編號：(113)017.0901

# 全球跨境隱私規則（CBPR）計畫要求之研究

本研究報告內容僅供本會業務參考

國家發展委員會

中華民國 113 年 12 月

編號：(113) 017.0901

# 全球跨境隱私規則（CBPR）計畫要求之研究

委託單位：國家發展委員會

受託單位：財團法人資訊工業策進會

計畫主持人： 林冠宇 主任

計畫期程：決標日至 113 年 12 月 22 日

## 國家發展委員會

## 中華民國 113 年 12 月

## 摘要

隨著全球數位經濟的快速發展，資料跨境傳輸成為國際經濟活動的核心動力之一。面對人工智慧（Artificial Intelligence，以下簡稱「AI」）技術的快速進步，資料保護的複雜性與挑戰進一步增加，尤其是如何在促進資料自由流動的同時保障隱私和資料安全，這對各國現有的法律框架提出了更高的要求。為有效應對這類挑戰，國家發展委員會及財團法人資訊工業策進會科技法律研究所長期推動跨境隱私規則（Cross-Border Privacy Rules, CBPR）倡議，並代表我國參與亞太經濟合作（Asia-Pacific Economic Cooperation，以下簡稱「APEC」）數位經濟指導小組（Digital Economy Steering Group）資料隱私次級小組（Data Privacy Subgroup）下設之亞太經濟合作CBPR體系（APEC Cross-Border Privacy Rules system）及全球CBPR論壇（Global Cross-Border Privacy Rules Forum）。

本研究旨在針對全球跨境隱私規則計畫要求（Global Cross-Border Privacy Rules System Program Requirements，以下簡稱「全球CBPR計畫要求」），進行系統性地探討，以了解全球CBPR計畫要求的潛在發展方向，並基此參與其國際規範及標準之發展。為確保我國在全球資料保護標準變革中保持競爭力，並在未來國際隱私法制議題上保有話語權，本研究對下列議題進行深入研析，並提出對我國政策制定與法制調整的建議：(1)相互可操作性（interoperability）、(2)事故通知機制的完善需求，以及(3)AI技術的快速發展與其隱私影響，以及(4)其他有關全球CBPR計畫要求發展之重要議題。

本研究透過在國內舉辦全球CBPR論壇之國際研討會，蒐集彙整了國內外政府代表、專家學者以及產業界的意見與建議。研討會聚焦討論全球CBPR計畫要求中的關鍵議題，包括：如何應對AI技術帶來的資料隱私挑戰、如何完善事故通知制度，以及如何增強不同法制體系之間的相互可操作性。本研究彙整和分析了這些討論作為我國政策

與法制調整之重要參考。

此份報告亦將對我國及國外的個資保護法制、現有的CBPR框架進行文獻回顧，探討主要國家在資料保護與跨境資料傳輸方面的政策與實踐經驗，透過對不同法制體系在推動AI技術應用、加強事故通知機制、促進相互操作性等方面的策略進行對比研究，探討全球CBPR計畫要求的發展方向，並辨別出我國可能面臨的挑戰與機遇。

## Abstract

With the rapid development of the global digital economy, cross-border data transfer has become a core driver of international economic activities. The rapid advancement of Artificial Intelligence (AI) technology has further increased the complexity and challenges of data protection, particularly in balancing the free flow of data with privacy and data security. This situation demands higher standards from existing legal frameworks worldwide. To effectively address these challenges, the National Development Council and the Institute for Information Industry's Science and Technology Law Institute have long been promoting the Cross-Border Privacy Rules (CBPR) initiative, and representing Taiwan in the Asia-Pacific Economic Cooperation (APEC) Digital Economy Steering Group's Data Privacy Subgroup, participating in the APEC Cross-Border Privacy Rules (CBPR) system and the Global CBPR Forum.

This study aims to systematically explore the Global CBPR System Program Requirements to understand its potential development directions and participate in the development of international norms and standards. To ensure Taiwan's competitiveness in the evolving global data protection standards and maintain a voice in future international privacy law discussions, this study delves into the following topics and provides policy and legal adjustment recommendations for Taiwan: (1) interoperability, (2) the need to improve incident notification mechanisms, (3) the rapid development of AI technology and its privacy impacts, and (4) other important issues related to the development of the Global CBPR Program Requirements.

Through hosting the Global CBPR Forum Workshop in Taiwan, this study gathered and consolidated opinions and suggestions from domestic

and international government representatives, experts, scholars, and industry professionals. The Global CBPR Forum Workshop focused on key issues within the Global CBPR Program Requirements, including addressing privacy challenges posed by AI technology, improving incident notification systems, and enhancing interoperability between different legal systems. The discussions and analyses from these discussions provide important references for Taiwan's policy and legal adjustments.

This study also reviews the personal data protection laws and existing CBPR frameworks in Taiwan and abroad, examining the policies and practices of major countries in data protection and cross-border data transfer. By comparing strategies in different legal systems for promoting AI technology applications, strengthening incident notification mechanisms, and enhancing interoperability, this study explores the development directions of the Global CBPR Program Requirements and identifies potential challenges and opportunities for Taiwan.

# 目錄

## 壹、前言

為研究全球CBPR計畫要求之發展方向，強化我國在國際隱私規範制定上的參與，因應AI與資料跨境傳輸之相互影響並規劃我國政策法制需配合採取之措施，財團法人資訊工業策進會科技法律研究所受託辦理國家發展委員會「全球跨境隱私規則（CBPR）計畫要求之研究」，執行蒐集、研析全球CBPR計畫要求之改革方向，並辦理研討會蒐集各界實務看法。

本計畫之實施將依循計畫執行團隊長期所建立的研究方法論進行本專案之相關研究（參見下圖）。


【圖 1】專案研究方法

資料來源：本研究自行繪製

此一研究方法論主要立基比較法之研究，其實施步驟與內容為以下：

### 一、確認施政需求（即研究議題）

配合全球CBPR論壇大會（Global Forum Assembly，以下

簡稱GFA，為論壇最高決策機制）推動更新計畫要求之進程及向委託機關確認計畫要求研析內容。

## 二、我國產業、政策與法制現況檢視

針對研究議題，透過邀請專家參與或自行蒐集資訊方式，整理計畫要求研討項目對應的我國規範面及實務面現狀。

## 三、國際相關政策、法規與措施研析

透過國際間對於計畫要求研討項目對應的政策、法規或其他管制措施的整理分析，掌握國際間議題的發展狀況，以充實討論。

## 四、廣納各界意見與審酌利害關係人需求

舉辦國際研討會，廣納國內外政府代表及產業界意見人士、專家學者等產、官、學、研各界就計畫要求研討項目提供來自不同地域、專業背景的觀點，以充實整體對於計畫要求討論的深度及廣度。

## 五、研提相關之政策、推動措施或法規調適建議

根據研究結果及專家意見，針對計畫要求的研討項目提出相關之政策規劃建議，以作為未來政策之參考。

依本計畫所舉行之研討會，由國家發展委員會作為我國政府代表，及財團法人資訊工業策進會作為全球CBPR於我國唯一之當責機構（Accountability Agent, AA），共同擔任主辦單位。

本研究於民國113年11月18日（一）至21日（四）分別舉行了「全球CBPR計畫要求更新多方利害關係人會議」（Global CBPR Multi-stakeholder Discussion of Program Requirements）以及「2024年全球CBPR論壇臺北秋季研討會：蛻變」（2024 Fall Global CBPR Forum Workshop in Taipei: Evolving）兩場國

際研討會。有約90人、涵蓋24個不同國籍的國外與會者報名，包括來自美國、日本、澳洲、新加坡、巴西、泰國、馬來西亞、南非、墨西哥、孟加拉、尼泊爾、卡達、英國、菲律賓、西班牙、南韓、阿根廷、德國、迦納、以色列、印尼等國之政府、產業及學界代表。

## 貳、議題討論與分析

### 一、相互可操作性（Interoperability）

#### (一) 前言

##### 1. 相互可操作性的背景與重要性

(1) 全球資料治理的碎片化現象

在全球範圍內，不同國家與地區制定的資料保護框架反映了各自對資料主權、隱私保護及經濟增長的優先排序考量。例如，歐盟的《一般資料保護規則》（General Data Protection Regulation，以下簡稱「GDPR」）被視為全球隱私保護的高標準，注重資料主體權利的保障；而美國的資料治理則更多聚焦於權衡創新與市場競爭力。全球 CBPR 則試圖平衡隱私保護與經濟靈活性，特別是為中小企業提供了可行的參與路徑。這種多元化的資料保護模式導致了國際資料流通過程中的標準不一致問題，進而影響了企業的跨境運營效率以及法遵成本。

(2) 跨境資料流通的經濟與技術驅動力

跨境資料流通是數位貿易的核心基礎。例如，國際供應鏈需要依賴全球範圍內的資料共享以實現高效運作，而人工智慧與大數據技術的發展更需要多國資料的流動與整合。跨境資料流通已是全球經濟中不可或缺的一部

分。然而，法律與技術障礙使這樣的潛力無法完全發揮，亦凸顯出建立相互可操作性機制的必要性。

(3) 相互可操作性的核心內涵

值得注意的是，相互可操作性並非試圖統一所有隱私框架，而是希望透過政策協調與技術適配，實現不同框架間的相互承認與合作。這種模式強調在尊重各國法規主權的基礎上，尋求跨境資料治理的共同原則與標準，以平衡資料安全與流通需求。

2. **本次研討會的討論焦點**

相互可操作性是本次全球 CBPR 論壇 2024 秋季臺北研討會的核心議題之一，並針對以下三大方面進行了深入討論：

(1) 全球 CBPR 框架與其他國際標準的互補性

與會者特別聚焦於全球 CBPR 框架如何與其他國際標準（如 GDPR）形成互補關係。例如，全球 CBPR 框架以當責機構驗證為核心，提供靈活的資料法遵機制，而 GDPR 則透過標準契約條款（Standard Contract Clauses，SCCs）實現資料傳輸的法律保障。這種互補性為多邊框架間的合作提供了新的可能性。

(2) 技術與政策的協同作用

隱私強化技術（Privacy Enhancing Technologies，PETs）

如同態加密[1]、差分隱私[2]及聯邦學習[3]等在本次研討會中被多次提及。與會者認為，這些技術能夠在保護隱私的同時促進資料共享，是實現相互可操作性的重要途徑。此外，政策層面的協調則需要在多邊對話中建立共同原則，以降低企業法遵負擔。

(3) 推動亞太地區資料治理的示範作用

亞太地區作為全球經濟增長的主要驅動力，其資料治理模式具有重要的示範作用。例如，我國[4]的全球 CBPR 計畫要求實踐與新加坡[5]在資料共享協議中的靈活設計都展示了本地法規與國際框架結合的可行性。本次研討會中，來自亞太各國的代表深入探討了如何在區域合作中推動相互可操作性，並進一步影響全球資料治理趨勢。

## 3. 國際趨勢與挑戰

[1] 同態加密（Homomorphic Encryption）是一種加密技術，在不解密資料的情況下，直接對加密後的資料進行特定的運算，且解密後的結果與對不解密資料進行相同運算所得的結果一致。換言之，資料在加密狀態下即可被處理，無需揭露原始內容，從而在確保隱私的同時，進行運算。KUNDAN MUNJAL & REKHA BHATIA, *A systematic review of homomorphic encryption and its contributions in healthcare industry* (2022), https://link.springer.com/article/10.1007/s40747-022-00756-z (last visited December 16, 2024).

