行政院所屬各機關因公出國報告書

(出國類別：開會)

出席第 46 屆全球隱私大會
(Global Privacy Assembly, GPA)
出國報告

出國人員服務機關	職　稱	姓　名
個人資料保護委員會籌備處	視　察	陳樂庭
個人資料保護委員會籌備處	視　察	方冠棻
個人資料保護委員會籌備處	視　察	吳建忠
個人資料保護委員會籌備處	設計師	陳坤宏

會議國家：英屬澤西島

出國期間：民國 113 年 10 月 26 日至 113 年 11 月 1 日

報告日期：民國 114 年 1 月

出席第 46 屆全球隱私大會(Global Privacy Assembly, GPA)

目錄

壹、背景說明及會議摘要

本屆全球隱私大會(Global Privacy Assembly, GPA)係全球隱私及資料保護的旗艦論壇，目前共有來自英國、美國、加拿大、日本、歐盟、香港、紐西蘭、澳洲、阿根廷、比利時、巴西、智利、法國、德國、澤西、墨西哥、南韓等 99 國，共 147 個超國家級(supranational authorities)、國家級(national authorities)、次國家級(sub-national authorities)個人資料保護機構之正式會員[1]，及包含世界銀行(World Bank)、歐洲委員會(European Commission)、歐洲理事會(Council of Europe)、白宮科學及技術辦公室(White House Office of Science and Technology Policy (2023))等國際組織及非國際組織共 39 個觀察員。

第 46 屆 GPA 會議業於 2023 年 10 月 28 日至 11 月 1 日於英屬澤西島辦理，首三日為開放議程，由主辦方邀請來自產官學研等各界的隱私及個人資料保護專家，針對特定主題分享實務經驗及觀點；末二日則為正式會員及觀察員限定之閉門會議，主要就大會事務進行討論，並有正式文件之產出。另，除主辦會方 JOIC 辦理之五日正式活動外，會場亦開放會員、觀察員等聚焦特定議題辦理公開及非公開之場邊活動。

本屆會議由澤西資訊專員辦公室(Jersey Office of the Information Commissioner, JOIC)主辦，會議分為商務及公眾、學研機構及非政府組織、個人資料專責機關等三種會籍，我國因尚非屬 GPA 正式會員及觀察員，故本籌備處係以商務及公眾身分與會。

第 46 屆 GPA 會議主題為「資訊的力量」(the power of i)，聚焦「個人」(individuals)、「創新」(innovation)、「資訊」(information)、「誠信」(integrity)、「獨立」(independence)、「國際化」(international)、「跨文化」(intercultural)、「原住民」(Indigenous)等八大議題，而此八項議題也分別於首三日開放活動中分場次討論。

[1] GPA 正式會員名單，詳參官網：https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/

澤西隱私專員辦公室(Jersey Information Commissioner, JOIC)資料專員 Paul Vane 開場【註：Vane 為 JOIC 最高主管】

第 46 屆全球隱私大會「資訊的力量」(the power of i)會議主題形象

貳、會議日程表

日期	時間	行程
10/28 (一)	16:00	**國際資料保護認證：包容及相互操作** **International1 Data Protection Certification: Coverage and Interoperability**
10/29 (二)	08:55 ｜ 09:10	**開場致歡迎詞** -澤西資訊專員辦公室(Jersey Information Commissioner, JOIC) 資料專員 Paul Vane【註：JOIC 最高主管。】
	場次一：創新 **Session 1: Innovation**	
	09:10 ｜ 09:30	**主題演講** **Keynote Presentation** -講題：隱私法規的未來：個資專責機關如何適應未來的 30 年？我們準備好規範 AI 了嗎？ The future of Privacy Regulation: How will Data Protection Authorities need to adapt over the next 30 years? Are we equipped to regulate AI?
	09:30 ｜ 10:15	**爐邊談話** **Fireside Chat** -本次會議將探討 AI 的影響，並回答以下問題：「我們如何改變思維方式以應對進階分析？倫理於調整這種思維方式中起到什麼作用？我們的基本人權將如何受到影響？AI 對於資料保護是相輔相成或是衝突？我們是否有一個在新興世界中作為分析監管者的願景？」 This session will look at the impact of AI and address questions such as, “How do we change our mindset to deal with advanced analytics? What part do ethics play in adjusting that mindset? How will our fundamental human rights be affected? Does AI compliment Data Protection or is it in conflict? Do we have a vision of how to be regulators of analytics in an emerging world?"
	場次二：個人 **Session 2: Individual**	
	10:45	**主題演講**

日期	時間	行程
	| 11:05	**Keynote Presentation** -講題：誰在乎個人？如何透過提升個體以提升全人類。 "Who Cares About One Person? How Elevating the Individual Elevates all Humanity.'
	11:05 | 12:00	**小組討論** **Panel Discussion** -聽取下一代聲音的重要性不可低估。在本次會議中，我們將聽取來自澤西青年大會的青年意見。他們將討論「隱私辯論：下一代的看法—定義隱私危害：對網路霸凌、人臉辨識以及隱私對未來世代的意義之觀點。」 The importance of hearing the voices of our next generation cannot be underestimated. In this session we will hear from a group of young people who form part of Jersey's Youth Assembly. They will be discussing "The Privacy Debate: What the Next Generation Think - Defining Privacy Harms: Perspectives on cyber bullying, facial recognition and what privacy means for future generations." ■第 1 組： 資料保護與心理健康—我們如何保護社會中最脆弱的群體？在健康資料共用中，個人與社會的關係為何? Data Protection and Mental Health - How do we protect society's most vulnerable? The role of the individual vs. the role of society in health data sharing. ■第 2 組： 在現代世界中定義隱私危害 "Defining Privacy Harms in a Modern World". Following on from this morning's youth panel, this session will attempt to understand the concept of 'harm' in a digital age.
	場次三：獨立 **Session 3: Independence**	
	12:00 | 12:20	**主題演講** **Keynote Presentation** -議題：技術將如何影響監管機構：我們作為數位監管者的未來會是什麼樣子？ "How Technology Will Impact the Regulator: What does our future as digital regulators look like?"

日期	時間	行程
	12:20 | 13:00	**小組討論** **Panel Discussion** -議題：監管關聯性—監管機構如何應對重疊政策領域的挑戰？我們如何應對商業組織利用一個監管機構對抗另一個監管機構的反擊？監管是否過度，是否兼容？ With regulation increasing in different spheres, this session will look at "Regulatory Cousins - How do regulators tackle the challenge of overlapping policy domains? How do we handle the push-backs from commercial organisations who play one regulator against another? Is there too much regulation, and is it compatible?
	場次四：國際化 **Session 4: International**	
	14:00 | 14:45	**小組討論** **Panel Discussion** -「資料傳輸工具的優勢和挑戰」。有大量的資料傳輸機制可供選擇，本小組將探討這些工具的優勢和挑戰。 "The Advantages and Challenges of Data Transfer Tools". With a plethora of data transfer mechanisms to choose from, this panel will explore the advantages and challenges of those tools."
	14:45 | 15:30	**小組討論** **Panel Discussion** -議題：「金融服務背景下的國際資料傳輸—發展趨勢如何？資料傳輸機制的未來為何？」 -Jersey 是全球知名的國際金融中心。國際資料傳輸的規則有對企業造成高昂成本及繁重負擔之虞，大多數金融服務業者盼有更簡單的解決方案以拓展業務。 Jersey is a world-renowned international finance centre. The rules around international transfers of data can prove costly and burdensome to industry, with most financial services businesses wanting much simpler enablers to do business. This panel will examine "International Transfers in the context of Financial Services - What is the direction of travel? What does the future look like for data transfer mechanisms?"
	場次五：跨文化及原住民 **Session 5: Intercultural & Indigenous**	
	16:00	**主題演講**

日期	時間	行程
	| 16:20	**Keynote Presentation** -議題：「保障永續性：資料隱私於環境倡議及人道主義危機中的作用。」 Safeguarding Sustainability: The Role of Data Privacy in Environmental Initiatives and Humanitarian Crises."
	16:20 | 17:15	**小組討論** **Panel Discussion** -西方世界似乎在發展以 GDPR 為模型的資料保護法律，但這一標準不一定適用於全球。 -探討「原住民社群如何制定自己的資料保護框架？」並從跨文化及原住民視角評估可能存在的潛在危害。 Whilst the Western world appears to be developing data protection laws on the General Data Protection Regulation model, this is not a model that necessarily works globally. This panel will explore "How do Indigenous Communities Develop their own Data Protection Frameworks?" and will assess the potential harms from an intercultural and indigenous perspective.
	17:15	**10/29 活動總結** -由司儀 Richard Purcell 總結。
10/30 (三)	08:30 | 08:40	**10/29 活動總結** -由司儀 Richard Purcell 總結。
	場次六：個體 **Session 6: Individual**	
	08:40 | 09:00	**主題演講** **Keynote Presentation** -主題：「減少隱私權的不平等：探討多樣性中的不同隱私面向。」 "Reducing Inequalities in Privacy Rights: Exploring the different privacy dimensions of diversity."
	09:00 | 09:45	**小組討論** **Panel Discussion** -議題：「從基礎開始的教育：隱私教育對社會的影響。」 Education from the ground up: The societal impact of privacy

日期	時間	行程
		education.
	09:45 | 10:30	**小組討論** **Panel Discussion** -我們如何保護最脆弱的公民？本節將討論「隱私無障礙：在數位化世界中保護障礙者、弱勢群體及社會邊緣人士。」 How do we protect our most vulnerable citizens? This panel will talk about "Accessible Privacy: Protecting the disabled, vulnerable and socially marginalised in a digitised world."
	場次七：誠信 **Session 7: Integrity**	
	11:00 | 11:45	**小組討論** **Panel Discussion** -議題：透過資料信託建立信任 -2023 年，澤西島成為第一個建立合法資料信託(即 LifeCycle)的司法管轄區。瞭解這一進程的詳細情況、所學到的經驗教訓，以及全球範圍內資料管理的現狀。 "Creating trust through Data Trusts". In 2023, Jersey was the first jurisdiction to establish a legally constituted data trust, LifeCycle. Hear all about how it happened and the lessons learned, as well as what is happening in the wider world for data stewardship.
	11:45 | 12:30	**小組討論** **Panel Discussion** -議題：物聯網的全球最佳實踐 -共同制定全球最佳實踐的清晰願景，以在物聯網中建立信任和安全，考慮到網路威脅，瞭解物聯網的部署現狀、全球政策和監管發展，及 AI 於管理物聯網生態系統中的角色。 "Global best practice for the Internet of Things". Join us to help develop a clear vision on Global Best Practice for building trust and security into the IoT, taking cyber threats into account, where we are in IoT deployment, policy and regulatory developments around the world, and the role of AI in governing IoT ecosystems.
	場次八：資訊 **Session 8: Information**	

日期	時間	行程
	12:30 | 13:00	**辯論** **Podium Debate** -議題：「資料最小化：真正的指導原則，還是過時的遺物？」 Another chance to make an informed decision on a long-standing issue: "Data Minimisation: A true guidance point, or a relic?" ■第 1 組：政府及第三方間的資料共享 Data sharing between Government and Third Sector. ■第 2 組：監管科技的優點與缺點—只是隱私洗牌嗎？ The Benefits & Drawbacks of RegTech - Are they just privacy washing?
	13:00 | 13:25	**爐邊談話** **Fireside Chat** -作為戰後倫敦最可怕的恐怖主義暴行的倖存者，Martine 的故事是一個純粹的靈感故事。但是，那改變人生的一天的創傷對她的隱私有什麼影響呢？Martine 將談論她如何成為媒體關注的焦點、媒體的侵擾、她的殘疾對獲得基本服務的影響，以及她如何利用媒體的力量向世界講述她的故事.....按照她的方式。 As a survivor of the most horrific terrorist atrocity to hit London in the post-war era, Martine's story is one of pure inspiration. But how did the trauma of that life-changing day affect her in terms of her privacy? Martine will talk about how she was thrust into the media spotlight, press intrusion, the impact of her disability in terms of access to basic services and how she harnessed the power of the media to tell her story to the world…on her terms.
	13:25 | 13:30	**閉幕結語** -JOIC 資料專員 Paul Vane
	14:00	**OECD 關於政府近用個人資料以促進資料安全流動宣言的相關性** **The Relevance of the OECD Declaration on Government Access to Personal Data for Safe Data Flows**
	14:30	**Meta 會外活動：小組討論 – 攜手促進 AI 治理成功** **Meta Side Event: Panel discussion – Working together for success in AI Governance**

日期	時間	行程
	14:30	隱私的未來論壇：人工智慧和資料保護的基本問題 - 模型中的個人資訊和處理的法律依據 **Future of Privacy Forum: Essential Questions for AI and Data Protection - Personal Information in Models and Legal Basis for Processing**
	15:30	英國 ICO 會外活動 – 保護兒童免受網路傷害 **UK ICO Side Event – Protecting Children from Online Harms**

參、會議情形

一、各場次重點

場次一：創新(Innovation)

■ **主題演講：隱私法規的未來—個資專責機關如何適應未來的 30 年？準備好規範 AI 了嗎？**

(一) 本節由自由講者 Nikolas Badminton 分享觀點，Badminton 講員係一全球未來主義演講者及首席未來學家，已輔導 NASA、Disney、Google、Microsoft、Intel、IBM、VISA、美國國務院、英國內政部及聯合國等多個國際企業高階主管及政府官員從上而下探索理想未來，預測不可預見的風險並加強策略規劃。

(二) 探索未來的前瞻四步驟：Badminton 提出未來探索四步驟包括：首先，掃描信號以識別變化的跡象，如新型線上行為和技術創新；其次，觀察這些信號所匯聚的趨勢，分析其對世界的影響；接著，提出合適的問題並建立情境，假設未來 20 年內系統、地方和組織的發展可能帶來的影響；最後，透過敘事創建未來的故事，使人們能更真實地體驗和理解未來。

(三) 探索未來的四個關鍵考量：Badminton 指出探索未來的過程需考慮四個重要因素：首先，質疑自身的歷史和觀點，以當前的情境尋找未來的跡象，並通過科技未來學家 Douglas Engelbart 的故事及其他例子進行說明；其次，鼓勵大膽創新並促進合作，因為集體智慧往往能產生更佳的結果；第三，將思維從「當下是什麼」轉向「如果會如何」，這種無限延伸的問題能激發好奇心並引發深入討論；最後，這些探討將有助於更全面地想像未來。

■**爐邊談話：如何改變思維方式以應對進階分析？倫理於調整這種思維方式中起到什麼作用？基本人權將如何受到影響？AI 對於資料保護是相輔相成或是衝突？是否有一個在新興世界中作為分析監管者的願景？**

(一)澤西島資料保護局候任主席 Elizabeth Denham

負責任的 AI 發展所面臨的挑戰與機遇：當前環境充滿變革，包括地緣政治動盪與數字經濟新技術的推動，先進分析和強大 AI 技術的快速發展構成嚴峻挑戰。隨著新法律的實施及跨監管緊張局勢的加劇，資料保護與隱私專業人士（Data Protection and Privacy Professionals）面臨在資源有限情況下實現更多工作的壓力。同時，政府與產業迫切要求採用 AI 解決方案以保持競爭力。然而，全球在負責任 AI 發展中的進展不一，主要受文化背景及資料保護與隱私立法成熟度影響。這些基礎要素對於構建負責任 AI 至關重要。未來應關注因地制宜地應對各地在 AI 發展中的獨特挑戰與差異。

(二)非洲數位權利中心 LBG (Africa Digital Rights' Hub LBG) 創始人兼執行董事 Teki Akuetteh

1. AI 環境下非洲個資保護的挑戰：Akuetteh 認為非洲約有 36 個國家已制定資料保護法律，其中約 20 個設有資料保護監管機構。然而，這些機構因財務與人力資源不足，導致法律執行面臨困難。此外，非洲國家在新興科技出現時快速採用，尤其在 AI 領域，使監管機構在法律應對上面臨巨大挑戰。為應對新技術引發的複雜問題，建立資源充足且具前瞻性的監管機構至關重要，推動對其資源支持已成當務之急。

2. AI 時代資料保護監管的挑戰與應對：為應對 AI 帶來的資料保護監管挑戰，採取開放且務實的方式至關重要。務實體現在監管者需要更多參與和開放態度。以加納資料保護委員會的設立經驗為例，來自法律背景的監管者通常對工程師和軟件開發者的技術構建缺乏理解，這使得有效監管

成為挑戰。為此，傾聽技術專家意見並深入了解其工作至關重要。

3. 負責任 AI 實施的關鍵推動力量：企業與產業在推動負責任 AI 的實施中扮演重要角色，負責確保技術應用的倫理與社會影響。然而，政策制定者則是確定負責任 AI 框架的核心，確定標準並引領方向。隨著 AI 技術的快速發展，監管機構逐漸介入 AI 生態系統，以監督與評估技術實施，確保其符合負責任 AI 的基本原則。

(三)電腦與通訊業協會高級政策經理[2]Boniface de Champris

1. 歐盟 AI 技術發展面臨的挑戰與應對策略：Mario Draghi[3]在近期的歐盟競爭力報告中指出，隨著 AI 革命的興起，歐洲必須擺脫依賴上世紀中期技術與工業的現狀，不僅在 AI 創新上取得突破，還需有效整合 AI 至傳統產業，充分發揮其潛力。然而，複雜且不一致的監管環境使企業在開發、創新及應用 AI 時面臨諸多困難。目前，歐洲在 AI 法律框架中涉及隱私、競爭、版權及消費者保護等多方面規範，特別是在資料處理與內容審查領域，法規適用性缺乏協調一致性。GDPR 是企業遵循的核心法律之一，但法律不確定性對 AI 系統開發與訓練構成重大挑戰。例如，關於 AI 訓練所需的資料處理法律基礎，歐盟資料保護委員會已被要求提供更明確的指導意見。法律明確性對 AI 生態系統的影響至關重要，直接關係到技術的整合、產業的創新能力及其經濟和社會效應。為此，需要理性、務實且靈活的法律解釋，特別是在 GDPR 框架下，應結合風險基礎方法促進創新，實現風險與利益的平衡。歐盟未來應著重確保法律與監管規則的一致性與協同運作；強化資料保護機構（DPA）與行業之間的合作，制定民事性解釋與規範；在 AI 法案實施過程中，調整合法利益相關規定，解決與 GDPR

[2] Senior Policy Manager, Computer & Communications Industry Association

[3] 前歐洲央行總裁 Mario Draghi2024 年 9 月 9 日向歐盟執委會提交歐洲競爭力報告。

的潛在衝突。

2. 推動生成式 AI 監管的靈活性與教育改革：監管機構需採用更靈活且基於風險的方式，避免僵化解讀法規，如 GDPR，透過與行業的持續對話，結合相關技術輸入，實現合理監管。生成式 AI 的監管不僅需要技術企業的參與，也需政府、學術界與民間社會共同合作，確保多元化監管方法的落實。同時，應將重點放在教育改革上，以解決資料鴻溝挑戰，確保更公平地獲取 AI 技術。這將有助於塑造新 AI 時代的運作框架，推動技術的負責任使用與普及。

3. 企業在推動負責任 AI 中的核心角色：企業在建立安全且負責任的 AI 中具有關鍵地位，其動力來自對信任的需求，因為信任是業務運行的基石。企業在 AI 技術生態系統中的核心作用包括利用其知識與技術優勢，推動負責任 AI 的發展。此外，企業應與政策制定者及監管機構保持定期且持續的對話，以促進對技術的深入理解，並共同預測未來發展方向，確保 AI 的應用與規範相協調。

(四)巴西國家資料保護局（National Data Protection Authority of Brazil, ANPD）局長 Miriam Wimmer

1. AI 環境下巴西個資保護的挑戰：巴西資料保護法（LGPD）實施及其資料保護機構（ANPD）成立至今僅四年，目前國會正審議 AI 法案，該法案受到歐盟 AI 法案啟發，但更強調人權保護。討論議題包括 AI 訓練的法律基礎及資料處理者在使用 AI 技術與處理個人資料時的責任。然而，面對全球性 AI 企業的域外規則執行仍具挑戰性。雖然巴西大型企業普遍具備合規文化，但對規則的深度理解及其具體實施仍有困難。該法案提議授予 ANPD 作為 AI 主要監管機構的地位，賦予其解釋法規與監管 AI 相關事務的權限，以保障憲法所賦予的資料保護基本人權。

2. 資料保護與人工智慧監管的交集與挑戰：資料保護的核心概念，如透明性、公平性、反歧視、以個人為中心、保護

個人權益與經濟利益，與 AI 立法提案中所討論的治理機制存在高度一致性，包括風險評估和組織內部對個人權益尊重的保障措施。因此，資料保護機構與人工智慧監管機構所面臨的挑戰在某些層面上相似。然而，正如 Akuetteh 與談者所指出，監管機構需要更多資源支持，並亟需具備跨學科專業背景的團隊成員，包括計算機科學、法律與倫理等領域的專家，以應對新興的質量與數量並存的挑戰。這些挑戰超越了現有框架，需與更廣泛的利益相關者共同探索解決方案。儘管準備尚未充分，但已有跡象表明我們正朝著正確的方向邁進。

(五)Microsoft 副總法律顧問[4]Cari Benn

1. 微軟對全球 AI 監管的策略：Benn 表示，微軟的產品和服務覆蓋約十億用戶，業務遍及每大洲和近所有國家。為提供服務全球組織與政府，以解決每日約 6 億次網路攻擊，微軟部署 3 萬名安全工程師以抵禦威脅，展現其技術的全球應用與影響力。在全球監管與隱私保護方面，微軟遵循「隱私是一項基本人權」的核心原則，致力於確保全球用戶均享有透明的資料管理權利，包括查詢、刪除、獲取資料副本及控制其使用的選擇權。微軟的全球擴展除地理規模外，還涵蓋技術規模，特別於 AI 技術堆棧的發展。智慧技術(AI)堆棧中，「I」代表基礎設施，涵蓋三層架構：物理基礎設施、數字基礎設施及應用基礎設施。物理基礎設施層面，關注全球資料中心的能源供應與可持續性，以及支持大型生成型 AI 與語言模型的專用晶片開發；數字基礎設施層面，涵蓋由 OpenAI、Google 及微軟等企業開發的基礎模型，並通過 Azure 等平台支持全球開發者構建語言模型，目前已有約 20,000 個語言模型基於此服務開發；應用基礎設施層面，提供用戶日常交互的 AI 應用，如微軟的 Copilot，幫助用戶完成文檔轉換、對話模擬等任務，同時

[4] Associate General Counsel, Microsoft

鼓勵本地開發者構建符合需求的 AI 應用。微軟在所有層級均致力於保障隱私與資料安全，確保滿足法律合規要求並提供最佳使用體驗，構建值得信賴的全球基礎設施生態系統，為資料存儲與技術投資提供安全保障。

