較沒有意見，國發會反而是與金管會介接，金管會在意的重點還是資安問題、流程簡化與最大化擴展服務。後續有和業者進行 2 至 3 次的座談，業者提出許多不管是在技術面還是行政面上的意見，像是申請流程複雜、頁面跳轉過多、資料介接彈性程度、希望直接與 MyData 平臺後臺的 API 對接、技術上加密（對稱式加密、雙向憑證）等等，我們就是針對可以調整的去做討論、修改。

3、 請問您，MyData 平臺未來規劃增加哪些資料集或服務？

未來規劃增加的資料集與服務有非常多，以今年底要增加的資料集來說，包含原住民身分資料集、親屬關係擴及二等親、財稅資料、輻射安全證書等等，在服務的部分，擬增加勞保生育給付線上申辦、證券業線上開戶（洽談中）、保險業線上開戶及理賠等等。

二、 衛生福利部中央健康保險署訪談摘要

- 時間：110 年 9 月 3 日（星期五） 下午 2 時 00 分
- 形式：線上會議（Google Meet）
- 摘要：

(一) 策略面

1、 請問您，貴單位推動 MyData 平臺的策略與目標為何？（組織內、外或第三方）

本署目前與 MyData 平臺介接的資料主要是保險業務（投保相關資訊），此類的資訊較容易給第三方應用程式（下稱「第三方 APP」）應用，在規劃時，本署也考量到醫療資料是特種個資，在保存及後續應用上有不同強度的規範，所以沒有提供 MyData 平臺醫療資料的詳細資訊。

2、 根據「健康存摺系統軟體開發套件使用管理要點」，貴單位除擔任健康存摺 App 的服務提供者，也是 SDK 資料提供者。基於資料雙向共享互惠的原則，想請教貴單位推動第三方開發者的規範與想法。

首先，資料應用是以「必須經過民眾的同意才能進行」為原則，規劃初期，遇到許多不同的想像與壓力，舉例來說，根據個資法要求，同意只能透過書面同意或使用自然人憑證數位簽章，但在署內的環境中無法完全符合，目前本署的做法是套用健保卡網路服務註冊的精神，以健保卡進行裝置認證並視為民眾同意。

再者，即使本署在處理軟體開發套件（Software Development Kit, SDK）介接健康存摺（下稱 SDK）非常謹慎，資料的取用也是根據「健康存摺系統軟體開發套件使用管理要點」控管權限，但還是無法確認第三方 APP 的嚴謹度，本署能確定的是第三方 APP 在呼叫（call）SDK 時有固定畫面且畫面是由署內開發的，以確保使用者的帳號密碼、個資等資料不會被第三方劫走。

最後，本署一直期待能透過不同第三方 APP 的參與，讓資料更容易解讀、更貼近民眾的使用。

(二) 法規面 /知情同意

1、 請問您，根據「健康存摺系統軟體開發套件使用管理要點」，貴單位如何確保介接提供當事人個人資料時，能確保個人化資料之蒐集以最小化原則？其次在當事人同意提供其下載之個人化資料前，以何種機制確保當事人對服務條款知情瞭解？

本署在提供資料給第三方 APP 時，為了限縮資料範圍，民眾可自行選擇要直接提供近三年所有資料，或自行挑選項目、月份給第三方 APP。此外，為了確保民眾清楚健康存摺保存了自己的哪些資料以及民眾對服務條款的知情瞭解，本署在與第三方 APP 簽約時，有兩個強制規定，第一，第三方 APP 在身分驗證時，需附上超連結，串聯健康存摺，若民眾要查看，可直接連結，瞭解細項資料；第二，需在服務條款知情同意的頁面設置畫面停留秒數（根據內容設定秒數，因為內容不多，一般設定為 5 秒），避免民眾略過條文閱讀就按下一步。

(1) 請問您是否能提供與第三方 APP 介接時的相關文件給團隊參考？

團隊可以參考署內網站[166]，目前與第三方 APP 介接 SDK 分為兩個階段，第一階段為簡易申請，主要是要讓 APP 測試、瞭解環境，第二階段為正式簽約，簽約前會要求第三方 APP 提供相關資料，簽約完畢才會讓第三方拿到個資。

(2) 請問您剛提到每個同意會停留五秒（一段時間），這個多的步驟，僅停留畫面，還是有多設置一個勾選框呢？

知情同意書只是進行陳述，並沒有要民眾同意什麼條款，時間倒數完畢後「同意按鈕的勾選框」會浮出，讓民眾選擇，按下「同意」按鈕就等於同意上述說明，若不同意就離開。

2、 請問您，健康存摺在知情同意流程與呈現方式該如何精進以達成民眾資料自主管理的目標？

目前本署也在討論是不是不要以開放所有資料給第三方 APP 為原則，第三方 APP 申請時可以鎖定部分項目，舉例來說，今天設置的可能是 COVID-19 疫苗資料，那就不用給第三方 APP 門診就醫的紀錄等等，希望針對目的能更明確，在介接時就限縮範圍、設定好提供的資料集，避免民眾誤點項目，提供不必要的資訊。

(1) 在研究過程中，發現一樣的業務，但不同廠商要的資料去不一樣，目的拘束性，在理論上，應該從第三方 APP 去管理，健保署應該負責的是第三方 APP 跟當事人間個資提供資料，及傳遞資料是否有逾越範圍，您的看法是？

[166] 衛生福利部中央健康保險署（2021）。SDK 健康服務連結，2021 年 9 月 6 日，取自：https://www.nhi.gov.tw/Content_List.aspx?n=A5407A276376FECC&topn=5FE8C9FEAE863B46。

第三方 APP 的需求很零星，本署除了需要考慮資料處理的複雜性，在資訊提供的許多面向上也需要考量，資料提供在醫療面上較豐富，像是健保醫療藥歷雲端分享系統，醫院端及民眾端可以查看相同範圍，後續就有許多發展可能；在資訊面上，資料處理難被臆測；在應用面上，這個業務並沒有想像中蓬勃發展，還仍在嘗試性服務的階段，也因此，到目前為止，一直沒有很好的應用面。

(三) 風險效益面

1、 請問您，貴單位推動健康存摺時，是否評估過個資保護或資料傳遞時的資安風險？

本署無法延伸管理民眾就醫資料，也無法確認第三方 APP 如何延伸資料，第三方 APP 處理的方式都不相同，有些第三方 APP 是下載資料後放在 APP 中，有些第三方 APP 是下載資料後帶回後臺，在這方面比較難稽核。但本署在個資保護或資料傳遞上做了許多加強保護，首先，在封包資料給第三方 APP 時，都是不同把加密與解密的鑰匙，每個第三方 APP 都會有一把鑰匙，其中每個檔案也都會各再有一把鑰匙，且一次最多只能拿 5 包檔案。健保署是 A 級機關，在資安防護上要求很多，但本署無法要求第三方 APP 做到跟我們同等級，只能要求第三方 APP 需要每年進行資安檢測[167]，而資安檢測也成為廠商進入 SDK 的門檻，上個月，本署才正式停權未進行資安檢測的 15 家 APP。

