行政院「2025 全球數位人權大會場邊活動-臺灣第二部國家人權行動計畫數位人權議題國際諮詢座談會」

▼ 開幕致詞

林明昕政務委員：

來自美國的前聯合國意見與言論自由特別報告員 Mr.Kaye、斯里蘭卡前資料保護機構主任 Mr. Fernando、澳大利亞的個人資料保護委員 Ms.Kind、日本隱私倡議機構 Privacy By Design Lab 的創辦人 Mr.Kurihara、行政院人權及轉型正義處賴處長、國家資通安全研究院人才培力中心鄭主任，還有來自世界各國的與會嘉賓、人權工作者大家早安，大家好！

今天很高興可以跟大家齊聚一堂，參加 2025 年全球數位人權大會，本人謹代表臺灣政府，誠摯歡迎來自世界各地的專家、學者和人權工作者，共同探討數位時代的人權議題。這次是全球數位人權大會首次在東亞地區舉行，並且選擇在臺灣辦理實體會議，不僅是著眼於對於我國在全球數位科技領域的關鍵地位，更是對我國在數位民主與人權發展成果的最大肯定。

不論是民主法治或是各項人權議題，面對數位科技的演進及應用，一方面讓所有關心數位人權議題的人們，可以更有效率的凝聚共識，帶來發展的契機，就如同接下來這週即將開展的對話機會；但數位發展同時也引發了對於隱私、資料安全、言論自由等一系列人權的挑戰，對於女性、多元性別、身心障礙者、兒童、原住民族等處境不利群體造成不成比例的危害，甚至破壞民主國家的根基。在這樣的背景下，如何在促進科技創新的同時，兼顧人權保障，是我們必須共同面對、

重要而且急迫的課題。

一直以來，臺灣致力於推動數位人權各項保障與發展。我們積極推動數位治理，強調資訊透明與公民參與，並透過立法與政策，確保公民在數位時代的權利不受侵害。

在具體行動方面，臺灣在 2022 年制定了首部「國家人權行動計畫」（National Hnman Rights Action Plan,NAP），鑒於數位發展對社群與國家廣泛而深遠的影響，特別將「數位人權」列為重要的議題，從完善的隱私保護、防治數位科技產生的各種歧視、扼阻網路性別暴力及精進媒體識讀、消弭數位落差等面向，提供具體的行動設定目標及期程。

透過國家人權行動計畫的擬定，我國也將於今(2025)年規劃成立個人資料保護獨立機構，這不僅是制度的改革，更象徵政府對於建構完善數位治理環境的決心。剛剛提到的那些議題，都迫切需要培育一批能夠跨越資訊、科技、法律、風險管理等領域的專業人才。他們不只要瞭解技術，更要具備前瞻的視野，才能在數位創新與人權保障之間，找到最適切的平衡點。

首部「國家人權行動計畫」對「數位人權」的關注，讓我們有了一些進展，但數位發展不會止步，也可能對民主、人權帶來更困難的挑戰。臺灣政府接下來也會著手研擬第二部「國家人權行動計畫」，非常希望可以藉由本次 RightsCon 的交流，徵詢各國專家、人權工作者的意見及經驗，各位的寶貴意見，我們都會詳實記錄起來，做為臺灣推動數位人權及個人資料保護專業人才培育的政策參考。在推廣數位人權的全球合作網路上，臺灣不會缺席，更會成全球夥伴的堅強支援。

最後，再次感謝各位的蒞臨，期待在這幾天的會議中與大家深入交流，共同為數位人權的發展貢獻心力，祝大會圓滿成功，祝各位身

體健康萬事如意，謝謝！

▼ 議題一：如何透過國家人權行動計畫強化數位人權保障

賴俊兆 Semaylay i Kakubaw 處長：

大家早安，今天非常榮幸，也非常開心能夠在臺灣首次加入 RightsCon 這樣的國際盛事，由我負責協助第一場的主持。等一下 David Kaye 以及 Jayantha Fernando 兩位講者，會來跟我們做第一個場次的分享。主要是從「國家人權行動計畫」去談怎麼樣促進「數位人權」的保障。作為主持人，我想今天 4 位的講者同時都在臺上，等一下一定會有很多精彩的分享跟對話，我簡要接續剛剛政委致詞所談到，臺灣在 2022 年推出首部「國家人權行動計畫」，這樣一個國家級的人權行動計畫，代表著臺灣對於人權保障，對於人權議題的重視。

實際上，臺灣的國際處境很特別，有一定的挑戰跟難度，沒有辦法參與國際人權組織跟事務，但是在相關人權的議題上，臺灣從來不缺席。從 2009 年開始推動聯合國國際人權公約國內法化，到目前為止，用自主承諾、在地審查的方式，已經辦理了 12 次國家報告國際審查，包括兩公約(ICCPR&ICESCR)、消除對婦女一切形式歧視公約(CEDAW)、兒權公約(CRC)、身權公約(CRPD)，還有消除種族歧視公約(ICERD)，總共 12 次的國際審查，我們希望能夠跟國際的標準同步。在人權公約同步的同時，我們也推出了「國家人權行動計畫」，2022 年的「國家人權行動計畫」就標舉著臺灣對重要人權議題的重視，其中「數位人權」也是 2022 年「國家人權行動計畫」8 個議題裡重要的議題之一，占了一定的篇幅。

用數據來觀察，當時提出 156 項行動、共 8 個議題，「數位人權」占其中一個議題，並提出 19 個行動，涵括幾個面向：第一個，是針對個人隱私、個人資料的保護方面，我們希望有一個獨立的機關，也考量要不要有個資保護官的獨立機制。第二個，我們特別重視在網路數位議題上，有一些處境不利的群體，包含女性、LGBTI、原住民族，甚至身心障礙者等等，可能會在網路數位環境底下，受到特別傷害的群體，也在當時的「國家人權行動計畫」裡特別重視。這兩年以來，也陸續有一些進展，包含像避免相關性別暴力的犯罪、涉及兒童影像的犯罪、Deepfake 等等的議題，我們也制定、修訂了相關的法律來因應。第三個，比較重要是相關的教育宣導，媒體識讀能力的提升，我們也注重數位落差的問題。所以在剛剛提到的幾個脆弱或者是處境不利的群體，如何讓大家的能力提升、意識提升，也弭平數位落差，這都需要實際的資源，不管是軟體、硬體等相關資源的投入。

我們在第一部「國家人權行動計畫」中，雖然「數位人權」的議題很大，不過當時跟公民社會討論的過程，把這幾個議題放入，絕對不是只限於這幾個重要的議題。例如，我們可能在其他的政策、計畫，譬如針對身心障礙者、無障礙／可及性、數位的議題也很重要。在 CRC 的討論上，也很重視兒少在數位環境下的權利保障，CRC 第 25 號一般意見裡面所提到的一些議題，甚至像臺灣很重視移工、漁工在海上，怎麼在海上的工作環境，讓這些來自國外的夥伴，他們也可以享有數位的資源，去確保他們的人權。這些都是在我們很多的政策面向，很多的行動計畫裡面會關注的。

我大概把臺灣這兩、三年的發展現況跟幾位專家，也跟與會的各位來賓來做說明。這個場次，其實是希望多一點時間留給我們的專家，希望能夠在這個時間點，準備研擬第二部「國家人權行動計畫」之際，有哪一些臺灣現在跟世界各個國家同樣面臨的挑戰，例如，假訊息，

或者網路的一些言論，怎樣既保障人權又可以避免相關的一些侵害，這都是在研擬第二部「國家人權行動計畫」的當下，希望能夠多聽取大家寶貴的意見。

好，以上是我簡要的引言，提供大家參考。期待等一下會有很精彩的對話，先依序邀請 Kaye 先生，來作接下來的分享。

講者一 David Kaye：

謝謝處長的邀請，也特別感謝行政院人權處，真的非常開心能夠受邀來參加今天的座談會。

我其實想要先談一談第一部「國家人權行動計畫」，也分享一下我對於在草擬第二部「國家人權行動計畫」也許可以有什麼樣的考量。政府在 2022 年的計畫，我覺得這是一份很重要的文件，對於推動人權發展、人權保護的執行都是很重要的。在這個文件中，政府將很多的人權措施國內法化。人權相關法規如果能夠國內法化，能夠在國內落實，成為一個準則是最重要的。臺灣致力於落實人權的保障，其實是一個起點，大家自願去執行，例如，聯合國的公約，就是在國內法化之前的重要一步。臺灣對國內法化相關這部分的努力，都可以體現在「國家人權行動計畫」裡。在 2022 年的行動計畫也提到，例如，公民權、經濟文化權、消除對婦女一切形式歧視公約、兒童權利公約相關等等的權益，另外也包含特定議題，我認為這個行動計畫其實非常地詳盡，大概有 200 頁這麼長，也談到一些特定的挑戰，例如，居住正義以及對於氣候變遷的因應等等。這真的是臺灣落實人權保障很重要的一個承諾，臺灣也有透過專家的評估，各種資源去落實，也有針對企業與人權去做努力。