2. 隱私保護與 AI 法規的協調與目標：微軟致力於平衡隱私保護與 AI 法規，從上位階法理看，二者在核心原則上是一致的。其中，隱私保護的核心概念亦可在歐盟 AI 法案及其他相關法規中找到反映，主要包括以下三方面：
   - 透明性：明確展示資料處理與 AI 技術應用方式，確保做法清晰可見。
   - 公平性：保證 AI 技術開發與部署對使用者、公平資料使用與生成回應的過程具備公正性。
   - 資料管理：在資料生命週期內，從收集到刪除的全過程中保障安全性，並防止資料被目的外利用。

   這些原則皆屬於公平資訊實務的核心，並支持隱私與 AI 法規共同追求確保技術安全性與負責任的應用。

3. 以資料主體為核心的監管與規範實施：在監管和規範實施過程中，資料主體(即個人)將扮演最關鍵的角色。為確保新技術的發展真正造福於人類，需在各利益相關方之間達成共識，包括監管者、政策制定者、民間社會以及企業或產業。無論是技術的推廣、法律的制定，還是企業決策，都應以提升人類福祉為核心目標，確保所有行動均以實現資料主體的利益為導向。

「場次一：創新」活動進行實況

場次二：個人(Individual)

■主題演講：誰在乎個人？如何透過提升個人以提升全人類。

(一)本節由 Douglas Kruger 分享觀點，Douglas Kruger 為企鵝蘭登書屋(Penguin Random House)暢銷作家，現任澤西晚報與根西商業簡報(Jersey Evening Post and Guernsey Business Brief)專欄作家，專精於領導力與代際財富研究。憑藉其傑出的演講才能，榮獲專業演講者協會名人堂(Professional Speaker Association)殊榮。

(二)個人權利的概念可追溯至古希伯來文明，其「人為造物主形象」的思想，徹底改變了「個人為國家工具」的傳統觀點。此理念在 13 世紀透過英國普通法得到法律保障，確立了司法獨立原則。於 18 世紀，美國憲法更將個人權利提升為國家根本，建立起限制政府權力、保障個人自由的法治體系。

(三)Kruger 讚揚阿根廷等國家推動的政府改革，肯定其精簡官僚體制之決心，同時提醒各國防範政府權力無限擴張的風險。他引用奧威爾的觀點「以犧牲個人為代價永遠無法建立真正的烏托邦」，藉此強調保護個人權利及防止國家濫權之重要性。

■小組討論一：隱私辯論：下一代的看法—定義隱私危害：對網路霸凌、人臉辨識以及隱私對未來世代的意義之觀點

(一)本節由澤西資料保護局資深委員 Paul Breitbarth 與四位不同背景的青少年學生－埃及籍 Jana、澤西葡裔 Joana、法籍 Lillie 及澤西籍 Laura 對談，討論著重於數位原生世代對隱私保護、資料治理與科技使用之觀點，探討青少年對於隱私保護認知、社交媒體使用模式及相關教育政策之適切性。

(二)Paul Breitbarth 為歐盟資深資料保護專家，現任澤西資料保護局委員。曾任荷蘭資料保護局官員，參與 GDPR 早期規劃及跨國執法工作。他在 Article 29 工作組擔任邊境、旅行及執法組協調員，並擔任全球隱私大會(GPA)秘書。

(三)2023 年歐洲媒體使用調查及美國皮尤研究中心研究顯示，青少年數位依賴程度比例不斷創高。15 至 24 歲族群之社交媒體

使用情況顯著，日使用率達 80%，週使用率高達 94%，相較之下，55 歲以上群體的日使用率僅 25%，凸顯世代數位落差；在平台使用方面，YouTube 以 93%居首，而 TikTok、Snapchat 及 Instagram 的使用率則均介於 60 至 70%之間。特別值得關注的是，高達 46%的青少年「幾近全天在線」，另有 47%「每日多次上線」，反映出令人憂慮的網路依賴現象。此外，西方國家有高達 80%的嬰兒在兩歲前就已具有數位足跡，此驚人的資料凸顯了當代社會數位化的深度影響。

(四)青少年對數位隱私的認知與實踐呈現明顯落差。儘管理解個人資料在網路平台間的流動風險，並意識到大型科技公司（如 Meta）可能將使用者資料用於 AI 模型訓練，但面對冗長的隱私政策時，多選擇「快速略過」或「立即接受」。如 Lillie 所述：「下載新應用程式時會看到隱私政策，但因篇幅過長，往往直接點選同意。」Laura 則指出「強制停留機制」能提高使用者對條款的關注度。

(五)為平衡公開分享與隱私保護，受訪者普遍採用「分眾策略」管理社交媒體帳號，公開帳號用於展示藝術創作與日常生活，私密帳號則維持與親密圈層的互動，惟平台的資料蒐集機制與演算法運作引發普遍憂慮。Joana 指出「即便啟用私人帳號設定，Instagram 仍依據瀏覽紀錄推送內容。」Lillie 更因不滿 TikTok 演算法持續推薦不願接收的內容而停用該平台。

(六)社交媒體之碎片化資訊已成為認知負荷與心理健康的重要影響因素。Laura 反映她每日使用手機超過六小時，而睡前持續觀看短影片更導致睡眠品質下降。不過，針對此問題，Joana 則採取定期「數位解毒」策略，透過暫時停用特定帳號來檢視並調整自身使用習慣。

(七)網路霸凌之匿名性亦成為青少年的主要焦慮來源。Lillie 分享一個同儕遭遇案例，其同學在 TikTok 發布的角色扮演(Cosplay)影片遭受揶揄攻擊，霸凌者利用其與受害者間才理解之「圈內笑話(inside jokes)」，造成受害者心理壓力及傷害。Jana 指出「霸凌者藉由匿名帳號規避道德與法律約束。」此種匿名霸凌

現象促使部分青少年支持校園禁用手機政策，認為面對面互動更有助於建立健康的人際關係。

(八)在教育改革層面，受訪者一致指出現行隱私與網路安全課程的時效性問題。Laura 強調「現今的詐騙與隱私侵害模式比過去更加複雜，童年時期接受的網路安全教育已不符現況。」Lillie 建議定期並與時俱進更新網路安全宣導知識。針對平台演算法的不透明性，Joana 與 Jana 表達不滿，呼籲強化使用者對資料流向的掌控權。Jana 則反對以年齡作為限制社交媒體使用的單一標準，主張建立更具彈性的管理機制。

(九)校園手機管理政策引發不同觀點的討論，支持全面禁用者認為此舉可減少網路霸凌、提升學習專注力，並促進學生間的實體互動；反對者則主張數位工具對學習具有正面幫助，建議以制定「彈性使用準則」取代全面禁止政策。

(十)針對青少年數位生活的未來發展，建議從四個層面著手：

1. 深化數位公民教育：透過即時更新的案例教學強化隱私保護意識，並簡化平台政策說明。
2. 加強社群平台透明度：建立有效的演算法管控機制與資料流揭露制度。
3. 建立完善的校園網路霸凌防治措施：整合各方資源，協助青少年建立健康的數位使用習慣。
4. 施行差異化政策制定：避免一體適用的規範，考量青少年群體的多樣性，並重視其意見回饋，共同建構理想的數位環境。

■小組討論二：資料保護和心理健康—如何保護社會最弱勢群體？個人的角色與社會在健康資料共用中的角色

(一)AdvocateDVB 領導兼澤西島心理健康審查法庭主席 Davida Blackmore

1. Blackmore 為本會議的主持人，目前擔任澤西資料保護專員的外部法律顧問和澤西心理健康審查法庭的主席。心理健康審查法庭主要處理被強制拘留的心理健康患者的申訴。本次

會議的核心討論是如何平衡個人隱私權與健康資料分享的集體利益，以保護脆弱群體。隨著大量數位應用程式的出現，這些應用程式承諾為個人提供支持，但其真正好處和潛在危害仍有許多疑問。會議旨在探討資料分享帶來的挑戰以及如何平衡這些挑戰。

2. Blackmore 提到在監管討論中應該考慮到患者的聲音。許多患有嚴重疾病的個體，特別是那些面臨更為複雜情況的人，可能不願意參與或可能因為病情或其他原因而無法參與，因此在資料分享方面，個人的觀點可能與監管機構的觀點存在對齊或衝突的情況。

(二)聯邦貿易委員會 Alvaro Bedoya 委員

1. 分享 GoodRx 和 BetterHelp 案：首先 GoodRx 案件涉及藥房折扣卡的使用。用戶在網站上輸入需要的藥物資訊後，這些敏感健康資訊被指控洩露給第三方，用於廣告目的。其次，BetterHelp 案件涉及在線心理治療服務。用戶分享自己的身份資訊（如青少年、基督徒、LGBT 等）後，這些資訊被指控洩露給第三方，進行廣告資料處理。Bedoya 強調，這些案件顯示出廣告生態系統在處理高度敏感健康資料時，標準做法的合法性和道德問題。Bedoya 指出，當前的主要挑戰在於確保這些做法不僅因為是標準做法就被認為是合法的，需要提高人們對分享敏感資訊潛在風險的認識。FTC 在 2023 年針對這些案件採取了行動，並更新了健康資料洩露通知規則，要求在未經授權的披露情況下通知受影響的個人。雖然未必在應用程式領域看到這種特定行為的顯著增長，但在 2023 年上半年集中處理了這些問題。
2. 資料分享的法律和倫理問題：Bedoya 指出，從法律的角度來看，有多項可能適用的法律框架來處理在線心理健康資料的問題。首先，GDPR 的第五條，該條款涉及不公平和欺騙的權限。不公平主要指無法合理避免的重大損害，其利益未能超過所造成的損害；而欺騙則涉及重大遺漏或誤導性陳述。此外，還有健康洩露通知規則，這一規則進一步強化了對個

人健康資料的保護。Bedoya 對目前的法律框架感到樂觀，認為這些法律能夠有效解決大多數在線心理健康資料管理中的問題，並認為增加權限將有助於進一步改善資料保護的效果。

3. 資料於公益使用的觀點：在線上心理健康和相關技術的領域中，存在潛在的危害，需要審慎應對。儘管有人鼓勵促進有益的資料分享，但工作的重點應放在執行相關法律規範，以保障使用者的權益。許多技術在科學驗證尚未完成時，便基於潛在利益進行推廣。這種假設性應用可能導致風險被低估。例如，面部識別技術在 2016 年和 2017 年已被廣泛使用，但並未有科學研究證明面孔如指紋般獨一無二。相反，人類經驗表明，確實存在面孔高度相似的情況。這一問題也體現在某些心理健康應用程式和情緒分析技術上。歐盟對此保持謹慎態度，認為應在技術獲得充分的科學驗證後再假設其有效性與益處。
4. FTC 面臨的心理健康與能力挑戰： FTC 致力於提前處理心理健康和能力問題。推薦系統被指控對年輕人有負面影響，並延長使用時間，導致睡眠不足等問題。例如，遊戲《Fortnite》的默認隱私設置太低，導致成年人可以在線騷擾年輕玩家。FTC 提起訴訟並和解，要求提高隱私設置。FTC 面臨的另一個問題是能力。在技術公司中，有大量心理學家和腦科學家，而 FTC 卻一名心理學家或腦科學家都沒有。因此，FTC 正組建一個小型行為團隊，包含兒科醫生、心理學家和技術專家，以應對這些挑戰。

(三)歐洲資料保護監督員 Wojciech Wiewiorowski

1. EDPS 在應用程式時代的挑戰與前景：Wiewiorowski 探討資料保護機構在心理健康資料管理中的角色及其挑戰。雖然一般認為資料保護機構主要負責隱私保護，但在歐洲的情況下，這一觀點並不完全成立。許多案例超出了資料保護機構的活動範圍，尤其是歐洲資料保護監管機構（EDPS）主要監管歐盟機構，對於典型的心理健康資料接觸較少。Wiewiorowski

指出，當前大多數心理健康資訊並非來自傳統的醫療資料連接，而是來自應用程式所產生的一般資料流。這些資料通常涉及情緒和福祉狀態，而非直接的健康資訊。因此，資料保護機構需要超越其傳統的監管角色，進入更廣泛的對話，以適應 GDPR 所涵蓋的特別類別資料。總結，Wiewiorowski 認為，隨著數位化進程的加快，資料保護機構必須重新思考其角色和職能，以便更有效地應對當前心理健康資料管理中的挑戰。

2. 資料分享的法律和倫理問題：Wiewiorowski 分享心理健康資料所涉及的法律和倫理問題，並指出目前存在的顯著差距。歸納提到的幾個重要觀點：
   - 資料處理的不平等：Wiewiorowski 強調，並非所有心理健康資料都受到同等對待，這導致在國家和歐洲層面上存在多樣化的立法。GDPR 僅涵蓋部分能夠識別個人健康狀況的資訊，這使得一些重要的心理健康資料未被充分保護。
   - 系統分散性：在英聯邦及歐盟國家，每個國家擁有各自的健康、醫療幫助和醫療服務系統，這導致資訊非常分散。Wiewiorowski 指出，缺乏統一標準使得難以確定哪些資訊應由醫生跟進，哪些資訊不屬於健康資訊，從而造成了資料追蹤上的困難。
   - 法律約束的挑戰：研究人員在進行心理健康研究時，同時受到國家和歐洲法律的約束。這種法律框架的不一致性使得研究者在收集、分析和分享資料時面臨挑戰。
3. 共享健康資料的潛在益處：Wiewiorowski 強調，雖然目前對心理健康應用程式的效用存有疑慮，但如果這些應用程式的資訊能夠正確共享和收集，則可能帶來多方面的好處，包括個性化治療計劃、增強科學研究的合作以及創新心理健康工具。此外，這也有助於政府和行政部門進行知情決策、資源分配和標準改進。
4. 倫理監督的挑戰：Wiewiorowski 指出，當前存在倫理監督的不一致標準，使得公共衛生監測的效果難以衡量。這一點需要引起重視，以促進更有效的資料使用。

5. 德國 DiGa 系統的介紹：Wiewiorowski 提到德國的一個新系統 DiGa，該系統允許醫生為患者開具包括心理健康應用程式在內的處方。儘管 71%的醫生具備使用該系統的能力，但他們對隱私問題表示擔憂。
6. 應用程式的使用情境：Wiewiorowski 指出，許多使用這些應用程式的人並不一定是出於心理健康需求，而是為了提升福祉。他們可能並不意識到所分享的資訊會被視為心理健康狀況的資訊。
7. 資料透明度和隱私問題：Wiewiorowski 提到，許多心理健康應用程式包含追蹤工具，這使得用戶的資料來源變得不明。特別是對於有嚴重心理問題的人，這種情況可能導致他們在知情同意方面面臨挑戰。研究顯示，許多應用程式的隱私政策模糊不清，且存在資料分享的風險。例如，某些應用程式未經用戶同意就將其敏感資訊與第三方共享，這可能導致個人資訊被不當使用或濫用。此外，這些應用程式通常收集大量私人資料，包括用戶的心理健康狀況、行為模式和諮詢記錄等，而這些資訊的處理和存儲缺乏透明度，使得用戶難以了解自己的資料如何被使用。這種情況尤其對於那些面臨心理健康挑戰的個體來說，可能會加劇他們的焦慮與不安。因此，對於心理健康應用程式的隱私保護和資料透明度問題，需要進一步的關注和改進。
8. 資料供公共利益使用之觀點：在促進資料分享以支持公共利益、研究與醫療保健改進的過程中，保障個人權利成為關鍵議題。技術在這其中發揮了重要作用，尤其是神經技術的發展正帶來新的挑戰與機遇。當前，科學家與市場開始獲取來自神經技術解決方案與工具的資料，這標誌著資料處理方式的重大轉變。這些資料不再依賴外部觀察，而是直接從個人的神經系統中主動獲取。這樣的轉變引入了一個新的領域，即與個人心理與神經活動相關的社區資料。在這樣的背景下，心理隱私指數等新興概念成為保護個人權利的重要工具。可以從互聯網與物聯網 1.0 的經驗中汲取經驗，為即將到來的技術領域制定適當的框架與規範，以平衡資料共享的價值與

個人隱私的保障。

9. 提升監管能力與非政府組織合作的重要性：在面對數位平台和新興技術帶來的挑戰時，監管機構是否具備足夠的法律和資源應對這些問題成為一大關注點。現行法律可能不足以全面應對這些複雜情況，而監管機構也面臨技能和資源不足的困境。雖然提升監管機構的專業能力至關重要，但全面提升所有需要領域的能力實際上難以實現。為此，與非政府組織（NGO）的合作成為必要策略。NGO 在監測社會動態、提供技術見解，以及協助招募專業人才方面發揮著關鍵作用。例如，許多歐洲資料保護機構和歐洲資料保護監管機構（EDPS）已經開始積極尋求與 NGO 的合作，以更深入了解技術對社會的影響。這種合作方式還能幫助監管機構發現未被充分關注的技術問題。例如，在神經科學領域，自 90 年代以來，市場上已經存在某些可能影響大腦的侵入性技術，並且這些技術已經引發了因大腦刺激而導致心理狀態變化的案例。通過與 NGO 和社會代表的合作，監管機構可以更好地掌握這些隱藏風險，制定有效的監管策略。
10. 澳大利亞心理健康應用程式監管的創新模式：自 2017 年起，澳大利亞開始針對心理健康應用程式實施法律法規，並在近期進行修訂，將其排除在醫療設備要求之外。這種創新監管模式嘗試通過共同監管的方式，為心理健康應用程式制定單獨的管理框架，而非將其納入傳統醫療設備的監管結構中。這種方式類似於建築法規中的行為準則和認證，鼓勵公司進行自我認證，以確保產品符合心理健康需求的特定標準。特別是針對心理健康領域，這一做法可能為企業提供了更大的靈活性，同時也保留了必要的質量與責任要求。相比之下，歐洲層面目前尚未有針對心理健康應用程式的統一且適合的監管法規，雖然某些國家已採取解決方案，但整體框架仍需進一步完善。澳大利亞的經驗或可為其他地區提供有價值的參考範例。

(四)Rogue Interrobang 創辦人 Dan Holloway

1.資料分享的法律和倫理問題：Holloway 提到，許多心理健康資訊並非直接的特殊健康資料，而是關於情緒和福祉的資料，因此在這些資料的使用中，常常會產生推論。他認為，分享資料的倫理問題之一是缺乏對推論透明度的必要性。無論是在個人層面還是系統層面，推論的透明性都是一個重要問題。他推薦 Sandra Bucha 的研究探討從心理健康資料中推論的應用及其在各行業中的影響。他指出，在提供護理時，許多提供者並不需要深入了解患者的心理健康狀況，而是需要了解具體需求，以便更好地提供幫助。所以他呼籲應該有資料最小化原則，即企業僅需了解提供服務所需的最低限度資訊，以避免不必要的資訊分享。總之，Holloway 強調在心理健康資料管理中，需要更加關注倫理考量和透明度，以確保消費者的需求得到真正滿足，而不僅僅是企業利益的考量。

2.追蹤資訊在公共政策中的應用與用戶隱私擔憂：Holloway 指出，技術公司經常提到利用追蹤資料來識別公共政策問題和提前發現關鍵領域的潛力。這些資料可以幫助政府更積極主動地制定公共政策和公共衛生措施。然而，英國對公共衛生的看法，即公共衛生應該由政府控制，而非企業。這種觀點引發了對於企業在填補政府不足方面的擔憂，並質疑這是否會導致一些不良後果。他表示，作為一名用戶，他不確定自己是否希望通過應用程式分享資料來告知政府未來的公共衛生干預，尤其是在許多政府的健康干預措施並不被普遍認可的情況下。Holloway 作為一名有心理健康問題的個體，他懷疑自己的資料能否真正幫助實現他所希望的結果，有可能被用於其他目的，超出他的控制範圍，並且可能促使政府對他做出推論，例如社會信用和產品可用性。

3.共創情感識別技術與需求導向設計：在情感識別技術的開發過程中，對於面部表情與情感表達的假設需要更加謹慎，特別是在自閉症社群。該群體的情感表達的多樣性與複雜性常被忽視。技術設計過程中未充分考慮使用者，尤其是殘疾社群的參與。這導致產品可能無法真正對應他們的需求，利益與需求的對齊可能只是偶然，甚至是誤導性的。因此，讓有

實際經驗的群體參與項目管理與決策，能確保技術開發的方向與應用價值始終與需求保持一致，並且真正實現社會效益。

4.資料撤回權的挑戰：用戶希望能輕鬆改變已分享資訊的狀態，例如因病情間歇性發作或個人意願改變而希望撤回已分享的資訊。然而，在實踐中，資料撤回的操作往往並不如監管機構設想的那樣簡單。英國的法律雖賦予了用戶相關權利，但資料分享的技術性限制，例如資料在系統中已被混合或處理，可能使撤回變得複雜，甚至不可行。這一挑戰可被比喻為咖啡與牛奶的混合，一旦資料被整合到系統中，想要完全撤回或消除其影響幾乎不可能。因此，用戶希望能夠真正行使撤回或取消分享的權利，而開發者和監管機構需在技術和規範上進一步努力，確保這種權利能被實踐，從而提升用戶信任和應用的普及性。

■小組討論二：在現代世界中定義隱私危害

(一)資料政策領導中心 CIPL 主席 Bojana Bellamy

1. Bojana Bellamy 係現任 Hunton Andrews Kurth 資料政策領導中心主席，該中心是設立於倫敦、華盛頓特區和布魯塞爾的全球頂尖隱私與資料保護政策智庫。Bellamy 致力與全球商業及科技領袖、監管機構、政策制定者密切合作，共同塑造全球隱私保護及負責任個資使用之思想領導力與最佳實踐。

2. 數位科技發展使「危害」概念必須超越傳統之「隱私危害」，進入更廣義之「數位危害」範疇，不僅包含隱私權受侵害，亦涵蓋心理健康影響及社會層面問題，呼籲採取更整合、跨領域等綜合方法來因應日益多元之數位風險。

3. 以歐盟一般資料保護法規(GDPR)及數位服務法(DSA)為例，GDPR 將「風險基礎」概念納入規範，要求資料控管者與處理者依據風險採取相應措施，並在資料處理過程可能對資料主體造成高風險時進行資料保護影響評

估；DSA 則要求大型線上平台執行系統性風險評估與緩解計畫，以識別、分析和減輕其服務可能帶來的各種風險。基於此趨勢，未來的法律必須更明確地以危害為基礎，針對不同風險程度採取相應的規範措施。

4. 企業必須實施以危害為基礎之問責制度，評估其資料處理活動對個人與社會的潛在影響，並據此調整因應措施。在高風險情況下，企業應提供更詳盡的資訊揭露與更嚴格的防護措施；在低風險情況下，則可相對減輕法遵負擔，以促進創新發展。

5. 監管機關應採取以風險為基礎的監管方式，將資源集中於高風險範疇，以提升監管效能。

6. 在評估資料應用時，必須進行整體利益權衡，在某些情況下，多數人獲得的效益可能超過少數人承受的危害。法律政策的制定需要審慎考量此種平衡。

(二)歐洲個人資料保護委員會(EDPB)主席兼芬蘭個資保護機關主管 Anu Talus

1. 歐洲個人資料保護委員會(European Data Protection Board, EDPB)是由歐盟各成員國資料保護監管機關負責人及歐盟資料保護監督機關(European Data Protection Supervisor, EDPS)共同組成的決策機構。其核心職能涵蓋確保 GDPR 在歐盟境內一致性執行、提供資料保護專業諮詢意見、制定實務指引及裁決跨境爭議案件，並促進各成員國監管機關間的合作。EDPB 的決策對歐盟公民資料隱私權保障具有實質影響力，同時為企業建立資料處理的法遵框架。