[2] 差分隱私（Differential Privacy）是一種資料保護技術，透過在資料中加入適當的隨機雜訊，使得對資料集進行統計分析時，無法確定某個特定個體是否包含在資料集中，從而保護個人隱私。其核心概念是，讓資料使用者無法從查詢結果中推斷出特定個體的資訊。YUVAL DAGAN & GIL KUR, *A bounded-noise mechanism for differential privacy* (2022), https://proceedings.mlr.press/v178/dagan22a/dagan22a.pdf (last visited December 16, 2024).

[3] 聯邦學習（Federated Learning）是一種分散式的機器學習方法，讓多個設備或機構在不共享原始資料的情況下，協作訓練共同的模型。每個參與方在本地使用自己的資料訓練模型，然後僅上傳模型參數到中央伺服器，伺服器將這些聚合，形成全局的模型。此機制確保了資料的隱私，因為原始資料始終保留在本地，未被移轉或共享。VENKATA NAGA SAI KIRAN CHALLA, *Federated Learning: Collaborative Ml without Centralized Data* (2022), https://www.ijaresm.com/products/download_document/document_file/Venkata_Naga_Sai_Kiran_Challatq5k.pdf (last visited December 16, 2024).

[4] 我國資策會科技法律研究所王德瀛組長在研討會第一天的當責機構座談（Accountability Agents Panel）中以基於我國《個人資料保護法》發展之「臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System，以下簡稱 TPIPAS）」與 CBPR 結合為題，並舉 TDCC（臺灣集中保管結算所）首先取得 TPIPAS，後成功通過 CBPR 認證，成為臺灣首家通過 CBPR 之公司為例，突顯出 CBPR 與我國現行 TPIPAS 的相容性，也是我國隱私保護制度與國際接軌的成功實務案例。

[5] 新加坡資訊通信媒體發展局國際關係、政策與策略主任 Evelyn Goh 在研討會第一天的當責機構座談（Accountability Agents Panel）中提到，新加坡以資訊通信媒體發展管理局（IMDA）為核心，透過結合新加坡《個人資料保護法（Personal Data Protection Act）》和 CBPR 系統，建立了國際標準與本地法規相融合的隱私保護模式。新加坡企業可藉由第三方審核機構完成認證，確保隱私管理法遵性，並藉此參與跨境業務，提升全球市場信任。

(1) 全球資料治理面臨的新挑戰

在國際資料治理領域，新技術的應用與地緣政治的影響亦帶來新的挑戰。例如，人工智慧、大數據及物聯網的發展對於資料流通的需求日益增長，但資料主權與隱私保護的要求，卻也可能限制了此等發展的前景。此外，地緣政治緊張局勢亦使得國際間的合作變得更加複雜，特別是在資料傳輸標準與技術規範的制定上，國家或聯盟間的對立儼然成為資料流動的阻力。

(2) 相互可操作性的實現潛力

面臨諸多挑戰，相互可操作性應被視為未來資料治理的最佳路徑。透過政策與技術的雙軌推進，可以在不同框架間建立互認機制，既保留各國的法規主權，又為跨境資料流通提供穩定的運行基礎。本次研討會中的討論強調，技術創新與政策協調的結合是實現相互可操作性的核心動力。

4. **小結**

相互可操作性作為全球資料治理的重要概念，不僅能有效解決當前國際框架間的分歧，還能為跨境資料流通的未來發展提供新的方向。本次研討會透過分析全球 CBPR 框架與其他標準的協作可能性，並探討技術與政策在相互可操作性中的作用，為全球資料治理提供了實踐經驗與戰略參考。

## (二) 國際框架間的挑戰

### 1. 法律與政策層面的分歧

國際資料保護框架的核心目標是促進跨境資料的安全流通，但各框架在設計理念、執行方式及重點關注領域上的差異，給多邊合作帶來挑戰。

(1) 理念差異：GDPR 與全球 CBPR 的比較

歐盟的 GDPR 以保障資料主體權利為中心，對資料的收集、處理、存儲及跨境流通設置了相對嚴格規範。GDPR 要求企業必須取得資料主體明確同意，並確保資料主體享有撤回同意、要求刪除及查詢使用目的的權利。相比之下，全球 CBPR 計畫要求則側重於透過當責機構的第三方驗證，強化企業法遵能力以符合課責（Accountability）原則 ，並為中小企業提供更加靈活的參與方式。這種理念上的差異使得兩個框架在法律適配性上面臨挑戰。

(2) 國家對資料主權的不同解讀

國家資料主權的概念越來越受到重視，特別是在地緣政治緊張局勢下，一些國家傾向於加強資料本地存儲要求，以保障國內產業與數位基礎設施的安全，且對於全球 CBPR 這樣的跨境資料移轉框架抱持消極的態度。

(3) 對隱私與經濟增長的不同權衡

部分國家在隱私保護與經濟增長之間傾向於更強調前者，而其他國家則認為資料流通的靈活性是推動創新與商業活動的核心。這種權衡的差異，影響各框架在優先事項上的設計，進一步加劇政策協調的難度。

2. **操作層面的障礙**

除了政策上的分歧，框架間的操作性差異，在實務上也帶來明顯的挑戰。企業在進行跨境資料流通時，需同時滿足多個框架的要求，這對於操作效率與法遵成本產生了直接影響。

(1) 多框架法遵的重疊性

GDPR 要求跨境資料流通需依賴標準契約條款或適

足性決定，這需要企業投入大量資源處理契約文件與內部審核流程。同時，全球 CBPR 框架要求企業透過當責機構驗證，以證明其在資料隱私保護上的法遵能力。這些要求的重疊使企業在全球多管轄權運營時需面臨複雜的法遵壓力。例如，一家科技公司若同時在歐盟、亞太地區及美國經營，需同時遵守 GDPR、亞太地區所在國及美國當地法律的多重規範，導致運營效率降低。

(2) GDPR 與全球 CBPR 的適用性議題

不同框架對於資料流通的適用範圍和標準定義不同。例如，GDPR 要求明確定義個人資料的處理範圍，而全球 CBPR 計畫要求則著重於跨境資料傳輸的管理與企業問責機制。這種適用性的不一致增加了操作層面的不確定性，特別是在新興技術（如人工智慧和大數據分析）應用中，企業往往難以確定應採用哪一套標準。

(3) 技術標準的差異

框架間技術標準的不一致進一步限制了操作的便利性。例如，隱私強化技術如同態加密和聯邦學習雖受認可，但在不同國家和地區的落地標準和技術要求上仍存在差異。這些技術在遵循不同框架的規範時往往需進行額外的調整，導致其應用的成本上升。

3. **企業參與的壓力**

在面對不同框架的要求下，許多企業，特別是中小型企業，面臨著越來越大的參與壓力。這種壓力主要來自於資源限制、技術能力不足及法遵成本增加等方面。

(1) 中小企業的法遵挑戰

中小企業往往缺乏足夠的內部資源來應對複雜的法

遵要求。例如，一家亞太地區的小型製造企業在拓展歐洲市場時，需滿足 GDPR 的要求，同時還需透過全球 CBPR 計畫要求下的當責機構驗證，針對同一事實可能需進行重複的驗證與行政作業程序，故而增加企業的財務及人力資源成本支出。

(2) 高成本對全球市場參與的影響

法遵成本的上升可能使得一些中小型企業無法參與國際市場。例如，中小型企業在實施 GDPR 的過程中平均需投入高額的法遵費用，而全球 CBPR 計畫要求的驗證成本則視企業規模而異，對於中小型企業而言亦將增加支出。這些成本壓力使得中小型企業往往選擇避開國際市場，導致全球市場參與降低。

(3) 技術能力的不足

中小企業在面對隱私強化技術或數位法遵工具的需求時，往往缺乏專業的技術能力來有效運用。例如，聯邦學習等技術的實施需要專業知識與技術資源，這對於技術儲備有限的企業而言可能是一項挑戰。

4. **小結**

國際框架間的挑戰不僅僅是政策設計上的分歧，更體現在操作層面的實施障礙及企業參與的現實壓力中。本次研討會明確指出，解決這些挑戰的核心在於促進政策協調、技術標準化以及降低法遵成本，從而為企業與政府創造更加友好的相互可操作性環境，而全球 CBPR 即可被視為解決隱私法制破碎化的可能解決途徑之一。

## (三) 相互可操作性的實現路徑

要實現相互可操作性，必須從政策協調、技術標準化及推動

最佳實務三個層面入手。本次研討會針對這些實現路徑提供了豐富的討論，並提出了具體的建議。

1. **政策協調**

政策協調是實現相互可操作性的核心，尤其是在多國框架間建立一致的原則與標準方面。

(1) 制定共同原則

本次研討會多次強調，建立共同的核心原則是促進政策協調的基礎。例如，資料透明性、資料主體權利及跨境資料流通的合法性已成為大多數框架的共識。在此基礎上，與會者建議應制定更具體的政策指導原則，例如資料用途限制和第三方分享的明確規範，以減少國際框架間的差異。