我想要談一下在「數位人權」的部分，也許可以作為草擬第二部行動計畫的一些想法。「數位人權」有一部分是談到資料保護，談到

臺灣目前的《個人資料保護法》(Personal Data Protection Act，PDPA)，也要求要成立一個專責的個資保護機關，政府目前也正在研議當中。在座有非常多個人資料保護的專家，所以我就不贅述。但是我認為這個行動計畫，特別談到國際對於資料保護的趨勢，其實就在強調國際準則的重要性。另外也談到要禁止歧視、打擊性別暴力和保護兒少，以及談到對於新興犯罪、女性、兒少暴力、網路歧視、私密影像的外漏等等，都是很重要的威脅。另外計畫裡面談到，要有一些機制去減少網路造成的傷害或是網路犯罪，保護網路犯罪的受害者，提供相關的協助。最後，根據這個行動計畫，提到網路上侵犯人權，會造成實質的權益侵犯，造成這些處境不利群體很大的傷害，政府應該要盡力的去提升施政的透明，透過問責的方式，來保護網路的言論自由以及公民權利，以上是我針對第一部行動計畫的見解。

有關第二部行動計畫建議的部分，政府應該可以去強化執行的面向，也就是深入去探討適用各個問題的相關實務，建議臺灣政府去援引可適用的相關國際法規或準則，在一些領域可以採取特定的做法。在 2022 年的 NAP 裡面，已經就有談到要透明，要保護言論自由，其實還可以再進一步去把整個保護的架構訂出來。公民與政治權利國際公約(ICCPR)第 19 條，保障意見自由及言論自由權，這不只確保了閱聽者的權利，還有保障發言者的權利。第 19 條也應該要針對第三方測試(three part test)，這是要透過法規提供一個框架，保護公共秩序、公共衛生等等。任何的政府機關必須要符合合法性、必要性跟比例原則。在 2022 年行動計畫裡面談到的議題都是確實存在的，也對於人權促進非常有幫助，對於臺灣成為一個民主韌性的社會，是很重要的基石。

我認為政府要能建立人權的相關標準，要清楚地用立法規定的方式，讓個人知道到底什麼是合法、什麼是非法，並且確保只採取必要、

最小侵害性的手段，要去明定以合法為最低基礎，並且參考 ICCPR 第 19 條，在實施的過程也必須要遵循透明、司法審查等監督機制。我就簡單分享到這邊，非常感謝行政院人權處以及處長的邀請，謝謝。

賴俊兆 Semaylay i Kakubaw 處長：

謝謝 Kaye 先生剛剛很迅速地幫我們回顧了第一部「國家人權行動計畫」，也特別針對言論自由的議題，尤其是 ICCPR Article 19 相關的精神、意旨給我們第二部計畫很重要的提醒跟建議。我這邊只補充一個很簡單的訊息，臺灣在人權方面的表現，其實有很多其他國家，像是非政府組織也注意到，例如國際人權組織 Article 19 在 2024 年也公布了言論自由的總評報告，臺灣得到 80 分，列為開放的分級，但是我們不以此自滿。

所以像剛剛 Kaye 先生所提到，我們接下來要面對的議題，其實都還有很多挑戰。我們第一部有提到的一些言論自由的議題，臺灣重視言論自由，不過因為在數位或者網路的環境底下，有一些言論的確是會對民主帶來一定的危害，甚至也會傷害到我剛剛特別提到的處境不利群體，所以中間怎麼平衡，我們在第一部其實也有未盡之處，還沒有做得很好的部分。所以像當時《數位中介服務法》草案，在臺灣的討論也受到一些挫折，也還蠻需要等一下進一步對話，在言論自由的這一塊怎麼樣去因應整個數位的環境。

時間的關係，接下來邀請來自斯里蘭卡的 Fernando 先生，他今天有準備簡報，接著請您分享，謝謝。

講者二 Jayantha Fernando：

謝謝處長，各位與談人大家好，非常謝謝行政院人權處的邀請。

首先，我想要先恭喜臺灣有非常完善的「國家人權行動計畫」來捍衛、促進「數位人權」。我今天想要跟大家分享斯里蘭卡通過、制定《個人資料保護法》的經驗，也分享一下在這個過程中遇到的挑戰，也許能夠作為臺灣的借鏡，給臺灣一些思考，然後去制定更完善的第二部NAP。我的簡報非常多頁，但因為時間的關係，我就很快速地講過去，簡報之後也可以分享給各位觀眾再去細讀。

這張投影片是斯里蘭卡 2022 年《個人資料保護法》第 9 號，經過 4 年半的時間去訂定，我想特別點出來的是這個法規的草擬委員會，我當時有參與法規框架的擬訂，對我們來說有一個很大的挑戰是，我們的憲法並沒有特別針對隱私權保障的規範，我們的憲法有包括如資訊取得權、言論自由這些規範，但憲法沒有直接保障隱私權，所以這對我們來說是一大挑戰。不過我們還是去看了所有的國際標準，包括 OECD 的隱私指南、APEC 的隱私框架，同時也去看歐盟委員會的 108 號公約，用這些國際規範來做參考。我們之所以參考前述規範，是因為斯里蘭卡是南亞第一個成為《布達佩斯網路犯罪公約》（the Budapest Cybercrime Convention）締約國的國家，並在 2022 年簽署了第 2 附加議定書(Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224))，內容包括有關在雲端裡面要如何處理資訊等，斯里蘭卡、澳洲、日本等國家都有一起參加整個協商的委員會，我們希望能夠發展出另外一個新的協議，去處理如何建立申訴機制、在雲端服務上面要怎麼獲得保障。除了剛剛講到的《布達佩斯網路犯罪公約第 2 附加議定書》第 14 條有個人資料保護之外，同時還有《聯合國打擊網路犯罪公約》(United Nations Convention Against Cybercrime)，我相信大家應該都非常熟悉。基本上，我們是採行多方利害關係人諮詢的做法，包括有公民社會組織、國際利害關係人，以

及私部門共同參與，對於我們的《個人資料保護法》提出一些建議。

而且我們每一個版本都會在線上公布，所有版本的變更也全部都會在線上公布。這是為什麼呢？因為我們知道既然要起草這樣一個法規，第一個，我們會需要的是國際跟國內的利害關係人都能夠提出意見，能夠發聲。等一下就會提到斯里蘭卡的《個人資料保護法》，這部法律要怎麼規範個人資料以及賦予資料當事人擁有一定的權利。這個不只適用於斯里蘭卡國內的公民，甚至是海外公民，也可能是非公民但持有居留證，或是人在斯里蘭卡工作、擔任協調員等等，也都能夠獲得相關的保障，這部法律其實是非常廣泛的立法。在這個投影片裡面可以看到這個法律的適用範圍，是想要去強化資料當事人的權利，給他們一些以前沒有的權利，特別聚焦在個人資料的處理。我們也建立了一個新的資料主管機關，其實真的要有這樣的一個機關，是非常困難的，我們可以看到政府實施的日期一再地延後，為什麼延後呢？主要是因為需要一個完善、真的運作良好的資料機關，需要把員工都訓練好，清楚知道要怎麼樣執法。但是，我們也知道，如果真的能去實施這些相關草案跟法案，相對來說保障的效果會比指引還要好。

其實這一個指引現在都已經公開出來，在我們的網站上已經有公開。法律前言、引言裡面就有非常具體的提到，第一個，法律是為了要去確保真的能夠實現數位經濟的成長和發展，所以，未來的立法者也可以把這樣的發展納入考量。譬如，去制定一些新的規範，明定一些新的罰則，針對新興的數位服務，能夠有新的不斷演進的規範，包括怎麼樣去改善斯里蘭卡國內的整個數位環境。然而，值得注意的是，該法律不僅適用於斯里蘭卡境內的實體／單位，也適用於從海外向該國提供商品和服務的實體／單位。所以在這部法律裡面，可以看到有關《個人資料保護法》都有特定詞彙類別相關規範，這邊我有稍微列出一些不同的用語的定義，包括什麼是個人資料？資料當事人是什麼？

在個人資料裡面特別的類別是什麼？譬如在處理健康、宗教等等，這些相關類別都有非常清楚的定義。同時還有講到資料控制方的相關角色，他的責任是什麼？這些我們也都有定義。這一些條文我先跳過，稍微跟大家講一下處理個人資料的原則，還有資料當事人的權利是什麼。基本上當事人的權利，大家如果對於資料保護熟悉的話，應該都清楚有哪些權利，所以這些條文先跳過。