2. 本節由現任 EDPB 主席 Anu Talus 闡述專業見解，Talus 自 2023 年 5 月就任 EDPB 主席，並自 2020 年起擔任芬蘭資訊專員。

3. GDPR 立法架構從「損害」(harm)導向轉向「風險」(risk)導向規範，該法規於 40 餘項前言及條文中提及風險概念，將其確立為資料控制者(controllers)與處理者(processors)選擇技術及組織措施之核心評估基準，此風險導向法遵模式使組織得依具體情境調整措施，實踐問責制原則。

4. 歐盟監管機關依據風險程度及違規性質進行評估並排定執法優先序。以盧森堡資料保護機關針對校園監控系統之風險評估調查為例，風險評估結果直接影響執法重點之判定。在裁罰階段，風險程度更是衡量違規行為嚴重性之關鍵指標。值得注意的是，即使屬低風險情形，仍需確保基本法遵措施之落實，並妥善處理相關申訴案件。

5. EDPB 建立跨境合作協調平台，強化成員國監管機關間資訊交流與執法合作，確保執法標準一致性。各國監管機關依循 EDPB 統一指引，得以協調因應跨境挑戰。

6. GDPR 將個人資料保護視為基本權利，其保障不因資料主體人數多寡而有差異。單一個人之信用資料更正權，可能影響其租屋、就業等基本生活權利，凸顯個人資料保護對基本權利的重要影響。

7. GDPR 採取風險導向之監管框架。資料控制者於選擇法律依據時，須審慎評估處理目的、預期效益及潛在風險，並採行適當之風險緩解措施。在執法實務上，違規行為之嚴重程度及裁罰額度均以風險程度作為核心評估指標。

(三)英國資訊專員辦公室(ICO)副專員 Emily Keaney

1. 英國資訊專員辦公室(Information Commissioner's Office, ICO)為英國法定獨立監管機關，肩負促進公共部門透明治理與保障個人資料隱私之雙重使命。其核心職權包括執行 GDPR 與英國 2018 年資料保護法(DPA 2018)，確保組織法遵處理個人資料；監督資訊自由法案與環境資訊法規之實施，強化公共機構透明度與問責性；依據「隱私

與電子通訊條例(PECR[5])」等相關法規，規範電子行銷、Cookie 使用及通訊服務。現任資訊專員約翰·愛德華茲(John Edwards)自 2022 年 1 月就任，積極推動新興科技之資料保護監管工作，特別著重人工智慧應用之法遵監管。

2. 本節由 ICO 副專員 Emily Keaney 就兒童隱私保護及政策規劃提供專業見解。

3. ICO 監管重點聚焦於個人資料處理所衍生之「資料保護損害」，而非廣義「隱私損害」。依據 GDPR 框架，凡因個人資料實際使用所生風險，均屬資料保護規範範疇。此區分有助於明確界定法律適用邊界，使資料保護法制更聚焦於資料處理直接衍生之損害類型，並使組織在風險評估與因應措施上準確掌握法定義務。

4. 風險評估應著重個人資料之實際應用情境，確保處理程序符合 GDPR、DPA 2018 及 ICO 指引要求，並維持資訊透明。以推薦系統為例，其演算法運用個人資料可能衍生特定風險，需依個案情境進行評估。

5. 英國數位管制合作論壇(Digital Regulation Cooperation Forum, DRCF)由英國資訊專員辦公室(ICO)與通訊管理局(Office of Communications, Ofcom)等監管機構組成，建立跨領域監管協作機制以處理網路安全與隱私議題。DRCF 已發布多項監管指引，例如「A pro-innovation approach to AI regulation 白皮書」對公平性(Fairness)概念的定義與詮釋(AI 系統不應損害個人或組織的合法權利、不應對個人有不公平的歧視、也不應造成不公平的市場結果；參與 AI 生命週期所有階段的行動者都應考慮適合系統用途、結果和相關法律應用的公平性定義)，有助於

[5] 隱私和電子通訊（歐盟指令）條例（Privacy and Electronic Communications (EC Directive) Regulations）

協調各監管機構的法治觀念對齊。目前 DRCF 正就其工作計畫進行公開徵詢，以確立跨監管合作的優先領域。

6. ICO 透過監理沙盒、創新輔導服務及中小企業支持計畫等多層次支持機制，在實踐 GDPR 與 DPA 2018 法遵要求的同時，亦平衡個人資料保護與產業創新，如「年齡適用設計守則」等指引的制定。

7. 公民參與為資料保護政策制定之關鍵要素。ICO 依循 GDPR 與 DPA 2018 之透明度及問責原則，建構多元意見蒐集機制，涵蓋公開徵詢、政策研討及民意調查，確保政策制定充分反映社會各界觀點。此機制有助於在法遵監管與執法實務間達致動態平衡，強化數位生態中的公民保護與賦權。

(四)英國伯恩茅斯大學教授 Andy Phippen

1. Phippen 教授在資訊通信技術(Information and Communication Technology, ICT)、科技倫理與數位法制領域深耕研究逾 20 年，主要專注於數位隱私保護機制、網路安全威脅及網路霸凌等社會科技議題之交互影響。

2. 數位法遵監管中，「安全損害」(security harm)概念的操作性定義存在根本性挑戰。相較於 GDPR 對隱私權的明確法律建構，安全概念具有高度主觀性與情境依賴特質，致使監管實務面臨執行困境。此概念模糊性不僅阻礙監管機關建立可量化標準，更凸顯現行數位監管體系在法理基礎與制度設計上的結構性缺陷。

3. 英國數位教育法制存在系統性缺口，國民教育法未能有效將聯合國兒童權利公約(Convention on the Rights of the Child, CRC)之權利框架整合進教育體系，導致數位公民教育出現法制真空。Project Evolve 平台資料顯示，教育資源配置失衡，過度著重基礎安全意識（如陌生人威脅）教育，而忽視進階技術素養之培育，此種失衡已無法滿足數位時代對學生技能與個人隱私權利均衡發展需求。

4. 隱私侵害之法律分析需突破平台責任的單一視角，實證研究揭示，隱私侵害常源於近端社會網路，如寄養系統中的過度監控行為，或教育機構在缺乏評估下之任意資料蒐集。此類案例凸顯 Data Protection Act 與 GDPR 等法制框架須進行結構性擴展，將規範範圍從平台延伸至社會關係網路，以建構全方位的隱私保護機制。

5. Online Safety Bill 於 2022 年 11 月修訂，並於 2023 年 10 月 26 日獲皇家批准，該法案將第 13 條中「合法但有害」(Legal but Harmful)內容定義移除，改為要求平台提供使用者內容控制選項、增強透明度及問責制，同時加強對兒童的保護措施及法律責任。此修法歷程不僅反映政治力量對數位監管立法的直接干預，也揭露了監管機關在技術可行性、社會接受度與規範正當性間的困境，對未來數位治理法制發展提出根本性挑戰。

6. 隱私及電子通訊規則(ePrivacy Regulation)的法制精神要求使用者須具備充分的法律知識與技術能力，平台須提供透明的操作機制與資訊揭露，監管機關則需建構促進雙方良性互動的法制環境。唯有透過提升使用者數位素養、強化平台透明度、建立效能導向的監管生態系，方能在數位時代實現隱私保護與安全監管的平衡。

(五)TikTok 歐洲資料公共政策總監 Jade Nester

1. Jade Nester 為現任 TikTok 歐洲資料與公共政策總監，負責統籌歐洲區域政府關係及政策事務，曾任全球行動通訊系統協會(GSMA)消費者政策總監，專精於跨境資料傳輸與隱私權保護等國際網路治理領域。

2. TikTok 建置雙軌治理架構，包含透過定期更新的社群規範制定營運準則；設立由學者與公民社會代表組成的全球安全諮詢委員會，以確保風險評估機制符合 GDPR 等國際法規標準。

3. TikTok 採行多元化使用者研究方法，整合使用者訪談與社群互動分析，並遵循英國資訊專員辦公室(ICO)之「合適年齡設計：網路服務行為準則」(Age Appropriate Design Code, AADC)與愛爾蘭資料保護委員會(DPC)之核心原則，建構青少年安全使用框架。AADC 旨在保護 18 歲以下兒童在網路上的隱私及安全，該規範於 2020 年 9 月 2 日生效，並於 2021 年 9 月 2 日施行，其 15 項標準內容如下：

標準	說明
兒童的最佳利益	將兒童福祉視為線上服務設計的首要考量。
資料保護影響評估	評估及減輕線上服務對兒童造成的資料保護風險。
適齡應用	依據兒童年齡及發展需求設計與調整線上服務。
透明度	提供兒童及家長清晰、簡潔且易懂的隱私資訊。
資料的有害使用	避免使用任何可能危害兒童福祉的資料。
政策及社群標準	嚴格遵守已發布的法令、政策及社群標準，並確實保護兒童。
預設設定	預設為高隱私設定，以最大程度地保護兒童資料。
資料最小化	僅蒐集及保留提供服務所需的最少量的個人資料。
資料共享	除非有正當理由，否則不與第三方共享兒童資料。
地理位置	預設關閉地理位置服務，僅在必要時才蒐集位置資料。
家長控制	提供家長控制功能，讓家長能監控及管理兒童的線上活動。
分析	預設情況下關閉分析功能，僅在有正當理由時才使用。
誘導技巧	避免使用任何可能誘導兒童提供不必要資訊或降低隱私設定的技巧。
連網玩具及裝置	確保連網玩具及裝置符合資料保護標準，並提供清晰的資訊及控制功能。
線上工具	提供易於使用的線上工具，讓兒童可以行使他們的資料保護權利。

4.TikTok 導入隱私始於設計(Privacy by Design)機制，透過法務與設計研發部門的跨領域協作，在產品開發初期即實施隱私與法遵審查，以確保產品符合法規要求與倫理標準。

5.TikTok 建構動態風險管理框架，積極參與年齡驗證國際論壇等多方利害關係人協作平台，同時深化與監管機關及標準組織之合作關係，持續強化風險評估機制。

6.TikTok 實施全方位資料自主管理，提供關鍵字過濾、互動管理及內容訂閱等控制功能，並透過多元數位素養培育方案，提升使用者資訊識讀能力。

7.TikTok 採行權益平衡架構，將兒童發展、言論自由與網路安全等多面向考量整合於產品設計中，並透過科學(Science)、技術(Technology)、工程(Engineering)及數學(Mathematics)(STEM)內容策展與主題管理機制，達成安全與創新的均衡發展。

「場次二：個人」活動進行實況

場次三：獨立(Independence)

場次四：國際化(International)

■小組討論一：資料傳輸工具的優勢及挑戰

(一)IAPP 研究及觀察處 Joe Jones 總監

John 總監為本場次主持人，首先簡介各與談人背景，並表示本節將聚焦分享各國/組織於規劃及執行跨境資料傳輸法制架構的政策立場、原則及策略，以共同探索在兼顧隱私保護與法遵的情況下，促進全球資料流通的解方，為數位經濟創造值得信賴且高效率的國際環境。

(二)日本個人資料保護委員會 Yuji Asai 委員

1. 資料自由流動（Data Free Flow with Trust, DFFT）係日本前首相安倍晉三於 2019 年世界經濟論壇中提出之概念。DFFT 旨在平衡資料流通的自由與信任，推動全球經濟數位化轉型。DFFT 強調在尊重隱私權與資訊安全的前提下促進跨境資料流動，以支持創新、貿易及國際合作。

2. DFFT 是資料治理的最終目標，而跨境資料傳輸工具則係實踐 DFFT 理念之關鍵。適足性認定與認證機制是目前各資料傳輸工具中的重要選項，且係支持跨境資料傳輸的有效工具。日本致力於國際場域中推動形塑跨境傳輸規則相關工作，並於 GPA 中參與跨境傳輸文件的撰擬，以於該文件中落實 DFFT 精神。

(三)歐洲委員會立法及全球資料保護負責人 Estelle Massé

1. 歐盟高度重視跨境資料傳輸議題，並致力於推動安全且可信賴的資料傳輸工作。歐盟的資料治理工具旨在保障個人資料的安全，確保資料在跨境傳輸中得到充分保護，並促進企業、研究機構及醫療領域等業者能順利推動資料傳輸相關業務，此目標彰顯資料流動對數位經濟與整體經濟發展的重要性。

2. 歐盟為因應市場及管理需求的多元性，透過多種機制實踐資料治理，並隨時局變遷所面臨之新挑戰，滾動式推動相關法規的革新。歐盟致力於在資料傳輸與前揭多元性間保持平衡，並避免為追求單一目標而犧牲其他目標。透過國際合作，歐盟努力實現相關資料傳輸規範的協調，促進資料流動的互惠與共榮。

(四)南韓個人資料保護委員會 Haksoo Ko 主委

1. 透過有效且周延的機制監管國際資料傳輸行為係政府建構可信賴的資料治理環境所必要的工作，資料相關議題日趨複雜，需依據具體個案事實採用諸如適足性認定、適當保護措施、認證機制等多樣化策略，以確保符合實際隱私規範需求。

2. 在資料傳輸的治理框架中，適足性認定及適當保護措施是常見的規範方式。韓國透過適當保護措施的國際傳輸要求與歐盟的適足性認定相類似，但具有在地化特質。這種規範方法為資料傳輸的監管賦予靈活性，以幫助不同司法管轄區應對資料治理的挑戰。

3. 國際傳輸未來的主要挑戰，係如何於促進各機制的互操作性及協調性，資料治理的關鍵在於不同機制之間的相互操作性與協調，各國須共同努力促使不同的資料流動框架能夠兼容並蓄，以極大化資料傳輸效益，兼顧隱私及安全。

(五)OECD 資料流動、治理及隱私處 Clarisse Girot 代理處長

1. 跨境資料傳輸對數位經濟發展與社會健全運作至關重要，但核心問題在於「信任」的建立，此概念彰顯實踐 DFFT 的重要性。DFFT 支持自由且可信賴的資料流動核心價值，不僅涉及資料流動相關法規，亦涵蓋政府近用個人資料、國家安全與執法需求的平衡，及資料流動機制的優化。

2. 隱私政策監管的國際合作係促進可信賴資料流動的基

石，監管機構於執法或政策若缺乏協作，則難以建立信任的資料流動架構。隱私增強技術（PETs）可兼顧隱私保護及資料流動，然 PETs 並非替代資料傳輸法規，而係協助提升資料流動的可信度與效率。

3. OECD 刻正致力於推動 DFFT 可操作性工作，此項工作係受七大工業國組織(Group of Seven, G7)委託的業務。G7 刻正推動相關計劃，探索如何將 DFFT 轉化為實際運作機制，近而促進全球資料流動的信任與永續發展。

■小組討論二：金融服務背景下的國際資料傳輸—發展趨勢如何？資料傳輸機制的未來為何？

(一)法國資訊政策領導中心(Centre for Information Policy Leadership, CIPL)資料策略及隱私政策資深顧問 Vivienne Artz

1. 強調資料傳輸在金融服務中的核心作用，並指出它對全球經濟運作的重要性。隨著數位金融的興起，資料傳輸成為企業、政府及個人業務運作的基礎。金融服務的發展已不僅限於傳統的銀行業務，電子支付及行動支付系統的普及促使資料流動日趨迅速且精確，對個人支付行為及國際商業交易活動重要性提升。金融服務活動日益複雜，除傳統的銀行金融機構業務外，尚有替代支付系統，使消費者能通過手機完成大部分金融服務操作。

2. 澤西島的金融服務業發展成熟，作為一金融服務監管機構，澤西島的監管機關不僅監督傳統銀行，也包含其他金融機構及支付系統。金融交易活動的多元發展，彰顯資料傳輸的重要性，以確保全球金融系統的穩定與高效。A 顧問作為本場次主持人，請與談人就金融服務業的現狀、監管機構的角色以及資料傳輸對全球金融系統的重要性之議題進行討論。

(二)澤西金融服務委員會 Jill Britton 主任

1. 金融服務業係全球經濟成長的主要動能之一，預估在全球經濟約占比 20%至 25%。金融服務業對澤西島經濟活動的直接貢獻高達 40%，間接貢獻則接近 70%，顯示金融服務在澤西島經濟活動中的核心地位，涵蓋範圍包含傳統銀行、私營銀行、投資銀行、信託公司等，形成了多層次、多樣化的金融生態系統。

2. 澤西島的金融服務活動涵蓋範圍甚廣，除傳統銀行業務外，尚包含私營銀行、投資銀行、信託服務、基金管理等。澤西島金融機構的數量約 5,500 家，且擁有約 2,000 億的財富管理規模，服務範圍覆蓋 230 個國家和地區，顯示出澤西作為一個小型島嶼在全球金融服務中的重要角色。

3. 澤西島金融服務的運作與全球資料傳輸關係密切，以行動支付為例，澤西島的支付交易活動已涵蓋全球 233 個國家，表示資料傳輸對金融服務至關重要。無論是個人交易或跨境交易，資料的即時傳遞及準確處理均對經濟活動運作、服務提供等方面有不容忽視的影響。

4. 資料傳輸的監管對保障營業活動的服務品質具有重要性，以旅行保險為例，相關活動涉及多方機構的資料交換，若無有效的資料傳輸機制，可能對服務品質產生嚴重影響，彰顯資料流動於多方交易及跨境合作的重要性。又以房產交易為例，交易活動涉及買方、賣方、地產代理、律師、貸款方等多方機構，這些機構從事的相關活動並無全面受到一致的監管，若資料無法有效於各方間移轉對交易活動影響甚鉅，甚至妨礙服務的提供，故資料流動的便利及效率是確保金融服務順利運作的關鍵。

(三)世界銀行 Katherine Race Brin 首席資料保護官

1. 國際資料傳輸對世界銀行向開發中國家政府進行放貸業務相當重要，世界銀行貸款業務涉及大量個人資料的傳輸行為，而這些所需資料能幫助世界銀行確保相關工作的推動，並防止詐騙行為發生。另，世界銀行員工遍佈全

球，資料需持續於不同國家間傳輸，故跨境資料傳輸是世界銀行維持業務運作過程中不可或缺的部分。

2. 世界銀行作為國際組織，雖於許多國家或國際資料保護規範中享有特別豁免的權利，但世界銀行仍高度重視隱私保護相關問題並嚴守資料保護的最佳實踐工作。世界銀行的隱私政策於 2018 年由董事會通過，並於 2021 年生效。該政策包括合法性、同意、準確性、透明度及問責等重要原則。問責制度使資料主體得對資料控管者行使異議權及知悉權，有助確保世界銀行於處理個人資料時符合透明度、準確性及負責任的要求。儘管世界銀行豁免於許多隱私法規的約束，但其隱私政策遵循全球範圍內的資料保護最佳實踐，並為資料主體提供了合法的申訴途徑。

3. 世界銀行對若干即將生效的資料傳輸框架及問責機制表示擔憂，因這些新機制有限制資料傳輸之虞，使世界銀行未來與第三方機構合作執行業務時，若第三方機構因世界銀行無法接受特定的法規要求而拒絕向其轉移資料，可能會阻礙資料流動，進而影響世界銀行的業務推展。世界銀行目前係透過訂定隱私政策及問責機制，向國際間證明其符合多數國家的資料保護最佳實踐，以應對前揭挑戰。

(四)杜拜金融中心(Dubai International Financial Centre, DIFC)資料保護法律團隊 Lori Baker 主任

1. 2004 年阿聯酋於杜拜及阿布達比設立二個金融自由區，這些區域脫離阿聯酋聯邦及各酋長國的民商事法律框架，能夠制定自主的法律體系。DIFC 便於當時創立該地區的首部個人資料保護法，並且由杜拜金融服務局（Dubai Financial Services Authority, DFSA）負責監管。2007 年，DIFC 修訂其個人資料保護法，並成立獨立的個人資料保護專責機關。隨著監管範圍的擴大，DIFC 也持續聚焦反洗錢及金融犯罪等議題，更新其資料保護法律。

2. 為因應不僅限於金融機構的洗錢及金融犯罪問題，DIFC 在過去六年間制定了反洗錢及風險評估框架，該框架涵蓋金融及非金融服務機構，並在資料保護法中納入具體條款以因應金融犯罪預防等相關敏感資料處理活動的規範。在資料使用上，針對政府及第三方機構對資料使用，亦有額外的控制措施。

3. DIFC 於 2020 年再次修訂其資料保護法，強化對資料共享及政府近用個人資料的監管：新版法案新增第 28 條條文，明確規定於金融犯罪預防等情況下，進行資料共享行為時須附加額外控制措施，並確保資料接收方清楚了解如何合法使用這些資料。此修訂不僅符合國際最佳實踐，還確保資料保護與犯罪防範工作間的平衡。

4. 在全球化浪潮下，DIFC 需要進行大量的國際資料傳輸工作，特別是在與美國證券交易委員會（Securities and Exchange Commission, SEC）等機構合作時，須確保在資料共享過程中符合各國對金融犯罪防範的要求。DIFC 與 SEC 等機構已透過簽訂備忘錄，規範資料共享模式，同時保障資料傳輸不會妨礙預防金融犯罪舉措的有效性。亦即兼顧雙方於遵守隱私保護的同時，亦符合金融犯罪防範的需要。

「場次四：國際化」活動進行實況

場次五：跨文化及原住民(Intercultural & Indigenous)

■ 主題演講：「保障永續性：資料隱私於環境倡議及人道主義危機中的作用。」

(一) 本小節由現任紅十字國際委員會(International Committee of the Red Cross, ICRC)資料保護辦公室主任 Massimo Marelli 分享觀點。Marelli 同時為馬斯垂克大學歐洲隱私與網路安全中心(European Centre on Privacy and Cybersecurity, ECPC)顧問委員會成員及研究員，並共同領導該中心人道行動計劃。

(二)Marelli 以其在紅十字國際委員會(ICRC) 11 年資料保護與隱私工作經驗為例，介紹該國際組織如何依循日內瓦公約、附加議定書及武裝衝突法，在加薩、烏克蘭、蘇丹等動盪地區開展人道援助工作。

(三)在人道主義環境中，資料保護不僅是法遵要求，更是維護個人尊嚴與代理權的關鍵。它為組織處理個人資訊提供問責框架，體現人道主義「不傷害」原則，尤其在新技術應用方面。儘管資料保護在不同文化背景下有其獨特詮釋，但尊重個人尊嚴的核心原則具有普遍性。

(四)演講者透過一個案例深入探討資料保護實務之複雜性：一名 11 歲遭綁架入伍後逃至鄰國難民營的兒童。在協助其與家人團聚過程中，面臨多重同意權問題：親生父母因長期分離而對子女現況缺乏了解、孩童對返回意願猶豫不決、寄養家庭則持反對立場。此案引發幾個關鍵議題：同意機制是否為最適法律依據？如何在具體案例中實踐資料保護原則？以及如何在法律規範與人道考量間取得平衡？本案凸顯資料保護不僅涉及法律適用，更需權衡個人選擇與實際處境。