(2) 推進多邊協議

全球 CBPR 作為跨境資料流通框架，其成功為其他多邊協議提供了借鑒。與會者建議應透過區域合作與多邊對話，推動全球 CBPR 與 GDPR 等框架間的政策對接。例如，可以考慮建立跨框架的合作機制，允許不同框架間的互認，並為企業提供更簡單的法遵路徑。

(3) 促進準會員制度的應用

在本次研討會中，日本代表分享了其在推動全球 CBPR 準會員制度方面的經驗。該制度允許新興經濟體以準會員（Associate）身分參與全球 CBPR 體系，從而逐步過渡到完全符合法令。這種靈活的制度設計為其他新興經濟體加入全球資料治理提供了新路徑，並有助於加速推進全球 CBPR 體系的全球化進程。

(4) 提升國家間政策透明度

政策協調的一大挑戰在於不同國家政策的透明度和一致性不足。亦有專家建議，應彙整各國資料法規資訊，促進法規細節的公開與交流，幫助企業更快速地了解不同框架的要求，從而減少法遵過程中的不確定性。

2. **技術標準化**

技術標準化在相互可操作性中的作用不可忽視。隱私強化技術（Privacy Enhancing Technologies，PETs）的應用已被多次證明能有效解決框架間技術障礙。

(1) 推動隱私技術的應用

隱私強化技術如同態加密、差分隱私及聯邦學習在多國的試點計畫中已取得成效。與會者指出，這些技術能夠在保護個人資料隱私的同時實現資料的有效共享，應被視為是實現相互可操作性的重要途徑。

(2) 建立通用的技術工具

目前不同國際框架對技術應用的要求尚存差異。例如，GDPR 強調對資料使用的透明性，而全球 CBPR 則更注重企業對資料的管理責任。與會者建議應開發一套通用技術工具，幫助企業在不同框架間快速適配。這些工具可以包括標準化的資料加密協議、資料流通的審核機制及跨框架的法遵評估工具。

(3) 標準化技術實驗與測試

技術標準化的另一個挑戰在於不同技術的實驗性質和適配性。與會者提到，國際合作中應設立一套統一的技術測試標準，例如在跨境資料傳輸中測試隱私強化技術的性能與安全性，以確保其在多框架環境中的應用效果。

(4) 鼓勵技術創新與公共資金支持

與會者一致認為，應進一步支持技術創新，特別是在隱私強化技術的研究與應用上。政府應提供公共資金支持，建立國際技術創新合作機制，確保技術能夠更快地轉化為實際應用。例如，G7 的技術創新基金和亞太地區的技術合作平臺，都為標準化的技術創新提供了重要的參考依據。

3. **最佳實務的成功案例分享**

成功案例是推動相互可操作性的重要實務案例參考，突顯出不同框架在操作層面相容的可行性。

(1) Google 的跨框架法遵實踐

Google 成功將全球 CBPR 驗證與 GDPR 法遵結合，透過內部資料管理系統實現了多框架下的高效資料處理。例如，Google 利用差分隱私技術，在滿足歐盟 GDPR 要求的同時，保障了跨境資料流通的安全性與透明性。該案例顯示，大型跨國企業能夠透過內部技術與政策整合，實現多框架間的相容性。

(2) 臺灣集保(TDCC)驗證的成功經驗

在本次研討會中，臺灣集保（TDCC）獲得 CBPR 驗證被視為是我國的成功案例。TDCC 在驗證過程中採用了多項創新技術，包括資料透明性報告工具及內部法遵監管平臺，這些技術不僅提高了法遵效率，還提升了企業的國際信任度。

(3) 日本與新加坡的政策整合

日本與新加坡在國內法規中成功融入全球 CBPR 體系，展示了政策協調與實踐的可能性。例如，日本的個

人情報保護委員會（Personal Information Protection Commission, Japan）採取了多層審查模式，確保企業在透過全球 CBPR 驗證的同時，滿足國內法規的要求。新加坡則透過靈活的資料共享協議，平衡當地政策與國際框架的需求。

(4) 新興經濟體的初步試點

與會者還分享了一些新興經濟體參與全球 CBPR 體系的試點計畫，探索如何將全球 CBPR 體系與本地法規相結合，以吸引更多跨國企業進入市場。

4. **小結**

政策協調、技術標準化及成功案例的實踐是實現相互可操作性的關鍵路徑。本次研討會提出了一系列切實可行的建議，包括制定共同原則、推動技術創新以及鼓勵新興經濟體參與多邊合作，這些措施將為全球資料治理提供重要的依據。

### (四) G7 可信任資料流通計畫（DFFT）對相互可操作性的啟示

G7 資料自由流通與信任（DFFT）計畫以「3C」原則（Commonality 共通性、Complementarity 互補性，與 Convergence 趨同性）為基礎，提出一套實現全球資料治理相互可操作性的框架，為其他多邊機制如全球 CBPR 提供了重要的啟示。在本次研討會中，與會者特別探討了 DFFT 的核心理念及其在促進跨境資料流通中的成功經驗。

1. **DFFT 的核心理念與實踐經驗**

DFFT 的「共通性（Commonality）」強調各國在資料治理中應識別相似之處，並透過共同的技術工具與政策原則建立資料保護的基礎框架。例如，G7 成員國在資料透明性和隱私技術（如差分隱私）的應用上已經達成了一致共識，這為跨境資料的安

全共享奠定基礎。

其「互補性（Complementarity）」則表現為各國資料保護機制在功能上的相輔相成。例如，GDPR 的嚴格資料保護條款可補充全球 CBPR 體系中針對中小企業的靈活驗證機制，形成一種既保證高標準又具實用性的全球資料治理模式。

「趨同性（Convergence）」的核心在於逐步縮小不同法規間的差距，這為全球性的資料治理標準化提供了可能性。DFFT 的倡議促使成員國在政策設計中考量如何適應不同的國際合作需求，此一理念對於其他體系的設計具有重要借鑒意義。

2. **DFFT 與全球 CBPR 體系的互補與協作機制**

DFFT 框架主要提供政策協調的宏觀框架，而全球 CBPR 則專注於微觀層面的驗證與法遵實施。與會者指出，這種「政策—實務」的協作關係為國際多邊合作提供了一種具有參考價值的依據。例如，在 DFFT 的指導下，G7 成員國探索了如何利用全球 CBPR 的當責機構機制加速驗證流程，同時保證驗證的合法性與透明性。

此外，DFFT 提出的技術標準化也為全球 CBPR 的進一步發展提供啟發。DFFT 倡導的隱私技術（如聯邦學習與零知識證明）不僅提升了資料處理的安全性，也為全球 CBPR 體系的技術適配提供了可行性。與會者建議，未來應將這些技術作為全球 CBPR 標準的一部分，進一步加強兩者的互補性。

3. **DFFT 的全球化價值**

DFFT 框架的成功推行表明，政策與技術的結合是實現全球資料治理的有效路徑。未來，DFFT 與全球 CBPR 的深度協作將不僅限於亞太和 G7 地區，還應擴展至更廣泛的國際合作中。例如，DFFT 的成功經驗可用於指導新興經濟體加入全球 CBPR 體系，透過政策與技術雙管齊下的方式，實現全球資料治理的

一體化。

## (五) 臺灣在相互可操作性中的角色

### 1. 作為區域資料保護合作的典範

我國在資料保護和治理方面展現了強大的適應力與創新力。TDCC 成為首家通過全球 CBPR 驗證的臺灣企業，其成功案例表明，我國在政策與技術協調方面具備實踐經驗，並為其他亞太經濟體提供了重要的參考。

TDCC 在驗證過程中，結合了本地法規與全球 CBPR 體系的要求，建立了一套高效的 TPIPAS 系統，該系統不僅提升了資料流通的透明度，也強化了國內企業的國際信任度。這表明，我國可以作為亞太地區推進資料保護合作的典範，特別是在本地法規與國際框架整合的實務經驗上。

### 2. 推動相互可操作性的技術與政策建議

我國在全球資料治理中的角色不僅限於上述案例，更可作為技術創新與政策協調的催化劑。我國的技術創新能力使其能夠在隱私強化技術的研究與應用上發揮領導作用。例如，臺灣在聯邦學習和資料加密技術的開發上已取得顯著進展，這些技術可以直接應用於全球 CBPR 體系中，以促進跨境資料流通的安全性與高效性。

同時，我國應積極參與多邊政策對話，特別是在 DFFT 與全球 CBPR 體系的協作中扮演更重要的角色。透過參與 G7 的政策設計討論，我國可以幫助橋接亞太地區與歐美國家的資料治理需求，進一步提升自身的國際影響力。

### 3. 人才培育與國際合作

為了長期支持全球資料治理，我國應加強資料治理相關專業人才的培養，特別是在技術創新與跨境法遵方面。政府應與

學術界及產業界合作，建立專業培訓計畫，投入資源，確保有足夠的人才資源支援我國在國際資料治理中的參與。同時，與國際研究機構的合作也將有助於我國掌握最新的技術趨勢，並將其應用於本地與國際體系中。

## (六) 建議與結論

### 1. 短期建議

(1) 推廣全球 CBPR 體系在我國的應用：

全球 CBPR 體系是一項同時促進經濟發展與保障個人隱私的戰略工具。對經濟發展而言，全球 CBPR 為企業提供了國際驗證的標準化工具，特別適合中小企業以較低成本進入全球市場。對於個人隱私的保護，全球 CBPR 體系的高標準要求，能有效提升資料主體對隱私權的信任。

為此，政府應加速推廣全球 CBPR 在國內的應用，尤其針對國營事業進行重點宣傳與支持，確保其在資料保護與經濟效益上的雙重提升。國營事業作為國內企業的標竿以及重要的經濟參與者，其率先通過 CBPR 驗證不僅能樹立示範作用，帶動其他企業跟進，還能提升我國在國際資料治理中的形象與信任度。建議將全球 CBPR 驗證納入國營事業的考成辦法，例如將其列為績效評估的加分項，以鼓勵國營事業率先取得驗證，進一步帶動其他產業參與。此外，國營事業的參與也能彰顯政府對國家安全與資料治理的重視，發揮帶頭作用。