(1) 請問您，貴單位是否有規劃（或期待國發會協助），在第三方 APP 介接時，能有管理規範（資格、認證等等）？

其實對要申請 SDK 的第三方是有基本要求及規範的，基本要求[168]的部分，包含申請廠商不得為陸資企業、不得使用匿名、假名、人頭、虛設行號或虛設法人團體等等；規範的部分就是以「資安檢測」為主，資安檢測一年費用約10至12萬，對第三方 APP 來說已成為一個門檻。另外，在第二階段簽約時，第三方 APP 需要提供給本署知情同意書的文本，讓我們確保知情同意的落實。

2、 請問您，貴單位推動健康存摺時，是否評估過有效加快行政效率或民眾（使用者）滿意度？

[167] 依據經濟部工業局「行動應用 App 基本資安規範」App 資安等級分為「L1、L2、L3」3 級。

[168] 依據「衛生福利部中央健康保險署健康存摺系統 軟體開發套件使用管理要點」。

民眾沒有滿意與不滿意的問題，目前還有許多民眾尚未完全接受到此類資訊，在民眾端，透過民眾的反饋，健康存摺反而成為本署對醫院診所的查核工具，包含民眾反映就醫次數與實際不同、病例用語的認知差別等等，民眾也有反應，希望第三方 APP 能改以手機開機密碼就可以使用；在第三方 APP 端，APP 介接時都提出希望將 B2C、C2B 的方式更改為 B2B 的方式，並採持續性同意，但在行政面上有遇到相關法律見解的困難，所以現況還是以單次授權為主。

(1) 目前 MyData 平臺為單次授權，在貴單位與 MyData 平臺介接時，是否會造成困難？

配合 MyData 平臺，本署現在也是以單次授權為原則，比較有趣的是，保險業者其實非常希望取得資料，我們早期與南山人壽也有討論過介接，但金融管理監督委員會認為，不可以將健保資料當成民眾接受投保與否的依據，因此停止 SDK 的提供，主管機關看重的是，第三方如何使用資料，如果是站在輔助健康跟醫療面就完全不一樣，為避免保險公司在民眾投保後，讓民眾在不清楚的情況下簽署同意書與健保署要資料，現在的模式為，本署給固定欄位（只提供什麼時候就醫的相關資料），保險公司批次請求，若保險公司對資料有疑慮，就在自行行文到醫院去要資料。

(四)推廣應用面

1、 請問您認為健康存摺開發上的服務缺口為何？（如資訊素養、人員抗拒）

本署的態度是以資料開放為原則，至於資料是不是給太多或太雜，署內後續會再不斷精進修正，在開發第三方 APP 介接時，對我們造成的心理壓力是更大的，因為我們無法確保第三方如何儲存資料及資料防護的強度，這也成為署內內部的隱憂。在稽核上，因為能量不足，我們對醫療醫事機構採「抽審」的方式。醫療醫事機構可以批次和我們申請隔天看診病患的醫療相關資料，並在 24 小時內刪除。

民眾端反應的詬病是註冊太過困難，雖然現在有手機門號及插卡兩種方式，但有些民眾手機門號不是自己的，只能插健保卡、查戶口名簿做驗證，綁定的模式太過複雜。

醫療領域還是有資訊落差，永遠都存在，健保署願意將資料開放給民眾成為 MyData 的概念，讓民眾更在意自己的健康。

2、 想請貴單位就健康存摺服務，以及如何保障民眾知情同意、及資料利用的未來發展提出一些建議。

曾經想將健康存摺資料給資訊與通信科技（Information and Communication Technology, ICT）產業廠商，讓他們發揮最大效益，但在審視資料治理的過程中，我們靈機一動，反過來想，在某些情況下，不如將 ICT 資料收載，若民眾同意，甚至可以透過健保醫療資訊雲端系統，讓醫生能看到民眾的資料。

三、 臺灣銀行訪談摘要

- 時間：110 年 9 月 8 日（星期三） 上午 10 時 30 分
- 形式：線上會議（Google Meet）
- 摘要：

(一) 策略面

1、 請問您，貴單位推動 MyData 平臺的策略與目標為何？（組織內、外或第三方）

我服務於臺灣銀行（下稱本行）創新實驗室，創新實驗室主要負責導入創新服務與金融科技。MyData 平臺是政府提供的一個創新服務，最直接的好處，是資料的正確性及標準化，資料不會經過變造，也能確保資料提供的一致性，未來也能夠結合服務流程，讓服務更數位化。我們也期許在未來，民眾使用手機透過 MyData 平臺就可以完成申請，銀行也可以取得最完整的民眾資料。因此本行推動 MyData 平臺的期待可以達成兩項目標，第一，希望帶動作業流程的精進；第二，未來數位化的預先準備。

(1) MyData 平臺在提供個人資料時，會有斷點，並不是即時的（real time）傳送，對您會造成影響嗎？

以貸款業務為例，本行目前仍以行員進行人工徵審，在這部分斷點（約 30-40 分鐘）就不會對作業流程造成太大的影響。然而後續如果要導入至 AI 即時徵審，無法即時回傳資料，就會影響到服務流程。

另外對業務影響較大的是資料回傳失敗的問題，受到部分資料回傳的等待斷點問題，本行必須等待一段時間，才知道資料是否回傳成功，然而民眾已經離開申辦環境（電腦、讀卡機），銀行若再要求補件或重新辦理，民眾常常無法理解，產生客訴問題。如果此業務是即時的（real time），申請系統可以馬上告知民眾重新授權或準備資料，將可避免客訴及後續額外增加的作業。

(2) 請問您，民眾透過 MyData 平臺申請貴行信用卡的比例是？

本行線上信用卡，考量風險及業務發展，必須為本行既有存款往來客戶，且需要插上晶片金融卡驗證身分。而使用 MyData 服務須以「自然人憑證」進行授權，與本來需插卡驗證之模式一致，且本行較多公教人員客戶，持有自然人憑證比例也較高，因此本行以 MyData 平臺申請信用卡比例達 30 至 40%。

2、 根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，銀行除擔任 MyData 平臺服務提供者外，也可申請成為平臺的資料提供者。基於資料雙向共享互惠的原則，想請教貴行對成為 MyData 平臺資料提供者的看法？

對於成為資料提供者（DP）的想法，可以分為兩個面向來說，第一面向是法規面，首先，根據銀行法第 48 條第 2 項，銀行對客戶有關資料具有保密義務，不能提供給他人知悉。再者，雖然現在銀行有開放銀行（open banking）的業務，但根據銀行公會自律規範[169]，銀行提供資料給第三方服務提供者（TSP）有非常嚴格的規範，MyData 平臺的性質作為第三方資料中介平臺是否能符合規定，又是另一個問題；第二面向是競爭性面，目前 MyData 平臺的資料提供者（DP）都是政府機構，然本行屬商業銀行，有市場競爭問題，無法確保提供客戶資料後，客戶會不會流失、競爭力是否會有所改變。也因此，本行暫時沒有評估是否成為 MyData 平臺的資料提供者（DP）。

(二) 法規面 /知情同意

1、 根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，貴行擔任服務提供者，如何確保介接 MyData 平臺提供當事人個人資料時，能確保個人資料之蒐集以最小化原則？其次在當事人同意提供其下載之個人資料前，以何種機制確保當事人對服務條款知情瞭解？