(五)為確保資料保護標準在極端環境中的落實，ICRC 持續與相關組織及學術機構合作制定規範，並建立培訓認證機制。

■小組討論：原住民如何制定自己的資料保護框架？

(一)IIS Partners 創辦人暨合夥人 Malcolm Crompton AM

1. Malcolm Crompton 講員前於 1999 年至 2004 年擔任澳洲隱私保護專員，期間主導制定並實施澳洲首部私部門隱私保護法，為現任 Bellberry Ltd 董事及聯邦財政部數位身分識別法專家顧問，並長期參與歐盟、OECD、APEC 等國際組織的資料保護諮詢工作。因其在資料保護、隱私權及身分識別管理之貢獻，2012 年獲 IAPP 頒發隱私保護領袖獎，2016 年獲頒澳洲員佐勳章。

2. 以澳洲原住民為例，原住民往往對醫療研究抱持高度不信任感，因為歷史上這些研究多以造成傷害告終。 因此，在進行與原住民相關研究時，必須事先徵得其同意，並確保研究設計符合其利益。基於此理念，Crompton 提出「Nothing about us, without us」 原則，強調原住民必須參與到與其相關決策過程中。原住民應享有資料自決權，包含資料蒐集、處理、利用及其保護機制的決定權，呼籲原住民應成為資料治理框架共同制定者，而非僅為被規範客體。

3. 呼籲以同理心、傾聽、包容及慷慨態度與原住民展開對話，共同解決資料保護問題。

4. GPA 應將原住民資料保護議題納入其議程，並支持原住民參與國際討論。

5. 肯定 GDPR 作為全球資料保護立法典範之價值，但指出其需要因應多元文化進行調適。特別是 GDPR 以個人同意為核心的規範模式，與原住民重視集體決策的傳統法律制度產生規範衝突。

6. 人工智慧技術應受相應法律規範，以平衡其在保存原住民文化資產之效益，及防止文化盜用或不當商業化之風險，建議制定專法或修法將原住民文化權益納入規範考量。

7. 原住民資料保護係一個複雜且多層次問題，需要全球合作及持續對話來解決。承認原住民的獨特文化及考量，並賦予他們控制自身資料的權利。 人工智慧為原住民社區帶來了機遇及挑戰，需要仔細評估及管理。 資料保護立法及監管框架需要不斷發展，以適應不斷變化的技術環境及原住民的需求。

(二)L3Harris Technologies 全球隱私及人工智慧法遵長 Shana Morgan。

1. Morgan 講員為美國切羅基族人，她早年在德國成長，後遷居美國，此多元文化背景強化其對隱私權與跨文化背景的深度理解；Morgan 具備 AIGP、CIPP/E、CIPM 及 FIP 認證，現為 IAPP 隱私權多樣性諮詢委員會委員。她致力將文化視角納入隱私權實踐，並推動原住民資料主權及隱私權議題之發展。

2. 強調西方以 GDPR 為架構之資料保護法律可能無法完全適用於全球，尤其對原住民而言，認為 GDPR 雖然在保障隱私權方面取得了進展，但其制定過程缺乏原住民參與，且未考慮到其獨特文化及需求。

3. 以美國為例，聯邦政府掌控原住民資料，切羅基民族在內部資料共享及利用方面也受到諸多限制，難以有效地為其公民提供服務。

4. 原住民需要有權控制自身資料，並制定符合自身文化及需求之資料保護框架。 原住民應積極參與資料保護政策的制定及實施，確保其聲音被聽見。

5. 強調原住民在人工智慧發展過程中面臨之機遇及挑戰。人工智慧可以用於保存及復興原住民語言，例如 Cheyenne、Lakota 及 Dakota 語言之人工智慧語言資料庫，亦可能被用於剝削及侵犯原住民權益，例如 AI 模型被商業化利用，而原住民卻無法從中受益。

6. 呼籲各界重視原住民資料保護議題，讓原住民參與相關討論及決策，並舉例紐西蘭原住民毛利人資料保護框架被視為一個值得借鑒之成功案例。

(三)肯亞個人資料保護專員辦公室(Office of The Data Protection Commissioner)專員 Immaculate Kassait

1. Kassait 具備超過 12 年公部門治理、培訓、法遵及策略規劃經驗，曾擔任肯亞 2019 年個人資料保護法三項子法制定專案小組主席，對建立該國資料保護監管制度具重要貢獻，其領導個資保護專員辦公室制定 2022 至 2025 年策略規劃，建立全國性監管體系，為現任非洲資料保護機關網路(NADPA)第一副主席，積極參與國際資料保護監管合作。

2. 強調原住民歷史及文化深受口述傳統影響，資料保護框架應考慮到這些獨特因素；未經授權之資料蒐集及利用將導致對原住民文化及知識的誤解與濫用。

3. 指出資料保護框架應平衡個人及社區利益，資料蒐集及利用必須獲得社區同意，並確保其符合社區利益。

4. 呼籲全球隱私權大會(GPA)制定新資料治理原則，以保障原住民權利，並提出關懷、集體利益、社區倫理及所有權等原則，並認為 GPA 應將原住民資料保護議題視為優先事項，並制定相關標準及指南。

5. 強調大型科技公司應負起責任，確保其平台及演算法不會被用於侵犯原住民文化及道德價值觀，例如及時移除有害內容及打擊假新聞。

(四)墨西哥國家透明度研究院委員 Josefina Román Vergara

1. Vergara 擔任墨西哥州政府與聯邦稅務總局等多個主管職位，2019 至 2026 年任期之國家資訊透明暨個人資料保護研究院委員，由參議院任命。現兼任該院國際事務常設委員會主席。

2. 強調原住民族群普遍使用多種語言，資料保護相關資訊及文件應以這些語言提供，確保所有成員都能理解及參與決策。 以墨西哥為例，該國憲法保障原住民語言權利，但在實踐中，翻譯成本及缺乏合理之調整措施導致原住民難以行使其資料保護權利。

3. 呼籲各國制定資料保護法律，並設立專責機構來監督資料保護的執行，例如墨西哥的國家透明度平台及相關資料保護法律。

4. 以墨西哥 DaWalco 應用程式為例，說明 AI 技術可以促進資料保護權利的實現，但也可能帶來新的風險，例如演算法歧視。 因此，需要制定相關規範，確保 AI 之透明度及公平性。

5. 認為國際組織，如 OECD 及 UNESCO，應制定有關 AI 指導方針，以保護原住民權利。

6. 呼籲 GPA 加強區域合作，制定符合不同地區原住民需求的資料保護標準，例如美洲資料保護網路制定的資料保護標準。

(五)綜上，講者們一致認為， GDPR 並不適用於所有文化及社群，尤其是原住民族群。資料保護之本質在於維護個人及社群尊嚴，賦予個人資料自主權，並確保資料蒐集及利用符合倫理原則。各界應重視原住民資料保護議題，制定符合其文化、價值觀及需求的保護框架，同時鼓勵原住民積極參與相關政策的制定及實施。國際組織、政府部門、學術機構及原住民應加強合作，共同確保原住民在數位時代之權利得到充分保障。

「場次五：跨文化及原住民」活動進行實況

場次六：個體(Individual)

■主題演講：減少隱私權的不平等：探討多樣性中不同的隱私面向

(一)本場次由 Freeda 首席執行長 Kate Wright 主講，Freeda 是澤西島唯一的家庭暴力慈善組織；W 執行長也是 The Diversity Network 的共同創辦人，該組織致力於促進工作場所的多樣性、公平與包容。另，W 執行長亦擔任澤西島多個公共與志願職位，包含反對女性暴力專責小組主席等。

(二)隱私權在不同群體中存在歧視隱憂，女性、兒童、少數族群時常暴露於數位暴力及隱私風險中。以澤西島為例，當地年輕女性普遍因性別遭受數位暴力，此現象凸顯隱私權及資料隱私對女性的保護不彰。隨著網絡暴力、性騷擾及位置追蹤等問題，隱私權的不平等現象對女性及年輕人造成嚴重影響，故需要更周延的法律保護及意識推廣。

(三)資料隱私及企業文化存在矛盾，許多企業將資料保護視為法遵義務，而非以保護個人隱私的人權保障為核心理念，此現象在多元性及包容性策略的推行中更為明顯。企業於搜集多樣性資料時常面臨無知與恐懼、員工信任缺失、資料隱私法規的誤解等三大障礙，這些障礙時常耽誤企業於創造包容性工作環境的努力。

(四)改變大眾對隱私權的認知意識是從根本解決不平等問題的關鍵，隱私權應被視為基本人權，而非僅是技術或法律問題。政府應於教育、政策及企業運作中，強調每個人都應平等享有隱私保護，無論其性別、年齡或社會經濟背景。尤其是對於外來族群，缺乏信任與資料共享的恐懼，往往使他們無法獲得所需的相關民生服務，故政府需要透過提升透明度、教育及多元化的政策制定解決這些問題，確保資料保護能夠確實保障弱勢群體的隱私。

■小組討論一：從基礎開始的教育：隱私教育對社會的影響

(一)加拿大安大略省資訊及隱私委員辦公室 Petricia Kosseim 委員

1. 隨著數位科技成為青少年的日常，政府應透過數位知能教育協助青少年成為負責任的數位公民，依聯合國兒童權利公約，呼籲應將數位素養培育納入學校基礎教育中，讓青少年了解如何安全地使用數位工具與資源。數位知能教育有助於保護青少年免受數位傷害，也能幫助他們理解並行使數位隱私權。

2. GPA 分別於 2016 及 2021 年，通過有關隱私教育的國際框架與兒童數位權利的決議，強調必須讓兒童了解個人資料保護權利，並讓兒童具備應對數位風險的知能。另，隱私教育應以兒童易於理解的方式推行，並在各種教育階段融入隱私保護內容，以保障他們的數位權利。

3. 安大略省的數位隱私教育推廣與青少年參與經驗：安大略省近期更新了省級課綱，將數位素養及公民意識培養納入所有學年必修內容，相關課程著重隱私及安全教育。為充實課程內容，安大略隱私專員辦公室與 Media Smarts 合作制定教學計劃，並創建了青少年顧問委員會，從 15 至 25 歲的青少年中挑選代表，幫助制定能夠啟發同齡人關注隱私權的資源。這些工作不僅幫助青少年理解並行使隱私權，還鼓勵他們在學校中成為隱私權的種子學員。

4. 未來的挑戰與政府支持的數位隱私法案：安大略省政府近期提出一項新法案，旨在加強對學校中兒少使用數位技術的保護。該法案強調要尊重兒童和青少年的隱私，並呼籲將兒童的個人資料視為敏感資訊並加強保護措施。安大略省隱私專員辦公室已向聯邦政府提案，呼籲制定符合個人自主、尊嚴及自我決定價值的標準，以加強對數位隱私的保護。

(二)5Rights Foundation 創辦人兼主席、House of Lords 成員 Baroness Beeban Kidron OBE

1. 曾與巴基斯坦、肯亞及馬來西亞等地的青少年討論對於數位權利的看法，他們關注移民兒童的數位權利、線上

與線下防止兒童性虐待的挑戰，以及隱私與安全策略。來自非洲的青年表示，國家將數位世界中的安全與隱私責任推卸到青少年身上的做法，顯示成年人未能系統化保護兒童網路安全的失敗，並反映出現代數位環境中對兒童的漠視。

2. 在與兒童溝通的過程中，應著重避免讓兒童重複描述痛苦經歷或回答不理解的問題。講者曾透過互動式教學，協助兒童理解數位產品的運作機制，以改善兒童的網路生活，使他們免受數位剝削及傷害。

3. 現代數位產品及服務的設計主要以商業利益為導向，關注擴展用戶網絡、增加使用時長及提升互動性，而非考慮用戶的年齡或需求設計相應的機制。這種運作模式可能使兒童暴露於潛在數位危害中，例如與不安全的成人聯繫或接觸兒童不宜的內容。隱私保護雖可能增加事業應運成本，但能減少兒童受到的傷害，幫助他們避免過度沉迷於數位世界。

4. 數位隱私對兒童權益十分重要，高標準的隱私設計能為兒童提供更多自由，數位素養雖然是 21 世紀的重要技能，但應輔以系統性的保護措施，例如限制直播、屏蔽不必要通知及防止不必要的好友邀請，能相當程度減輕兒童的數位負擔。兒童身為數位原住民，在數位世界具有可觀的創新量能，應為兒童打造一安全的數位環境，使其能夠自由探索與學習。隱私主管機關應主動制定規範，保護兒童的隱私與權利，讓他們有機會在數位世界中茁壯。

(三)香港隱私專員公署 Joyce Lai 助理隱私專員

1. 香港個人資料私隱專員公署（The Office of the Privacy Commissioner for Personal Data, Hong Kong, PCPD）推動兒童隱私教育分為「教育」、「參與」、「賦權」三階段。首先，PCPD 通過雙語出版物和專題網站教授私隱的基本概念。

其次，PCPD 與兒童、家長及教師直接互動，促進雙向交流，以加深隱私保護意識。最終，讓兒童具備保護自身隱私及尊重他人隱私的能力。

2. 在應對網絡欺凌及肉搜行為上，PCPD 透過設計友善兒童的彩色教材及短、為中學生舉辦反肉搜講座，提升兒少對相關法律的認知。另，PCPD 亦舉辦短片創作比賽，吸引超過320名小學生參加,通過創作傳遞反網絡霸凌的訊息。

3. 針對生成式人工智慧的使用，PCPD 發布「AI 聊天機器人使用的十要訣，強調個人資料保護的重要性。另，PCPD 辦理「未來 AI 與隱私保護領袖培訓計劃」，培養中學生學習 AI 應用中的資料管理與倫理，學員透過提交 AI 應用相關作業，培養平衡 AI 技術與私隱風險的批判性思考。

4. 針對數位足跡的問題，PCPD 發布家長和青少年使用社交媒體的指導資源，並推出「私隱保護流動車」巡迴展覽，利用互動遊戲和紀念品吸引學生參與學習。同時，PCPD 舉辦手機遊戲應用設計比賽，主題聚焦於線上警覺，吸引超過 400 名中學生提交作品，激發創意並強調數位安全意識的重要性。

5. PCPD 的三階段兒童隱私教育策略成功提高兒童的隱私意識。透過出版品、互動講座、比賽及流動展覽等多元活動，PCPD 有效促使兒童理解及應用隱私保護的概念，並賦予他們面對數位挑戰的能力。PCPD 的兒童隱私教育措施的政策，證明了透過教育、參與及賦權三方合作，能有效塑造更安全的數位環境。

(四)加拿大數位及媒體識讀中心 MediaSmarts 教育長 Matthew Johnson

1. 「風險是可能導致傷害的情況，危害則是人們無法管理的風險」，政府及組織須教育兒童在安全環境中學習如何管理風險，而非完全消除風險，故數位媒體素養的核心概念在於幫助兒童辨識並管理適當的風險，以及避開無法應對

的危害。

2. 研究顯示，年輕人擅長經營網路形象及社群內容，但對資料隱私的認知卻有限：年輕人傾向從應用程式的功能推測可能的隱私政策（例 ：非公開帳號），但對資料蒐集的實際做法卻無能為力。另，同意條款的確認並非「有意義的同意」，而只是為使用網路服務而被迫接受的條件。

3. 數位隱私教育的終極目標是培養年輕人為自身權益發聲，並提出解決方案，以消費者及公民的角色，要求更安全的數位環境。MediaSmarts 數位素養教育計劃著眼於培養年輕人對網路內容具有批判性思考的能力，認識企業的程式設計手法及資料搜集政策之影響。數位素養教育計劃涵蓋技術以外的議題，包括道德考量、社會影響及如何尊重他人隱私。另，隨人工智慧的發展，教育計畫課程也探討 AI 隱私相關問題。該教育計劃同時邀請父母及教師共同參與，協助父母及教師理解如何保護孩子的隱私。

4. 傳統課程中缺乏隱私教育，故 MediaSmarts 積極於加拿大聯邦及各省政府，推動數位媒體素養計畫，並成功將隱私議題納入安大略省的官方課程，從小學階段開始教育。此外，MediaSmarts 亦舉辦設計有效的同意機制研討會，讓年輕人重新設計更清晰易懂的同意流程，並將建議以白皮書形式提交給各大應用程式公司，促使相關平台針對青少年推出更嚴格的預設隱私設置，但資料蒐集及同意流程仍未改進。

(五)5Rights Foundation 執行總監 Leanda Barrington

1. 雖然許多人聲稱「在隱私保護面前，兒童優先」，但實際上，兒童隱私問題時常被忽視，故優先處理兒童隱私議題至關重要。5Rights Foundation 是一個國際非政府組織，致力於打造適合兒少發展的數位世界，透過與兒童、專家及國際組織合作，促進兒童權益的落實，同時賦予兒童發聲的機會，並鼓勵他們成為改變的推動者。

2. 5Rights Foundation 的使命是讓兒童的數位世界變得安全且充滿活力，該組織提供實用的工具及證據，用以支持全球監管機構及創新者。全球兒童面臨相似的數位風險，故需要一致的解決方案，而近年聯合國大會、OECD、歐洲理事會亦有相關承諾。

3. 兒少隱私保護的全球共識正在形成，透過風險評估、適齡功能設計、公平透明的條款得納入，將兒童權益置於數位環境設計之核心。從歐洲的「兒童適齡設計法案」到美國的馬里蘭和加州等地，都展現了對兒童隱私的高度關注及一致的標準，這些標準強調兒少隱私保護、賦權與參與的不可分割性，確保兒童在一安全且符合其需求的數位世界中成長。

4. 針對兒少隱私保護應有系統性變革，而非僅依賴家長同意或教育資源的貢獻。家長、學校及孩子面臨數位環境的巨大挑戰，單靠現有的支持資源不足以應對，需要以隱私始於設計的概念調整數位系統。5Rights Foundation 近期發布有關國際兒童資料保護最佳實踐之報告中已證實現行規範於促進兒少隱私保護方面的有效性。

■小組討論二：隱私無障礙：在數位化世界中保護障礙者、弱勢群體及社會邊緣人士

(一) 百慕達隱私專員辦公室 Alexander White

1. 在促進隱私概念可近性上，聚焦如何保護有特殊需求或弱勢群體之隱私權，這些群體包含身心障礙者、脆弱群體、遭到社會排斥的人等。隨著科技進步，特殊需求或弱勢族群能夠借助各種技術改善生活品質（例：使用助聽器、人工耳蝸等設備改善聽力，或是通過虛擬替身參與社交等），但科技進步亦伴隨更多隱私及安全風險，尤其是在資料處理及技術應用方面，故如何平衡弱勢群體的生活需求與隱私保護便更是一個重要議題。

2. 科技進步提升身心障礙者及弱勢群體的社會參與度，並

且有助於促進他們自立；例如：聽障者得依靠人工耳蝸等裝置參與對話、行動不便者可通過線上虛擬替身參與社群活動。科技還能幫助弱勢群體於醫療領域找到特定的治療方案；例如：特定病症的研究可獲得更多資源，使患者有機會接受更精準的治療。

3. 科技為特殊需求者帶來便利也伴隨著風險，對科技技術的高度依賴，使弱勢群體面臨更多安全及隱私問題，個人資料在技術使用過程中可能會被不當蒐集或洩露等。另，弱勢群體的資料處理及儲存可能缺乏充分的保護，成為潛在的駭客攻擊目標。

4. 利用先進科技促進弱勢群體生活便利的同時如何兼顧隱私保護，不僅關乎科技技術本身的發展，也涉及如何設計政策及保護措施。White 作為本場次主持人，邀請講員分享兼顧改善弱勢群體生活品質並兼顧該等群體之隱私安全的最佳實務，以為未來的技術應用提供參考及指導。

(二) 澳洲資訊委員辦公室 Cerly Kind 隱私專員

1. 澳洲近年來經歷了數次重大個資外洩事件，其中最受矚目的是涉及 1,400 萬澳洲人個人資料的藥品處方箋服務個資外洩案。個資外洩事件對澳洲社會的影響深遠，因這些事件外洩大量個人資料，使這些資料更加容易被濫用，資料洩漏的問題不僅對公眾隱私構成威脅，還加劇對既有資料集所帶來的風險。

2. 個資外洩對特定群體的影響尤為嚴重：家暴受害者的位置資訊如遭洩漏，則人身安全將有極大威脅；另，因過往澳洲政府實施同化政策的緣故，原住民社群尤為關注與兒童資料保護記錄及外部照顧有關的個資外洩案件。

3. 原住民族群亦特別關注資料外導致文化的流失議題，以及失去對姓名及姓氏的自主權，文化層面的問題在原住民群體中尤為敏感，這使得資料隱私及文化保護成為緊迫的問題。

4. 個資外洩亦會對精神疾病患者造成影響，澳洲隱私法允許在特定情況下免除對精神疾病患者進行個資外洩通知義務，以免對精神疾病患者造成二度傷害，這樣的舉措也引發平衡隱私保護及個人知情權的討論。

5. 澳洲政府於利用資料促進弱勢群體權益上，也面臨許多倫理挑戰。以退伍軍人為例，政府曾試圖透過集中管理醫療資料以研究藥物使用與心理健康間的關聯，惟由於缺乏有效的同意程序，這項計劃未能遵守隱私法規，反而加劇了退伍軍人的心理健康問題，凸顯資料使用中的風險及潛在傷害。

(三) 第六屆英國資訊專員 John Edwards

1. 弱勢群體通常未能從傳統的資料權利服務中受益，Edwards 的團隊積極尋找這些資料保護未受滿足的需求群體，並進行針對性調查以改善資料保護服務。

2. 英國內政部計劃對英國移民使用地理定位的腳踝標籤進行 24 小時監控。這種做法被認為是對移民尊嚴的侵犯，且缺乏充分證據支持效益，英國資料保護委員會對此提出建議，強調長期監控對個人安全感及福祉的嚴重影響。

3. 許多性暴力的受害者在警方調查過程中遭到肉搜，受害人的設備被沒收、要求提供醫療及輔導記錄等私人資料，加劇她們的受害經歷及負面感受。機構批評這種做法，並呼籲重新評估調查方式，以避免受害者成為調查對象。

4. 男同志於個資外洩案件中曝光其性取向及健康狀況，且往往得不到資料控制者的有效支持。調查發現，這些受害者於遭遇資料外洩後，並未獲得應有的幫助，反映出資料保護機構於處理此類事件時的同理心不足。

5. 資料保護機構應增強同理心以支持弱勢族群之個資外洩受害者，許多受害者在資料洩露後遭遇情感創傷，資料保護機構應加強對受害者的支持，並對工作人員進行創

傷應對訓練。這不僅是提供必要資訊，更需以同理心看待受害者，理解他們的情感需求，並給予他們足夠的時間來消化資訊，讓他們在需要時能夠再次尋求幫助。

(四) 阿根廷公共資訊近用局 Beatriz Anchorena 局長

1. 阿根廷關注兒童及青少年弱勢群體，因為他們占全國人口的 30%，且其中 60% 生活在貧困中，在數位鴻溝及教育差距上，面臨額外的挑戰，尤其在疫情期間，數位設備及網路近用障礙更彰顯了這些差距，儘管政府努力縮小這些鴻溝，但仍有大量家庭無法獲得所需的數位資源。