(2) 提供資源予我國隱私主管機關與智庫：

國家隱私治理的成功離不開穩健的政策設計與執行能力。我國隱私主管機關與智庫應被視為國家安全、

經濟發展與個人隱私保障的基石。政府應投入必要資源以增強這些機關（構）的專業能力，例如提供政策研究經費、增聘技術人才及提升行政效率。這將使我國在國際資料治理對話中更加主動，並在資料安全與隱私保護議題上成為區域領袖。

資源支持還應包括培養公眾隱私意識，透過與智庫合作開展教育計畫，提升民眾對於跨境資料治理與隱私權的理解。這不僅能鞏固國內的社會共識，也能強化我國在推動全球 CBPR 落地中的法制與文化基礎。

(3) 建立國際多邊協作機制：

全球 CBPR 體系為國際合作提供了實現資料治理目標的典範。臺灣作為亞太經濟體的重要成員，可透過建立多邊協作機制，促進資料治理的國際對話與合作。例如，成立一個以臺灣為中心的區域資料治理聯盟，結合產業、學術界及政府資源，推動亞太地區的資料保護標準化與技術創新。

這種協作將有助於同時實現三大戰略目標：首先，在國家安全層面，跨境資料合作可加強對潛在威脅的防範；其次，在經濟層面，與全球市場同步的標準有助於吸引外資並提升產業競爭力；最後，隱私保障的提升將進一步穩固我國國民之信任，為資料驅動型經濟奠定基礎。

2. **中長期建議**

(1) 推動全球 CBPR 與其他體系的深度整合：

隨著資料治理議題的全球化，全球 CBPR 體系與 GDPR、DFFT 等國際標準的互操作性將成為未來的趨勢。我國應主動參與相關國際對話，促進體系間的深

度整合。例如，可透過雙邊或多邊合作，制定跨體系資料傳輸協議，建立統一的驗證機制，減少企業在多體系間法遵的重疊成本。

此一整合策略不僅能幫助企業在全球市場中更靈活地運作，也能進一步提升我國對資料流通安全的掌控力，實現國家安全與經濟發展的雙贏。同時，參與這些國際合作還將鞏固臺灣在全球資料治理格局中的地位，為未來進一步參與更多國際體系奠定基礎。

(2) 強化技術創新能力：

隱私強化技術是實現全球 CBPR 體系長期目標的重要技術支柱，包括同態加密、差分隱私及聯邦學習等創新技術。這些技術能有效保護個人隱私，並提升資料處理的效率與安全性。建議政府設立專項資金支持此類技術的研發與商業應用，並與國際技術機構合作，將臺灣打造為全球資料治理技術創新的樞紐。

例如，我國可建立跨部會的技術創新促進機制，針對隱私強化技術提供專業指導與資金補助，並鼓勵企業在實際業務中進行試點應用。同時，可推動這些技術標準納入國際資料治理框架，強化臺灣在隱私技術領域的影響力，為國家安全、經濟發展與個人隱私提供更堅實的技術保障。

(3) 支持新興經濟體參與國際合作：

臺灣在全球 CBPR 體系中的參與經驗為新興經濟體提供了寶貴的參考價值。建議我國發揮技術與政策協同優勢，協助亞太地區的新興經濟體融入全球 CBPR 體系。例如，可提供技術培訓、政策設計諮詢以及驗證支持，幫助這些國家快速適應全球資料治理的

需求。

透過這種合作，臺灣不僅能推動區域整體的資料治理進步，也能鞏固自身在國際隱私議題中的話語權。同時，新興經濟體的參與將進一步強化全球 CBPR 體系的全球覆蓋力，為臺灣企業進入更多新市場提供便利，從而實現經濟利益與國家安全的平衡發展。

### 3. 未來展望

隨著全球資料治理進一步深化，臺灣在推動全球 CBPR 體系的應用中具備獨特的戰略優勢與潛力。未來，全球 CBPR 體系不僅將成為臺灣與國際接軌的重要橋樑，也將成為鞏固國家安全、促進經濟發展與保障個人隱私的核心基礎。

展望未來，臺灣應以四大目標為主軸，明確發展方向：

(1) 成為亞太區域資料治理的領頭羊

臺灣可透過技術創新與政策協調，成為亞太地區資料治理的楷模。未來應進一步優化國內的全球 CBPR 推行機制，確保企業在資料隱私與跨境資料流通中具備國際競爭力。臺灣亦可藉由參與亞太經濟合作（APEC）相關論壇與框架，擴大在亞太區域內的影響力，提升資料治理的標準化程度。

(2) 打造隱私技術的創新中心

在隱私強化技術（PETs）快速發展的背景下，臺灣有潛力成為全球隱私技術創新與應用的核心基地。未來應投入更多資源支持技術開發，特別是在聯邦學習、差分隱私及同態加密等領域，打造技術研究與實踐的生態圈。同時，鼓勵國內企業與國際機構合作，將這些技術納入國際標準，確保臺灣在資料治理技術層面

的領先地位。

(3) 深化與主要經濟體的國際合作

臺灣應加強與主要經濟體(如美國、歐盟及日本)的資料治理合作，透過雙邊或多邊協定，實現政策對接與技術共享。這不僅能為我國企業創造更多參與國際市場的機會，也能提升臺灣在資料治理領域的國際話語權。與此同時，持續參與國際資料治理討論，確保臺灣的利益與立場能夠在未來全球體系設計中被納入考量。

(4) 強化本地資料治理能力，推動數位轉型

臺灣在推進全球 CBPR 的過程中應同步加強本地資料治理能力，建立全方位的隱私保護與法遵機制，為我國國內數位經濟轉型提供穩定基礎。這包括提升中小企業的法遵意識與技術能力，鼓勵更多企業參與全球CBPR體系,打造更具競爭力的數位經濟生態圈。

未來，我國可將全球 CBPR 體系視為與全球接軌的策略性工具，不僅促進跨境資料流通的便利性，還能鞏固臺灣在數位時代的國際競爭力。透過持續的政策創新、技術突破與國際合作，臺灣有望成為全球資料治理領域的重要參與者，並以此推動國家安全、經濟成長與社會信任的全方位進步。

## 二、事故通知（Breach Notice）

### (一)前言

在數位經濟快速發展的背景下，個人資料的保護已成為國家治理的重要議題。本次「全球 CBPR 國際研討會」針對隱私保護與跨境資料流通進行多層次探討，特別聚焦於事故通知

（Breach Notice），討論其在國家安全、經濟發展與個人隱私三個層面的核心意義及影響。事故通知是一項要求資料控制者或處理者在資料事故發生後，迅速向受影響的個人或主管機關通報的制度。

全球 CBPR（Global Cross-Border Privacy Rules）體系作為一項基於共通原則的驗證制度，應否將制度標準化規範，有助於促進跨境資料安全流通，同時兼顧隱私保護與經濟發展需求。本報告將結合會議中專家學者的分享與相關國際案例，從上述三個層面闡釋事故通知制度的重要性，並總結全球 CBPR 體系如何通過制度設計實現多重目標。

## (二)事故通知的核心意義

### 1. 國家安全層面：應對資料事故風險，維護關鍵基礎設施安全

個資事故小至影響個人，更可能提高為國家安全的漏洞，特別是當涉及關鍵基礎設施（如金融、能源或醫療系統）時，其影響更為深遠。全球 CBPR 體系通過要求企業建立事故的應對計畫與通知流程，確保事故的快速響應與處置，從而降低資料事故的國家安全風險。

以本次會議討論的馬來西亞 2024 年個人資料保護法修正為例，該國在法規中新增資料外洩通知的要求，針對控制者向主管機關、處理者向控制者，以及控制者向資料主體的三類通知作出規範，並設置具體時間限制（如 72 小時內通知）。這種快速通報機制有助於識別並遏制可能發生的國家安全威脅，並加強多邊合作以應對全球性的風險。

### 2. 經濟發展層面：提升企業信任度，促進跨境商業合作

在全球化經濟中，跨境資料流通是數位貿易的基石。然而，個資事故往往損害企業信譽，影響國際商業合作與經濟活動。全球 CBPR 體系以認證機制為核心，要求企業遵循標

準化的隱私保護與資料外洩通知程序，從而提升國際社會對企業資料治理能力的信任度，進一步促進數位經濟的發展。本次會議中亦有與會者曾提及在亞洲標準契約條款（MCCs）與 CBPR 體系比較下， 可知 MCCs 針對中小企業提供靈活的規範，而 CBPR 則通過驗證機制建立更高層次的信任。期望兩者能相輔相成，為地區企業參與全球數位貿易創造更多機遇，並且降低資料事故對經濟活動的負面影響。

3. **個人隱私層面：強化個人權利保護，提升隱私透明度**

事故通知直接關乎資料主體的知情權與隱私保護。通過向受影響的個人及時通報資料事故，事故通知機制可以幫助個人評估潛在風險，並採取相應措施來保護自身權益。例如 CBPR 體系要求企業提供透明的資訊揭露流程，包括事件性質、可能影響的範圍以及資料主體可以採取的保護措施等，確保資料主體能夠及時作出反應；又例如韓國代表在本次會議中分享的合成資料[6]（Synthetic Data）應用案例，展示如何結合技術創新與隱私保護來提升資料治理的透明度與安全性。韓國推出的資料參考模型（data reference model）提供 5 個領域的合成資料集，透過匿名化處理與安全評估，既保障個人隱私，同時支持 AI 模型訓練等創新應用[7]。

## （三）全球 CBPR 體系制度改革方向

在推動事故通知制度的進程中，全球 CBPR 體系提出多項創新與實用的改革方向，為提升隱私保護與跨境資料治理奠定

[6] 合成資料是指通過資料生成技術人工創建的虛擬資料，其統計特徵與原始資料集相似，但不包含任何個人的實際資料。這種技術的目的是在不揭露個人隱私的前提下，提供可用於研究、開發和測試的資料集。SURENDRA .H, DR. MOHAN .H .S, *A Review Of Synthetic Data Generation Methods For Privacy Preserving Data Publishing* (2017), https://ijstr.org/final-print/mar2017/A-Review-Of-Synthetic-Data-Generation-Methods-For-Privacy-Preserving-Data-Publishing.pdf (last visited December 16, 2024).

[7] South Korea: PIPC releases synthetic data generation reference model, DataGuidance, https://www.dataguidance.com/news/south-korea-pipc-releases-synthetic-data-generation (last visited December 16, 2024).