資料標準化與最小化的這件事，第一，與組織文化有關，我們銀行作風較保守，因此取資料時會確保此份資料確為辦理業務所必須；第二，與組織架構有關，本行拆分為創新實驗室與業務部門，創新實驗室會負責把關資料，去確認業務單位申請的資料集是符合資料最小化的原則。

2、 根據國發會「個人化資料自主運用（MyData）平臺服務條款暨隱私權保護政策」中規範：「若您為未滿二十歲之未成年人，...當您使用本平臺時，即推定您的父母或監護人已閱讀、瞭解並同意接受本條款之所有內容」。貴行目前是否將未成年線上開

[169] 中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範。

戶（數位存款帳戶）的服務與數位化個人資料自主運用平臺服務機關連結？倘若欲準備連結，如何確保線上申請並非未成年人自行操作？

本行尚未開放未成年線上開戶服務。然而於授權面上，銀行公會於安控基準[170]上業已訂定好銀行在身分確認方式能使用的工具（自然人憑證、金融卡、OTP、網銀帳密等等）及規範，對銀行來說，相關確認機制將跟隨安控基準之規範。

3、 請問您，MyData 平臺在知情同意流程與呈現方式該如何精進以達成民眾資料自主管理的目標？民眾在線上申請貴行信用卡業務時，需要點選 7 個彈跳式視窗，容易造成知情疲勞，請問您的看法是？另外，有些銀行信用卡會綁定功能（悠遊卡…）如果民眾不想綁定此功能，貴行有相應措施嗎？

我認為，以使用者習慣來說，條款的設計很難影響到使用者要不要看條款。另外本行網站的條款閱讀設計方式是一開始設計網站時就規劃好的，因此要大幅度調整條款設計閱讀方式有一定難度。另外我們需要遵從法遵，使用者必須看完所有條文（至少下拉至最後）才能勾選同意按鈕，所以在知情疲勞上，改動的彈性是較小的。

我們的信用卡目前只有一張有綁定其他支付功能，但做法是此張卡片強制搭配，沒有提供選擇。

(三) 風險效益面

1、 請問您，貴單位推動 MyData 平臺於線上申辦是否評估過個資保護或資料傳遞時的資安風險？

我們以資料不落地的概念去思考，設置了閘道器（gateway），銜接 MyData 平臺，而後，MyData 平臺的閘道器（gateway）會再連接到業務申辦系統（雲端銀行、就學貸款入口網），中間都是立即性的傳送，資料只會在雲端銀行暫存一段時間，提供民眾查詢申請之資料，在較短的保存時間到後，資料就會清除，儲存在銀行更後端的業務系統，以確保個資保護。而在每一層系統間，也都有防火牆的保護，以確保相關駭客攻擊。

2、 請問您，貴單位推動 MyData 平臺於線上申辦是否有效加快行政效率或民眾（使用者）滿意度？

行政效率面，有兩大問題，第一，銀行如要進行相關申請，需同時向金融監督管理委員會之資訊服務處、銀行局及國家發展委員會進行申請，橫跨多個機關，影響申請時效；第二，在過去試營運期間，測試區是可以持續使用的，但現在測試區每次

[170] 金融機構辦理電子銀行業務安全控管作業基準修訂摘要。

使用都必須申請，一次最多 3 個月，然而為求謹慎，本行每次變動相關類型的業務都需要重跑測試區，有時候變動並不大（例如 UI 微調…），但我們卻要為此重跑測試區申請，申請時長也不一定，至多需要 1 個月，導致我們在行政效率上無法掌握，也使推動服務變得愈加困難。

民眾滿意度面，最大的問題還是在授權上，只要需要插卡驗證，就會增加推動的難度，就算民眾有插卡機，但接下來還有電腦安裝元件錯誤的問題。另外，MyData 平臺為了解決自然人憑證普及率不高的問題，開放晶片金融卡進行身分驗證，很感謝 MyData 平臺有提供民眾更多元的認證方式，然而現在設計民眾在第一次申辦 MyData 平臺時仍需要進行雙重驗證，民眾在服務提供者（SP）端驗證完，還需要到 MyData 平臺再進行一次身分驗證，每增加一道流程，就增加一次民眾放棄的機會，即使只有第一次使用 MyData 服務需要雙重認證，但 MyData 平臺的服務大多都是非經常性的，很多民眾都只使用過一次 MyData 平臺或使用間隔非常長，這就會產生斷點及不便利性。此外，雖然現在有行動認證，但在臺灣，還是有一定比例門號非本人使用的情況，例如未成年人、公司戶等等，門號非本人，也會使驗證方式減少、增加不便，這都是我們未來在推動 MyData 平臺會遇到的問題。

(四) 推廣應用面

1、 請問您認為 MyData 平臺開發上的服務缺口為何？（如資訊素養、人員抗拒）

首先，MyData 平臺近期有些情況讓我們措手不及，第一，廠商曾突然表示要下架本行就學貸款的服務，因為此項服務為限定時間之服務，廠商要求我們必須重新申請，所幸經過溝通後，已解決此項問題；第二，本行資訊人員開發時突然發現無法登錄測試區，才知道現在使用測試區需要經過申請。這些變動如果能夠事前先與服務提供者（SP）先溝通或是了解情況後再行調整，這樣服務提供者（SP）才能夠馬上的因應。若執行相關措施皆無事先通知，會讓服務提供者（SP）的相關維護與開發人員措手不及。再者，銀行端也會有人員抗拒的服務缺口，無法馬上看出成效的創新服務，需要花更多的時間去進行內部溝通。

2、 貴行是參與國發會 MyData 平臺、擔任服務提供者的銀行業者之一。想請問貴行就 MyData 平臺未來的發展提出一些建議。

針對「資料源」可以提出一些建議，希望能夠有「服務客製化」資料源供服務提供者（SP）使用。有些資料源的內容太多，對

於使用業務上來說，就會有取得太多個資的問題，但又有些業務同時需要兩個相近的資料源才能辦理業務，又額外多一個資料源需要處理。主辦單位或許可以反向思考，以常用的服務（如申辦信用卡、貸款）思考，反向建議資料提供者（DP）組合出專屬運用情境的資料源。

「資料源」的另一個問題是，目前資料源有兩種檔案格式，第一種，JSON 檔，可以直接帶入系統給機器讀資料，方便後續以 AI 辦理業務。第二種，PDF 檔，資料呈現完整、上級長官易懂，便於日後保存與稽核。但現在申請服務只能有 5 個資料集，部分資料源 JSON 檔與 PDF 檔無法都納入使用，只能從中選擇，但左右為難，甚至部分資料源沒有 JSON 檔可以運用，希望 MyData 平臺未來可以解決此問題。

最後，在銀行服務剛上線時，內部其實也有在討論「資料蒐集最小化」的問題，同一個服務，不同銀行拿的資料不一樣，是不是要由銀行公會訂定規範，雖然最後雖然不了了之，但我認為這也是需要處理的問題，有一個統一規範，銀行不用擔心自己會逾越「資料蒐集最小化」原則，民眾與銀行都可以更放心使用服務。