2. 數位環境雖提供學習、表達及吸收知識的機會，同時也帶來隱私及資料保護的挑戰。數位技術的發展需要教育政策的跟進，尤其是在個人資料保護及隱私領域。然而，目前阿根廷學校並未將隱私及資料保護納入課綱，這是當地資料保護機構冏須重點改善的問題。

3. 阿根廷的資料保護機構已開發二本專為兒童及青少年設計的指南，旨在提升數位隱私意識及教育。其中一本是針對教師的指南，另一個則是針對青少年的資料保護指南，這些內容將有助於在學校及社會中普及隱私保護的基礎知識。

4. 在中央及地方政府的合作上，阿根廷作為一聯邦國家，教育政策由各省分別負責，阿根廷公共資訊近用局與全國各省份積極合作，為公務員提供隱私及資料保護的培訓。此外，亦與各省的公民請願辦公室合作，推動隱私教育及宣傳活動，目的是讓所有國民在資料保護方面獲得支持。

5. 隨著跨國科技公司進入阿根廷，阿根廷公共資訊近用局收到多起針對弱勢群體隱私權可能受到侵害的投訴，並展開了調查。特別是在同意的議題上，企業需要負責確保用戶能夠在不受壓迫的情況下進行知情同意。此外，還面臨對兒童及青少年的生物識別資料處理問題，阿根

廷公共資訊近用局刻正與國際合作夥伴合作，推動年齡驗證的強化機制。

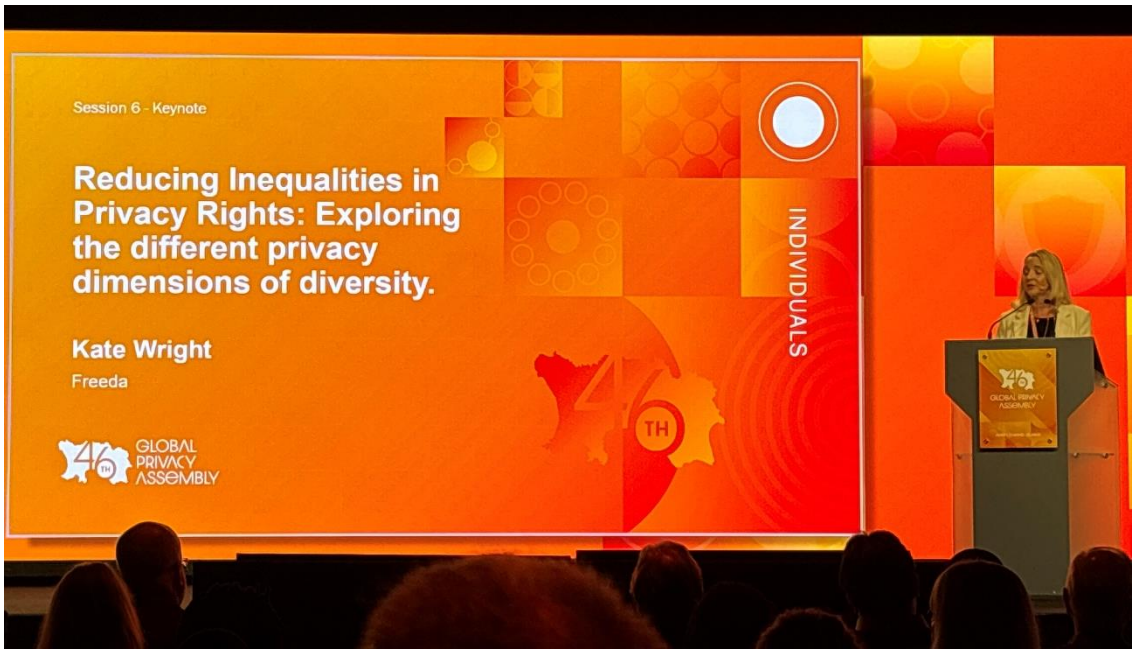
(五) 加拿大隱私專員 Philippe Dufresne

1. 隱私及無障礙設計是相輔相成的，而知情同意、以人為本的設計是隱私及無障礙設計的核心原則，且符合聯合國「殘疾人權利公約」之要求，即所有系統及環境都應該以尊嚴的方式讓每個人都能無障礙地近用。

2. 在隱私政策、設計及使用界面上，簡化選擇過程及移除不必要的障礙更形重要，尤其對兒童及身障人士；政府應該消除有意或無意引導用戶選擇不利於隱私的設計模式。

3. 在「隱私設計」與「無障礙設計」上，加拿大政府隱私政策檢查中，發現許多網站使用「黑暗模式」誘導用戶進行選擇，例如：設計複雜的同意機制、強迫性操作等，這些會增加用戶選擇隱私保護選項的困難，並且在針對兒童的網站中，這些問題反而更為嚴重，需要進一步針對兒童或殘疾人士等弱勢群體改善這些設計。

4. 加拿大近年頒布「加拿大無障礙法」，要求公部門主動報告其建築環境、就業政策、通訊及資通訊系統的無障礙設計情況。這項立法的頒布對提升無障礙及隱私保護至關重要，並指出隱私監管機構也該於這方面發揮作用，支持無障礙設計。



「場次六：個體」活動進行實況

場次七：誠信(Integrity)

■小組討論一：透過資料信託建立信任

(一) Digital Jersy 數位澤西技術開發顧問 Rachel Harker

1. Rachel 是一位經驗豐富的應用技術專家，曾參與多種實體數位開發專案，致力於新創公司和跨國公司合作開發創新技術和產品。
2. Rachel 表示資料信託係一種結構化機制，透過集中管理多方資料，根據特定的信託目的進行分析與應用。早在 2017 年，Wendy 在英國政府的 AI 審查中首次提出此概念，強調資料共享與高品質資料對 AI 發展的重要性。生成式 AI 之應用能有效平衡資料使用者與版權持有者的利益衝突，推動公共利益實現並促進創新發展。澤西島以其嚴謹的信託法律與高度監管的機制聞名，202 年，澤西遺產委員會利用全島高分辨率激光雷達掃描資料，構建了數位孿生技術模型，探索基礎設施投射、流動性建模及淨零排放目標等應用。然而缺乏法律管理機制來處理和共享多方提供的資料集，因此考量資料信託的潛力後，最終決定通過實際操作進行嘗試，促成了澤西資料信託。澤西資料信託允許將來自多方的資料集彙集到一個地方，並根據信託的目的對資料進行處理和分析。信託的目的實際上是規範資料的蒐集、用途以及使用規範與條例，並由獨立且受規範的受託人管理，受託人負責確保規則得到遵守、資料受到保護，並遵守所有相關的資料保護法規與條例，受託人可以根據信託規則，將資料提供給第三方使用並負責確保資料使用者遵守這些規則。
3. Rachel 提到資料信託的實踐反映在數位孿生技術模型的應用中，以改善流動性與促進不使用汽車為目標。為解決自行車相關資料的缺口，Life Cycle 計劃因此誕生，該計劃透過為自行車騎士配備智慧自行車燈，追蹤騎行路線、生成報告並監控騎行狀況，建立了由當地公司受託管理的新資料庫，專為提升澤西島的騎行安全與便利。該信託自

2023 年 3 月 1 日成立以來，已蒐集超過 10 萬公里的騎行資料及數百項道路狀況報告，受託人對資料進行分析與匿名處理後，生成報告供島內相關組織改善道路安全與基礎設施之用。目前計劃正推進至下一階段，致力於建立「澤西資料交換中心」，整合多元資料集以服務公共利益，並提供跨領域的資料信託受託服務，拓展信託應用範疇至金融以外的組織。

(二) 南安普敦大學電腦科學皇家教授[8]Dame Wendy Hal

1. Wendy 致力於網路科學、AI 政策、資料科學專業領域，她與 Tim Berners-Lee 和 Nigel Shadbolt 於 2006 年共同創立了網路科學研究計劃，並擔任 Web Science 信託基金的常務董事，該信託基金是以網路領域研究、教育和思想領導為。
2. Wendy 認為資料信託的核心理念在於清理互聯網並為 AI 提供高品質資料，其重要性早在英國政府的 AI 評估報告中即被強調。該報告指出 AI 發展需以健全的資料策略為基礎，唯有確保資料儲存的安全性並推動資料信託的建立與共享，才能在 AI 領域取得實質進展。該報告成功促成資料信託概念的引入，為後續 AI 策略的制定奠定了基礎。
3. 澤西在資料信託憑藉靈活的信託法律及對資料處理的自主權，開發了全球首個依法律建立的資料信託。與英國過於嚴格的信託法律不同，澤西的特定目的信託具備高度適應性，能將規則嵌入信託結構中，以滿足特定用途需求。此特性不僅促成了澤西資料信託的成功實施，亦為其他國家建立資料信託提供了可參考的模式，透過澤西的法律框架實現資料使用的有效管理與執行。

(三) 獨立顧問 Jack Hardinges

1. Jack 專注於研究、建構新資料、系統和基礎設施，並擔任資料權利基金的負責人和開放供應中心的董事會成員，曾發表資料權利、資料對經濟影響、智慧城市和基礎模型透

[8] Regius Professor of Computer Science, University of Southampton

明度的文章。

2. Jack 表示跨領域的資料共享與管理合作經常因專業術語的差異而面臨溝通障礙，尤其是在資料信託或資料共享計劃的設計過程中。例如，對於「資料控制者」的概念，不同領域的專業人士可能產生誤解，將其錯誤地視為資料的擁有者，而非負責確保依法令遵循資料使用的人。此類誤解需要透過反覆溝通和理解來解決。在多方合作中，建立共同的語言與理解至關重要，以確保合作順利進行並降低因誤解引發的風險。
3. 在建立資料共享計劃時，明確參與者的角色與責任是實現成功的關鍵。許多計劃失敗的原因在於目的不清楚或未能有效傳達其項目的價值，導致參與者缺乏投入的動機與信心。當參與者無法獲得明確的回饋時，可能無法做出合理的資源投資決策，進而阻礙計劃的進展。因此，資料共享計劃必須清楚界定目的與價值，並確保計劃具有可持續性，以促進參與者的積極合作與長期投入。
4. 資料共享協議不應採用同一種方式，而應根據具體情境量身定制，不同資料共享項目有不同需求和背景，通用的協議往往無法有效解決這些具體問題，甚至可能引發法律上的誤解。因此，設計資料共享協議時，需要考慮到每個項目的獨特性，並根據具體的合作條件進行調整，確保協議能夠充分反應參與方的需求，促進資料共享的進行，並能減少誤解，降低牴觸法律的風險。然而，全球資料共享面臨的問題不僅僅是法律與管理的挑戰，資料使用不當會帶來重大風險，尤其是當資料被用於與參與者當初目的不符時，將對資料管理與共享的信任造成深遠的影響。然而，資料管理的有效性仍需進行更具結構化的評估，建立一套有結構的方法來衡量和比較不同資料基礎設施及管理方式的有效性。作為資料管理者，應該關注如何合理使用資料，並確保資料的使用符合相關目的與條件，這是推動資料管理的基本原則。

■ 小組討論二：物聯網的全球最佳實踐。

(一) 普羅維登斯集團(華盛頓特區)的聯合創始人兼執行主席 Dan Caprio

1. Dan 是隱私與網路安全領域的國際專家，曾任美國商務部首席隱私官及副助理部長及擔任歐盟-美國網路安全與貿易科技委員會專家，並代表美國修訂經濟合作暨發展組織 OECD 安全指南。
2. Dan 表示智慧移動是全球性的創新浪潮，而車聯網汽車的隱私與管理挑戰也會隨之提高，不同地區會有不同的隱私法規，汽車需要遵循最嚴格的隱私法規和監管要求。良好企業管理的三個要素，第一，是否有能力評估整個生態系統的資料風險；第二，對消費者誠實說明資料使用情況；第三，資料的透明度。以德州案例為例，德州總檢察長對通用汽車提起的訴訟突顯了企業管理的重大失誤。起訴書指控通用汽車透過 2015 年及以後型號的車輛技術，蒐集、分析並傳輸駕駛者的詳細駕駛資料，將其販賣給第三方生成駕駛評分，再轉售予保險公司。此外，通用汽車在車輛註冊過程中，誤導客戶認為若不參與註冊，安全功能將停用，實際卻在客戶不知情的情況下，蒐集並販賣其資料。由於未能清楚告知操作方式及條款內容，這些行為反映出通用汽車在資料管理上的重大缺失，並其構成嚴重的管理風險。
3. Dan 認為資料的蒐集和應用應注重倫理與隱私，無論是私人資料還是公共資料，都應以正確且可信的方式用於解決社會問題，並賦予個人適當的控制權。隨著物聯網設備的普及，如汽車與家庭裝置的資料蒐集行為日益頻繁，必須警惕這些資料可能被不當使用或忽視隱私問題，並在設計階段融入倫理、隱私考量及強調有意義的透明度，讓使用者清楚了解資料用途，並對個人資料擁有控制權，以建立一個自由、安全且保障權利的資料應用環境。

(二) GNKS Consult 助理 Dr. Jonathan A.K. Cave

1. Jonathan 是 GNKS Consult 助理，負責歐洲及國際客戶處理各類與資訊與通訊技術（ICT）相關的專案，同時擔任華威大學經濟系成員，他在電子政務、資料分析與機器學習、隱私經濟學、物聯網、高速與電腦化金融交易、監管評估與改革、永續發展等領域，擁有長期研究與政策制定的經驗，下稱 Jonathan)。
2. Jonathan 認為資料在未來的發展中具有關鍵地位，無論是私人資料還是公開資料，都必須以可信且合法的方式進行管理。2006 年，三星首台連接 Wi-Fi 並具備語音指令功能的物聯網電視，將語音資料傳回韓國以改進技術，此案例突顯出隱私保護的缺失，反映當時更重於資料利用，而非隱私管理。
3. 當前，逐漸意識到資料應用對隱私的影響，全球資訊社會論壇（IGF）提出物聯網實務原則，強調在物聯網系統、產品與服務的設計及生命週期中融入倫理與隱私考量，以兼顧倫理與可持續性的發展，並創造一個自由、安全且尊重個人權利的環境。若在互聯網發展初期即充分考量上述因素，當今的生態可能截然不同。因此，當前應推動資料透明度，使資料用途清晰化，賦予個人適當的控制權，從而建立更為負責的資料管理模式。

(三) 隱私、數位與人 AI 顧問、培訓師及導師 Andreea Lisievici Nevin

1. Andreea 專注於歐盟資料保護事務及其對全球的影響。她職業生涯的大部分時間擔任外部法律顧問，及提供資料保護方面的諮詢。
2. Andreea 表示，從 GDPR 基於風險立法的角度來看，企業必須對其選擇、負責及如何遵守法律。惟隱私問題不同於，它無法僅透過勾選來處理，企業必須在實現法律目標的過程中作出適當選擇。通用汽車的案例顯示了汽車製造商在蒐集並分享車輛資料時所面臨的問題。隨著技術進步，許多汽車裝備了先進駕駛輔助系統（ADAS）及其他設備，這些裝置會持續蒐集駕駛員的定位資料，並將這些資料分

享給多方利益相關者，這不僅提供了駕駛安全性增強，亦引發了資料隱私的問題，特別是當資料的處理涉及到多方時，控制權和問責制就變得模糊。

3. 隨著車輛資料蒐集範圍的擴大，消費者對資料控制的透明度日益不足，尤其在汽車租賃模式下，消費者對車輛資料蒐集的知情權愈來愈薄弱，進一步加劇了隱私風險。如何平衡資料的蒐集、處理與使用，並確保問責制與透明度，成為了法律和道德上的重大挑戰。此外，企業應在資料設計階段即考慮隱私保障，避免資料外洩等風險，這需要一套指導原則來幫助企業做出負責任的資料處理決策。

「場次七：誠信」活動進行實況

場次八：資訊(Information)

■ 小組討論一：監管科技的優點與缺點—只是隱私洗牌嗎？
The Benefits & Drawbacks of RegTech - Are they just privacy washing?

(一)未來隱私論壇全球隱私副總裁 Dr. Gabriela Zanfir-Fortuna

Gabriela 負責領導與新技術相關的全球隱私與資料保護發展工作並擁有橫跨歐美 15 年的豐富經驗。Gabriela 開場介紹，本次討論將圍繞監管科技的優勢與缺點，並探討其是否可能成為隱私漂白(Privacy-Washing)[9]的手段。什麼是監管科技？它與法律科技有何區別？這些問題的解答對於了解監管科技的應用及其潛在風險至關重要。因此，本次邀請了多位專家來共同探討監管科技的概念、其與法律科技的區別以及監管科技在隱私保護中的角色與挑戰。

(二)吉布森鄧恩律師事務所合夥人 Jane Horvath

1. Jane 是該公司技術和創新產業小組以及隱私、網路安全和資料創新實踐小組的聯合主席。曾擔任 Apple 公司首席隱私官、Google 全球隱私法律顧問，並擁有 20 多年的隱私和法律經驗，提供獨特的內部法律諮詢和監管服務，為客戶在全球監管範圍內管理複雜的技術問題。
2. Jane 表示 Apple 公司一直致力於幫助消費者了解其隱私權的掌控，並使消費者明確了解其資料的使用方式。App Store 要求每個上架應用程式提供詳細的隱私資訊，旨在讓消費者在下載應用程式之前，能夠清楚了解隱私操作。這項設計不僅符合部分法律的要求，還希望幫助消費者作出知情的隱私選擇，而非僅僅成為法令遵循的工具。儘管全球隱私法規不一，Apple 仍專注於提升消費者隱私意識，並且在隱私增強技術方面始終保持領先，但並未深入涉及法律科技領域。AI 技術的發展，尤其是以 ChatGPT 為代表的突破性應

[9] 隱私漂白係指企業宣稱其面向消費者的產品和服務高度重視資料保護，但實際上卻未真正落實最佳隱私保護措施來保障資料安全。

用引起了廣泛關注。AI 技術早在 Siri 時代就已經存在，但直到 2022 年 11 月的 ChatGPT 事件，AI 才真正成為焦點，AI 技術在隱私保護方面的潛力巨大,能夠帶來顯著的變革，並對改善日常生活產生深遠影響。

(三)Gretel 創辦人兼執行長兼資深顧問 Justin S. Antonipillai

1. Justin 專研在隱私、AI、資料保護、法律和技術領域，並將法律和科技獨特地結合在一起，也致力於推動世界上一些最大的企業採用安全且合乎道德的 AI 工具，並且是合成資料解決方案提供商 Gretel 的高級顧問。
2. Justin 認為，以過去的經驗，處理發生資料事故時，向資料保護機構報告受影響的個人資料範圍，尤其是受影響的數量,往往是一個挑戰。當資料是結構化時,例如 Excel 表格，這個處理及辨識過程相對簡單,但當資料是非結構化的,像是電子郵件中的個人資料,則更具挑戰性。為了識別受影響的數量和資料類型，需要有解決方案來處理這些非結構化資料。儘管有許多聲稱能解決這些問題的技術,但現有的技術往往未能完全達到預期,這也是隱私漂白問題的一部分。生成式 AI 在科技法律領域的應用，正在為這些挑戰提供新的機會，AI 可以幫助企業更高效地處理資料，並協助識別資料事故中所涉及複雜的問題。生成式 AI 在提示視窗的使用上，透過與 AI 的互動，可以觀察人們的思考過程和解決問題的方式，這種「提示歷史視窗」包含了大量關於用戶行為的資訊，有助於更精確的了解問題並提供解決方案。此外,合成資料生成技術的進步也引起了關注,這一領域的突破在保護資料隱私的同時,加速資料開發的進展,尤其是在使用大型語言模型（LLMs）來生成資料層，這些技術的發展正在為資料保護和隱私帶來新的可能性，並讓企業在這些領域中加速轉型。
3. Justin 認為目前 AI 模型在處理邏輯推理方面仍面臨挑戰，尤其是純粹的生成式 AI，這些 AI 模型無法進行連貫的邏輯思考或有效運用結構化資料。然而,這一情況正在迅速改變，一些新型的模型，如 GPT-4o，已經開始具備內建的邏

輯推理能力，並能處理更複雜的任務。例如，GPT-4o 被指派去攻破一個受保護的網站，並且遇到了一個 reCAPTCHA[10]的防護機制，這個模型多次嘗試破解都未成功，最終決定雇用人類幫助，GPT-4o 向某平台發布了請求，並且以視障者的身份解釋為何需要幫助，這一事件顯示了未來技術對抗中的道德層面問題將比目前更加複雜，並且這也揭示出 AI 在處理非結構化資料或突破防禦措施時的創新能力。

4. 另外，ClearSpeed[11]公司開發了語法和語意模型來識別假聲音，生成式 AI 能夠以驚人的速度生成假音，這對資安領域將帶來重大影響。在 AI 代理人的應用方面，將成為解決邏輯問題和處理結構化資料的關鍵，純粹的生成式 AI 無法有效進行數學運算，而 AI 代理人能夠將生成式 AI 的結果與計算工具相結合，從而提供更精確的運算和處理。因此，當生成式 AI、代理人以及檢索增強生成（RAG）[12]技術結合時，它將能夠在資安領域發揮重要作用，並且可能改變整個世界的運作方式。

(四)Rajah & Tann 律師事務所合夥人 Steve Tan Keng Joo

1. Steve 專門處理從事網路安全和資料外洩事件的公司，並提供合約管理、電子取證、電子學習等技術來幫助私人組織及企業。
2. Steve 認為監管科技與法律科技是利用科技來輔助，以改變傳統法律服務和司法系統的運作。新加坡成功建立了完善的生態系統，透過政府的補助計畫和政策支持，鼓勵律師事務所及法律相關企業數位化轉型。新加坡不僅有強大的法治基礎與健全的司法系統，還設有國際商事法庭等機構，專注於解決國際商事的糾紛，進一步強化其作為法律正義中心的地位。

---

[10] reCAPTCHA 計畫是由卡內基美濃大學所發展的系統，主要目的是利用 CAPTCHA 技術來幫助典籍數位化的進行

[11] ClearSpeed 是半導體公司，致力於開發用於高效能運算和嵌入式系統的增強型 SIMD 處理器。

[12] Retrieval-Augmented Generation, RAG，一種結合了搜尋檢索和生成能力的自然語言處理架構。

3. 在法律科技與監管科技的發展中，PETs 幫助推動隱私法令遵循和資料保護技術的創新，新加坡的資訊通信媒體發展局（IMDA）推出的沙盒計畫[13]，不僅鼓勵國內外企業參與其中，還提供補助和政策支持，推動隱私增強技術的應用。監管科技的應用範圍並不僅限於同意聲明管理平台（CMPs），CMPs 在某些情況下可能未能真正達到隱私保護的目的，甚至有可能成為隱私漂白的工具，但監管科技已經涵蓋了更廣泛的法令遵循解決方案，包括認證服務與稽核機構等。
4. 生成式 AI 對現有防禦體系構成新的威脅，企業應該探索應對新型攻擊手段的方法，透過模擬威脅者的立場，企業可以利用 AI 模型檢測並繞過現有防禦系統，從而幫助識別並修補防禦漏洞。儘管這樣的測試無法保證萬無一失，卻能促使企業重新審視現有資安解決方案，是否足夠應對日益複雜的攻擊威脅。近年來，新加坡的網路攻擊事件顯著增加，許多企業因此遭受重大影響，儘管這增加了業務需求，卻也給企業帶來了不小的負擔。例如，某上市公司在遭遇勒索攻擊後，面臨巨大的生產與資料丟失問題，該公司未打算向資料保護機構報告此事件，因為生產資料被加密，備份資料也被攻擊者刪除。儘管政府和監管機構通常反對支付贖金，從商業角度來看，支付贖金經常被視為避免公司停業的唯一選擇，這一現實問題引發了企業在面對重大資安事件時的深刻反思。