接著我很快跟大家說明，資料保護相關權責機關必須要履行的職責是什麼、要做些什麼樣的事情。我要強調的是，單有一個全方位的《個人資料保護法》其實是不夠的，我們必須真的去打造一個尊重隱私的文化，將這個文化塑造出來以後，才有辦法真正實現個人資料的保護。當然我們必須要有一系列的行動，要有大量的投資，才能夠塑造這樣的文化。斯里蘭卡在經濟復甦後，發現要讓政府部門完全符合標準是有點困難的，這也是為什麼法律施行的時間一直延後到今年，後來公布自 2025 年 3 月 18 日施行。但是不論如何，目前我們知道延後的主要原因，就是因為公部門還沒有準備好。我想，就像剛剛政委以及處長有提到的，我們要培訓個人資料保護官，這其實也是很漫長的過程。首先，你必須要去培力一群人通過相關的認證，再來，是必須透過有這些認證的單位，幫他們安排一系列的培訓課程，讓這些官員都能夠擁有足夠的資訊跟能力。同時，也必須要能夠建議跟提供這些資料控制方，到底我們要做哪些事情？要遵守什麼原則？不只是遵守剛剛講到的公約，還有 OECD、GDPR 相關指引的內容。

所以，我覺得這整個設計跟實施的本身是蠻有挑戰性的，因為，第一個，我們必須要有好的人才；再來，也必須要有還不錯的薪酬，才能吸引這些人才願意加入，不只是斯里蘭卡內部的人才，同時也讓海外的人才願意加入我們。所以光是通過這一個計畫本身就花了 8 個月的時間，這也是目前斯里蘭卡面對的挑戰。當然我們有透過非常多

國際合作方式持續促進，包括透過歐盟、美國的協助，還有跟日本的合作等等，非常多的國家都非常親切友善，跟我們資料保護的機關合作，讓斯里蘭卡的機關能夠把最基本的計畫規劃完成。因為時間的關係，我就先分享到這裡。

賴俊兆 Semaylay i Kakubaw 處長：

謝謝 Fernando 先生，非常用心地跟我們分享斯里蘭卡的經驗，簡報的內容非常豐富，也可以給臺灣以及與會其他國家的夥伴作為蠻重要的參考。個資保護的議題，特別是怎麼樣去形成那樣的文化，以及人才培育的工作，因為等一下第二個場次也會有一些更深入的討論，在我們這個場次，剛剛蠻多的分享，也是回饋到我們現在「國家人權行動計畫」這個議題，特別著重在整個機制面要先有一個機關，後面相關立法的行動，或者一些行政的配套、指引，也可能需要同步地來對接。這個我們也可以在等一下的對話來做討論。

很感謝剛剛兩位講者都針對你們所關心的議題提出具體的建議。同時，在臺上的是我們下一場的講者 Kind 和 Kurihara 先生，我們還有一點點時間，我建議先請臺上兩位講者，看有沒有針對剛剛第一場次的分享及回饋，接著我再開放臺下，也許蒐集兩到三個問題。希望最後還是給兩位第一場的講者可以有一定的時間回應。我先邀請 Kind 委員，謝謝。

講者三 Carly Kind：

謝謝，因爲我自己對這個議題非常有興趣，所以想要請問 Fernando 先生，您有參與設立資料保護機構的經驗，我自己本身加入現職機關的時候，相關機制就已經開始在運作，所以我想要知道，您剛剛提到

您曾有一些國際合作的經驗，譬如歐盟、日本跟美國，對你們來說，斯里蘭卡的個資保護監管機構（Data Protection Agency 或 Data Protection Authority, DPA）需要的合作是什麼？譬如，我們機關，可能有相關的能力可以提供這些國際的協助跟合作，以您的經驗來說，目前最有幫助的方式是什麼？是資料、材料的交換？還是培訓相關的人員？或者還有哪些其他的資源是你們覺得最有用的？

講者二 Jayantha Fernando：

謝謝 Carly。我知道妳也是來自類似的專業背景，但是你們的個人資料保護機關有相關的資源去做整個執法的行為。斯里蘭卡的資料保護機關，基本上，整個設置一路以來是蠻有挑戰性的。

我們整個立法框架的建構基礎，明定在《個人資料保護法》裡面。當時起草的時候，我就是在公部門，我們非常努力要對抗傳統議會，當時國會是想要用傳統的典型模式，把它列在部會的模式底下，這並不是斯里蘭卡針對其他監管機構模式（如反貪腐委員會 Anti-Corruption Commission,ACC、中央銀行等）所採取的方法。在那之後，我們雖然非常辛苦，但是我們成功了，在我們的堅持之下，確保法律本身能夠讓個人資料保護機關是一個獨立的機關，一旦資金到位以後，它就能夠成為一個獨立的機關，但是為了要達到這件事情，我們其實面對了非常多的憲法挑戰，但總之我們成功了。當我們真的做到這件事情的時候，建立一個獨立的機關，代表人員是必須有足夠的能力。當時我們在成立的時候也跟歐盟、美國商務部、日本還有很多我們的夥伴合作，我覺得對我們蠻有幫助的地方是，他們提供給我們資源，還有專家給我們建議，甚至自願做一些訪查。譬如我們有挑選幾個斯里蘭卡的人才，讓他們真的到當地瞭解在整個不同的產業和領域裡面，法規要怎麼樣適用。同時我們必須要去發展出相關不同部門、不同領

域的指引，包括兒童保護、財務領域，甚至是 AI 本身。因為法律本身也有有限的一些保障，譬如自動決策或是申訴機制等等，這些全部都在我們的《個人資料保護法》裡面稍微有提到。

但不論如何，這算是我們覺得蠻有助益的合作方式，在去年與歐洲資料保護委員會的討論中，我們最初的起草委員會中的一些人，尤其是我本人，同意以志願者的身分，為資料保護局提供 6 個月至 12 個月的支援，我們會去讓這一些新進人員能夠逐漸熟悉業務。當然因為我們希望是獨立機關的模式，所以我們面對的第一個挑戰是，讓相關的財務部門去批准，把經費真的能夠留到裡面，這對我們來說是一大挑戰，以目前來說，確實還是有進展的。另外你剛剛有提到國際合作如何提供斯里蘭卡資料保護專責機關幫助，對於這個新創的單位來說是需要講求去執行落實。我們要怎麼去落實，實際的具體措施是什麼？要保護的對象是誰？同時怎麼樣去推動數位科技網路的發展，避免帶來的危害，去取得一個平衡，我想也是很重要的。

所以我們也針對很多議題去做研究，很多剛剛有提到的國家也提供我們資源，提供我們專家，讓我們能夠去參考、借鏡，讓我們能夠推動成立資料保護機關，還有去推行計畫。

講者四栗原宏平：

我覺得這個討論真的非常有意思，我主要是在私部門，其實我想要請教 Jayantha 的是，在實務上公私部門怎麼去協力。因為我們在隱私的部分有很多的相關法規，我們也談到說對於業界來講，要做到法遵當然很重要，但是我們也要保護基本的權利。所以您會建議公私部門怎麼樣去合作，透過多方利害關係人的機制，不知道有沒有什麼建議或是想法。

講者二 Jayantha Fernando：

非常有趣的觀點，其實我剛剛在簡報中有提到，我們的 PDPA 跟其他的法案、法規不太一樣，剛剛有提到，我們每一個版本及更新版本都會放在網路上，所以不管是公民大眾或者產業都可以看到，都會提供一些反饋及想法，會影響我們後續的政策實施或是擬定。針對您的問題，我覺得要找到一個好的平衡，會需要私部門，也就是業界跟公部門大家齊聚一堂，去做交流，有充分的討論一起去做創新。我們常常看到，有時候利害關係人他們意見可能不一致，對於政府來說，要找到共識也不容易。我們認為在法律的用語上，必須要夠精確，能夠去調和各方利害關係人的利益，去有效因應不同相關單位他們遇到的挑戰，不管是隱私或是其他的問題。具備一些法律基本的要素，像我們在前言中就有談到，要去推動數位經濟的發展，把你的重點列出來，我們在條文中，應該是第 32 條還是第 33 條有提到監管機關必須要建立一個產業諮詢委員會，透過這樣的委員會去草擬相關的個資保護法規，還有研擬相關的指令。在這樣諮詢的過程中，監管機關就能夠去跟利害關係人做討論，找到一個正確的或是好的平衡點。

賴俊兆 Semaylay i Kakubaw 處長：

好，我們大概還有 10 分鐘左右的時間，現場徵求 2 到 3 個問題。因為有關個資保護的議題，等一下第二場次我們 4 位講者都還是會在臺上，會有蠻多對話，看看我們現場有沒有要提問的，請先告訴我您來自哪裡，問題也儘量精簡。