四、 嘉義縣政府訪談摘要

- 時間：110 年 9 月 13 日（星期一） 下午 2 時 00 分
- 形式：線上會議（Google Meet）
- 摘要：

(一) 策略面

1、 請問您，貴單位推動 MyData 平臺的策略與目標為何？（組織內、外或第三方）

整體的規劃與未來預期達成的目標如**圖60**及**圖61**所示，另外，本府針對組織內、外部及第三方也有不同的策略及目標，詳述如下：

(1) 組織內部：採取「由上而下」、「由下而上」的策略，定義清楚的範圍，並讓承辦人習慣線上申辦的作業流程，再將其精進。

(2) 組織外部：例如透過基層地方首長的力量，推動 MyData 平臺業務（包含 MyData 知識教育），如辦理鄉鎮巡迴說明會、特定社團（身心障礙社團、長照中心及數位機會中心）宣導或教育訓練。面對高齡化、少子化、人口流失衝擊，希望讓嘉義子弟有優良就業機會、良好生活環境，得以回鄉工作、照顧父母，推動發展及改善生活品質。

(3) 第三方：透過社群媒體的觸及，引導縣民了解本府推動的各項線上申辦服務。

圖 60：嘉義縣政府 MyData 應用服務規劃

資料來源：嘉義縣政府資訊管理科。

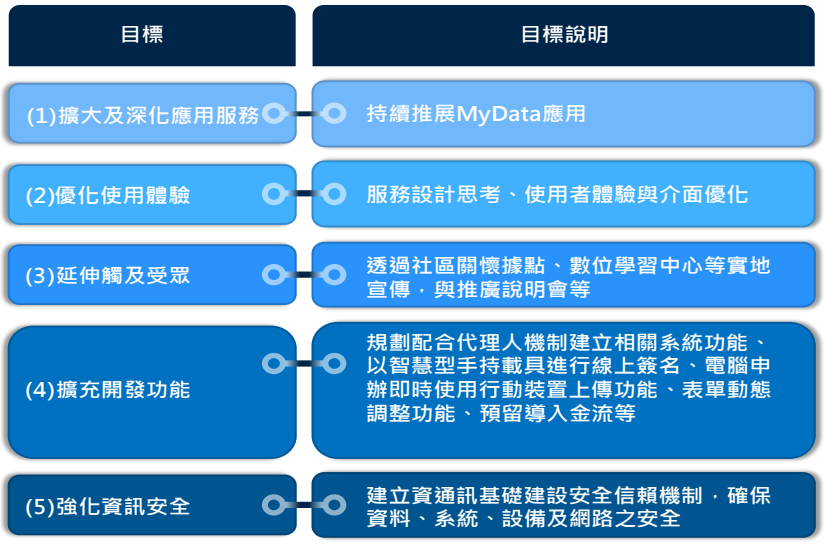


圖 61：嘉義縣政府預期達成目標

資料來源：嘉義縣政府資訊管理科。

2、 請問您，貴單位加入 MyData 平臺服務，考量的因素是什麼？（如接取中央資料、提供更快速的線上申辦服務、有效的資安防護等）

我們期望提供民眾、業務單位的申辦系統有以下方向：

(1) 縮短申辦時效、民眾有感：本府幅員廣大，尤其偏遠山區，實施臨櫃服務對於許多縣民仍不方便，加入 MyData 平臺

服務，除了希望減縮數位落差之外，透過 MyData 平臺的整合，讓民眾減少應備證件，加快線上申辦效率，是最直接的考量。可連結多項跨機關資料：申辦系統必須提供可信任的佐證資料，讓民眾不用四處奔波，承辦人也可以方便及放心查閱參照。

(2) 資料集正確性即時性：透過 MyData 系統資料不落地，且為最即時，承辦同仁信任度高，可縮短審核時間，提高效率。

(3) MyData 平臺資料集來源資安防護嚴謹。

(二) 法規面 /知情同意

1、 對於民眾申辦資料的保存或分析，依照什麼樣的個資保護規範？是否有稽查機制？

為確保系統之機密性、完整性、可用性，以防護駭客攻擊與入侵，防範人為之疏失與不法使用，維持資料安全與資訊、通訊、系統正常運作，本府既有資訊安全政策，包含下列主要項目：

(1) 強化資安管理

落實本府資安管理政策，避免因各種因素導致資料不當使用、洩漏、竄改、破壞等情事發生，其中主要可分為安全暨風險管理、資產安全、安全架構與工程、通訊及網路安全、識別暨存取控制、安全性評估與測試、安全性作業等多個領域；此外也將依循 NIST 網路安全框架，確保資訊安全，並參考 ISO27001 及 ISO27701 精神進行資安管理。

(2) 第三方弱點掃描

系統弱點掃描主要是將由行政院經評選之第三方檢測公司確保是否存在資訊安全弱點，將同時使用工具與人工檢測驗證，除可提早發現安全弱點，及時修補，避免遭受入侵攻擊。

(3) 滲透測試

以委任受信任的第三方評估網路安全，以駭客思維及攻擊模式對系統進行安全測試，並瞭解系統主機及程式存在漏洞，找出脆弱的環節，並提供修復及防禦建議。

(4) 落實資料備份機制

利用自動化的系統及安全異地原則，採用日備份機制或自

訂循環的備份機制，並有專人親送外接式儲存媒體，確保線上線下皆完成，並定期執行復原演練確保資料可用性及完整性。

(5) 實施內外稽核及追蹤管理

邀請內部人員及公正第三方進行內外部稽核，審視系統是否符合資安規範，並提早發現問題然後針對問題進行改善，後續並列管及追蹤相關改善建議，確保資訊安全。

2、 請問您，MyData 平臺在知情同意流程與呈現方式該如何精進以達成民眾資料自主管理的目標？

(1) 提供線上同意書。

(2) 要授權系統能取回哪些 MyData 平臺，系統出示清單告知。

(3) 取回 MyData 平臺後，民眾在送件前能即時預覽自己的 MyData。

(三) 風險效益面

1、 請問您，貴單位推動 MyData 平臺於線上申辦是否評估過個資保護或資料傳遞時的資安風險？

有評估，並針對本府一站式便民服務網對於個人資料的保護，目前機制如下：

(1) 作業系統面：

a. 相關軟硬體設備存放於本府電腦中心，人員進出須刷卡及申請，並有專人控管，提供安全環境。
b. 系統對於個人資料集蒐集目的僅限於業務單位規定之最小範圍。
c. 系統對於個人資料處理方式及流程符合嚴謹，且不會複製到與蒐集目的無關之儲存載體中。

(2) 資訊安全管制與個人資料保護機制查核，已完成以下檢查項目：

a. 系統相關主機、電子文件與紀錄，已存放在具有保護之處所，並具有存取權限保護之環境（本府資訊安全機房）。
b. 系統相關主機系統具備適當的保護措施，包括作業系統、防毒軟體、弱點掃描及修補、存取控制、稽核紀錄管理等。

c. 系統目前保存當事人資料傳輸相關紀錄可達兩年以上。
d. 系統主機之營運持續，若需要停機維修，將依國發會 MyData 平臺之服務品質水準規定，應於上班時間 4 小時內，非上班時間 8 小時內修復系統，並通知 MyData 平臺團隊。

(3) 弱點掃描、滲透測試面：

a. 委託資安公司定期進行網站應用程式弱點掃描，並提出網站修補建議。
b. 委託資安公司定期進行網站主機弱點掃描，並提出系統修補建議。
c. 委託資安公司白帽駭客進行網站整體滲透測試（攻防演練），並提出網站修補建議。