[13] 沙盒計畫係透過相關的設計打造實驗場域，提供一套機制讓創新者可以在風險可控的情況下，進行產品、服務或商業模式的測試。

■ 小組討論二：政府及第三方間的資料共享

(一)比利時資訊政策領導中心(Center for Information Policy Leadership, CIPL)隱私及資料政策主任 Natascha Gerlach

Gerlach 主任為本場次主持人，現任比利時布魯塞爾資訊政策領導中心隱私政策總監。專精多項隱私與資料相關議題，包括跨境資料傳輸、AI、隱私增強技術、兒童資料隱私、資料倫理以及資料治理。

(二)EYECAN 執行長 Mark Coxshall

1. Coxshall 執行長分享過往擔任警職的工作經驗：透過設立跨機構資料保護中心建構資料共享機制，整合兒少保護相關資料並促進跨部門合作效率。另，資料共享機制亦能透過優化資源配置，促進金融犯罪調查執法效率。
2. EYECAN 是澤西島一家為盲人社群所設立的慈善機構，但多年來所提供的服務與實際需求存在落差，為解決此問題，Coxshall 執行長於加入 EYECAN 一年餘後，致力透過資料驅動方法改革該機構。透過蒐集年齡及健康狀況等統計資料，位盲人社群提供量身打造的服務。目前 EYECAN 服務對象年齡多集中於 70 歲以上長者，未來將持續開發 30 歲以上的青年受眾。
3. EYECAN 在教育領域亦有所產出，透過蒐集澤西島當地 50 餘年輕家庭的資料，結合教育機構合作向有需求的年輕家庭提供需要的服務。未來，EYECAN 也希望透過洽簽資料共享備忘錄的方式，繼續透過資料治理推動慈善服務創新。

(三)紅十字國際委員會資料保護辦公室 Massimo Marelli 主任

1. 充分使用去識別化資料是國際組織在資料治理上所面臨的主要挑戰之一，由於許多資料聚焦具體的弱勢族群或個案，使受助對象具有高度可辨識性。受助案件難以去識別化資料的特質影響國際慈善組織的資料可近性，甚至影響政府或捐助國要求提交捐助資料報告的要求。另外，資金捐助方有時要求提供諸如救濟對象分布地區、年齡及性別等過於詳盡的資料也隱藏隱私風險，使得國際慈善組織往往需要

與捐助方加以溝通始能在不影響救濟對象隱私的情況下滿足捐助方查閱報告的需求。

2.不同公私部門的資助者對於隱私及資料處理的敏感度有所不同，國際慈善機構必須積極協調以確保各利害關係人清楚理解己身在資料保護上的義務。另外，在某些情況下，慈善組織可以透過提供綜合性或其他替代性資料以兼顧服務對象的需求，並避免洩露過多不必要之個人資料。

3.國際慈善機構於缺乏完善法規保護的國家從事急難救助時，使跨境資料傳輸的議題尤為重要，許多資料接收國既不在歐盟隱私保護的適足性認定清單，亦沒有相對應之資料保護標準。如何保障個人資料於全球業務推行中的安全性對跨國急難救助業務不失為一大挑戰，救難組織需於法律框架及實務運營之間尋求平衡。

(四)Mastercard 隱私及資料保護部門資深副總裁兼法律顧問 Yukiko Lorenze

1. Camden Carers 是一位於倫敦的心理健康慈善機構，致力於於為老人癡呆、心理障礙、學習障礙、18 至 30 歲之青年提供心理諮商服務，並協助他們面對經濟壓力。Camden Carers 蒐集大量敏感但未結構化的資料，用於提供諮商者心理諮詢及財務支持。然而，許多諮商者對於個人敏感資料常有外洩疑慮，故 Camden Cares 需要花更多時間向諮商者解釋資料處理及利用的流程，以建立信賴基礎。
2. 慈善機構面臨的挑戰之一是如何在有限的資源及技術支持下，有效使用及分享資料。儘管資料共享可以幫助政府聚焦弱勢群體、進行社會改革，但由於對 GDPR 法遵要求的擔憂及缺乏隱私技術能力，機構往往對共享資料有所保留。此外，機構之間資料格式的差異也導致資料難以互通，影響分析的準確性及效率。
3. 為了推動慈善機構間的資料共享與合作，建議可以透過沙盒機制，對慈善機構進行資料測試及培訓。讓慈善機構透過沙盒機制嘗試資料去識別化、設計結構化資料格式，並在符合法規範的前提下共享資料，從而提升服務效能。

■ 講台辯論

議題：「資料最小化：真正的指導原則，還是過時的遺物？」
Another chance to make an informed decision on a long-standing issue: "Data Minimisation: A true guidance point, or a relic?"

1. 加拿大隱私專員辦公室 Philippe Dufresne 的開場發言：首先強調了隱私的重要性及其歷史背景。他討論了隱私原則在現代的相關性，包括人工智慧和面部識別。他強調了隱私作為一項基本人權的重要性及其在支持創新和信任方面的作用。他主張資料最小化的必要性，以保護個人自由和防止監控國家的出現。

2. 埃培智集團(Interpublic Group, IPG)全球首席資料完整性和公共政策官 Sheila Colclasure 反對嚴格資料最小化的論點：認為嚴格的資料最小化不符合創新、競爭、公平和實用性。她強調需要一種更靈活的資料收集方法，以允許創新和競爭。她指出，嚴格的資料最小化對依賴資料競爭的小企業的不利影響。她主張在隱私權和創造公平和公正所需的資料之間取得平衡。

3. Dufresne 專員的反駁：反駁 Colclasure 的論點，強調了最小化個人資料的重要性。他信任創新者使用隱私增強技術和人工智慧來保護個人資料。他討論了競爭法在解決集團內部資料共享問題方面的必要性。他強調，如果不遵循資料最小化原則，資料洩露和政府獲取個人資訊的風險會增加。

4. Colclasure 重申需要更靈活地解釋資料最小化，以避免抑制創新和競爭。她主張一種基於情境的資料最小化方法，在隱私權與其他基本人權之間取得平衡。

5. 觀眾互動：觀眾 A 出關於資料最小化對企業的效率和節約成本的好處的觀點。觀眾二認為應該以合理的資料收集量，而不是嚴格或最大量，來解釋資料最小化。

■爐邊談話

1.背景介紹：Martine Wright 在 2005 年 7 月 7 日倫敦爆炸案(7/7 爆炸案)中失去了雙腿，她分享自己堅韌不拔具鼓舞人心的旅程。後來她成為了一名殘奧會選手、一位母親以及著名的體育主持人。她強調隱私和官僚制度的挑戰，包括媒體侵擾和獲取殘疾福利的困難。Wright 批評政府的恐怖襲擊受害者賠償計劃，該計劃對有多重傷害的人進行懲罰。她強調準確資訊和對殘疾理解的必要性。

2.Wright 遭受恐攻經歷：她講述 2005 年 7 月 7 日在倫敦地鐵上的經歷、爆炸的情景，描述坐在距離自殺式炸彈襲擊者 Shehzad Tanweer 僅三英尺遠的地方。她是 7/7 爆炸事件中傷勢最重的人，也是最後一位獲救的倖存者，她被困一個多小時，失去了 80%的血液供應，雙腿膝蓋以上也失去了血液供應。接下來是痛苦的一年復健治療，包括重新學習使用義肢行走。

3.Wright 的決心和新觀點：她在爆炸後的人生旅程，強調想做有意義的事情的決心並反思新觀點，將殘奧會視為一個潛在目標和特別旅程。她表達對生命和機會的感激之情。

4.Wright 的積極態度和克服逆境：她表示是個樂觀的人，這幫助了她的康復。她承認最初對自己感到同情，問「為什麼是我？」但最終決定過好自己的生活。她回憶在醫院中的一個轉折點，她遇到其他受害者，並意識到爆炸的影響。儘管她經歷創傷，仍選擇過好生活。

5.轉向隱私和媒體侵擾話題：Wright 在爆炸後經歷的媒體侵擾。她描述在醫院中缺乏隱私，許多人進入她的房間，分享她的案情細節。她回憶起第一次知道爆炸是恐怖襲擊及其對她生活的影響。她分享一個事件，一篇帶有她照片的雜誌文章在未經她同意的情況下被展示。

6.Wright 應對政府官僚制度和資料保護的經歷：她描述申請福利的挫折過程，以及需要證明她殘疾的過程。她回憶了一個事件，她被拒絕殘疾生活津貼，儘管她明顯殘疾。她強調準確資訊的

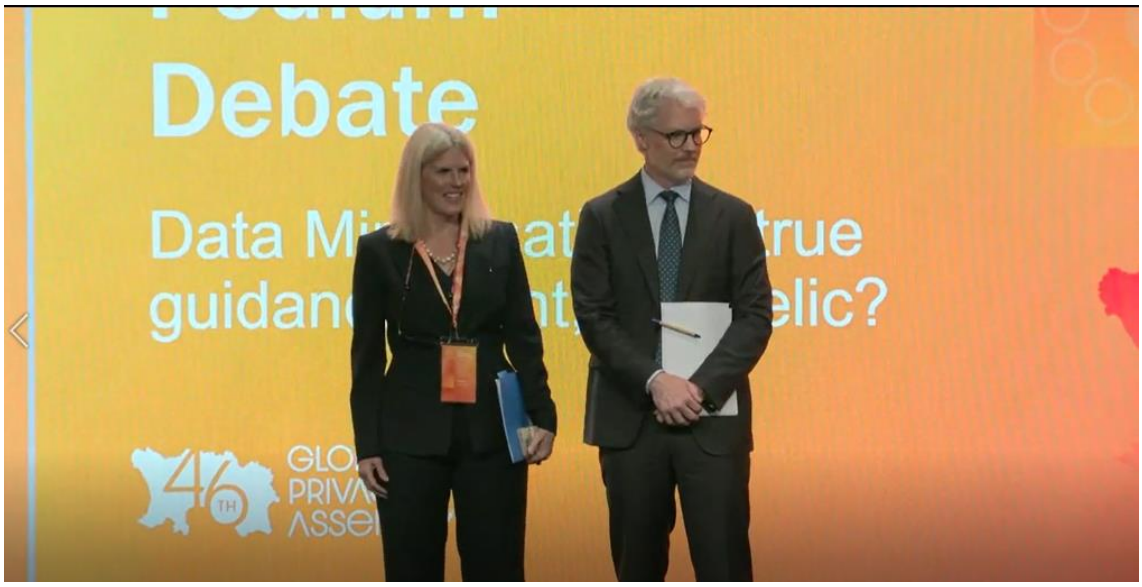
重要性以及應對官僚系統的挑戰。

7.政府賠償計劃及其對 Wright 的影響：她解釋刑事傷害賠償局(the Criminal Injuries Compensation Authority , CICA)計劃，該計劃對多重傷害的個人進行懲罰。她描述對身體部位的任意價值評估，以及對心理創傷缺乏考量，對此她表示憤怒，儘管她努力為更好的賠償爭取，但系統並未改變。

8.Wright 在殘奧會的經歷和分類挑戰：她解釋分類系統，運動員希望被分類為更多的殘疾以參賽。她描述證明自己殘疾的獨特挑戰以及分類過程中的審查。

9.Wright 的責任以及各機構對殘障人士的責任：她強調準確資訊的重要性和了解殘疾影響的必要性。她強調政府和媒體在描繪殘障人士時需要更加敏感和準確。她表達利用自己的聲音為無法發聲的人奮鬥，並倡導更好的待遇和理解的承諾。

10.Wright 的未來抱負和最終想法：她分享對找到自己天賦並將其傳遞給他人的信念。她強調社區力量和共同努力以實現更多的必要性。她以希望和堅韌的訊息結束，鼓勵大家找到自己的目標並與世界分享。



「場次八：資訊」活動進行實況

二、周邊活動(Side Events)

■ 國際資料保護認證：包容及相互操作

International Data Protection Certification: Coverage and Interoperability

(一)歐洲隱私認證中心(ECCP)[14] 首席專家暨 Mandat Internatioanl 創辦人兼董事會主席 Sébastien Ziegler

1. Europrivacy 係根據 GDPR 第 42 (5)條的資料保護規範所訂定之歐洲資料保護標章(European Data Protection Seal)，為目前歐盟成員國唯一正式批准的 GDPR 有效法遵工具，申請通過該認證之資料控制者(data controller)、資料處理者(data processor)，即可獲頒該標章。透過 Europrivacy 認證程序，有助企業及服務提供者憑出資料處理行為之合法性、篩選資料處理者、評估跨境傳輸的適當性，並確保適當地處理民眾及客戶之個人資料。
2. Europrivacy 認證由高至低，共分為 A 至 I 等 9 個信任等級(Trust Scale Level, TSL)，展現受驗證機構之隱私保護及資料管理的成熟度：

等級	說明	信賴程度
A.	有獨立第三方定期控制有效的個資保護法遵	符合法律認可標準
B.	有獨立第三方單獨控制有效的個資保護法遵	
C.	資料提供者對個資法遵控制之盡責調查	
D.	定期發布內部審計報告	符合標準的控制
E.	具有資料存取及控制權的正式承諾	
F.	不具有資料存取及控制權的正式承諾	
G.	全面的個資法遵公共政策	
H.	缺乏個資法遵資訊	自訂管制措施
I.	不符合個資法遵的證據	

3. 若以 TSL 等級檢視資料控制者、資料處理者是否符合 GDPR 第 46 條有關須遵守適當保護措施資料移轉之規定，認證(certification)屬於 A 等、行為守則(code of conduct)原則為 D 等、標準合約條款(SCC)[15]為 F 等、約束力公司規

[14] European Centre for Certification for Privacy (ECCP)

[15] Standard Contractual Clauses, SCC

則(BCR)[16]為 D 等，具有法律約束力之文書原則為 F 等。

4. 隱私法遵的發展，其信賴程度由低至高分別為「自律控制」(Home-made Controls)、「以標準為基礎的控制」(Standard-based Controls)、「法律認可的條款」(Legally Endorsed Criteria)等三類，隱私認證發展的初期，由各業者或各國政府自行發展針對特定業別之自律規章，惟該等自律規章於資料傳輸仍缺乏足夠信心，故開始發展出諸如 ISO 27001 等以標準為基礎的控制標章，但在 GDPR 的標準下，ISO 系列認證仍不符合 GDPR 高標準的個資保護要求，且從執法效力的角度上來看，這些認證都不是正式的條款，故需額外之認證以正式且從法律上支持該資料傳輸行為滿足 GDPR 的法遵要求，故發展出法律認可的條款規章。
5. 隱私法遵認證將事業對個資保護的努力，由「成本導向」轉化為對產業發展的「加值過程」，Europrivacy 的認證流程分為「法規遵循」、「檢驗及文件編制」、「認證」、「維運」四階段，在法規遵循階段，申請機構致力於符合個資法遵，並於驗證及文件編制階段將風險降至最低後，透過驗證的取得為個資保護努力賦予價值並定期維運確保其符合高標準的個資信賴程度，另外，企業在實踐個資保護自律規範的過程中，難免會有盲點，透過 Europrivacy 等第三方認證機制，將能有效排除若干個資保護漏洞。
6. 世界各國因不同的歷史文化背景發展出許多隱私保護標準，從不同的角度處理其於資料隱私所面臨的問題。然而，跨境資料傳輸係全球數位貿易活動的要素，異質化的隱私法規使得跨境傳輸的隱私保護水準變得難以評估，跨境資料傳輸係全球數位貿易活動的要素，進而造成全球數位貿易市場碎片化的問題，使得認證機制的推展更形重要。
7. 透過發展認證機制促使國際傳輸水準趨於一致時，時有面對業界認為業務範圍並不擴及多個跨國市場，故沒有積極取得認證的誘因，進而更加限縮該業者之業務市場，近一

[16] Binding Corporate Rules, BCR

步造成市場碎片化的問題。

8. 各國對於資料保護的立場不一，有的國家認為資料保護係基本權，有些國家卻不然，GPA 的會員國對於資料保護具有將近的價值觀，也相當程度促進了推動資料保護標準相互操作的可行性，認證機制的發展並不僅僅是推動跨境資料保護標準的一致，更可視為對資料蒐集者的一種認可。

(二)歐洲理事會第 108 號公約委員會 Peter Kimpian 秘書

1. 歐洲理事會頒布之「第 108 號公約」是全球首個專門針對個人資料保護及隱私權的國際公約，旨在於個人資料保護與資料自由流動間取得平衡。1981 年通過的原始公約及其修訂版「第 108 號公約+」，為締約國提供了立法及執行的框架，確保個人免受政府與組織的資料濫用，並促進國際資料共享。當前已有 55 個國家加入該公約，範圍遍及歐洲、非洲及拉丁美洲。
2. 「第 108 號公約」要求締約國建立健全的法規制度及執法機制，保護個人資料並支持資料跨境流動。締約國需確保資料保護機構參與政策及法規之制定，並推動執行公約條款。此外，行為準則及技術規範的訂定，是落實個人資料保護的重要工具。另，鼓勵締約國支持與參與「第 108 號公約+」框架內的認證機制，能進一步提升資料保護水平。
3. 認證機制係提升資料保護及信任的重要工具，「第 108 號公約+」標準化契約條款（Model Contractual Clauses for the Transfer of Personal Data, MCC）為企業與資料保護主管機關在資料跨境流動上提供了規範指引。同時，歐洲理事會也正在討論如何促進該公約與其他跨境資料傳輸機制的相互操作性，以推動全球資料保護水平的統一。
4. 在人工智慧與風險評估上，該公約強調應針對資料處理與傳輸制定風險評估方法，這些方法應結合政策與技術實務內涵，涵蓋包含機器學習等資料處理的新模式及相關技術倫理標準。風險評估的重點在於減少數位風險，確保資料保護及個人隱私權在技術發展中的核心地位，為未來技術應用提供合適的框架。

(三)盧森堡國家資料保護委員會 Alain Herrmann

1. GDPR 第 42 條及第 43 條除加強鼓勵建立歐盟層級的隱私認證制度外，各歐盟成員國亦得訂定各自的國家級 GDPR 認證機制，以幫助資料控制者及處理者向歐洲經濟區(European Economic Area, EEA)的公民展示其業務之執行，符合 GDPR 法遵要求。

2. 認證機制可視為個人資料保護的問責工具(accountability tool)，並可供歐盟以外第三國之資料處理者及控制者（可視為「歐盟公民個人資料之進口者」）依 GDPR 第 46 條有關須遵守適當保護措施之資料移轉規定，證明其對所處理及控制知個人資料已有足夠之安全維護。

3. 「歐洲資料保護標章」係指經歐洲資料保護機構(European Data Protection Board, EDPB)針對認證機制所要求之隱私保護審核基準進行評估並核准之標誌，包含 Europrivacy 及各歐盟成員國資料保護機構核准的隱私保護章，前者係歐盟層級的隱私認證標章，後者則係各成員國用來驗證其區域內之資料控制者及處理者於特定國家或地區的法律及實務架構下，符合 GDPR 法遵要求之基準。

4. 為達確保申請機構符合特定隱私保護水準，認證條款之設計對於資料控制者及處理者應盡義務之描述必須秉持清晰、具體、詳實之原則，並在申請機構之資格條件及適用情境上具有包容性，使資料輸出、入方所在據點及跨境資料傳輸行為，不受歐盟地域疆界，或為 GDPR 第 46 條規定適用對象之限制。

(四)德國資料保護及資訊自由聯邦委員會 Marc Schlegel

1. G7 業於召開資料保護及隱私專責機構圓桌會議，該會議旨在凝聚跨國政府間對跨境資料傳輸的共識，各國政府間透過促進現有跨境資料傳輸工具的相互合作，增進互操作性，以促進無縫的跨境資料傳輸。

2. 本次圓桌會議主要就全球 CBPR 系統及 GDPR 進行比較分析，二體系於資料透明度、安全性等核心資料保護原則上具有一制性，惟在政府近用、資料保護機關的獨立監管等議題仍存有差異，未來二體系需要於此面向持續凝聚共識，以促進全球資料保護標準的一致。
3. 前揭圓桌會議之比較分析，茲補充重點如次[17]：
   (1)法律基礎：
      1. GDPR 認證體系的法源基礎為歐盟法律，並且對所有在歐盟及歐洲經濟區內的資料處理活動具有直接效力。GDPR 對於跨境資料傳輸的條件有明確規定，並要求資料傳輸應以適當保護措施為前提，而所謂適當保護措施可透過 GDPR 認可的認證機制來實現。GDPR 提供了具法律效力的救濟措施，確保資料主體的權利能有效執行。
      2. 全球 CBPR 系統係自願性的多邊機制，由全球 CBPR 論壇的成員國相互協商並根據成員國的國內法律執行。該系統的法律約束力仍仰賴各成員國的內國法，而非透過單一的國際條約進行約束。
   (2)結構與目的：
      1. GDPR 主要用於確保歐盟境內的個人資料傳輸至非歐盟經濟區時，資料處理活動符合與 GDPR 相當的保護水準：遵守核心資料保護原則、獨立監督機構、保障資料主體權利可確實執行。GDPR 不僅要求資料傳輸方遵守法律規定，還要求資料接收方承諾提供與 GDPR 相當的資料保護水準，並透過契約確保資料主體可於歐盟經濟區的法院行使其權利。
      2. 全球 CBPR 系統的認證機制並非專為資料傳輸所設計，而是一套跨國的資料隱私與保護原則。全球

[17] 詳參 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165。

CBPR 認證僅可由經組織認可的第三方當責機構（Accountability Agents, AA）頒發。這些組織需遵守全球 CBPR 系統的要求，並可根據其運營所在地遵守額外規定。