觀眾一：

大家好，我叫 Matt，來自全球網絡倡議 Global Network Initiative。

我想要請教來自斯里蘭卡的 Jayantha Fernando 主任，我想要問的是適用性。有兩個問題：第一個是針對斯里蘭卡，第二個是比較一般性的。第一個是想要問，您提到獨立的委員會有資金、有預算，例如網路安全委員會，你們要怎麼確保任命是獨立的？第二個，跟網路安全法相關的疑慮或討論，《網路安全法》與 PDPA 的關聯？或者是你的觀察是什麼？

講者二 Jayantha Fernando：

謝謝你的問題。現在因為我不在公部門了，所以可以比較自由的回答。談到獨立的資料保護專責機關，目前的框架設計確實是有一個主席，還有委員會成員。他們是透過三階段審核或是任用遴選規則產生的。我們會去看相關的人選聘用規則，把三階段的評選訂出來，一旦訂好了以後，就算政府的機關在遴選的時候偏離了這些階段，因為有這種方式，我們還是可以確保，是可以一路上訴到最高法院去尋求救濟，因此當這個標準沒有符合的時候，是可以有相關的一個審查機制的。據我所知，我們最高法院在這類任命上做出的裁決中，包括在斯里蘭卡上訴法院成功申請的「職位擔保令」（writs of quo warranto），已證實這一點。

主席一旦被指派以後，我們會去確認到底有沒有違反《個人資料保護法》跟其他相關法律的情形。第一個，我們要確保，部會不能夠對資料保護專責機關下指令，或是部長不能指示說要做些什麼事情。第二個，他有一個任期的保障，在這個任期之內，委員會的主席是不能夠被撤銷職位，除非某些合理的原因，合理的原因，列在《個人資料保護法》裡，這個認定標準是非常嚴格的。因為有這些保障，當然就代表我們可以有比較獨立一個機關。另外，我們還有一些相關的監管的設計，譬如說中央銀行，這個是在《個人資料保護法》通過之後，

我們把它納在裡面，代表我們的董事會不是從公部門這邊去拿錢。基本上，能夠真的去確保他們有獨立性。我們就是希望透過這種文化上的轉變，來推動《個人資料保護法》，而這種精神最終也融入了一年半前通過的《中央銀行法》，我們對此非常滿意。

第二個問題，網路安全委員會的部分。你剛剛提的問題蠻有趣的，我自己其實不太喜歡《網路安全法》裡面很多的條款跟內容，為什麼呢？因為它確實可能潛在跟 ICCPR 的一些應用是有違背的，而且斯里蘭卡是在 1980 年代的時候，就已經簽署批准 ICCPR，所以我現在有聽到的消息是，第一個，網路安全委員會可能是要透過《網路安全法》來設立，但是他們其實並沒有獲得預算，今年的預算分配他們甚至沒有拿到任何的預算。這其實就是對我們這些利害關係人是有傳達出一個訊息，代表他們是想要讓這個法律退場的。因為我們看到的是，他其實在實施上是有落差，而且並沒有好好的去適用整個相關的國際規範。另外，雖然在網路安全委員會裡面可能是有申訴的機制，但是卻沒有非常完整的設定。

第三點，我要跟大家提到網路安全委員會是不是能夠去適用《個人資料保護法》的職責。在《個人資料保護法》第 3 條，非常清楚講到，如果要去規範個人資料處理，包括刑事相關目的，只要跟個人資料處理有關，該法具有優於其他法律的效力。我們不太確定未來這些監管者會不會真的照著這個法律來管，或是個人資料的保護機關是不是能夠真的有強力的執法，位階真的能夠凌駕於在網路安全委員會之上？我們還要看未來的發展。《網路安全法》的時效跟《個人資料保護法》之間，如果有違背該怎麼辦？這個未來還需要觀察。但至少我們在法律裡面是有規範的，自然我們也可以看到也許在《網路安全法》會制定修法，譬如在委員會裡面，政府有一些機關確實是有一些挑戰。但因為過去我有一些職責，所以有些東西我可能沒有辦法完全說出來，

但至少在這樣的框架裡面，我是可以分享的。

賴俊兆 Semaylay i Kakubaw 處長：

謝謝 Fernando 先生詳盡的回應，因為個資的問題，我們第二場還可以繼續討論。最後的 5 分鐘，我比較想要再讓 David Kaye 先生給我們一點回饋，針對我們第一部「國家人權行動計畫」裡面會擔心言論會有害，怎麼樣去面對這個有害的言論，ICCPR 第 20 條也課予要求國家要有一定的義務，想要針對這個問題再進一步請教 Kaye 先生，我知道大家也很關心言論自由與意見自由的問題，請您再給我們一點建議，謝謝。

講者一 David Kaye：

好，謝謝，這是個非常重要的問題。老實說很難真的去深入回答，因為講到言論，要分成很多不同的種類。所以簡單來講，在這麼複雜的框架底下，我只能稍微回應，如果國家要對於言論做任何限制的時候，無論是什麼類別，剛剛講到的相關行動計畫也有提到，有疑慮的這一些領域，我覺得最必要的是，這個類別相關的規範，相關的限制，必須要非常清楚地列出來、找出來，這個是非常重要。

當說到要清楚列出相關規範及具體限制的時候，不只是清楚講到問題到底是什麼。譬如說可能是假資訊或是不實資訊（disinformation），這確實可能是其中一個問題，真正的困難在於要去定義這個問題到底是什麼。不實資訊，當然有各個不同的類別，對於言論自由來說，可能又是最困難的一塊，因為言論自由的權利，是代表能夠去尋求各式各樣的資訊，這代表不只限於真實的資訊，對吧？所以，現在在這個領域裡面，我們確實開始有一些限制，特別是在講不實資訊的時候。

這雖然是最困難的一個領域，但同時也是最好的一個類別，第一個要能去識別並且定義你到底想要解決什麼樣的問題，具體想要解決的問題是什麼，這其實也是行動計畫可以協助的。譬如說在資料保護裡面，就有提到其他世界各地的資料保護相關機關，以及趨勢到底是什麼？同樣地，我們也可以用這種方式，譬如提到歐盟的《數位服務法》，就可以看到透明度的規範到底是什麼？限制的原則到底是什麼？我想，也許是這一塊可能是在行動計畫裡面可以採行的作法，確實是可以去參考其他的機關跟其他國家的作法。

另外，我覺得比較重要的是整個脈絡本身，因為行動計畫不只是提到公約，其實也有提到其他的權利。因為行動計畫裡面有提到非常多對兒童有害的資訊或對兒童造成的傷害。我們必須要知道，當我們在面對兒童的傷害，兒童在兒童權利公約裡面，也有權利享有言論自由以及資訊的取得權。所以，就算我們是在面對這個非常清楚而且廣泛，大家都同意的認知裡面，我們必須要解決對於兒童的傷害，在解決問題的同時又必須確保與兒童享有的權利是一致的。特別是兒童現在發展的是批判性思考，這樣的思考也是必須要被保障，必須要兼顧。

所以，再次強調，這是一個整體層次的一個大致回應，在具體做法上，要有很多不同的範例，第一個，是去確保獲得明確的定義；第二個，是規範要非常明確；再來，是去回應處理問題，而且這些回應必須符合必要性以及比例原則。

賴俊兆 Semaylay i Kakubaw 處長：

時間差不多到了，我想很多的議題的確很困難。ICCPR 是 50 幾年前國際重要的一個人權典章，時間走到今天，我們面對數位當代，其實人權的問題是越來越困難，挑戰越來越多，但是還是有很多本質重要的問題跟原則，是值得我們回頭再來參考的。第一個場次，非常

感謝 4 位講者的對話，第二個場次這個對話可以持續。我們再次謝謝臺上 4 位講者，第一個場次到這邊結束，謝謝大家，謝謝。

▼ 議題二：個人資料保護專業人才之培訓

鄭瑋主任：

各位來賓大家好，我是國家資通安全研究院人才培力中心主任，鄭瑋，同時也在國立臺灣大學圖書資訊學系任教，歡迎各位貴賓來到議題二場次，個人資料保護專業人才之培訓。很開心 4 位講者都在臺上，與我們參與這個議題討論。想進一步介紹關於議題二所要發表觀點的講者，讓我們歡迎現任的澳洲資料保護官 Carly Kind，以及來自日本 Privacy By Design Lab 的創辦人栗原宏平先生 Kohei Kurihara，謝謝。在接下來的引言前，想要再進一步的介紹兩位來賓，Carly Kind 是擔任現在澳洲資訊委員會辦公室的隱私委員，平時致力於研究人權跟科技交錯的領域，她同時今天會給我們帶來包括個資保護相關的機會跟挑戰。栗原先生，是在一個社群文化裡的工作者，他創辦的 Privacy By Design Lab 是支援企業的資料保護措施，個人專業領域就是資料保護、數位行銷跟區塊鏈，並從 2017 年起擔任美國非營利組織，政府區塊鏈協會的日本代表，對多方的利害關係人這些議題都有研究。