基礎：

1. **標準化規範以強化跨境資料保護能力**

全球 CBPR 體系致力於為不同區域提供統一的方針，改革方向聚焦於加強當責機構的設置，以協助監督企業遵守事故通知要求。這有助於在降低跨境法遵成本的同時，促進成員國之間的信任與合作，進一步提升跨境資料流通的安全性。

2. **靈活性設計以適應多元法律環境**

允許成員國根據其國內法制進行調整，未來可能涵蓋事故通知的具體時間限制與通報程序設計，成員國可結合其司法需求設定具體要求，既保持制度的一致性，又反映地方法律的適用性，為多元化法律環境中的跨境合作提供更靈活的彈性。

3. **第三方認證以增強企業責任與透明度**

為進一步完善第三方驗證流程，確保企業的資料保護政策與事故通知程序符合國際標準。同時，當責機構在事故發生後的迅速介入與支持角色也有望強化，從而提升事件應對的效率與加強企業責任的透明度。

(四)**挑戰與未來展望**

儘管全球 CBPR 體系在事故通知方面取得顯著進展，但仍需面對以下挑戰：

1. **技術標準化的不足**

不同司法管轄權對資料外洩的定義與應對標準存在差異，影響跨境執行的效率。未來需進一步推動技術標準的國際化，以實現體系間的互操作性。

2. **中小企業的法遵壓力**

對於技術資源有限的中小企業而言,遵守外洩通知要求可能帶來額外的成本與負擔。建議未來可考慮引入更靈活的指引與支持措施，幫助中小企業提升法遵能力。

3. **政府機構的合作與信任**

全球 CBPR 體系需進一步促進成員國之間的監管合作，特別是在處理涉及國家安全的事故時,需建立更高效的通報與協作機制。

### （五）小結

事故通知作為隱私保護的重要機制，其價值不僅在於個人隱私保障，還延伸至國家安全與經濟發展領域。全球 CBPR 體系通過標準化的制度設計、靈活的政策調適與創新的第三方認證，為實現跨境資料保護與隱私治理提供有效的途徑。

未來，全球 CBPR 應繼續深化國際合作，完善技術與政策的協調機制，推動更具包容性與實用性的資料治理模式。隨著數位經濟的持續發展，事故通知制度的完善性，將為全球隱私治理與個資保護奠定更加穩固的基礎。

## 三、人工智慧（Artificial Intelligence）與隱私

### （一）AI 的隱私風險問題

1. **AI**

AI 目前沒有一個通用的定義，AI 所指為何，部分取決於當下關心的問題為何。在討論 AI 的隱私風險時，成為討論核心焦點者，是在當今得到大量投入運用的商業模型，而不是 AI 研究初期所指的有效的老式人工智慧（Good Old-Fashioned Artificial Intelligence, GOFAI）。

根據 OECD「理事會針對 AI 的建議（Recommendation of the Council on Artificial Intelligence）」，AI 系統是「一個為了外顯或內隱的目標，從其收到的輸入中推斷出如何生成輸出，例如可能影響物理或虛擬環境的預測、內容、建議或決策的機器系統。不同的 AI 系統在部署後的自主性和適應性程度各不相同。」[8]從當今 AI 開發的實務來看，此些機器系統的自主性與適應性透過一系列功能、機制來展現，例如：為了輸入環境、物件和語言等外部資訊的電腦視覺（Computer Vision）、語音辨識（Speech Recognition），為了儲存、處理輸入資訊以供資料處理的知識表示（Knowledge Representation），對資料進行分析、運算輸出的自然語言處理（Natural Language Processing）、執行和訓練演算法的機器學習（Machine Learning）、自動推理（Automated Reasoning）和與環境進行互動的機器人學（Robotics）等。根據不同的功能與機制組合、目的設定與訓練差異，被稱為 AI 的機器系統間彼此之間所展現的差異非常巨大，因此，所謂 AI 的隱私風險也必須取決於在具體脈絡中，個人資料在機器系統的各項功能和機制組成之生命週期中可能如何儲存、傳輸與處理，以及個人與組織是否及如何參與當中，影響其過程與結果。

2. **隱私風險**

於評估 AI 的隱私風險時，分析風險應包含三個子元素：危害（Hazard）、暴露範圍（Exposure）和弱點（Vulnerability），並檢視 AI 如何導致其變化，亦即確認個資在 AI 生命週期的各個環節中可能如何被儲存、傳輸與處理及可能被誰處理，

[8] Organization for Economic Cooperation and Development [OECD], Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 3, 2024), available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (last visited December 16, 2024).

並從而標示出隱私規範上的重點，其隱私危害、暴露範圍與可能使當事人蒙受損失的弱點，在此基礎之上，才能進一步討論如何界定對相關人員在具體規範上的要求與責任。

所謂的隱私危害，指的是因資料外洩或濫用等個人資料之不當處理，致生個人或群體的隱私損害，以及因此所損及之隱私權所欲直接保護或間接促進的個人和社會利益，包括：日常生活中自我呈現管理的控制、名譽、自主性、安全、平等、福祉和政治民主。基本上，不論 AI 是否被採用，隱私危害所指涉的對象基本上不會有太多變化。與此相對，AI 大幅地影響了風險暴露的時間與空間範圍，也放大了當事人的弱點。

在組織外部，AI 隱私風險主要涉及個資安全，亦即個資之機密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。惡意的使用者可能會利用 AI 帶來的強大且即時的資料處理能力攻擊組織的系統，以不法存取、編輯或銷毀組織所保管的當事人個資。世界經濟論壇（WEF）網路安全中心的研究員 Giulia Moschetta 和 Joanna Bouckaert（2024）就觀察到，「AI 將導致現有戰術、技術和程式的發展和增強，降低網路犯罪行為人的門檻，減少發起網路攻擊所需的技術知識。新的大型語言模型（LLM）也推動了社交工程（Social Engineering）的發展，行為人藉此創建了越來越複雜的魚叉式網路釣魚活動。」[9]換言之，這可能放大了組織、當事人的弱點，增加了隱私風險。

而在組織內部，AI 的採用大幅改變了個資處理的模式，從而改變了個資生命週期中各個環節的風險。以包含個人資料的巨量資料分析（Big Data Analytics）為例。巨量資料分

[9] World Economic Forum [WEF], Giulia Moschetta & Joanna Bouckaert, AI and cybersecurity: How to navigate the risks and opportunities (2024), available at https://www.weforum.org/stories/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/ (last visited December 16, 2024).

析，透過機器學習、資料探勘，能從關於個人及群體的資料中發掘出資料間的相關性和模式，據此建構模型，進而利用當事人所提供看似無關的個資進行具相當準確的推論及預測，產生關於當事人的個資並用於決策。舉例來說，研究曾指出，透過 Facebook 的使用者的「按讚」紀錄，能夠相當準確的推論出其政治傾向、年齡、性別和性傾向等敏感資訊。在過去，Facebook 的演算法就曾將俄羅斯的使用者歸類為「有興趣叛國」，儘管這並非公開的分類，但這仍使有心人能夠針對這些使用者投放惡意釣魚廣告，例如連署活動，以試圖揭露這些人的身分[10]。

此外，當個資被投入 AI 模型訓練時，若無適當的限制，AI 模型其實也可能會向 AI 商品的使用者揭露原始資料。且即便原始資料可能受到限制，但由於 AI 增幅了推論及預測資料的取得和運用能力，這也會相當程度削弱了當事人對其個資的掌控，因為即便是當事人所拒絕提供的特定類型資料，藉由運用他人自主提供的資料所建構的模型，該特定類型的資料也能夠被相當精確地推論得出。並且，即便模型所做的預測或推論是錯誤的，只要它們被用於做成關於當事人及其他人的決策，它也積極創造了不利隱私的條件，因為受影響的人將必須被迫不情願地揭露以糾正決策，或選擇承受不利決定。換言之，AI 系統可能減少了當事人的控制，放大了其弱點，並且擴大了暴露於風險中的當事人範圍，從而增加了隱私風險。

### 3. 全球 CBPR 與 AI 隱私風險

在初步辨識出來的 AI 的隱私風險後，下一步便是從規範面切入，以尋求界定組織、個人的具體責任。在此最相關的

[10] Gwen Petro & Miriam Metzger, Group Privacy, in THE ROUTLEDGE HANDBOOK OF PRIVACY AND SOCIAL MEDIA, 50, 45-53, (Sabine Trepte et al. eds., 2023)

CBPR 規範是其隱私原則架構之「防止損害原則」（preventing harm），該原則要求組織應負責維護個資的完整性，和實施適當風險防護措施，防止當事人的個人資料遭致不當蒐集、濫用等不當處理。為了對組織是否符合體系要求進行更具體的檢視，CBPR 並就組織之隱私管理計畫擬定了基本計畫要求。

著眼於外部風險，應首先聚焦於安全管理之相關要求，初步發現，儘管全球 CBPR 隱私網領與計畫要求第 30 點均要求保護措施必須與威脅破壞機密性質或敏感資料的機率與嚴重性以及資料所處環境成比例，但是 CBPR 並沒有提供可供參考、操作的比例原則或事例。儘管 CBPR 強調尊重會員間各自不同的法律體系，但提升規範調和程度，尤其是透過確立規範底線（normative baseline），仍是促進 CBPR 會員間及全球間隱私管制框架之相互可操作性所不可或缺的。而在 AI 帶來新隱私風險、弱點與風險級距也相應被拉大的情況下，各國隱私框架間固有的歧異自然有可能擴大，因此，更有理由就何謂「成比例」的適當安全管理措施，建立標準、參考基準、事例或採納某種共識機制，以確保 CBPR 在組織及會員間實現相互可操作的隱私保護機制。

再著眼於組織內部的風險，當涉及推論、預測個資並基於此進行決策時，CBPR 的規範有不明確之處。推論、預測個資是否會被認為是一種蒐集、其完整性的意義為何，仍有待釐清和建立共識。另外，CBPR 對利用的規範主要著眼於利用個資是否在達成該蒐集目的及其它共通或相關目的之範圍內，易言之，主要仰賴於目的限制原則。然而，正如前述例子所示，即便符合「投放行為廣告」目的，傷害仍然非常可能因為演算法進行的受眾分組結果而造成，因此在落實