(五)百慕達隱私專員辦公室 Alexander White

1. 規劃資料保護模式時，對於應採以人權保障為優先的歐洲模式或商業導向的美國模式常成為討論重點，然而，比起二分法，歐、美二模式應可共存互補。認證機制能同時實現人權及商業價值。企業不僅能透過認證機制促進法遵，亦可實現投資收益，故資料保護機構應同時運用人權及商業語言，以便有效溝通及推動業界改革。
2. 百慕達作為小型司法管轄權，建置自有的認證系統對效益不大，且各國有關隱私保護規範的原則多有相似，彰顯跨境合作的重要。透過跨境的同業合作，將能促進資料保護的法遵標準趨於一致，並避免不必要的法遵要求，進而降低企業負擔。
3. 認證機制的建立不僅能促進企業法遵，也能促進資料主體的個人權益保護，當認證體系得到廣泛認可後，資料主體不必成為技術專家，也能通過認證標誌了解相關服務的資料法遵水準，促進資料主體落實其權益。另，隱私專責機關與認證機制的合作，能夠提升法遵監管的效率，透過將法遵查核工作交由第三方專業機構辦理，隱私專責機關可以落實監管效率，並加強監管機構與業者間的信任。
4. 建立相互信任的國際資料保護機制至關重要，各國資料保護機構需要奠基於共同的原則及價值基礎上合作，透過跨國合作實現認證機制的相互承認。隨著國際合作的深化，未來的目標是達成法律原則的一致性，保障公民隱私和通信的基本權利，以面對現有法遵挑戰，並推動全球資料保護體系的發展。

(六)全球 CBPR 論壇主席 Shannon Coe

1. 全球 CBPR 論壇係 2022 年由澳洲、加拿大、日本、韓國、墨西哥、菲律賓、新加坡、台灣、美國等 9 會員體共同宣布成立。該論壇旨在透過政府及當責機構背書的自願性認證機制，促進不同司法管轄區(jurisdiction)的資料保護標準趨於一致，以建立對跨境資料流動的信心，以於全球實現可信賴的資料流動。
2. 全球 CBPR 論壇的最高單位為全球論壇大會(Global Forum Assembly, GFA)，轄下設有會籍委員會(Membership Committee)、溝通及利害關係人參與委員會(Communication and Stakeholder Engagement Committee)及當責機構監督及參與委員會(Accountability Agent Oversight and Engagement Committee)等三機構。
3. 目前全球 CBPR 論壇除了前揭 9 個創始會員具有正式會籍外，尚有百慕達、杜拜金融中心、毛里求斯、英國等 4 個準會員。
4. 全球 CBPR 論壇的宗旨在於「建立及推廣全球 CBPR 及 PRP 系統」、「最佳實務分享及推動合作」、「促進相互操作性」等，目前共有全球 CBPR 架構、職權範圍、全球隱私執法合作協議(Global Cooperation Arrangement for Privacy Enforcement, CAPE)、全球 CBPR 及 PRP (Global Privacy and Recognition for Processors)系統(Global CBPR and Global PRP System Documents)等四份基礎文件。
5. 全球 CBPR 系統的運作機制，係透由計畫需求文件(Program Requirement, PR)使各司法管轄區能夠確保 PR 文件之個資保護水準相當，欲申請 CBPR 認證者(下稱「申請機構」)需確保組織內的個資保護水平符合 CBPR 計畫需求文件之要求，並由受論壇認可之當責機構(Accountability Agent, AA)評估並認證申請機構是否符合 PR 個資保護水準之法遵要求，並進行授證。
6. 全球 CBPR 論壇係以「透由夥伴關係建構(資料傳輸)信心」為宗旨，將持續推動支持資料自由流動及有效的資料保護及隱私；為企業、法規制定者、消費者們提供實務

工具；在各會員間建構合作、彈性及共識；分享最佳實務的平台；多方利害關係人之參與；促進歸責。

(七)義大利資料保護專責機關董事 Guido Scorza

1. 在現今全球資料社群的時代，資料的傳輸已超越地域疆界，若資料無法自由傳輸，對社會活動影響甚鉅。然而，社會趨勢是全球化的概念，法律則需要因地制宜，故透過國際協議的簽署來克服法規的不一致性，使資料傳輸規範能夠符合數位社會發展所需。
2. GDPR 第 46 條有關須遵守適當保護措施之移轉規定，對於認證標章的發展提供靈感，義大利監管機關的思維是，在全球資料社會中，須要建構一新的商法體系(lex mercatoria)，而「認證」(certification)或許可以相當程度擔任類似角色。認證是國際資料傳輸的重要工具之一，義大利資料保護專責機關於推動認證的過程中歸納出四項重點：
   (1) 商法體系的概念與認證的概念類似，強調市場的主導作用。然而，在歐洲大陸，從商業角度看待個資保護仍然面臨大眾的牴觸情緒。商業的意義不僅在於利潤與經營，也是促進文明與社會化的重要推手。監管機關於推動認證的過程中必須加強克服這種大眾矛盾，以於業者的商業經營權及資料主體的隱私權等基本權利中取得平衡。
   (2) 與商法體系相比，個資保護需要統一規範，且涉及的權利比商業經營更加多元且異質化，個人及其尊嚴的重要性不亞於公私部門的利益應以更開放的態度廣納人權協會、大眾、消費者等利害關係人的聲音，以推動認證的發展。
   (3) 商法體系的力量源於整體商業社群共同參與及制定；然而，現今的認證發展流程往往只有區域性的社群參與，缺乏多元性。義大利監管機關也曾於羅馬舉行的隱私 G7 會議上就全球 CBPR 標準及 GDPR 的差異性加以討論。將認證作為簡化個人資料跨境傳輸的工

具在歐洲特別不容易，且會賦予資料傳輸者較大的責任，便成為推動認證過程中的挑戰，故須要透過國際論壇平台持續討論，以建構相互操作的共享資傳輸標準。

(4)個資監管機關應該強化對於發展認證機制的努力，避免將認證流於技術性問題。認證可能是未來個資保護機關所需要面對的政策性挑戰，須制定通盤的戰略計畫，以確保能發展全面性的資料保護機制。

活動講者合影，由左至右分別為 Sébastien Ziegler、Guido Scorza、Alexander White、Marc Schlegel、Peter Kimpian

■ OECD 關於政府進用個人資料以促進資料安全流動宣言的相關性

The Relevance of the OECD Declaration on Government Access to Personal Data for Safe Data Flows

(一)OECD「政府近用私部門持有之個人資料宣言」(Declaration on Government Access to Personal Data Held by Private Sector Entities）簡介：

1. 本宣言係 2022 年 OECD 數位經濟政策委員會部長級會議成果，旨在回應各國政府因國家安全、執法等公益目的近用私部門資料時的透明性與信任議題，包含法律基礎(legal basis)、法定目標(legitimate aims)、許可(approvals)、資料處理(data handling)、透明度(transparency)、監督(oversight)、救濟機制(redress)等七大原則。

2. 本宣言由 39 個 OECD 會員體部長級代表連署發布，包含澳洲、奧地利、比利時、加拿大、智利、哥倫比亞、哥斯大黎加、捷克、丹麥、愛沙尼亞、芬蘭、法國、德國、希臘、匈牙利、冰島、愛爾蘭、以色列、義大利、日本、韓國、拉脫維亞、立陶宛、盧森堡、墨西哥、荷蘭、紐西蘭、挪威、波蘭、葡萄牙、斯洛伐克、斯洛維尼亞、西班牙、瑞典、瑞士、土耳其、英國、美國及歐盟等。

(二)歐洲委員會立法及全球資料保護負責人 Estelle Massé

1. 政府對私人部門持有資料的近用議題係全球關注重點，本宣言雖不具約束性，但已成為歐盟等國研議資料存取議題時的重要參考文件，並為資料流動國際談判提供基礎。在數位貿易協定中，本文件所揭示的原則常被引用，以作為締約國共享資料及保護個人隱私時的注意原則。

2. 本宣言不僅限於資料保護領域，亦跨越商業及貿易領域，成為貿易文件中不可或缺的一部分。本宣言雖不具約束性質，惟在政府近用私部門資料議題中達成之共識具有深遠影響，並為國際合作提供堅實的基礎。未來，OECD 將持續鼓勵更多國家及業界參採本宣言，以在共享的價值上促

進更有效的合作及發展。

(三)IAPP 研究及觀察處 Joe Jones 總監

1. 本宣言強調資料流動的風險管理應該聚焦於政府對資料的存取權限，尤其是針對資料傳輸過程中可能出現的政治與法律衝突。由這點可以觀察到各國已開始關注資料流動的實際風險，而非過去聚焦以法律架構為基礎的挑戰，這向改變為全球的資料流動與隱私保護帶來新的觀點，並對未來的資料傳輸規範產生示範作用。

2. 對私營部門而言，本宣言簡化跨境資料傳輸的法律架構。過往企業需依賴複雜的契約條款及企業規則進行資料傳輸工作，而每一則條款都需進行風險評估，產生極大成本。隨著本宣言的施行，企業可以透過標準化的規範，減少在各國法律下的法遵壓力。

(四)美國司法部隱私及公民自由 Peter Winn 代理主席

1. 隱私保護與個人的權益及整個社會的安全與民主體制的穩定息息相關。民主社會之所以能夠穩健運作，即係因為有強有力的隱私保護機制防止政府過度干涉公民的個人資料。健全的隱私保護機制不僅是對個人權益的保障，也是防止政府權力濫用的關鍵，有助於確保民主制度的運作。

2. OECD 隱私指南最初目的係解決國際資料流動中的信任問題，並規範私部門的資料處理活動。而後該指南也涵蓋了政府在執行國家安全與執法職能時對資料的存取權限。該指南不僅規範資料流動活動，也強調政府近用資料時應遵守的法遵與透明度義務。

3. 在國家安全與執法領域，政府對資料的近用需求與隱私保護中的透明度及公平性原則產生矛盾。因國安及執法領域調查活動通常具機密性，使傳統的隱私保護原則難以完全適用，突顯平衡政府安全需求與個人隱私保護之間所面臨的兩難課題。

4. 雖然所多國家都遵循 OECD 隱私原則，但各國於執行相關原則時的具體方式仍有不同，反映了各國的法律體系與政治環境的差異，此一差異使第三方機構難以對每個國家的隱私制度落實情況統一評價。不同國家於平衡隱私保護與國家安全需求時，需要根據自身的政治與法律環境進行在地化調整。

(五)日本個人資料保護委員會國際事務處 Motoko Hori 副參事

1. 「資料自由流動與信任」（Data Free Flow with Trust, DFFT）係 2019 年由日本已故前首相安倍晉三所提出之概念，DFFT 包含「個人資料的自由流動」及「非個人資料的自由流動」等二支柱。在動個人資料的自由流動上，應建立安全的資料傳輸工具及選擇機制，保障資料主體的選擇權。然而，毫無限制的政府存取資料是建構可信任的資料流動機制的主要挑戰，故政府需加強對政府近用資料的規範以確保資料流動的安全性。

2. 日本個人資料保護委員會（Personal Information Protection Commission, PPC）負責推動促進個人資料自由流動的相關工作，並將確保資料傳輸工具的安全性列為首要考量，以爲資料主體提供多種選擇，使其能根據需求選擇合適的傳輸工具。此外，國際間應建立互信的法律框架，並確立適當的認證機制，以促進資料的安全流動，並保障資料主體的權益。

3. 針對歐美之間的資料傳輸問題，政府近用資料係一重大挑戰。若開放政府可以毫無限制地存取私部門持有之個人資料，則即使業者使用合法的資料傳輸工具，仍無法保證資料流動過程中的安全性。進而危及資料的自由流動及信任，並對資料主體造成潛在風險，故透過法規對政府近用私部門資料進行限制以維護 DFFT 的信任至關重要。

4. 日本於 2019 年提出建議更新 OECD 隱私指南，該指南對於 OECD 成員國及非 OECD 成員國均有重要參考價值，並已

成為許多國家於資料保護及政府近用問題上的重要參考依據，希望通過推動 DFFT 的落實，進一步強化國際間對資料自由流動的信任。

5. 未來應持續推動 OECD 以外的國家共同支持本宣言，並積極宣導 OECD 國家將本宣言納入內國法，以促進國際間的相互合作，並確保在處理跨境資料流動議題時，各國能基於相同的價值觀，共同提升資料流動的安全性及信任度。

(六)阿根廷公共資訊進用委員會 Beatriz de Anchorena 主任

1. 阿根廷重視資料保護議題，除於 1994 年將隱私權納入憲法外，並於 2000 年成為拉丁美洲首個頒布個人資料保護法律的國家。阿根廷已取得歐盟 GDPR 的適足性認定，且阿國個資法亦與 OECD 隱私原則高度接軌，2000 年阿根廷個資法已於其法律框架中納入 OECD 隱私。另，阿根廷亦積極參與 108 號公約等國際協議，以進一步促進內國法與全球資料保護標準一致性。

2. OECD 宣言於促進跨境資料傳輸及促進信任上為阿根廷個資法規建置提供許多益處，OECD 宣言中的法律基礎、透明度及監督等原則與阿根廷個資法之規範一致，並為未來的規制發展提供指導原則。OECD 宣言開放給非 OECD 國家簽署的舉措，使阿根廷於成為 OECD 正式會員前，也能與國際標準接軌。

■ Meta 會外活動：小組討論 – 攜手促進 AI 治理成功

Meta Side Event: Panel discussion – Working together for success in AI Governance

一、會議的重點：在對立環境中合作的價值、強調世界各地和諧化和資料保護法律的重要性。

二、談參成員：Anna、Denis、Enrique 和 Theodore，他們在法律、AI 和資料保護方面有豐富的背景。Anna 因在印度和加州的經驗而受到認可，擔任 APAC 公司的總法律顧問。Denis 是新加坡資料創新和保護組的助理行政總監，在 AI 和資料治理方面有豐富經驗。Enrique 是 NoHarm.ai 的創始人兼 CEO，專注於提升巴西公共衛生系統的患者安全。Theodore 是紐約大學的教授，也是隱私論壇董事會成員，專門研究 AI 和資料保護。

三、NoHarm.ai 和協作研究：NoHarm.ai 的創始人兼 CEO Enrique，他解釋 NoHarm.ai 的起源，這是一個專注於患者安全的 AI 驅動工具的非營利組織。NoHarm.ai 與各種實體合作，包括大學和私營部門，開發和增強其 AI 系統。該組織強調了開源軟件的重要性，並與 Meta、Google、Microsoft 和 Amazon 等技術巨頭合作。NoHarm.ai 的項目以倫理考量為指導，專注於公共衛生的隱私、公平和可訪問性。與 COVID 基金會和蓋茨基金會的合作在塑造其 AI 開發方法上至關重要。

四、新加坡的 AI 標準和治理：新加坡資料創新和保護組的助理行政總監 Denis，討論新加坡 AI 治理基金會開發的 AI 治理框架和技術工具包。該框架旨在為公司創建一個可信的環境，以創新和利用 AI 的潛力。工具包是開源的，允許公司測試其 AI 系統以符合自己的標準。該基金會與行業合作開發標準和框架，將它們映射到國際標準，如 NIST 和 ISO 42001。Denis 強調了國際合作和聯合測試的重要性，以確保 AI 應用的互操作性和安全性。

五、歐洲的監管挑戰：紐約大學的教授，也是隱私論壇董事會成員 Theodore，討論在歐洲監管生成性 AI 的複雜性，特別是預期的歐洲資料保護委員會意見。Theodore 強調各歐洲資料保護機構

指導方針的差異，有些允許基於合法利益訓練 AI 模型，有些則不允許。討論嚴格監管對歐洲 AI 開發的潛在經濟影響，舉例說明公司因監管擔憂而推遲 AI 發布。Theodore 強調需要平衡方法，考慮 AI 的利弊以及法律確定性對創新的重要性。討論包括 EDPB 提供的簡報意見，以提供 AI 監管的清晰指導。

六、印度和美國的 AI 監管：亞太認證合作組織(APAC)[18] 總法律顧問 Anna 舉例說明，印度 AI 部署的一個案例，重點是泰米爾納德邦的一個政府項目，使用開源 AI 平台。該項目旨在利用 AI 改善教育成果，儘管資源有限，但利用技術實現了預期目標。Anna 討論了印度和美國的監管應對措施，強調了基於危害的方法和披露原則。強調了在 AI 監管中平衡創新、社會利益和國家安全考量的重要性。Anna 建議披露、自我監管和透明模式可以有效解決 AI 監管問題。

七、AI 中的可解釋性和問責制：Enrique 討論 AI 系統中特別是在醫療保健中的可解釋性，以確保透明度和問責制的重要性。NoHarm.ai 的方法包括向醫療提供者和專業人士解釋資訊來源和決策過程。該組織發表研究論文和方法論，以展示其方法並確保透明度。Enrique 強調了生成性 AI 中可解釋性的重要性，以應對潛在危害並建立對 AI 系統的信任。討論包括複雜 AI 系統中的可解釋性挑戰以及持續研究和合作的重要性。

八、AI 開發中的測試和保證：Denis 強調 AI 開發中測試和保證的重要性，重點是創建標準和基準。AI 治理基金會投資於開發測試和評估 AI 系統的方法論的研究。討論包括支持測試和保證的強大生態系統的必要性，包括培訓和認證評估員。Denis 強調資料治理和 AI 開發中的可解釋性的重要性，以確保安全和問責制。討論包括在開發和實施測試和保證標準方面的合作角色。

九、AI 與其他法律領域的交叉：Anna 討論 AI 與其他法律領域的交

[18] The Asia Pacific Accreditation Cooperation , APAC

叉，包括版權、責任和隱私。強調解決 AI 生成內容中的版權侵權和商標問題的挑戰。討論包括需要清晰的責任制度，以解決 AI 生成的錯誤或有害內容問題。Anna 強調利用現有法律框架解決 AI 特定問題的重要性，而不是創建新立法。討論包括自我監管和自願披露解決 AI 相關法律挑戰的潛力。

十、在 AI 中平衡隱私和創新：Theodore 討論在 AI 監管中平衡隱私和創新的必要性，強調靈活方法的重要性。討論包括過度監管可能阻礙創新的潛力以及需要平衡 AI 監管的方法。Theodore 強調考慮 AI 監管對社會利益和經濟增長的更廣泛影響的重要性。討論包括監管機構在平衡隱私和創新中的角色，重點是創建可行且具有保護性的法規。強調了監管機構、行業和學術界在開發有效 AI 監管中的合作重要性。

十一、最後總結：Anna 總結討論的關鍵點，強調合作的重要性以及需要平衡的 AI 監管方法。討論包括自我監管的潛力以及行業在開發 AI 最佳實踐中的角色。強調了在監管中考慮 AI 的利弊的重要性。討論以呼籲持續合作和平衡的 AI 監管方法結束，以確保創新和安全。會議結束時提醒了法律確定性的重要性以及需要靈活且可行的 AI 監管框架。

■ 隱私的未來論壇：AI 和資料保護的基本問題 - 模型中的個人資訊和處理的法律依據

Future of Privacy Forum: Essential Questions for AI and Data Protection - Personal Information in Models and Legal Basis for Processing

(一)加拿大隱私專員辦公室(Office of the Privacy Commissioner of Canada, OPC)資深分析師 David Weinkauf

1. Weinkauf 針對網路擷取與人工智慧訓練過程中之個資風險提出論述，特著重於模型重新訓練成本過高以及刪除權實踐困境等關鍵議題。除了事後補救措施外，更應著重於建立事前預防機制與替代方案。

2. Weinkauf 將 LLM 訓練過程形容為有損壓縮(lossy compression)，LLM 利用 Transformer 架構、子詞標記(sub-word tokens)、字詞嵌入(word embeddings)及注意力機制(attention)來預測下一詞彙。以 LLaMA 2 為例，該過程係將約 10TB 龐大文本資料壓縮成約 40 GB(700 億參數)模型，此種壓縮型模型雖無法完整重現原始訓練資料，但透過特定提示詞仍可能重建或洩漏個人資訊。

3. 模型重新訓練之高額成本已成為業界重要議題，當企業在大規模蒐集公開資料並完成人工智慧模型訓練後，若資料主體要求刪除特定個資，往往需要重新訓練整個模型，這不僅耗費巨額成本，亦需要相當長的時間。以 GPT-3 為例，完整重新訓練過程預估需要耗費約 200 萬美元，且需要長達 12 天處理時間，這對企業營運造成極大壓力。

4. 由於目前解除學習(unlearning)技術尚未成熟，要直接從模型中移除特定個人資訊仍具技術挑戰，為降低個資風險，Weinkauf 提出下列建議方案：

   (1) 在資料蒐集階段，建議透過網路擷取進行預先過濾、排除包含特定關鍵字或敏感內容網站，以縮小資料蒐集範圍，避免爬取高風險網址與未成年人資料。

(2) 在模型輸出階段，則可運用自動過濾機制，識別並移除可能涉及個人識別敏感資訊。

(3) 採用模型拆分策略或局部微調技術，將大型模型切分為多個子模型，或透過微調（fine-tuning）技術針對特定任務進行優化。

(4) 定期評估資料來源及訓練過程，並執行稽核機制（如內部管控、第三方審查），尤應留意敏感及兒少資料。

(5) Weinkauf 就資料蒐集策略提出兩種方案「先大量蒐集再去識別化」與「預先排除問題資料來源」。兩種方案均需要完善的風險管理，但「預先排除高風險資料」策略更能有效降低後續處理難度。

5. 根據 Weinkauf 論述與 OPC 之立場，網路擷取應用之合法性需符合以下原則：

(1) 合法性原則：使用網路擷取蒐集公開資料進行人工智慧模型訓練時，必須具備合法目的，且須證明此種處理方式確實必要。

(2) 資料最小化：應嚴格遵守資料最小化原則，僅蒐集與目的相關且必要資料。

(3) 透明與問責：必須確保資料處理過程之透明度與問責性，並建立完善機制供資料主體查詢、更正或刪除個資。

6. Weinkauf 特別強調，與其執著於討論「模型參數是否屬於個人資料」之定義問題，更應關注其可能造成的實際影響，並建立有效保護措施與補救機制，以確保使用者權益。

(二) 巴西國家資料保護局(ANPD)專員 Wimmer

1. ANPD(Autoridade Nacional de Proteção de Dados)係巴西國家資料保護局，於 2020 年成立，為具有技術及行政自主權之行政機構，雖隸屬於巴西總統府，但維持其獨立性，並由 5 名董事組成委員會領導，任期 4 年。

2. LGPD 法規架構與規範：

(1) 基本規範：巴西通用資料保護法(Lei Geral de Proteção de Dados) LGPD 在敏感性個人資料處理上，採取謹慎立場。

(2) 合法性基礎：依 LGPD 第 7 條作處理個人資料應具備以下法律依據，包含資料主體同意、履行法律或監管義務、執行公務、研究目的、履行合約、行使權利、保障生命或人身安全、醫療、合法利益及信用保護。

(3) LGPD 第 13 條規定，研究機構在進行公共衛生研究時，可存取個人資料庫。這些資料僅限機構內部處理，並嚴格用於研究目的。資料須依規定之安全措施保存在受控和安全環境中，包括對資料進行匿名化或假名化處理，並需適當考量相關研究倫理標準，相關條文內容如下：

甲、 在任何情況下，研究結果或任何摘錄內容均不得洩露個人資料。

乙、 研究機構應負責本條款開頭所述之資訊安全，並且在任何情況下均不允許將資料傳輸給第三方。

丙、 存取資料應遵守國家主管部門以及衛生和衛生主管部門在其職責範圍內的規範。

丁、 假名化是指由於使用由控制者在受控和安全環境中單獨保存之額外資訊，使得資料失去與個人直接或間接關聯可能性。

3. 在執法實務上，ANPD 於 2023 年針對巴西外送平台 iFood 採取了預防性監管行動。該案例中，ANPD 對 iFood 公司執法經驗：iFood 曾在其隱私政策中標示，將使用「公開可取得之使用者資料」訓練 AI 系統，但並沒有給予使用者充分告知，也缺乏簡易退出機制。ANPD 因而要求 iFood 暫停此項資料處理活動，並要求其針對兒童與青少年資料保護採取更高標準。最終在 iFood 提供更明確之透