在這個議題裡，想要跟各位分享的是，很榮幸今天參加這場重要的座談會，其實資通安全跟個資保護是密切相關的，我本身在國家資通安全研究院有進行國家人才的培育，想要跟大家分享，在資安領域，從頭開始去打造人才培育策略的一些想法。首先，想要跟各位分享的是，我們發現從頭開始在打造資訊安全人才培育中，有幾個關鍵的因

素：第一個是，如果我們對想要培育的人才作分類，我們能知道，他不是一個非常籠統的資安人才，或是個資人才，而是我們使用國際間通用的框架，將這些人才培育跟人才的類型去做一個細分，然後明確地劃分出他們的能力、任務、知識跟技能，未來我們就有機會進行精準的培育。比起籠統地去從事教育，把各位人才放到教室裡面去進行學習，如果能給予更明確的框架，譬如說技術型的人才，他更適合使用數位靶場，或者是攻防平臺、桌上兵推...等等的實戰演練，也許他可以迅速增強實戰的經驗。另一方面，我們也發現如果產、官、學三個方向可以做公私協力，譬如說在政府端，可以制定分類清楚的能力框架，由大專院校進行培訓產業間提供實習的機會，或是甚至後面實務的導引，這都有機會為人才培育做出一個更完整的生態區分。以下我們想要歡迎 Carly Kind 來為我們分享一下她的見解。

講者三 Carly Kind：

謝謝主持人，謝謝行政院人權處的邀請。非常開心能夠來這邊跟臺灣的夥伴一起去探討關於個資保護主責機關的相關議題。關於個資保護部分不只是關乎人權，也關乎臺灣的「國家人權行動計畫」，還有《個人資料保護法》等等相關的議題，是一個跨領域的主題。我想臺灣在這部分一定可以做得非常的好。在隱私的部分，其實是一個很重要的基本人權，隱私以人權為本，訂定一個很完善的隱私相關法規非常重要，也要有非常多的人才，才能夠打造這樣的隱私文化，凝聚隱私意識，所以除了人才，還有隱私的法規等等，都必須要相輔相成。我過去 20 年從人權到隱私的領域都有涉略，身為澳洲隱私保護官，大概擔任這個職位 1 年多的時間，就培養個資保護人才方面，可以分享一些想法，也提供臺灣成立個資保護專責機關一些建議。澳洲其實有一部較舊的《隱私法》，是在 1988 年通過的，其實現在來講有一

點過時了，臺灣個資保護法的要素，可能都會比我們的《隱私法》更現代化。像歐盟的 GDPR，澳洲現在還有一些是還沒國內法化，另外也有一些國際法它是比較概念性、原則性的，也需要再去因地制宜。

澳洲的《隱私法》也是一樣，可以應用在公部門、私部門，沒有特別區分資料處理者和控制者的部分，也不涵蓋年收入低於 300 萬澳元的小企業，因此，年收入低於此門檻的組織不受《隱私法》的約束，另外針對預算的部分也有訂定。它不要求組織必須擁有個人資料保護官(Data Protection Officer, DPO)，因此這似乎是和臺灣制度的一個區別點。《隱私法》要求單位組織要去針對隱私保護有一些舉措，但監管機構並沒有認證 DPO 的職能。另外有一個專門適用於政府機構的實務準則，有列出一些其他的要求，例如政府一定要有隱私大使或是隱私代言人，每一個部門必須要有一個專責的負責人等等，這邊就是我剛剛大概講到，澳洲在隱私方面的相關法規。剛剛其他的與談人也有談到，第一步，就是要有一個獨立的專責機關，獨立性真的是至關重要，因為這個相關的法規，會影響到政府也影響到其他業界。獨立的意思，首先就是要財務獨立，所以，我們跟斯里蘭卡的情況也非常的像，這個單位它是有完全的自主性，可以有自由去運用它的預算，它也應該是政治獨立，是一個獨立的監管機關，它的問責的機制，還有跟國會呈報的方式都有清楚的訂定。我們在法規裡面也有列出，我們不能跟政府部會去分享特定的資訊，除非有特別的情形。我是隱私保護官，我們也有資訊官，還有言論自由保護官，我們 3 個其實就像是一個委員會的成員，然後各自在專責的領域去推展業務。

有這樣的基礎，就是個資專責機關有獨立性確保之後，下一個問題就是，新法規出來，大家要怎麼要求他們做到法遵。我覺得可能要恩威並濟，在「恩」的部分，要怎麼樣引導大家給誘因，就像剛剛前面與談人講到的，好的隱私規範，應該是要能夠凝聚公共信任，在資

料蒐用的部分要做好。政府應該要能夠以促進公眾社會利益的方式去運用個人資料，同時獲得大眾的信任，所以誘因的方式，我想是可以透過研究，還有用數據去支持。我們每兩年其實會去針對澳洲的國人，做一個隱私相關的調查，這其實也是一個溝通工具。我們可以很有信心的跟大家分享，澳洲人其實很重視隱私。今天如果一個品牌隱私做不好，他們會寧願去選另外一個品牌，所以這代表一個隱私意識的文化的建立是對商業有利的。我總是從人權的角度出發，但我認為能夠提出這些務實的論點也非常有幫助。

再來就是「威」，執行的部分，在執行上我們必須要用非常穩健、有序的方式來執行。所以教育是很重要的，必須要去教育大眾什麼是隱私？他們要在乎的事情是什麼？告訴這些納管的單位他們要做什麼。教育，可以透過媒體、透過辦理研討會活動、透過教育宣導的活動等，讓我們去傳達訊息告訴他們，遵循法規是非常重要的。主管機關必須要很擅長跟社會大眾溝通，它是一個面向公眾的單位，另外還有就是提升成效，就是發揮最大的 CP 值。澳洲人口大概是 2,500 萬人，我們的單位大概有 150 名員工，必須去監管公領域及私領域，所以我們一定要在使用資源上有策略思維，希望能夠把影響力放到最大。今天一個法院判決可能就會對我們有很大的影響。在時間的管理上，可以透過金字塔的方式去思考，最底層的就是你今天花最多時間的教育宣導。就是研擬相關準則、手冊，說明法規如何適用，它對於各個產業如何去適用，我們對於臉部辨識技術有特定的指令或者是原則，還有隱私評估怎麼做等等，怎麼樣在網路上追蹤圖元等等，所以我們針對特定的科技或是特定的產業有明定準則，教育是我們花最多時間心力的部分，在金字塔最底層占最多的。

接下來是跟法規相關的特定舉措，例如我們可能辦工作坊給一些單位，讓他們瞭解法遵的部分，你可能面臨什麼挑戰，可以怎麼做。

英國這部分就做得很好，他們有一個熱線，讓各單位可以打去詢問，這個部分如果我想要有一些創新或是想要隱私做得更好，我有什麼相關法規可以去借鏡遵循？英國有這樣的熱線去提供輔導跟諮詢，我覺得也不錯。

再往上一層，範圍相對較小，就是稽核，法遵的稽核，或是去調查特定的產業，去做申訴的處理等等。至於金字塔的頂部，就是去思考針對少數違規的案例，我會做什麼樣的處理或是處罰。所以基本上最上面這一塊，相對來說只是法律未獲遵循的時候，專門針對個案去處理，所以你做完法規遵循以後，就不會進到最上面這一塊。當然我們主要是協助遵循，真的沒有辦法的話，我們才會進行執法去處理相關的申訴。當他違反某一個法規的時候，譬如他可能會影響到處境不利群體，或者是我們的介入，是真的能夠改變整個產業的話，我們就會使用金字塔最頂端的這種做法。當然在最上面的時候，你影響到的是一個比較小的對象範圍，但是反而可以造成更大的影響，你會影響到整個環境。

我最後再講幾件事情。如果你們要建立自己的個資保護監管機關，第一個，必須要在法院建立一些專業人才，以及在法律領域裡建立一批人才。根據臺灣司法的制度來說，可能會需要發展的，是在監管單位以外，還必須要有相關的一些專業人才做仲裁跟裁決。再來是我們要怎麼樣去回應危機，剛剛我同事有提到網路安全的部分，我們持續看到的是在管轄區都會碰到各種資安的問題，在澳洲，之前有一個大型的資料外洩事件，這時候我們機關就會介入說，為什麼我們需要相關的法律。因為我們看到這種大規模的資料外洩，他影響到的是每一個人，我們利用這個機會，真的去善用我們需要的立法和實施。另外，是去確保法遵的同時，你也要瞭解到，有時候好的法律，大家如果有錯誤的詮釋，這些不良、非善意的詮釋，會影響到你的監管成效。譬