防止傷害的精神下，因利用產生的風險似值得參考除目的限制外的其他標準或機制。

## （二）研討會上討論的核心議題

### 1. GDPR、隱私法原則與 AI

GDPR 針對 AI 的隱私風險已制定了若干特定的明確規範。有關自動化決策的方面，GDPR 課予組織告知當事人自動化決策之利用及其邏輯資訊之義務，並明文保障當事人對前開資訊之知情權、拒絕接受全自動化決策之權，以及請求人類介入決策（human in the loop）和挑戰決策之權。此外，有關 AI 之研發和配置，GDPR 確立的基本原則如合法性、公平性、資料最小化等原則，也對使用個人資料發展之 AI 構成實踐上之限制，這些原則透過組織為採納新興科技時應執行資料保護影響評估（data protection impact assessment, DPIA）程序中發揮了事前審查作用。

但有規範並不代表 AI 的隱私風險得到了完整的解決。GDPR 所採納的隱私法原則與 AI 發展間仍有著非常多待解決的緊張關係。以合法性原則為例，AI 訓練和佈署過程中可能會涉及欠缺法律基礎的個資處理。比如 Clearview AI 利用網路上可取得之個人臉部資料建立模型，受到荷蘭、法國、英國等國之 DPA 以欠缺合法基礎為由開罰，於此同時，歐盟資料保護委員會（European Data Protection Board, EDPB）也針對 Open AI 在公開網站上爬蟲蒐集文字訓練 ChatGPT 組成了工作小組，旨在檢視其合法性。前述指出的推論與預測資料，也有其合法性的疑慮。又再以資料最小化、目的限制原則為例，AI 需要巨量且多樣的資料進行訓練、研究、分析與運作，尤其是當需要避免 AI 模型的偏見時，它尤其需要資料多元化，這意味著蒐集且保存更多的資訊，且所蒐集

來建立模型的資料，若包含為了其他目的而在網路上提出或公開的資料，哪些二次資料利用符合目的限制原則，考量到其數量與來源的多樣性，事實上非常難以檢視。也因此，有些人甚至形容從資料最小化的角度看，AI 像是背負著原罪（original sin）。

在透明義務上，儘管 GDPR 課與了說明義務，但其確切內容仍有爭議。當事人很少被告知其資料被處理的邏輯，也很難請求一個當事人能夠理解該處理活動對其造成的影響。

2. **AI 治理、由上而下的傳統管制與產學落差**

以基於過往資料處理現實（data processing reality）所設定的規則、義務為基礎，建立對 AI 隱私風險加以管制之框架，在面對前述的緊張與矛盾關係時，若一板一眼地執行規則，則在產業和政府基於地緣政治與國際經貿競爭等原因皆投入 AI 研發和佈署之情況下，可能會導致利益不平衡，妨礙了對公共有益的 AI 創新與發展。如何平衡個人資料保護與其他利益處在 AI 治理和隱私規範現代化與國際調合問題之核心。考量到現在產業對 AI 的快速研發和佈署明顯快於規範與管制，有論者質疑以從上而下的傳統管制（top-down approach）方式執行隱私規範，將無法充分理解 AI 的實際機制，或公允地考量 AI 對社會的效益。在這個脈絡下，實際上採納或研議採納 AI 的產業和組織端是否有能力認識其行為的後果和應採取何種措施預防侵害，換言之，第一線採用 AI 的組織是否具備適配的 AI 治理能力，至關重要。

然而，在對 AI 之機制、其風險及應對措施的理解上，存在著產學的落差。學界對 AI 的運作和其風險有更多的理解，也因此更能理解治理的重點和可能方式，惟產業著眼於 AI 應用，對 AI 治理的理解與學界之間有明顯的落差。舉例而

言，Apple 日前推出「Apple Intelligence」時，記者調查公司使用之提示語（prompt）時發現，其為了避免 AI 的風險，例如產生不準確的資訊時，所使用的卻是已經被指出沒有幫助的提示詞，如「不要幻覺（hallucination）。不要捏造事實資訊。」

在應對 AI 的隱私風險上，克服產學落差是有效從下而上之管制條件。換句話說，在面對「對齊問題」（alignment problem）時，除了技術外，產業必須與學界的認知與討論對齊，在開發 AI 應用的過程中，就意識到 AI 的風險，並在開發、設計的同時就開始採納有效的應對方式。

3. **資料二次利用與知情同意的極限**

依照風險自我承擔之法理，既有隱私法律框架下仰賴當事人是否同意作為資料處理合法與否之標準，進行風險管制。然而事實上，因為時間與法律知識的缺乏，當事人實際上對其個資運用方式和其風險認知並不足夠。他們通常難以在提供個人資料時就了解其可能會受到的影響。尤其在對 AI 發展來說重要的資料二次利用而言，儘管二次利用在許多情況下需要獲得同意，但由於資料政策的更新往往難以詳細確認，當事人經常對自己的資料是否用於 AI 訓練，其實並不清楚。論者甚至認為，若當事人面對各式各樣服務的隱私政策，光是去理解其內容和變化，幾乎成為一個全職工作時，則以知情同意模式為基礎的風險管制，應該算已經失敗了。

## （三）初步討論與建議

1. **CBPR 作為問責與法遵機制之意義**

前述對於 AI 的討論呈現出在 AI 管制當中，資料控制者或 AI 提供者採取負責任行為的重要性，而這種負責任行為需要組織性的措施來確保，且這些措施不能只是確保組織人

員遵循事先確定的行為規則，而是必須建立起對價值的承諾以及合理解釋、補充規則，做成判斷之能力。

為此，除了執法機關以外的中介性機制能夠發揮其作用。論者觀察到，CBPR 基於其跨境傳輸的出發點，自始就面臨各國規範不一、衝突的問題，因此在設計其原則及計畫要求時，一開始就朝向一個風險應對能力（risk mitigation capability）取徑，而非以遵循規則為基礎的方向設計，著眼於組織辨識和評估風險，以及依據自身條件和脈絡制定應對政策的能力。儘管這不能完全取代明文紅線規範的功能，然而，藉由要求制定政策和解釋理由，論者認為 CBPR 能夠強化組織及其人員對 AI 的隱私風險的意識，並增強問責性和其法遵能力，確保規範更高機率獲得遵循。易言之，CBPR 透過第三方認證確立的問責機制，能夠扮演銜接政府規範、產業發展與學界研究的輔助管制工具。

在本次研討會當中，CBPR 計畫要求修正工作小組也明確作成結論認為，AI 治理的問題必須持續進行討論，以便於未來能確立更有效的風險控制措施的共識。與此同時，CBPR 在本次修正案中確定將強化組織風險應對能力的要求，要求組織設立風險評鑑（risk assessment）機制，若此機制能夠一部或全部與 GDPR 下的 DPIA 有所對應，則這對 AI 的隱私風險管控將具有重大意義。

2. **政策建議**

短期內，基於歐盟 AI 法及 GDPR 的管制應該會持續被作為焦點受到討論，考量到 AI 法與 GDPR 的執法可能頻率，它們將會持續成為數位社會在應對 AI 的隱私風險時最主要的參照點，因此有必要持續觀察其發展和趨勢。中長期而言，我國實有必要確保《個人資料保護法》針對 CBPR 新修正的

要求以及 AI 發展進行調適，蓋儘管 CBPR 已經導入了風險評鑑機制，但我國個人資料保護法仍然沒有相關的規範，這導致我國《個人資料保護法》與外國隱私法之間差距變得更大了。此外，《AI 基本法草案》目前僅有原則性的規定，且與《個人資料保護法》之間關係不明。這將導致我國欠缺基於本土案例的管制經驗，致使我國更難以參與國際規範的制定和修改，進而成為規範的追隨者，這可能將損害到我國的司法主權和公共利益。因此，中長期來看，我國應該透過觀察 AI 法與 GDPR 的實施，以及透過全球 CBPR 論壇的交流，在此基礎上與國內利害關係人溝通，建立適合於我國的管制方法論，不僅確保國內的隱私保護，也確保國際規範形成過程中我國的利益。

## 四、全球 CBPR 計畫要求改革方向

本次論壇亦探討了全球 CBPR 計畫要求的改革方向，聚焦於敏感資料的保護、直接行銷的選擇權、事故通知的標準化、隱私負責人角色的強化、風險評估機制的建立及兒童資料的特殊保護需求等關鍵議題。這些改革不僅旨在提升全球 CBPR 體系的法遵性與實用性，亦有助於因應數位經濟快速發展下的新挑戰，特別是在人工智慧與跨境資料流通日益普及的背景下。

### （一）主要改革方向與挑戰

#### 1. 敏感資料的保護

CBPR 計畫要求改革新增了敏感資料保護的規範，要求申請組織識別並為敏感個人資料提供適當的保障措施，包括通知、同意、安全性或其他必要的保護手段。然而，敏感資料的分類與處理標準在各國法規間存在差異，導致企業在實施過程中面臨適配挑戰。當責機構需進一步明確敏感資料的

認定與處理規範，確保跨境操作的一致性。

2. **直接行銷的選擇權**

直接行銷活動涉及個人資料的大量使用，此次改革要求企業必須提供個人選擇退出直接行銷的機制，並確保該機制的可操作性。這項改革反映了對個人自主權與隱私保護的重視，但企業在技術實現與政策調整上需投入更多資源，特別是在多司法管轄權同時運營的情境下。

3. **事故通知的標準化**

改革要求企業在資料洩漏事件中通知受影響個人，特別是在洩漏可能導致重大風險或損害時。該規範還詳細列出了通知應包含的內容，包括洩漏範圍、可能後果、補救措施及聯絡資訊等。與此同時，各司法管轄權對事故通知的門檻設定與時限規範仍存在顯著差異，這成為跨境企業面臨的一大挑戰。

4. **隱私專責人員（Privacy Personnel）角色的強化**

此次改革明確要求申請組織指定具備專業資格的隱私專責人員（Privacy Personnel），並提供足夠資源以確保其執行隱私法遵相關職責。這一規定旨在提升組織內部資料保護能力，特別是在大規模資料處理活動中的法遵與應對能力。

5. **風險評估機制的建立**

CBPR 改革新增了風險評估要求，要求企業建立評估機制以識別與緩解個人資料處理中可能出現的風險。這一要求的實施將進一步促進企業採取預防性措施，減少資料濫用與損害個人權益的可能性。