(4) 系統備份面：

a. 相關主機共有 5 台（申辦 AP 主機、申辦 DB 主機、API 主機、測試主機、NAS 主機），其中 AP、DB、API、測試主機皆透過自動排程備份程式備份到 NAS 主機。
b. 作業系統備份透過 Windows Backup 軟體，每日自動排程備份到 NAS。
c. 申辦資料備份透過批次檔，每日自動排程備份到 NAS。
d. 申辦資料庫備份，透過資料庫維護程式，每日自動排程備份到 NAS。

2、 請問您，貴單位推動 MyData 平臺於線上申辦是否有效加快行政效率或民眾（使用者）滿意度？

有加快行政效率及民眾（使用者）滿意度，舉例來說，「重陽節敬老禮金金融帳戶申請」線上申辦，這 2 個月來，超過 4000 件線上申請案件，可見民眾已逐漸習慣使用線上申辦作業，減少臨櫃辦理，尤其在疫情期間，線上服務佔大多數比例。

(四) 推廣應用面

1、 請問您認為 MyData 平臺開發上的服務缺口為何？（如資訊素養、人員抗拒）

目前比較缺乏的是國發會政策，造成開發上的不便，包含：

(1) 申請介接 MyData 平臺皆必須透過紙本申請書與發文程序，公文往返、紙本文件修訂，花費許多時間，建議應開發線

上申請機制。

(2) 申請介接作業須交付非常多測試報告，需提供檢核表、試辦報告，且每一項都要經過 5 組人測試，從提出申請書申請、測試、試辦、試營運至服務正式上線約 1 個月，若該縣市申請 50 項，就要產生 2 x 5 x 50 = 500 組測試報告，非常耗時，且如果中途又另有問題，流程需重新來過，一次申請介接作業需要不只 500 份測試報告。

2、 請問您，MyData 平臺未來規劃增加哪些資料集或服務？

(1) MyData 平臺建議儘速全面導入代理人制度。

在老人人口比例佔多數的嘉義縣，多由其居住外地的親屬、子女代為洽公申請業務，許多臨櫃作業都可以用紙本委託，國發會正積極開發測試 MyData 平臺代理機制，輔助登記案件專業代理人確認當事人身分，及查驗資料；本府期待是項功能儘速完成，並全面導入，提供代理人為數位能力較弱的長者申辦服務。另本府建議之代理人機制如**圖62**。

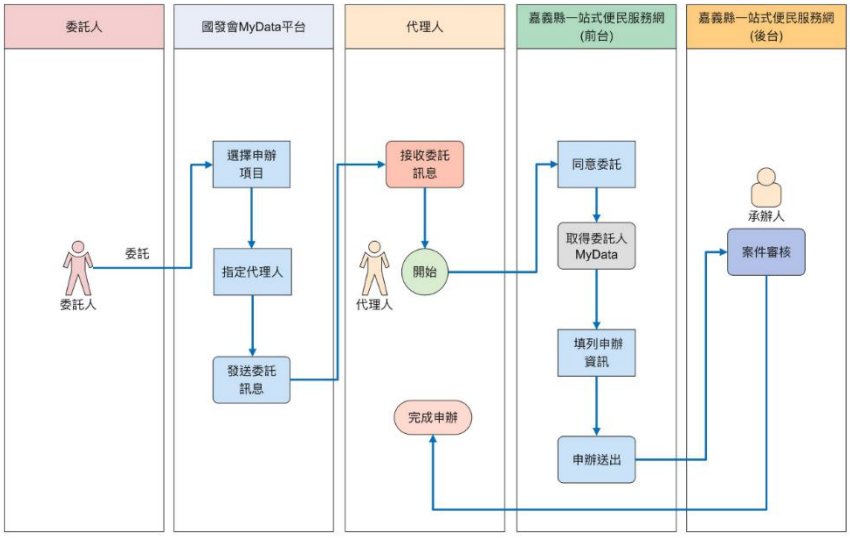


圖62：嘉義縣政府建議之代理人機制

資料來源：嘉義縣政府資訊管理科。

(2) MyData 平臺多種驗證方式仍以實體卡為主不易推動，且不適用於行動裝置。

MyData 平臺雖然已新增多種驗證方式下載資料，但還是以實體卡片為主，像是自然人憑證、晶片金融卡或健保卡等，都是民眾手邊經常持有，第一次使用平臺下載個人資料，須在個人電腦或筆電安裝元件，對於數位能力較低的長者容易造成障礙，且不方便由行動化裝置操作，臺灣行動身分識別（下稱 TW FidO）雖然可用於行動驗證，且結合生物特徵後續免插卡，但首次綁定依然需要自然人憑證透過晶片讀卡機註冊。

其他如雙證件驗證（健保卡卡號+戶口名簿戶號）的無實體卡方法無法適用於大多數常用的個人資料集（如戶政國民身分證資料），因此對於需要下載多種類別資料的申辦服務，也無法適用。

(3) 到宅服務有別於線上及臨櫃申辦。
本府地理基於環境與人口結構因素，不是所有業務都適合線上與臨櫃申辦，反而是更需要推動到宅服務，以便能更深入服務那些弱勢的族群，例如久病在床的民眾、獨居老人等，但推動到宅服務，需要有大量的人力資源投入，包含村里長、村里幹事、社工、志工等；考量案主狀況，到宅申辦可能無法親自線上操作，也無法像臨櫃時由承辦人員直接辦理業務，僅能由服務人員錄案、確認申請的佐證資料，因此需要簡易的操作流程，及一套有別於方便線上及臨櫃申辦使用的管理方式，協助到宅申辦。

(4) 各縣市間業務會重疊，可考慮整併，或者發展關鍵業務。
縣市政府都有類似或相同的申辦業務，但缺乏共通的線上申辦共構平臺，必須各自建置，但卻擁有不同功能、版型、使用方式的管理系統，也產生高額的經費及後續維護費用。以中央機關的角度建置一個共通性的線上申辦共構平臺，讓縣市政府透過申請就能自建申辦項目，也可整合 MyData 平臺、資料交換機制、多元身分識別等平臺，並以類似 K8s 等容器化服務型態存在，可快速部署管理，是未來可規劃方向。
如**圖 63** 所示，前端介面平臺可以由各縣市政府自訂，並有一致性的案件管理平臺辦理或者追蹤案件，透過 API 介面程式可以把資料回傳到縣市政府自行管理，如此類似系