如在歐盟的 cookie 通知，對於這項具體要求，企業將其解釋為要求提供 cookie 通知，最終使人們對《隱私法》感到相當惱怒和沮喪，因為人們會覺得為什麼每次我進網頁都要點回應。所以這其實反而讓《隱私法》沒有真的做到他要發揮的功能，所以你要非常清楚知道，到底法遵應該做到什麼事情。如果能夠具體化，對於規範對象來說，也能夠更有利。

再來講到的是，我們要建立起私部門的專業能力，首先，要去掌握的是現有的專業，譬如在國際企業裡面，在面對其他的管轄權，他們可能已經有相關的隱私專業人員，你先建立起一個私部門的社群，讓這些專業人員能夠站在裡面，他們會是你盟友，他們自己在公司內部裡面，本身就已經在討論說為什麼要進行法遵，他們已經在自己公司裡面，在要求對於隱私應該有的資源，所以這些私部門的盟友會是個人資料保護監管機關（Data Protection Agency 或 Data Protection Authority, DPA，以下簡稱 DPA）的盟友。所以，花一些時間去建立這樣的社群跟盟友，對你們來說是非常重要，因為他們也會仰賴你提供資料給他們，再讓大眾知道，為什麼他們的公司、他們的董事會、他們的執行長要把錢丟在隱私法遵上面，所以這是彼此相輔相成的。再來講到的是專業人才，我們也對公部門的隱私專業人員進行培訓，去建立起這些專業人才，他們的相關的技術。再來我們在國際上看到有非常多非常棒的資料跟資訊提供給 DPA。我想要推薦亞太隱私機關，每年召開兩次會議，這是一個非常好的亞太地區數據保護機構的聚會，凝聚大家在一起的一個討論空間跟活動，另外監管單位本身彼此之間的分享也會非常有用，謝謝大家。

鄭瑋主任：

非常謝謝 Ms. Kind 的精彩分享，剛剛提到了 DPA 這個獨立的機

關，政治跟財務上的獨立是非常需要。當然 Carly 也有提到了相對精準的個資保護人才，像是資料保護官或是資訊官或甚至是言論自由官，這些都需要併肩一起合作。Carly 還幫我們提到了在執行個資保護的時候，會需要有一個金字塔。從最底層的教育，到中層落地實作的解釋，到上層的稽核或處理一些細部的申訴管道等等，都帶給我們很系統性的瞭解。

再進行下一位講者的演講之前，我想要迅速請教 Carly 一個問題，可不可以請您大概講一下在澳洲個資保護人才的培育過程，也許用剛剛您所提到的金字塔，跟我們分享這三層所需要不同的人才，大致上會進行什麼樣的訓練，讓他們來協助全國各地的個資保護人才的實踐，謝謝。

講者三 Carly Kind：

其實我們沒有一直聚焦要提供培訓，因為在澳洲我們沒有特別的計畫，並沒有提供 DPO 認證。但是整體來說，我們大多數的個人資料專業人員，不管你是在監管單位，還是在私部門，基本上都是律師的背景。所以你要跟法務人員、大學的這些機構合作，因為他們可能開始在大學的階段就在教《隱私法》，因此我們的個人資料官會去跟私部門一起合作，一起建立彼此之間的理解，這是第一點。

第二點，我們認為落實執法本身就有一個教育的意義，因為你非常具體地在跟大家講，相關法律在這個案例裡面應該怎麼適用。同時我們也跟法院互動，有時候跟法院的不同層級互動，就會開始有更多不同的辯論，因此法官、律師跟大律師(barristers)他們也都參與在這個過程中，他們也會有更深入的瞭解，因為他們必須要花時間去思考我們提起的這些個案，也慢慢就會培養出他們的能力，所以我想這是需要時間的。

我們會參與這些對話，過去曾參與的對話，第一個就是我們透過執法的方式，譬如去年我發布一個裁定(issued a determination)，指出在零售店使用臉部辨識，在特定的脈絡底下是不合法的。所以我就把我的裁定帶到這個對話裡面，接著就有很多媒體、電視的報導，然後大家也開始討論，所以開始公眾的討論，接著我們就有學術的文章開始去檢視我們的裁定。目前案件已經進入其中一個法院，接著可能會提出上訴，所以我覺得在這樣的一個過程中，越來越多人會參與我們的對話，知道說到底法遵是如何，這個法律應該要怎麼樣去詮釋等等。所以我覺得不是單純只去看培訓，當然培訓本身是非常有價值，但我們是透過論述，然後透過加入對話，讓大家真的可以一起去討論，譬如有法律系學生、律師、法律的專業人才，甚至是學術界也一起參與。

鄭瑋主任：

非常謝謝 Carly 的補充，Carly 補充到培訓本身之外，執法的過程更像是一種對話還有教育。Carly 也提到去年，我沒記錯的話應該是一個五金行零售商的 case，後來上了新聞媒體就連臺灣這邊都有看到相關的新聞，非常謝謝您的分享。接下來我們請栗原先生來分享，他在 Privacy By Design Lab 的見解，他的題目是 Training Of Professionals In Personal Data Protection。

講者四栗原宏平：

謝謝大家，謝謝臺灣政府邀請我來到這個非常漂亮的城市。非常榮幸來到這裡能夠跟大家一起討論這樣的主題。我們就開始，來看一下投影片。

稍微講一下我個人的自我介紹，接下來再跟大家介紹我的主題。其實我在科技的領域裡面是有一些參與，疫情之前我是在區塊鏈與身

分識別相關領域工作，但是在那個過程中，我發現其實是有一些問題的，譬如在資料保護上面，有一些倫理規範並沒有被實踐，很多時候公司可能只注重成長，但我覺得這其實對未來是不好的，也因此我們應該要改變大家的思維，去聚焦在保障大家的基本權利，同時能夠去驅動創新。因為我是從新創的新興科技背景，再進入到隱私跟個人資料保護的工作，這也是為什麼我們知道在這個過程中，跟多方利害關係人合作是非常重要，才能一起打造更好的未來。

接下來跟大家工商廣告一下，這是我們 2025 年 Privacy By Design 的會議。我們也有一個「個人資料日」，在 1 月 28 日才剛舉辦完這場活動。如果大家有興趣，我可以分享更多的會議相關資訊給大家。我們主要的活動當然是希望能夠提升意識，因為隱私的意識是非常重要的，我們必須要有這樣的一個隱私意識，才能跟各個不同的利害關係人合作。不然的話，就會遺漏很多東西，譬如可能產業就沒有辦法加入其中。這也是為什麼我們基本上會參與兩種活動，第一個是剛剛講到的 Privacy By Design 的會議，我們每年的 1 月 28 日會舉辦，跟各個不同國家的資料保護從業人員一起合作，今年我們有邀請了一些講者，包括歐盟的資料保護監督機關、臺灣的唐鳳、新加坡的相關資料管理局，還有加拿大以及日本政府。所以不只是私部門，我們同時也有邀請日本的這些政府代表，因為重點是這不只是私部門，監管單位也非常重要，我們需要的是公私部門一起參與這個討論。另外我們也有一些訪談，譬如我們有邀請資料保護相關的專業人員，同時也邀請 NGO 等等去分享他們的經驗跟資源，以及我們要怎麼樣一起打造更好的社會，這些都是我們採取的行動，希望能夠提升國內的意識。

在我進入到細節之前，我想要先跟大家分享的是 Privacy By Design 這一個概念，Privacy By Design 就是在設計時就加入隱私，這個為什麼重要呢？對於網路安全為什麼不可或缺？Ann Cavoukian 她

先建立起這個概念，她那時候就有提到一個很重要的概念，我們應該在設計的時候就應該要納入隱私跟安全，當然這也納入培訓還有相關的內容創造裏面，因此我們開始進入到這樣一個討論。我們的組織就是因為她的理念來做命名，Privacy By Design 就是設計的時候就必須納入隱私。我們也試著不只是說服隱私領域，同時還有產業，一起要做到這件事情。不然業界的做法可能就不會在產品跟服務裡面納入這個元素，這也是為什麼我們也鼓勵業界，在整個產品的設計跟服務設計時，就必須要先納入隱私在裡面，當然隱私跟安全也必須要被整合在一起。

講到培訓，培訓本身其實是很重要的。第一點，是在引起興趣，因為大家想要參與隱私討論的話，他們要先有興趣。當然一開始我們必須用探索式的方式來一起討論，針對這個主題，我們到底應該要怎麼樣進行討論。接著，當然就是對話，在這個階段，我們開始去分享、討論我們的想法，大家的做法還有概念等等，這些算是彼此互相之間的學習，這一點也非常的重要。當然我們在年度會議的時候，會用這種做法，譬如所有參與的人會分享他們的想法跟經驗，不只是回答答案而已，而是真的去分享大家的經驗跟想法，然後一起去討論未來。這也是為什麼我們會議就是用這種概念，我們希望用一個永續的網路方式去討論，用這種長期的方式，跟比較大型的主題，我們就可以一起討論。