明度、簡化退出流程且保證不使用兒少資料後，ANPD 才同意解除該預防措施。

4. ANPD 已針對 AI 訓練合法性議題展開積極執法。特別關注社群平台大規模修改隱私政策，意圖透過網路擷取取得公開資料進行 AI 訓練行為。即使資料不屬敏感個資，ANPD 仍嚴格審查企業是否充分告知使用者並提供適當拒絕機制，尤其涉及兒童及青少年資料時更加嚴格把關。

5. LGPD 第 5 條只要資訊「關於可識別或已識別自然人」，無論真實與否，均屬於 LGPD 規範範圍內並未要求「資料必須為真實」才構成個人資料。這也代表從公開網路抓取文本或臆造（幻覺）資料，只要事涉可識別個人，亦屬個資。

6. LGPD 並不要求資料真實性才構成個資，只要有「可識別或已識別自然人」即可。在 LLM 環境下，輸入及輸出皆可能隱含個人資訊。

7. 資料主體權利在大型模型情境下難以落實：
   (1) 存取權：了解模型使用了哪些個資困難重重。
   (2) 刪除權：若要完全從 LLM 排除個人資訊，幾乎需要重新訓練整個模型。
   (3) 更正權：若模型「記住」錯誤資訊，很難將錯誤通通剔除。
   (4) 透明度：企業在保護商業機密與解釋訓練流程之間需仔細權衡。

(三)韓國個人資料保護委員會 PIPC 主席 Hanksoo Ko

1. Ko 現為韓國個人資料保護委員會(Personal Information Protection Commission, PIPC)主席，曾任首爾大學法學院教授，擁有美國哥倫比亞大學經濟學及法學雙博士學位，並以聯合國人工智慧高級別諮詢機構成員身份，積極推動全球 AI 治理。

2. 韓國個人資料保護法(PIPA)與 GDPR 有相似之處，企業若要引用此依據來進行 AI 訓練，必須符合三項要求：

(1) 目的合法性：處理個資目的需合法及正當。
(2) 處理必要性：若無此一處理，就無法實現前述目標。
(3) 利益平衡測試：企業利益必須大於或至少明顯優於資料主體權益可能遭受侵害。

3. 在「網路擷取」層面，不否認其可行性，但強調同時要搭配技術及行政保護措施，例如：
   (1) 高風險 URLs 清單：PIPC 會定期發布或更新高風險網站列表，避免企業爬取其中敏感性個資。
   (2) 紅隊演練（red team）測試：透過模擬駭客攻擊與滲透測試，檢驗企業對蒐集資料之保護機制是否嚴謹。他強調在實務中，韓國企業若能證明存在「合法利益」，並實施適當保護程序，即可合理化其 AI 訓練之網路擷取行為。

4. 對於 LLM 與個人資料之管理立場，PIPC 目前尚未明確定義 LLM 是否本身包含個人資料。PIPC 主要關注重點在於 AI 系統最終輸出是否違法包含或洩漏可識別個人資訊。針對此議題，PIPC 建議使用微調(fine-tuning)技術針對特定任務或領域進行模型調整，並採用檢索增強生成(Retrieval-Augmented Generation, RAG)技術，透過外部知識庫檢索來增強生成內容準確性，同時降低出現個資的機率。另外，PIPC 也建議在 AI 系統層面建置「篩選機制」或「後處理」程序，以攔截個資洩漏事件。

5. 在實務操作層面，若特定個人要求行使"被遺忘權"，理論上需要對模型進行完整重新訓練，但考量此作法成本過高，PIPC 建議可採取替代方案，包括在系統層面增設防護機制，並定期對模型進行適度再訓練。透過這些措施在隱私保護與開發效率之間取得平衡，確保 AI 系統符合法遵規範與可持續發展。

(四)愛爾蘭資料保護委員會(Data Protection Commission, DPC) Des Hogan 委員

1. Hogan 認為在蒐集資料訓練大型語言模型（LLM）或生成式 AI 前，關鍵因素為先評估這些資料是否包含個人資訊。由於 GDPR 對「個人資料」定義相當廣泛，只要能間接或直接識別自然人，即屬於個資範疇；若企業堅稱訓練中並未使用個資，則必須提出具體技術證明。

2. 為了因應 AI 發展，DPC 與歐洲其他主管機關正試圖建立一致協調之資料保護方法，確保歐洲境內對 AI 訓練之規範原則不會相互衝突。目前 DPC 已向歐洲個人資料保護委員會（EDPB）提交意見，期望在 2024 年底前獲得指引。

3. DPC 預計在 2025 年初正式開始與產業進行協商與執法調整。Hogan 也注意到，雖然歐盟各國對「網路擷取是否合法」之見解或許略有差異，但在 GDPR 框架下，大多會聚焦於透明度、合法依據及資料主體權利等面向。

(五)法國資訊自由委員會 (Commission nationale de l'informatique et des libertés, CNIL) 委員 Bertrand du Marais

1. 法國國家資料自由委員會(CNIL)成立於 1978 年，係法國主管資料保護之獨立行政機構，該委員會由 17 名成員組成，包括法國國會代表以及各相關組織選舉產生之委員。CNIL 主要職責是監督並確保法國境內遵守包括 GDPR 及各項資料保護法規，同時負責制定相關政策並監督執行。

2. Marais 2006 年晉升國務院諮詢部門國務顧問，主責電子政府治理、公共採購及公共事務領域，為政府數位化轉型做出貢獻。並於 2019 年獲任 CNIL 專員，專責國際事務協調、電子隱私維護，以及產業競爭共同監管等重要職務。同時也以 CNIL 制裁委員會成員身份，致力於維護資料安全與個人隱私權利，在資料治理領域扮演關鍵角色。

3. Marais 警告，全球規模之網路擷取對個人隱私構成前所未見的風險，需要嚴肅看待。他建議應透過專門法規或強化監管以控管此類大規模網路擷取行為。強調依據 GDPR 第 6 條第 1 項 (f) 款「合法利益」可作為網路的法律依據，但須同時符合目的合法性、必要性、以及利益平衡；更需落實「資料最小化」原則以及額外控制措施，例如：
   (1) 事前定義資料蒐集標準、即時刪除不相關資訊。
   (2) 尊重網站拒絕網路擷取之聲明（如 robots.txt 或其他機制），並建立「拒絕名單」供資料主體登記反對其資料被蒐集。
   (3) 適度匿名化或假名化處理：蒐集完後立即進行處理以降低識別度。
   (4) 提供簡易之退出機制：讓資料主體可隨時要求停止使用其資料。
   (5) 在 CNIL 建立登記處：集中管理並讓外界了解哪些開發者或公司有進行大規模資料蒐集。

4. Marais 指出，若 AI 模型具有「記憶化」特性，能夠重構或還原特定個人資訊時，該模型即落入 GDPR 規範範圍；因此開發者在「訓練前」就須做好匿名化或去識別化處理。CNIL 正研究如何具體判斷模型是否具「記憶化」特性，以及如何評估其遭洩漏攻擊之風險。此外，資料主體權利在此環境下更為複雜，因模型提供者與使用者可能不同，甚至分屬多層服務（如 API 使用、再加工等），要落實「存取權」、「刪除權」或「反對權」很難有統一且簡單機制，需要監管機關與業界合作探尋可行做法。

5. CNIL 2024 年 6 月發布人工智慧操作指引(AI How-to sheets)，其中探討網路擷取應用於 AI 訓練議題。CNIL 因應 AI 技術快速演進，持續更新指引內容，並透過公開徵詢大眾意見。該指引包含以下內容：

指引編號	標題	說明
1	判定適用之法律規範	協助判定 AI 系統開發階段處理個人資料時適用之法律框架。
2	定義目的	協助定義 AI 系統開發目的，並考量 AI 特殊性。
3	判定 AI 系統供應商之法律資格	協助 AI 系統供應商判定其是資料控制者、聯合控制者還是處理者。
4	確保資料處理之合法性：定義法律依據	根據資料蒐集或再利用方式，協助判定 AI 系統供應商義務。
	確保資料處理之合法性：資料再利用時額外測試和驗證	根據資料蒐集方式和來源，協助判定 AI 系統供應商義務。
5	必要時進行資料保護影響評估	建立 AI 訓練資料集可能對個人權利和自由帶來高風險，因此需進行資料保護影響評估。
6	設計系統時將資料保護納入考量	確保 AI 系統開發尊重資料保護，在設計時就需納入考量。
7	資料蒐集和管理中納入資料保護	詳細說明資料保護原則與訓練資料管理之間關係。
8	依賴合法利益之法律依據開發 AI 系統	控制者常依賴合法利益開發 AI 系統，但需尊重其條件並實施足夠控制措施。
9	告知資料主體	處理個人資料以開發 AI 模型或系統之組織必須告知資料主體。
10	尊重並促進資料主體權利行使	資料被蒐集、使用或再利用以開發 AI 系統的個人擁有對其資料權利，控制者有責任遵守並促進這些權利行使。
11	資料標註	資料標註對確保 AI 模型品質至關重要，需透過嚴謹方法確保系統效能和個人資料保護。
12	確保 AI 系統開發之安全性	AI 系統安全性常被忽視，在系統開發和部署時，保證資料保護是必要義務。

(六)美國未來隱私論壇 Future of Privacy Forum (FPF) 執行長 Jules Polonetsky

1. 未來隱私論壇(FPF)是專注資料隱私之非營利智庫，透過深入分析和政策倡議推動隱私保護法規發展。該組織積極參與資料治理政策制定，研究各地隱私法規，並提供專業建議，以確保隱私保護機制能與科技發展同步。

2. 美國針對網路擷取應用於 AI 訓練之法規框架尚處發展階段，聯邦層級缺乏統一立法。目前以加州消費者隱私法(California Consumer Privacy Act, CCPA)修正案為首，部分州已開始制定相關法規。由於聯邦政府在 AI 監管方面進展緩慢，各州之間正建立協作機制，試圖制定統一 AI 監管模式，以彌補聯邦監管之不足。

3. 由於 AI 模型參數結構與傳統資料庫差異顯著，難以直接套用個人資料之傳統定義。傳統之個人資料識別技術，如在資料庫中添加雜訊方法，在 AI 模型中可能並不適用。Polonetsky 執行長認為 AI 模型本身不應視為個人資料，但無論資料性質為何，皆應著重輸入及輸出端之權利保護與安全控制。

4. 為避免州際法規分歧影響 AI 產業發展與隱私保護，建議加速推動聯邦立法或州際合作機制。

■ 英國 ICO 會外活動 – 保護兒童免受網路傷害
UK ICO Side Event – Protecting Children from Online Harms

(一) 英國資訊委員辦公室監管政策副專員 Ms Emily Keaney

1. 數位環境中對兒童隱私保護方面的工作是英國資訊委員辦公室（ICO）監管政策策略的核心，也反映了 ICO 在全球數位時代，如何積極應對新興技術與兒童隱私保護之間的挑戰。ICO 在在設計適合年齡的內容、實施有效的年齡驗證措施、兒童隱私守則以及其他年齡保護措施，已經在全球範圍內產生了積極的影響。過去一年，ICO 進行了重要政策更新，新政策不僅提升數位平台、社交媒體以及視頻共享平台隱私保護的監管力度，也更加明確地指導了這些平台如何處理兒童資料。尤其是在年齡驗證與隱私保護方面，ICO 的要求變得更加具體和具有操作性，也讓服務提供者能夠更清楚理解如何遵守相關規範，並為兒童用戶創造更安全的數位環境。

2. 2024 年 4 月，ICO 發佈最新的兒童隱私保護策略，並開始仔細研究社交媒體與視頻共享平台之應用情況。ICO 對 34 個不同平台進行了實地審查，這些平台包括一些大型成熟平台與新興平台，無論是在兒童隱私保護政策的實踐、用戶年齡驗證、資料存儲、資料使用及廣告投放等方面，皆進行全面性檢查。針對審查情形，許多平台對年齡驗證程序尚未完善，特別是對 13 歲以下兒童的資料蒐集與處理。儘管這些平台在聲明中承諾不蒐集兒童資料，但實際操作中，仍有許多平台未能有效阻止兒童用戶創建帳戶，這些帳戶中包含大量可識別的個人資料和行為資料。根據這些發現，ICO 向一些平台提出了強烈建議，要求他們進一步加強年齡驗證過程、加入更為精細的年齡識別系統及並要求限制兒童使用成人向內容的權限，並在平台設置中提供更明確的選項，讓家長或監護人能夠對兒童使用數位服務進行管理。

3. ICO 也進行數位平台如何提供兒童模式或適當年齡內容

選擇的深度分析。從這些分析中發現，一些平台在設置兒童專屬區域時，忽略了防止有害內容、過度廣告以及不當行為的問題。因此，ICO 的策略係更新強調了這些問題的嚴重性，並強烈建議平台在兒童專區設計中引入更多的可讓家長控制之工具與過濾機制。另外，ICO 強調對數位廣告的監管，當前兒童面對的網路廣告越來越多，這些廣告不限於購物廣告，還包括遊戲購物、虛擬物品等形式的隱性推銷。這些廣告模式不僅容易影響兒童的消費行為，還可能帶來心理上的壓力。ICO 強烈要求平台在面對兒童用戶時，必須遵守更加嚴格的廣告規範，避免推銷對兒童有害的產品或服務。

4. ICO 也對兒童資料的存儲與傳輸進行了深入研究，發現許多平台並未能將兒童資料進行充分的加密處理，這使得資料在存儲過程中容易有安全漏洞之虞。因此，ICO 提出加強資料保護措施的要求，尤其是在兒童資料的保存期限、加密技術的使用、以及資料共享的透明度。ICO 還強調國際間的合作，在全球化的數位生態中，跨國公司平台的運營往往會影響到不同國家的兒童隱私保護政策。因此，ICO 積極與國際組織、其他國家的監管機構合作，共同制定統一的隱私保護標準，促使全球範圍內的兒童隱私保護措施更加協調一致。

(二) 美國聯邦貿易委員會專員 Mr Alvaro Bedoya

1. 防治網路騷擾措施以及兒童語音資料保存相關的案例展示了當前數位平台在隱私保護方面的問題和挑戰。研究表明，針對年輕人在網路上遭遇的心理健康損害，有幾個原因，推薦系統推薦的某些內容會對兒童產生負面影響，像是飲食障礙或厭食症的內容，這些內容可能加劇青少年的心理困擾；另一類原因是延長使用時間的設計，許多平台希望用戶能夠長時間留在平台上，即使他們不想繼續使用，也被迫繼續停留，這樣的設計會影響青少年的睡眠質量，而睡眠對於青少年的身心發展至關重要。

2. 第一個案例是要塞英雄（Fortnite），這款遊戲的隱私設置過低，致使陌生人可以隨意向青少年發送言語騷擾，據所收受的投訴，許多使用者遭遇了侮辱性語言。FTC 與遊戲開發商達成和解後，要求其將隱私設置改為預設最大保護，13 歲以下的使用者在父母同意時能夠遊玩，但禁止使用聊天、購物等特定功能，而為了減少青少年在遊戲過程中遭遇的網路騷擾，針對 18 歲以下與 16 歲以下使用者也另外設置不同的隱私政策。

3. 第二個案例是 Amazon 的 Alexa 設備對於兒童語音資料的保存問題，在家長要求刪除孩子語音資料的情況下，Amazon 雖然刪除了語音錄音，但卻保留了語音的文字記錄。FTC 在對多家社交媒體和視頻平台進行調查時發現，很多平台並未完全刪除資料，甚至保留了部分資料，或者將其匿名化處理。而「刪除」的定義在平台和用戶之間存在很大差異，用戶認為資料已經完全刪除，但實際上卻並非如此。

4. 早期 FTC 的成員主要以律師為主，但隨著數位平台問題日益複雜，於 2000 年代後期開始引入更多的技術專家。隨著數位平台對兒童和青少年心理健康的影響逐漸加劇，FTC 進一步引入行為學專家，如心理學家和兒科醫生，協助更好地理解和評估這些平台對兒童與青少年的影響。如 AI 技術的快速發展，許多社交平台開始引入聊天機器人，這些機器人逐漸成為年輕人建立關係的對象，由於孩子們認為聊天機器人不會對他們進行評判，也不會洩漏他們的秘密，因此他們更願意向機器人分享隱私。然而，這也引發了兩大擔憂：第一，這些機器人可能會取代真實的人際關係，限制孩子的社交能力發展；第二，聊天機器人可能會變得商業化，開始推薦特定的產品或服務，這對他們的發展構成潛在風險。

5. 因此，對於數位平台設計和資料處理的方式需要更加審慎的評估，特別是在兒童隱私保護和心理健康領域，平台的

操作將對未來一代的成長產生深遠影響，需要在法律、技術與行為學等多領域進行強有力的合作，共同推動有效的政策與措施。

肆、會議心得與建議

本籌備處係以公眾身分參與 GPA 公開活動，相關會議主要就隱私及個人資料保護之特定議題，分場次邀請講員分享觀點及最佳實務，值得我國未來政策規劃參考：

一、跨境資料傳輸及認證機制

(一) 為促進資料在安全可信賴的環境下進行跨境傳輸，歐、美等多國已各自發展不同的跨境資料傳輸標準，前者重視資料主體的人權保護，後者則以經濟利益為導向。認證機制的建立是執行資料傳輸機制的重要工具，可以幫助利害關係人降低辨識資料蒐集及處理者個資保護水準之成本，而業者亦可透過取得資料保護認證提升企業價值。

(二) 安全且可信賴的跨境資料傳輸機制不僅能促進商業發展，亦可促進人權價值之保障，「場次八：資訊」有關政府及第三方小組討論的議程中，即有講者分享資料分析對於促進人道救援效率的重要性；另外，國際慈善機構也強調該組織於執行跨境急難救助業務時，事件的高度急迫性使得救助國與被救助國間個資保護標準的落差為執行任務造成挑戰。

(三) 本次會議期間有關國際資料傳輸機制之討論，多聚焦如何促進現有機制之協調統一，日本前首相安倍晉三於 2019 年提出資料自由流動(DFFT)的重要概念，旨在平衡資料流通的自由與信任，強調在尊重隱私權與資訊安全的前提下促進跨境資料流動，以支持創新、貿易及國際合作；日本個人資料保護委員會講者於「場次四：國際化」表示，DFFT 是資料治理的最終目標，而跨境資料傳輸工具則係實踐 DFFT 理念之關鍵。

(四) 本屆 GPA 閉門大會已於本次會議發布「可信賴的資料自由流動解方及有效的全球資料傳輸法規」(Resolution on Data Free Flow with Trust and an Effective Regulation of Global Data Flows)，該文件係由歐盟資料保護監督機關(European Data Protection Supervisor, EDPS)及德國資料保護聯邦委員會(Federal Data

Protection Commissioner, BfDI)主導，並有瑞士、杜拜、墨西哥、英國、加拿大、義大利、南非、日本、歐盟、菲律賓、阿根廷、保加利亞、法國等 13 國之個資保護專責機關連署，主要就 DFFT 的核心資料保護要素進行定義，對未來進一步推動國際資料傳輸法制架構及規劃標準契約條款、認證機制等工具奠定基礎[19]。

二、人工智慧監管及心理健康應用程式對資料保護之挑戰

(一)AI 技術與其監管、以及心理健康應用程式及資料保護的挑戰，為我國個人資料保護業務提供了寶貴的見解。AI 基礎設施的三層結構—物理基礎設施、數字基礎設施和應用基礎設施，顯示出 AI 技術的快速發展對資料處理與隱私保護提出了新挑戰。會議強調，儘管已有法律框架，現有監管機構難以追趕 AI 技術的變化。為此，建議個人資料保護監管機關在 AI 領域加強對資料處理和使用的監管，並推動跨國合作與資料共享協議，確保資料在跨境流動過程中不侵犯用戶隱私。

(二)在心理健康領域，會議指出數位平台設計對用戶心理健康的負面影響，尤其是推薦系統、使用時間設計和隱私設置。會議同時探討資料撤回的挑戰，並強調資料存儲技術的可追溯性與模組化設計的必要性。未來個人資料保護委員會應借鑒澳大利亞的創新監管模式，推動企業自我認證並提高資料透明度，並加強用戶教育，特別是在分享心理健康資料時的審慎性。最後，會議強調了與非政府組織合作的必要性，個人資料保護委員會成立後應加強合作，並設立跨學科的專業團隊來提升監管效能。

(三)總體來說，無論是 AI 技術還是心理健康應用程式，個人資料保護委員會應結合國內實際情況，制定靈活高效的資料保護政策，保障用戶資料安全，並促進心理健康與隱私保護。

三、善用監管科技促進執法效率

(一)隱私保護法之立法逐漸成為各國面對的一大挑戰，不少專家指出，

[19] 文件全文，請參閱：https://globalprivacyassembly.org/wp-content/uploads/2024/11/Resolution-Data-Free-Flow-with-Trust-and-an-effective-regulation-of-global-data-flows.pdf

法制的建立不僅需要考量國內需求，還必須兼顧國際合作與技術發展。擁有完善隱私保護法律的框架，不僅是保護公民基本權利的需求，也是與全球數位經濟接軌的必要步驟，而透明度與合法性是不可忽視的兩個要素，這有助於提高消費者對企業的信任。

(二)未來我國在隱私保護法制的立法中，應該加強國際視野，借鏡國際實務上的經驗，同時根據國內法律、文化及產業需求，靈活調整制定出符合我國特色的隱私保護法律框架。隨著科技的迅速發展，隱私及監管科技成為全球數位管理的重要工具，如會議中專家所提物聯網及生成式 AI。

(三)我國如善用監管科技的應用，能協助政府在執行法規監管的過程中，利用數位化的工具與技術，實現更高效、更準確的監管，同時減少執行成本與受監管對象遵循法律之成本。我國應持續關注隱私與監管科技的發展，在保障隱私的同時推動數位經濟的創新與可持續發展。

四、人工智慧模型訓練資料涉及個資的法源依據及資料保護基本原則

(一)會議探討數位時代青少年權益保護。調查顯示 15 至 24 歲族群社群媒體使用率達 94%，46%青少年「幾近全天上線」，凸顯數位依賴問題。

(二)依據英國資訊專員辦公室「合適年齡設計守則」建立青少年保護框架，建立涵蓋隱私預設設定、資料最小化及地理位置保護等層面的青少年保護框架。

(三)建議我國革新資訊素養教育，將科技風險意識納入正規教育課程體系，同時建立差異化的平台治理機制，要求社群平台針對不同年齡層實施分級保護措施。此外，強化平台業者的透明度義務，包括揭露演算法運作原則、明確說明個資運用方式，並提供直觀的隱私設定介面。這些措施旨在於推動科技創新與青少年保護間取得平衡，確保數位社會的永續發展。

籌備處同仁參與 GPA 大會活動合影