統不用重複開發，成本可以發揮最大效益，中央統一維運運管等。

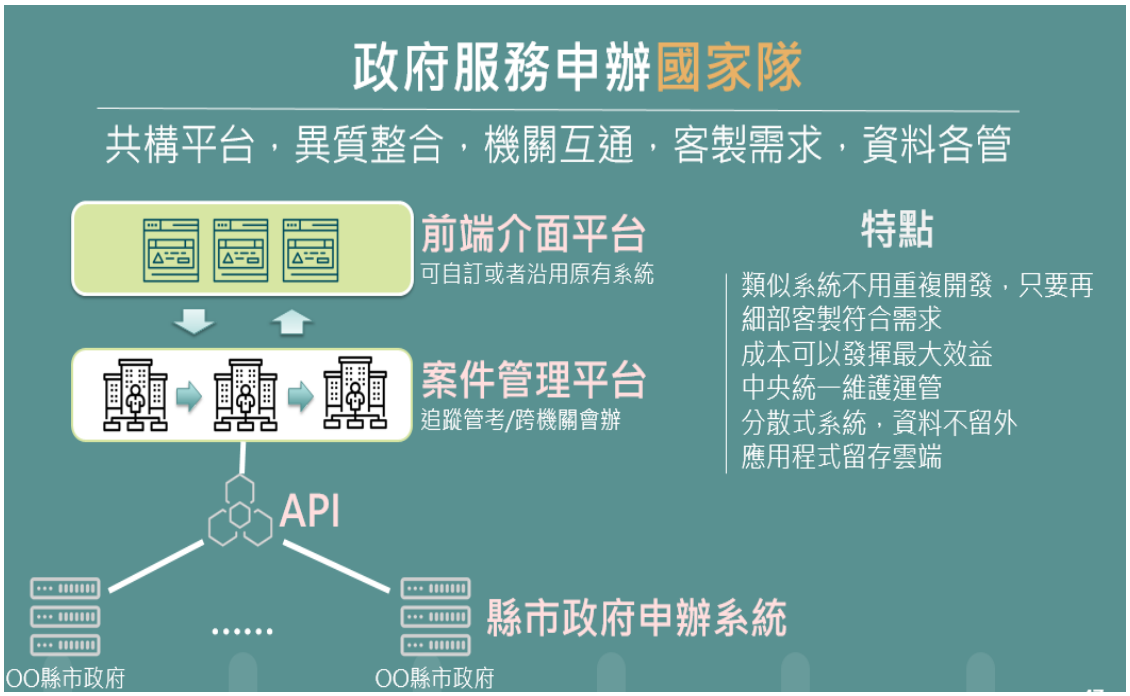


圖 63：嘉義縣政府建議之線上申辦共構平臺架構

資料來源：嘉義縣政府資訊管理科。

(5) 建議一些個人健康方面的資料集，增加民眾使用意願及彈性。

(6) 介接或下載農委會農糧署資料，提供民眾線上申請農損補助，農民無須在公所排隊等候，縮短農民申請時間。

(7) 中央業管單位開發供地方政府使用的線上申辦系統（如警政署及財政部）也介接 MyData 平臺服務，或由地方政府介接 MyData 平臺服務。

五、 金融監督管理委員會訪談摘要

- 時間：110 年 9 月 14 日（星期二） 上午 10 時 30 分
- 形式：線上會議（Google Meet）
- 摘要：

(一) 策略面

1、 請問您，貴單位推動 MyData 平臺的策略與目標為何？（組織內、外或第三方）

先談談 MyData 平臺為何會先選擇與金融業合作，首先，金融業在這方面較其他行業更有需求，再者，金融業在個人隱私保護上一直是比較嚴謹的，以及，在試辦過程中，不論是金融機構或外商都一再提到希望金管會參照「新加坡 MyInfo 平臺」，剛好國發會推出 MyData 平臺，金管會也樂於合作。

金管會推動 MyData 平臺有三大目標，第一，推動金融科技，不管是監理沙盒、新創協助、開放銀行（open banking）還是介接 MyData 平臺都是為了蓬勃金融科技業；第二，便民服務，MyData 平臺可以讓消費者在申辦業務上更便利且更友善；第三，機構內部效率的提升，以往紙本與影像式的提供效率較低，透過電子化服務，能節省機構處理的效率。

(1) 開放銀行（open banking）是消費者將其金融機構的資料提供給其他銀行或第三方，MyData 平臺是民眾將其在政府的資料提供給第三方，請問您認為，這兩個管道未來的發展會是整合亦或是競爭呢？金融科技業者，有機會透過 MyData 平臺存取民眾的資料嗎，如果金融科技業者想進入 MyData 平臺，能採取的途徑是？

開放銀行（open banking）與 MyData 平臺雖然都是屬於個人資料自主應用的一種模式，但兩者的資料提供者（DP）不同，因此我們將開放銀行（open banking）與 MyData 平臺視為兩種不同的管道，並沒有所謂整合或競爭的問題。

在國發會 MyData 介接要點[171]中有提到，介接機構以金管會所轄管的業者與金融單位為對象[172]，金融科技業者並不是我們的轄管對象，所以沒有辦法透過我們的管道去介接 MyData 平臺，老實說，國發會是可以去修改介接要點的，但他們也會擔心業者在處理個人資料保護的嚴謹度，業者是金管會的納管對象，

[171] 個人化資料自主運用平臺介接作業要點。
[172] 專營電子支付業者也包含在內（街口支付、悠遊卡等等）。

金管會才可以協助稽查，以確保資安安全，且在資安保護上目前金融科技業者與銀行相比還是有一定的差距。

(二) 法規面 /知情同意

1、 請問貴會針對所轄管之金融機構及周邊單位，申請成為 MyData 平臺的服務提供者，是否已經制訂了「審查作業要點」之類的規範，據以對其申請進行審查？若還在制定中，請問預計完成的期程是？

目前並沒有相關的「審查作業要點」，國發會負責審核服務內容，金管會負責審核服務目的，如果制定「審查作業要點」，會有准駁的問題發生，後續會產生行政救濟或訴願的問題，使得事情複雜化，基本上，我們非常支持金融機構應用 MyData 平臺，所以只要是我們納管對象，均有一定的資安防護程度，應用 MyData 僅有客戶資料取得管道之差異，於既有已經本會核准的金融業務範圍內提出申請，原則上我們都同意，我們只檢查該機構所要的資料集與他的服務是否適切。

(1) 貴會會針對金融機構的項目去做審查，但目前還是有申辦相同服務，但各家銀行索取資料不一的情況，貴單位審查的標準是？

制定標準可以讓事情簡單化，但各家銀行在做 KYC（Know Your Customer）時因應業務或客戶類型之差異所需資料不盡相同，為保留銀行自主的權力及避免限制銀行的發展，我們還是決定尊重銀行，由銀行自行判定需要客戶哪些資料，只要能提出合理的說明即可。

(2) 民眾透過 MyData 平臺申請信用卡服務，資料直接對接財政部財政資訊中心，財資中心不會經過過濾，就會將所有資料傳到 MyData 平臺，在「資料提供最小化」的原則下，應該如何去改善？

為降低資料提供者（DP）處理資料的難度，國發會目前的作法是資料集分類，將一項資料再細分為許多不同的資料集，雖然不一定有符合「資料提供最小化」的原則，但至少能確保資料提供者（DP）提供的資料，與民眾紙本申請所需要的資料是一致的。

另外，我們權衡（trade-off）的是，針對某幾項金融業務的定型化契約，裡面本來就清楚撰寫民眾須提供的資料，若需要其他文件，業者需要在服務流程或告知事項裡告知為何需要此文件，給予業者彈性外，也讓民眾了解文件的用處。