再來，我們需要的是合作、協作，合作基本上是非常重要的核心，在會議裡我們會邀請不同的利害關係人，譬如我們會邀請 Z 世代高中生在我們的會議裡去發表內容，說為什麼他們認為對年輕世代來說隱私很重要，不然的話，只是去制定法律我們就沒有辦法真的適用，因為我們需要的是年輕人能夠真的在意。有時候年輕人可能完全不在意隱私，他們更在乎的是使用上的便利性，所以我們需要在設計的時候，

提供給年輕人服務的時候，就能夠納入這一些，這是在我們會議中發現非常重要的要點。

接下來就透過這個流程去營造隱私意識文化，像今天這樣的場合，就非常的重要，能夠去促進意見交流，把相關的元素納入我們的培訓裡面。剛剛談到，我們每一年都會辦相關的活動，大家都可以來參加，瞭解隱私相關的議題，就算你是完全不瞭解相關的議題，這不是一個技術難度很高的議題，這就是整個活動的概念。我們也需要有一些國際研討會，邀請國際的重磅專家，或者是國際組織來一起做交流，我們每一年都會邀請 UNESCO 來跟我們談如何發展永續的網路世界，而這些我們就會再去分成 Privacy By Design Conference 2025 年會議的子議題。

我認為在亞太區應該要有一個特殊的做法，因為針對隱私保護，其實歐盟也有這樣的概念，但是後來我們發現，在東亞新年期間舉辦，也就是一、二月的時候，剛好是華人的農曆春節，時間比較難搭起來。如果未來我們能夠辦一個亞太區的資料保護盛會，我想會是非常好，也可以跟臺灣這邊一起來討論。簡單分享到這邊，大家如果對於我們哪一份年會的報告有興趣，也可以上網或是透過 email 來聯繫我，討論一下亞洲的資料保護日、提升隱私安全意識等等，謝謝。

鄭瑋主任：

非常感謝栗原先生的分享，栗原先生一開始就跟我們說，要有隱私的意識，實在是太重要了。再來，他透過流程去建立一個隱私的文化，包含一開始的興趣，再來是對話，到最後是多方的合作，甚至提升到國際之間不同文化的交流。這邊有一個簡單的問題，快速地想要跟栗原先生接著請教，在推動 Privacy By Design 的過程中，您剛剛有提到不同國家也會在這個會議上面一起進行，想要請教您，是否有觀

察到一些常見的，在推動隱私文化上，因為不同國情不同文化遇到一些有趣的事情。因為我們知道，不同國家跟不同文化，他在風險的規避、權力結構或權力距離上面都有可能會不同。這邊想請您在辦理國際活動，或是其他活動的時候，可不可以跟我們分享一些在推動上面的種種，謝謝。

講者四栗原宏平：

非常謝謝你的問題，我想我們必須要去尊重不同國家他們的隱私做法。因為語言、文化、種族都不一樣，所以我們對於隱私的認知也不一樣，這是我們必須要尊重的。

再來，就是我們要去分享各自的觀點，就算 privacy 都叫做隱私，我們的認知也可能不一樣，所以怎麼樣找到共識，怎麼樣一起去合作，我覺得很重要。每個國家不能夠只去管自己的問題，我想業界他們也會談隱私，但是業界、私部門、公領域跟 NGO 對隱私的認知可能都有一點差別，我們一定要去瞭解各領域對隱私的定義是什麼，所以每個人都可以自由的去抒發己見，這不只是監管機關的問題，不只是業界的責任，也不是 NGO 獨立可以去處理的。隱私涉及我們所有的人，所以大家可以一開始就分享，就去瞭解探索隱私是什麼樣的概念，這是第一步。

第二步，就是創造對話，這是非常關鍵的，我們今年的會議有邀請到一些 Z 世代的代表。我想澳洲算是在隱私走在前面，社群媒體的業者，必須要去保護一些處境不利的群體，我們從很多的案例分析、探討去找到一些結論，年輕世代他們也有自己在意的事情，我們也必須要尊重，把年輕世代的反饋帶到規則的制定，然後再去跟業界的利益對接，這些都是很重要的過程，要足夠包容不同的群體，這是我的看法。我們也是一直很強調多方利害關係人參與的過程，產、官、學

各界聚集在一起，我們也知道社會上有很多不同的群體，所以我們的過程要具備包容性，讓大家都能充分的參與，所以我後面才會寫到，不同國家、不同群體大家一起合作，非常的重要。

鄭瑋主任：

栗原先生說如果要面對不同國家不同文化，大家一起要推動隱私文化，他建議是回到隱私的本質，然後大家一起建構不同隱私的意義，最後產出一個比較包容並且透過社群的活動與年輕世代對話，對接回企業本身在做隱私的實踐，也就是他一貫秉持著要跟多個利害關係者來對話跟溝通，一起來朝向實踐隱私的文化，非常謝謝栗原先生。接下來，我想開放臺上兩位講者提問，想首先邀請到 David Kaye 先生，不知道您對兩位講者的演講，有沒有一些想法或者或是補充，甚至是跟他們提問，謝謝。

講者一 David Kaye：

謝謝，我覺得兩位講者的分享都非常的好，我的收穫很多。想要先問 Carly，可不可以請妳談談，你們有 3 個獨立的主委或是保護官（commissioners），你們彼此之間怎麼協作？因為隱私跟資料取得有時候其實是有一些衝突的，你們怎麼樣去處理這樣的問題。

講者三 Carly Kind：

這種 3 位委員的模式，其實每個國家不一樣，愛爾蘭有一個類似的模式。言論自由跟隱私綁在一起，我想很多國家也是這樣的模式。我覺得這個模式其實本身就蠻有意思的，有時候他們是一體兩面，有時候就是同樣的。我們這個立法框架其實有點複雜，它的整個設計就

是每個委員會都能夠去使用其它委員會的職能，所以言論自由那邊我也能使用。這個有點像是委員會成立之初，就內建這樣的衝突元素。我們的處理方式就是希望找到共識，共識治理的模式，所以我們這個委員會，我有我自己負責的專責領域，就是所有隱私相關的，但是我今天要去行使我的權利，一定需要跟其他兩位委員達成共識，意見一致。

當然過去有一些意見嚴重不合，非常不一的狀況，但我們平常就是密切合作，目前還沒有這種嚴重意見不合的情況，因為我們都是良好溝通、密切合作。所以制度的設計我覺得蠻重要的，我們很多時候在職能的分工上也都會一起去集思廣益，畢竟我們這些領域不管怎樣，都是以人權為本，澳洲也有去遵循 ICCPR 公約，有些義務他在面對其他權利主張時是可以去做一些取捨的，所以目前我們還沒有遇到重大衝突的情況。但我也瞭解你剛剛說到的，這種真的是有一點內建衝突，但有時候我覺得我們在思維這個想法上，可能會有一些不一，可以討論，謝謝。

鄭瑋主任：

非常謝謝 Kaye 先生的提問，他詢問了澳洲的 3 個委員包含資訊委員、言論自由委員還有資料保護委員，3 個管轄權會不會有衝突的情況，Ms. Carly 回答說當然是會有衝突的情況，但是有賴於健全的制度去設立，然後彼此溝通是非常重要的，這是一個非常有趣的問題也非常重要，謝謝。接下來我們想請教 Fernando 先生，不知道對兩位講者的演說有沒有什麼提問呢？

講者二 Jayantha Fernando：

謝謝兩位講者的分享，我覺得科技創新還有隱私的保護真的很需

要多方利害關係人一起來推動。但是我們也要體認到在設計的時候，一定要以人權為本、以隱私為本，去保護個人的隱私，然後在不同的考量中找到一個平衡。另外也很開心聽到 Carly 分享澳洲的模式，這也是我們借鏡的其中一個國家。David 剛剛提到說的 3 位保護官，感覺就是會有衝突，有時候利益是相衝突的。但是即便設計上是如此，你們還是能夠彼此協調去推動治理。在斯里蘭卡的法規裡，資訊取得的保障，其實也有相關的規範，並且適用在公部門。今天有《隱私法》適用在公、私部門，這個交界點，或者說在公部門這邊合法的資料蒐用，在公領域他就會變成一個議題，或是一個需要討論的事情。

在我們國家，因爲公共利益，會因此去要求公部門必須要公布細節、有關於個人的資料。雖然一開始我們沒有《隱私法》，但現在我們推出的《隱私法》，不是侷限或限縮，但至少要定義所謂「出於公共利益考量」，他的定義到底是什麼？我想這中間當然會造成一些緊張的張力，也許我們可以用澳洲的方式來去調整，我覺得這些都是蠻有趣的一些經驗跟分享。