6. **兒童資料的特殊保護**

改革針對兒童資料提出更高的保護要求，要求企業在收

集與處理兒童資料時需獲得家長或法定代理人的同意，並提供相關的審核與驗證機制。這一規定旨在應對兒童作為脆弱群體在數位環境中的潛在風險。

## （二）臺灣在改革方向中的角色與機遇

### 1. 對應國際要求的政策與技術調整

臺灣在推進全球 CBPR 計畫要求落地的過程中，應積極調整國內政策與技術標準，以確保與國際規範的同步性。同時，針對敏感資料保護與兒童資料法遵等新要求，政府可考慮制定專門的技術指引與政策工具，幫助企業快速適應改革需求。

### 2. 提升當責機構的能力建構

作為全球 CBPR 計畫的重要支柱，當責機構在改革方向中扮演關鍵角色。臺灣可通過強化當責機構的資源配置與技術支援能力，確保其能夠有效推動新要求的實施，並為國內企業提供高效的法遵服務。

### 3. 推動技術創新與跨境合作

面對事故通知標準化與隱私技術應用的挑戰，臺灣應利用自身在科技創新方面的優勢，開發更多自動化與智慧化的法遵工具。同時，通過與其他 CBPR 成員國的合作，臺灣有機會在全球資料治理中發揮更積極的作用。

## （三）結論

全球 CBPR 計畫要求的改革方向反映了資料治理在數位經濟新挑戰中的發展趨勢。臺灣作為 CBPR 成員之一，應積極參與改革落地與實踐，結合政策調整、技術創新與國際合作，提升自身在資料治理領域的競爭力與話語權。

## 參、結論與建議

本研究分析與討論了與全球 CBPR 計畫要求發展相關的議題。全球 CBPR 是在國際隱私法框架破碎之背景下，旨在協調規範、提升制度間相互可操作性，促進資料流通之機制。相互可操作性並非試圖統一所有隱私框架，而是希望透過政策協調與技術適配，實現不同框架間的相互承認與合作。G7 資料自由流通與信任（DFFT）計畫以「3C」原則（Commonality 共通性、Complementarity 互補性，與 Convergence 趨同性）為基礎，提出了一套實現全球資料治理相互可操作性的框架，為全球 CBPR 提供了重要的啟示。在相互可操作性的推進上，對我國之短期建議為強化我國參與全球 CBPR 及其他多邊機制，長期而言，為了在國際規範發展保有話語權，我國應更積極參與國際合作，支持理念相近之經濟體參與國際合作。

有關事故通知，本研究整理出通知機制的核心意義包括(1)國家安全層面，亦即維護關鍵基礎設施與人員之安全、(2)經濟發展層面，亦即提升企業信任度，促進跨境商業合作，以及(3)個人隱私層面，亦即強化個人權利保護，提升組織透明度和問責性。各司法管轄權對事故通知的門檻設定與時限規範仍存在顯著差異，這成為跨境企業面臨的一大挑戰。全球 CBPR 正在推動事故通知的標準化，要求企業在資料洩漏事件中通知受影響個人，特別是在洩漏可能導致重大風險或損害時。

有關 AI 與隱私的議題，儘管全球 CBPR 隱私綱領與計畫要求強調保護措施必須與威脅破壞機密性質或敏感資料的機率與嚴重性成比例，但 CBPR 並未提供具體的比例原則或事例。提升規範調和程度，尤其是透過確立規範底線，是促進 CBPR 會員間及全球間隱私管制框架相互可操作性的重要步驟。面對 AI 帶來的新隱私風險，建立標準、參考基準和共識機制尤為重要。在管制方法論上，研究討論了自上而下的管制以及自下而上的管制不同取逕，並說明了各自的困難。全球 CBPR 計畫要求工作小組認為，AI 治理問題必須持續討論，以確立更

有效的風險控制措施，目前，修正案中確定將強化組織風險應對能力，要求組織設立風險評鑑機制。對我國而言，持續關注歐盟 AI 法與 GDPR，作為應對 AI 隱私風險的主要參照點，有其必要性，並宜透過全球 CBPR 論壇交流，建立適合我國的管制方法論，確保國內隱私保護及國際利益。

整體而言，為我國數位產業在全球資料保護標準變革中保持競爭力，並在國際隱私法制議題上保有話語權，本研究建議持續追蹤和參與全球 CBPR 論壇及其他多邊機制，觀察歐盟、美國及其他國家在隱私法方面的進展，積極調整國內政策與技術標準，以確保與國際規範同步，並制定專門技術指引與政策工具，幫助企業快速適應改革需求。

# 參考文獻


1. KUNDAN MUNJAL & REKHA BHATIA, *A systematic review of homomorphic encryption and its contributions in healthcare industry* (2022), https://link.springer.com/article/10.1007/s40747-022-00756-z (last visited December 16, 2024).
2. YUVAL DAGAN & GIL KUR, *A bounded-noise mechanism for differential privacy* (2022), https://proceedings.mlr.press/v178/dagan22a/dagan22a.pdf (last visited December 16, 2024).
3. VENKATA NAGA SAI KIRAN CHALLA, *Federated Learning: Collaborative Ml without Centralized Data* (2022), https://www.ijaresm.com/products/download_document/document_file/Venkata_Naga_Sai_Kiran_Challatq5k.pdf (last visited December 16, 2024).
4. SURENDRA .H, DR. MOHAN .H .S, *A Review Of Synthetic Data Generation Methods For Privacy Preserving Data Publishing* (2017), https://ijstr.org/final-print/mar2017/A-Review-Of-Synthetic-Data-Generation-Methods-For-Privacy-Preserving-Data-Publishing.pdf (last visited December 16, 2024).
5. South Korea: PIPC releases synthetic data generation reference model, DataGuidance, https://www.dataguidance.com/news/south-korea-pipc-releases-synthetic-data-generation (last visited December 16, 2024).
6. Organization for Economic Cooperation and Development [OECD], Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 3, 2024), available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (last visited December 16, 2024).
7. World Economic Forum [WEF], Giulia Moschetta & Joanna Bouckaert, AI and cybersecurity: How to navigate the risks and opportunities (2024), available at https://www.weforum.org/stories/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and-opportunities/ (last visited December 16, 2024).
8. Gwen Petro & Miriam Metzger, Group Privacy, in THE ROUTLEDGE HANDBOOK OF PRIVACY AND SOCIAL MEDIA, 50, 45-53, (Sabine Trepte et al. eds., 2023)

全球跨境隱私規則（CBPR）計畫要求之研究
/林冠宇 主任計畫主持.
-- 初版. -- 臺北市 : 國發會, 民113.12
面; 表，公分
編號: (113)017.0901（平裝）
委託單位：國家發展委員會
受託單位：財團法人資訊工業策進會

隱私執法協議
553.4

題名：全球跨境隱私規則（CBPR）計畫要求之研究
委託單位：國家發展委員會
受託單位：財團法人資訊工業策進會
計畫主持人：林冠宇 主任
出版機關：國家發展委員會
電話：02-23165300
地址：臺北市寶慶路 3 號
網址：http://www.ndc.gov.tw/
出版年月：中華民國 113 年 12 月
版次：初版　　刷次：第 1 刷
編號：(113)017.0901　(平裝)

# 全球跨境隱私規則（Cross-Border Privacy Rules） 計畫要求之研究

## 研討會資訊

### 1. 全球 CBPR 計畫要求更新多方利害關係人會議

時間：民國 113 年 11 月 18 日

地點：臺北市大安區敦化南路二段 216 號 22 樓（財團法人資訊工業策進會科技法律研究所）

| Agenda | Description |
|---|---|
| 1 | Process overview: issues considered and outcome |
| 2 | Draft Program Requirements:<br>1. Sensitive Data<br>2. Direct Marketing Choice<br>3. Breach Notification to Individuals<br>4. Privacy Personnel<br>5. Risk Assessment<br>6. Withdrawal of Consent<br>7. Records of Processing and Consent<br>8. Children's Data |
| 3 | Proposal to revise existing Program Requirements 46 and 47 to all transfers (transfers to controllers and processors) and not just transfers to data processors as currently indicated |
| 4 | Certification Frequency |
| 5 | Implementation of new Program Requirements |
| 6 | Other? |

### 2. 2024 年全球 CBPR 論壇臺北秋季研討會：蛻變

時間：民國 113 年 11 月 19 日（二）～21 日（四）

地點：臺北市中正區中山南路 11 號（財團法人張榮發基金會國際會議中心）

Day 1

| Time | Session Title | Description | Speakers |
|---|---|---|---|
| **08:30 - 09:00** | **Registration** | | |
| **09:00 - 09:10** | **Opening Remarks**<br>**開幕致詞** | Senior Official from CT will provide a welcome remark. | **Shin-Ling (Sandy) Wu**, Acting Director-General, Department of Regulatory Reform, National |

| | | | |
|---|---|---|---|
| | | 由主辦單位國家發展委員會法制協調處吳代理處長欣玲進行開幕致詞 | Development Council, Chinese Taipei |
| **09:10 - 09:25** | **Updates on the Global CBPR Forum**<br>**全球 CBPR 論壇之更新** | Chair of the Global Forum Assembly will provide the latest updates on the forum's activities and developments.<br>全球論壇大會主席將說明近期論壇活動及發展 | **Shannon Coe**, Chair of the Global Forum Assembly |
| **09:25 – 09:30** | **Group Photo 大合照** | | |
| **09:30 - 10:00** | **The Merits of the Global Enforcement Cooperation**<br>**全球執法合作之效益** | This panel invites the Administrators and Participants of the Global CAPE to discuss the functions and benefits of the cooperation arrangement.<br>全球隱私執法協議之參與者及管理者將共同討論 Global CAPE 之功能與效益。 | Moderator: **David Lincicum**, Senior Attorney, Federal Trade Commission, United States<br><br>Panelists:<br>• **Issa G. Gayas**, Attorney IV, Policy Development Division, National Privacy Commission, Philippine<br>• **Kanoko Esaki**, Deputy Counselor for International Affairs, Secretariat, Personal Information Protection Commission, Japan<br>• **Lucia Cheng**, Section Chief, Department of Regulatory Reform, National Development Council, Chinese Taipei |
| **10:00 - 10:30** | **Coffee Break** | | |