當然，我們也期許國發會未來能發展成以「欄位」為主體的設

計，讓銀行勾選真正需要的資料集，以落實「資料提供最小化」。

2、 請問您，MyData 平臺在知情同意流程與呈現方式該如何精進以達成民眾資料自主管理的目標？

不論是何種服務，MyData 平臺在知情同意流程與呈現方式不會大幅度去影響到民眾是否看條款的決定，因為條款大多是專業法律學者所撰寫，用詞艱澀、繁瑣，大多民眾都會直接略過，現在的知情同意大多是為了符合「程序正義」的基本要求而已。目前遇到的問題是，民眾在申辦銀行相關業務時，需要多次跳轉畫面，因而產生斷點，使服務變得不流暢，銀行也提出希望可以在銀行端做驗證即可，這部分還需要跟國發會商議以逐步進行精進。

(1) 因為目前國發會還是保守的使用下載的 API，並非 API 與 API 對接，民眾資料暫存在 MyData 平臺後，待通知後銀行端才能去下載，是否會造成知情同意流程的一個斷點？另外，團隊所知的另一個斷點是，從國發會角度出發，他們不願意去規範服務提供者（SP）的操作介面，國發會認為這是事業主管機關所負責，是不是需要兩方一起做協調，將 UI 統一？

目前國發會 MyData 平臺的模式有 3 種，我們認為，國發會也應該考量相關軌跡制度提供 API 與 API 對接，但若以第三方角度去思考，MyData 的角色是否會因為流程簡化而消失，我們應站在推廣 MyData 平臺的角度，也避免民眾誤解銀行可以隨意存取資料，讓民眾了解所有的資料都是經過民眾自主管理、授權的。如何權衡 MyData 角色與流程順暢，或許是下一階段要來探討的問題。

(2) 請問貴單位對銀行資料再利用的看法是？

從兩個層面來看這件事情，首先，從行政流程面，不論民眾是使用 MyData 平臺或臨櫃辦理業務，對銀行來說他們都是資料接收端，銀行內部運用，都是同樣的處理流程，在民眾申請成功成為客戶後，銀行自然而然就把他們當成自己的客戶，後續資料也會留底在銀行，成為之後申請其他業務的相關文件。不過，若從法制面來看，我們必須重新檢視各銀行知情同意書內容，包含再利用應單獨標示、延伸應用的層面廣度、內容是否有逾越當初規劃。

(三) 風險效益面

1、 請問您，貴單位推動 MyData 平臺於線上申辦是否評估過個資保護或資料傳遞時的資安風險？

是，金融機構上線前都需要經過金管會審核，我們會檢查該機構索要的資料集與他的服務是否適切、是否有符合資安保護相關規範等等。

2、 請問您，貴單位推動 MyData 平臺於線上申辦是否有效加快行政效率或民眾（使用者）滿意度？

以我們的調查數字來說，是有大幅度加快行政效率的，以臺灣銀行為例，信用卡核卡成功率從 38.7%增加至 53.6%，人員核實文件時間由 2-15 天降低至 2 天，其他銀行也有反應，取得資料從原本的 1 天降低至半小時。

(四) 推廣應用面

1、 根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，貴會所轄管之金融機構及周邊單位，除服務提供者外，也可申請成為 MyData 平臺的資料提供者。故想請教貴會對於所轄管之金融機構及周邊單位，申請成為資料提供者的看法。

以金管會的角度來說供給與需求是相互對應的，我們也鼓勵金融機構證券單位成為資料提供者（DP），像臺灣集中保管結算所（TDCC）本身就有保管相關證券資料，中華民國人壽保險商業同業公會也有民眾的投保資料，近期也在推動保單存摺，慢慢的，或許這兩個單位也可以成為資料提供者（DP）。

2、 請問您認為 MyData 平臺開發上的服務缺口為何？（如資訊素養、人員抗拒）

問題可以分為三大面向，第一，推廣面，推廣力度可以再加強，讓更多機構加入 MyData 平臺，也讓更多民眾認識 MyData 平臺；第二，人權面，若未來大量地透過 MyData 平臺拿取民眾資料，可能會有人權團體的反抗聲浪；第三，MyData 平臺驗證方式，現在手機上的應用服務越來越多，雖然內政部有推出 TW FidO，但普及率不高，應多做努力。

3、 請問您，MyData 平臺未來規劃增加哪些資料集或服務？

就金融機構來說，我們目前積極在推的是法人資料的提供，以往是針對個別消費者，未來希望服務對象也可以拓展到法人，讓法人也可以線上開戶、貸款。

六、 中國信託商業銀行訪談摘要

- 形式：中國信託商業銀行提供文字稿回覆
- 摘要：

(一) 策略面

1、 請問您，貴單位推動 MyData 平臺的策略與目標為何？（組織內、外或第三方）

分為兩部份：(1)運用 MyData 提升數位化申辦效率，與提高授信業務核準率。(2)發展金融創新應用。現行 MyData 匯集了 12 大類的資料，且持續擴增資料集，有機會結合銀行資料發展出新的客戶服務模式。

2、 根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，銀行除擔任 MyData 平臺服務提供者外，也可申請成為平臺的資料提供者。基於資料雙向共享互惠的原則，想請教貴行對成為 MyData 平臺資料提供者的看法？

(1) 銀行成為資料提供者屬於 open banking 範疇，然國內現行開放銀行發展屬於「市場驅動模式」，而非「法規驅動模式」，也就是說不強制銀行開放資料，而是由銀行與銀行/TSP 業者依業務場景需求來決定是否開放資料、開放什麼資料。

(2) 目前中國信託在開放銀行一、二階段皆有投入資源參與。

以上為與「財金開放應用程式介面管理平臺」合作中，尚無規劃運用在國發會 MyData 平臺。

(二) 法規面/知情同意

1、 根據國發會「個人化資料自主運用（MyData）平臺介接作業要點」，貴行擔任服務提供者，如何確保介接 MyData 平臺提供當事人個人資料時，能確保個人化資料之蒐集以最小化原則？其次在當事人同意提供其下載之個人化資料前，以何種機制確保當事人對服務條款知情瞭解？

銀行在提供客戶 MyData 服務時，皆有經主管機關同意申請，且於業務流程中清楚揭示相關條款，客戶同意後才能運用(如**圖 64** 所示)

圖 64：中國信託線上申請頁面

資料來源：中國信託商業銀行。

2、 根據國發會「個人化資料自主運用（MyData）平臺服務條款暨隱私權保護政策」中規範:「若您為未滿二十歲之未成年人，...當您使用本平臺時，即推定您的父母或監護人已閱讀、瞭解並同意接受本條款之所有內容」。貴行目前是否將未成年線上開戶（數位存款帳戶）的服務與數位化個人資料自主運用平臺服務機關連結？倘若欲準備連結，如何確保線上申請並非未成年人自行操作？

本行未成年數存業務尚未規劃與 MyData 進行串接

(三) 風險效益面

1、 請問您，貴單位推動 MyData 平臺於線上申辦是否評估過個資保護或資料傳遞時的資安風險？

個資保護一直是本行高度重視且嚴格把關的重點，除配合主管機關提出的「介接機關(構)資訊安全與個資保護查核表」相關規範外，本行也主動申請使用雙向憑證(Mutual SSL)連線機制來加強安全性。

2、 請問您，貴單位推動 MyData 平臺於線上申辦的是否有效加快行政效率或民眾（使用者）滿意度？

本行目前運用 MyData 的業務為「新戶信用卡申辦」，取得民眾 MyData 資料後有助於提升徵審效率。惟因目前使用自然人憑證插卡機制，以及流程中民眾需在本行網銀及國發會網站兩者間進行跳轉，流程體驗仍期待優化。(未實際做過使用者滿意度調查)

(四) 推廣應用面

1、 請問您認為 MyData 平臺開發上的服務缺口為何？（如資訊素養、人員抗拒）

目前 MyData 後臺有客服機制可以線上提問，服務 SLA 實際感受約一天內可獲得回覆，尚可接受。惟因服務介接與系統測試需求，並無法配合夜間對測，高度影響業務串接上線的效率和時程。(銀行業務因避免日間影響民眾，系統過版多利用夜間進行封版測試，但現行 MyData 團隊並無法配合非上班時間測是，若有任何問題只能先單方面將 log 紀錄先存檔，隔日再於後臺提出問題。)

2、 貴行是參與國發會 MyData 平臺、擔任服務提供者的銀行業者之一。想請問貴行就 MyData 平臺未來的發展提出一些建議。

(1) 現在強調一站式服務體驗，目前與 MyData 串接流程民眾需跳轉網頁，一來有體驗被切割、二來銀行大多有 session timeout 機制，建議可評估跳轉國發會網站的動作改以 SDK 提供銀行嵌入服務流程中，並搭配文字說明來進行，以確保民眾知道該個人化資料自主化運用是由 MyData 提供服務，並可兼顧服務體驗。

(2) 目前 MyData 規範資料僅能一次性取用，下次再取用則需重新再來，建議可研議客戶同意於有效期間內可授權 service provider 取得資料，同 open banking 對 TSP 業者的授權方式，以提升資料運用價值。

附錄四、專家座談會會議摘要

- 時間：110 年 11 月 8 日（星期一） 上午 10 時
- 形式：線上會議（Google Meet）

一、議題一：請您就所知（或業務主管之經驗），分享國內外對知情同意授權機制的優化方式與挑戰（如資訊安全、資料保護、資料傳輸等）

(一) 根據歐盟 GDPR 的規範，經過當事人的同意可「隨時」撤回，未來我國在優化知情同意授權機制時，須考慮到此點，並確認資料控管者（data controller）是否有系統能停止處理或利用當事人該筆資料。在實務上，不論是當事人（data subject）或者企業都會希望知情同意書能夠一目瞭然，但礙於法規，無法同時兼具，研究團隊提出視覺化與階層化的表現方式應是恰當的。國外有類似作法，將蒐集目的及法規重點放在首頁，其他細節（GDPR 要求告知事項）整理成文件放置於第二頁。

(二) 告知（inform）與同意（consent）的最大公因數為「國民的共通素養（common context）」，在長期的推動上應讓國民更深入理解資訊安全及資料保護。

(三) 在資料保護上常見的問題是鑰匙（key）的保護並不完善，包含加密、解密鑰匙由誰持有、哪些人可以解密等等，這都是必須揭露的重要議題。

(四) 不建議在授權應用時使用同意，由於其規定繁瑣且可以隨時被撤回、更動，同意應作為最後的選擇。在討論個資法中的「特定目的外之利用」時，我們常常忽略兼容性（compatible），當新的目的與原始蒐集目的是具兼容性時，就不需要再另外進行同意。在 GDPR 立法理由（Recital）中有規定，若為實現公共利益、科學或歷史研究目的或統計目的之處理，可不被視為不符合原始目的。主管機關（國發會）應盤點服務項目中，有哪些是真正需要同意。

值得思考的是，我國目前並沒有資料可攜權，未來是否要提供請求權給當事人（民眾）。

(五) 資料層級的區分是一個困難的處理方式，需要獲得法制上的允許，法制上已規定最低保護限度，界線如何拿捏成為重點。舉例來說，由於 MyData 平臺是第一層次，MyData 平臺蒐集的資料將來使用的向度大且較為繁複，因此告知上的範圍及做決定的程度會比較高。「當事人可隨時撤回同意」尚待討論的是：個體資料很容易抽取，但若是已將資料納入去識別化的巨量資料分析，該如何停止處理或利用該筆去識別化資料。

二、議題二：請您就本計畫目前執行成果，提供對個人化資料自主運用平臺（MyData）資料釋出或知情同意授權機制的優化建議，以及未來平臺精進方式的建議。

(一) 認同團隊 icon 的設計，但針對個資法第 16 條「特定目的外之利用」需要另經當事人同意這點，需要再去思考如何符合法規規定。

(二) 政府應給予民眾一部份選擇的權力，像是近用權（right of access control），由民眾自己選擇是否要更深入了解知情同意內容，讓不同取向的民眾各自擁有適合的知情同意機制。未來或許可以朝定型化契約發展，在社會中已形成共識的共通素養，就不須額外的說明，以節省篇幅。

(三) MyData 平臺資料授權需考量資料最小化蒐集。我們很難用簡單的概念讓民眾了解個資保護，我認為這是民眾與政府間的信任問題，跳脫法律，站在民眾的角度去思考，如何讓他們相信 MyData 平臺資料釋出及轉移是安全的，也許會有不一樣的收穫。

(四) 同意應注意兩個部分，第一，需要有效率的退出，充分保留增刪修改空間；第二，層級化法律保留，個資法為個資保護的基本法，目前我國在個別領域的法規並不完整，我們應該去思考後續處理

以及一般資料是否也需要如同敏感資料這樣相對嚴謹的告知與同意。

(五) 我認為 MyData 平臺最關鍵的地方就在於平臺授權給第三方，包含直接蒐集方或間接蒐集方都會需要同意授權，但目前報告似乎沒有細分兩者。 建議報告可以在論述上將政府端與企業端做更細節的區分。

目前 MyData 平臺已設立會員專區，內含完整使用、下載紀錄，若未來能將資安保護（如平臺為單次授權、不保存資料等等）敘明，並將其優化成民眾使用資料的儀表板，我相信能夠大幅提升民眾對於平臺的信心。根據個人化資料自主運用平臺介接作業要點第七點「服務提供者就當事人資料之蒐集、處理及利用之流程，應每年辦理內部查核工作 」，但各機關落實資訊安全的程度不一，建議國發會應實際參與查核工作，偕同其他主管機關透過增加實務經驗、適度演練以提升民眾對於平臺的信心。為提升民眾對 MyData 平臺的好感度，平臺在未來應精選服務，盤點使用率前 20%的服務項目加強推廣以提升民眾使用平臺的動機。

(六) 若 MyData 平臺作一整合平臺，為便於民眾取得其個資，於個資法第 15 條範圍內，限於資料當事人向政府機關請求將其存於資料庫（database）中之個資提供給資料當事人僅需盡法定告知義務，無需同意，即各政府機關得委託國發會 MyData 平臺進行資料當事人的資料處理或利用，作為第一階層的同意，降低須多次取得同意之不便；至於平臺對接銀行和國營企業則或回溯個資法第 7 條第 2 項（此部分或需自源頭界定為何種同意），僅需提及特定目的外之同意為何，再取得一單獨同意，換言之，此設計可縮減目前 MyData 平臺隱私權政策篇幅。

(七) 法律為最低標，民眾對平臺的信心才是最重要的，應透過清楚揭

露資安保護措施，以提升民眾信任感。基於安全的設計（security by design），資訊安全應該在系統形成中就被考量進去，而不是用外加的。