| | | | |
|---|---|---|---|
| **10:30 - 12:00** | **Accountability Agents Panel**<br>**當責機構座談** | This panel will invite Accountability Agents (AAs) to share their experience and focus on certification methodology differences across AAs.<br>當責機構將分享對於驗證之不同經驗及觀點 | Moderator: **Shannon Coe**, Chair of the AA Committee<br><br>Panelists:<br>• **Aejin Lee**, Korea Internet & Security Agency<br>• **Dona Fraser**, Senior Vice President, Privacy Initiatives, BBB National Programs (tbc)<br>• **Evelyn Goh**, Director, International Relations, Policy and Strategy, Infocomm Media Development Authority, Singapore<br>• **Joanne Furtsch**, VP, Privacy Knowledge, TrustArc<br>• **Sanae Okuhara,** Japan Institute for Promotion of Digital Economy and Community<br>• **Te-Ying Wang**, Section Manager, Science & Technology Law Institute, Institute for Information Industry |
| **12:00 - 14:00** | **Lunch Break** | | |
| **14:00 - 14:45** | **Update on the G7 DFFT Interoperability Project: A Comparative Analysis of** | This panel will invite G7 members to provide an update on the G7 DFFT program and share their insights on the exercise and what next steps could be. | • **Greg Dunne**, Head of Multilateral Tools & Trusted Government Access, Department for Science, Innovation and |

| | | | |
|---|---|---|---|
| | **GDPR and Global CBPR System**<br>**G7 可信任資料流通相互操作性計畫之更新：歐盟 GDPR 與全球 CBPR 之比較分析** | 美國、英國、日本及德國等代表將分享七大工業國關於可信任資料流通（DFFT）相互操作性計畫之最新進展 | Technology, United Kingdom<br>• **Kanoko Esaki**,<br>Deputy Counselor for International Affairs, Secretariat, Personal Information Commission, Japan<br>• **Marc Schlegel**,<br>The Federal Commissioner for Data Protection and Freedom of Information, Germany |
| **14:45 - 15:30** | **Global Data Protection Regimes Fragmentation and Harmonization**<br>**全球資料保護法制之分與合** | This panel will invite experts and stakeholders to discuss the impact of global data protection regimes on enterprises, especially on efforts to address regulation fragmentation.<br>由專家與利害關係人從產業觀點討論全球資料保護法制碎片化現象對企業造成之影響 | Moderator: **Adetola Onayemi**, USAID - Digital Connectivity & Cybersecurity Partnership (DCCP) - AfCFTA Secretariat Digital Trade Protocol<br>Panelists:<br>• **Harvey Jang**,<br>Vice President, Deputy General Counsel, and Chief Privacy Officer, Cisco<br>• **Jun Chu**,<br>Head of Cybersecurity and Privacy Policy for Asia Pacific<br>, Google<br>• **Markus Heyder**,<br>VP and Senior Policy Counselor, Centre for Information Policy Leadership (CIPL)<br>• **Rory Malone**,<br>Principal, Global Privacy & Security Regulatory |

| | | | |
|---|---|---|---|
| | | | Compliance, Cloudflare |
| **15:30-16:00** | **Coffee Break** | | |
| **16:00 - 17:15** | **The CBPR System and National Privacy Laws**<br>**CBPR 體系及各國隱私法** | This panel will discuss how domestic privacy frameworks can accommodate the CBPR system, and how the Forum can support non-participants to embrace the CBPR System.<br>非 CBPR 成員之司法管轄權區域代表將討論其國內隱私保護框架與 CBPR 體系之相容性 | Moderator: **Evelyn Goh**, Director, International Relations, Policy and Strategy, Infocomm Media Development Authority, Singapore/ Deputy Chair of Global Forum Assembly<br><br>Panelists:<br>• **Alison Tilley**, Commissioner, Information Regulator, South Africa<br>• **Guadalupe Mercado**, Asesora, Dirección Nacional de Protección de Datos Personales, Agencia de Acceso a la Información Pública, Argentina<br>• **Hassan Olugbile**, Data Protection Commssion, Nigeria<br>• **Khalid N. Sadiq Al-Hashmi**, Assistant Under Secretary & Minister Advisor, Ministry of Communications & Information Technology, Qatar<br>• **Md. Farhad Hussain**, BGD e-GOV CIRT, Bangladesh |

| | | | |
|---|---|---|---|
| | | | • **Dr. Muhammad Sufyan bin Basri**,<br>Assistant Commissioner, Head of Monitoring Division, Malaysia<br>• **Prof. Prapanpong Khumon,**<br>Expert Committee, Personal Data Protection Committee, Thailand |
| **17:15** | Close | | |

Day 2

| Time | Session Title | Description | Speaker |
|---|---|---|---|
| **09:00 - 09:30** | **From MCCs to CBPR: Strengthening Data Privacy and Digital Trade in ASEAN**<br>**從標準契約條款到 CBPR：強化東協之隱私保護與數位貿易** | This presentation will explore how the Global Cross Border Privacy Rules (CBPR) framework serves as a crucial enabler of ASEAN's Digital Economic Framework Agreement (DEFA).<br>本專題演講將探討全球 CBPR 架構對於東協數位經濟架構協定之重要性 | **Nigel Cory**, Director for digital policy, Crowell Global Advisors. |
| **09:30 - 10:00** | **Enhancing Adequacy Requirement in Achieving International Data Protection Standard Through Malaysia's Personal Data Protection Act Amendment 2024**<br>**從馬來西亞 2024 年個人資料保護法修正看國際資料保護標準** | The Malaysian Parliament passed revisions to the country's data protection regime under the Personal Data Protection Act 2010 (PDPA 2010) in this July. This presentation will explain the impact of the recent amendments to Malaysia's PDPA 2010 and their alignment with efforts to enhance adequacy requirement in the cross-border data transfers within a global context. | **Professor Dr. Mohd Nazri bin Kama**, Commissioner of Personal Data Protection of Malaysia |

| | | | |
|---|---|---|---|
| | | 馬來西亞個資保護委員會將介紹該國 2024 年個人資料保護法最新修正內容，及該國法制與國際接軌之情形 | |
| **10:00 - 10:30** | **Coffee Break** | | |
| **10:30 - 11:00** | **The UK's new Data (Use and Access) Bill**<br>**英國新版資料法案之介紹** | A summary of the new UK Government's initial priorities on international data flows, and the new Data (Use and Access) Bill, which was introduced to Parliament in October 2024.<br>英國創新科技部將介紹該國最新資料法案有關國際資料傳輸之重點 | **Gemma Phillips**, Head of Policy and Engagement, International Data Flows Unit, Department for Science, Innovation and Technology, United Kingdom |
| **11:00 - 12:00** | **The Introduction of CBPR 2.0: the Updates of CBPR Program Requirements**<br>**CBPR 2.0 之介紹：CBPR 計畫要求更新** | This session will cover the latest updates and revisions to the CBPR Program Requirements.<br>全球論壇大會主席將說明全球 CBPR 計畫要求之最新發展 | **Shannon Coe**, Chair of the Global Forum Assembly |
| **12:00 - 14:00** | **Lunch Break** | | |
| **14:00 - 15:15** | **Privacy and Responsible AI**<br>**隱私及負責任 AI** | This panel will present the perspectives of regulators, industries, and practitioners on the interplay between privacy regulations and the responsible use of AI.<br>由產官學界代表討論隱私規範與負責任 AI 之交錯影響 | Moderator: **Prof. Ting-Chi Liu**, National Chengchi University, Chinese Taipei<br><br>Panelists:<br>• **David Lincicum**, Senior Attorney, Federal Trade Commission, United States<br>• **Dona Fraser**, Senior Vice President, Privacy Initiatives, |

| | | | |
|---|---|---|---|
| | | | BBB National Programs (tbc)<br>• **Isabel Hou**,<br>Secretary General, Taiwan AI Academy Foundation, Chinese Taipei<br>• **Markus Heyder**,<br>VP and Senior Policy Counselor, Centre for Information Policy Leadership (CIPL)<br>• **Shlomi Hod**,<br>praxif.ai |
| **15:15 - 15:45** | **Coffee Break** | | |
| **15:45 - 16:15** | **Exploring Privacy Enhancing Technologies: Solutions for Secure Data Collaboration and Protection?**<br>**隱私強化技術：安全資料協作與保護的新解方？** | This session will delve into the latest developments in Privacy Enhancing Technologies (PETs), highlighting their critical role in enabling secure and privacy-compliant data handling across diverse sectors. Additionally, the session will explore the collaborative roles that governments, industry, and international organizations play in promoting PET adoption and standardization.<br>本場次將深入探討隱私強化技術 (PET) 的最新發展及應用，並探討政府、產業及國際組織之合作可能。 | Moderator: **Te-Ying Wang**, Section Manager, Science & Technology Law Institute, Institute for Information Industry<br><br>Panelists:<br>• **Gemma Phillips**,<br>Head of Policy and Engagement, International Data Flows Unit, Department for Science, Innovation and Technology, United Kingdom<br>• **Justyn Chen**,<br>Machine Learning Engineer, National Institute of Cyber Security, Chinese Taipei<br>• **Sunup Park**,<br>Deputy Director, International Cooperation Division, |

| | | | |
|---|---|---|---|
| | | | Personal Information Protection Commission, Republic of Korea<br>• **Shlomi Hod**, praxif.ai |
| **16:30 - 17:00** | **Closing Remarks: Privacy in Taiwan**<br>**閉幕致詞：隱私在臺灣** | A senior official from the Institute for Information Industry (III) will deliver a keynote address on the current state of privacy protection in Taiwan. The speech will highlight Taiwan's strategies for data protection and discuss the country's role in facilitating cross-border data interoperability within the global data protection framework.<br>由資策會科技法律研究所所長以臺灣隱私保護法制及與國際接軌為題進行閉幕致詞 | **Chin-Li Wang**, Director General, Science & Technology Law Institute, Institute for Information Industry |
| **17:00** | Close | | |

Day 3

| Time | Session Title | Description |
|---|---|---|
| **08:30-09:00** | **Registration** | |
| **09:00-10:30** | **Government Only Discussion**<br>政府代表交流 | |
| **10:30-11:00** | **Coffee Break** | |
| **11:00-12:00** | **Post-Workshop GFA Meeting**<br>會後全球論壇大會會議 | |
| **12:00** | **Close** | |