這個場次我想問 Carly 一個問題，我記得剛剛好像有提到，法律不適用的實體包括低於 3 百萬澳幣的實體。假設現在有一個個人，他的權利受到影響，或者是真的有非常嚴重的資料外洩，這個資料可能是中小企業外洩的，可能是為了避稅的方式，低報了營收，或者是他可能是一個科技新創，他只是想要趕快在市場上推出一些新興的產業、產品，這也吸引了很多的消費者，但在這中間卻出現了資訊的外洩，如果是這樣子的話，有哪一些救濟的方式，或者是有哪一些申訴的方式呢？資料當事人是有權利？還是他就不適用？還是說我該怎麼樣？

講者三 Carly Kind：

中小企業有一個例外，如果這個公司本身販售的是個人資料，基本上它的設立目的就是要蒐集個人資料，就算它是小公司還是得適用《隱私法》。但是我覺得你剛剛講到的這個情況其實還蠻常見的，確實有一些實體可能隱私的做法非常糟糕，甚至有一些例子，會影響到個人，但是卻沒有涵蓋在整個《隱私法》裡面。所以當然我說的這些例外，應該要去移除，不應該有例外。

當然我們也必須要說，我們不會因為一個公司，譬如資料外洩，或者是被攻擊我們就處罰他，我們要證明公司真的有一些不作為，或者是已盡最大努力仍受攻擊，我想它可能就不會被處罰，因為公司做了一切能做的事情，卻還是因爲現在有越來越多精密的攻擊，造成資料外洩。回答有關救濟相關的問題，去年政府就有立了一個《新隱私侵權法》(new statutory tort of privacy)，現在個人是可以直接向法院提起司法救濟的，我想這個算是他可以做的司法救濟。此外，這也適用於侵害信賴義務的侵權行為（breach of confidence tort），個人得直接向法院提起救濟。

再來 David 提到的，如果各個不同委員之間存在緊張關係該怎麼辦？譬如資訊自由、言論自由跟隱私保護，在公部門的資訊自由、資訊取得、個人資料之間如果有交織的話，我們認為其實有某個單位可能會說，我們要拒絕這個要求，你直接去找隱私權，或者是說我們可能是為了要滿足資訊取得法，因此我們要去拒絕隱私的要求，這確實是一個挑戰。

最近我們開始討論的是，公部門使用的加密法，當然這個涵蓋的就是有關對象，第一個，會影響到公司紀錄是必須要去創造出來，而且要是法院判決也必須要知道這些判決是怎麼樣產生的，公民是有權利能夠獲得的。再來是我們也必須要把隱私納在其中，如果是這樣的話，我們應該要怎麼樣去傳達相關的資訊，當政府有這個判決的時候，

我們應該要怎麼樣呈現這些資訊。我想未來我們提供出的做法會非常有趣，把資訊自由及隱私權融合在一起。

鄭瑋主任：

非常謝謝 Fernando 先生的提問，Fernando 先生剛剛特別在最後詢問了 Ms. Carly Kind 如果像是在一些被稱為 entity 的實體，比較小型的公司或組織，在被個資外洩，或者是駭客攻擊的時候，受到的處罰等等的議題。Ms. Kind 有說到一個很重要的概念，如果一個公司或組織，做了所有可以做的準備，去保護公司的個資，但無奈是外界的環境，或者是駭客攻擊的手法非常的新穎，他們在處罰或是在究責上面，會看實際的狀況來考量。我想這是一個非常重要的概念。

在開放各位與會來賓詢問之前，我最後想再詢問栗原先生一個跟新創跟 IT 相關的問題。栗原先生面對我們現在都很喜歡討論的生成型 AI(Generative AI)的問題，他現在跟我們個人生活已經緊密結合了，您觀察到在推動這個 Privacy By Design 又遇到生成式 AI 已經沁入我們的生活，您有沒有一些想法或者是您在這幾次的 privacy talk 裡面，大家有沒有連接這方面的議題，可以跟我們分享一下您的想法，謝謝。

講者四栗原宏平：

謝謝你的提問。在我新創的經驗裡面，通常新創基本上就是在很短時間內成長得非常快速，你就會看到第一個大家的反應可能一樣，譬如像 Open AI，他們也是在非常短時間內，在整個培育的過程中獲得非常多的經費，然後成長得非常快速。

我想現在確實就是 AI 的時代，以 Privacy By Design 的觀點來講，我覺得對於新創來說，他們的誘因到底是什麼？為什麼他們在設計的

時候願意納入隱私，這個才是重要的一點。因為隱私如果只是為了法遵，對他們來說只是次要的，他們的首要目的當然是快速成長。但是如果隱私是能夠幫助他們達到很重要業務目標的一個手段或方式，他們當然就會願意去做。

我跟很多同事在討論，在歐盟他們甚至會想要鼓勵新創公司，如果你要通過新創，就必須要跟競爭對手比較，在跟競爭對手比較的時候，有將隱私納在裡面，當然能夠讓你與眾不同。再來，如果新創願意一開始在設計的時候就納入隱私，其實是蠻困難的，因為必須要花比較多的精力在裡面。幾年前的時候有一個國際的標準叫 ISO31700，我不確定具體的數字，但基本上這個 ISO 對於 Privacy By Design 的設計，能夠讓新創跟新的服務必須要去滿足這個標準，算是一個隱私基準，這一些從業人員必須要去遵守的規範。政府當然很重要，但同時我們需要不同的作法，必須要有標準化以及要有足夠的誘因，很多這些東西都要納在裡面，才能夠讓新創跟小企業有誘因這麼做。

鄭瑋主任：

非常謝謝栗原先生的回答。他同時指出了一個困境，就是這種快速成長的新創公司，他們最主要關注的面向當然是業務的爆炸型成長，隱私以及，我的領域，資安，其實都會被他們視為是次要的元素，未來就是加強溝通跟對話，希望他們把這些事情當作是最主要的事情。包含在他們的成本跟業務裡面，也許會看得到改變的曙光。

剛剛栗原先生也有提到跟隱私相關的國際標準，我也想到我們自己組織裡面的同仁，其實最近也有去考 ISO 27701，隱私科技相關的認證，也許這些都會是未來的趨勢。

現在我們還有剩下一些時間，開放現場的來賓提問，不知到大家有沒有問題，請。

觀眾三：

謝謝，我是來自 Third World Network 的 Sanya Reid Smith，我想請問 Kind，可不可以跟我們講一下，你們要怎麼樣去要求這些企業，譬如有一些科技公司可能沒有在澳洲註冊，也沒有在澳洲設立實體辦公室，要怎麼樣去要求他們遵守法律？如果他們違反法律要如何執法？真的告上法院，他們會願意出庭嗎？以及他們敗訴的話要如何執行判決？你們能夠去沒收資產？還是有什麼樣的作法嗎？

講者三 Carly Kind：

這是個很難的問題，要回答你的問題很困難，我不確定我們有沒有足夠的時間。事實上我們現在進入到這個數位領域裡面，我們看到現有的這一些監管工具是不夠的。在數位時代裡，大多數公司都是跨境營運，許多應用程式和技術也是如此。因此，我們必須想辦法運用現有的監管工具來應對。

在澳洲的話，其實我們在法律裡面是有域外管轄權的，但是企業必須要至少是在澳洲做生意，在澳洲做生意這件事情，已經有很多法理學去討論。我的辦公室其實跟當時的 Facebook 現在的 Meta 有一個訴訟案，就是 Cambridge Analytica 案。那時候 Facebook 有挑戰我們法律的管轄權，一路打到了高院，最後我們發現至少能夠證明 Facebook 確實在澳洲做生意，因此，這對我們來說也比較容易對外國的公司進行相關的要求。去年針對這個法案，我們跟 Meta 達成和解，Meta 也同意要賠償 5 千萬澳幣。

當然我們有一些其他的案例，譬如 Clearview AI，這是一個臉部辨識的公司，他們在發展的時候是使用什麼方式，我們曾就他們蒐集

澳洲人照片並開發辨識技術的行為，對他們作出裁決。他們質疑我們的管轄權，並在法院作出最終裁定之前退出了程序，因此我們並未就 Clearview 的案件獲得一個明確的司法判決。儘管我們的裁決仍然有效，但實際上要執行會非常困難。因此後來我們決定針對這個判決，決定不要進行執法，因為我們收到的法律建議，再加上其他策略的考量，這可能不是我們使用資源最好的方式，在這個案件，我們不想要再多花資源了。

所以上面 2 個案例，一個有成功，另外一個沒有那麼成功。但是，我想我們當然是有權力能夠去針對這些公司做出一些裁決，甚至能夠發布民事的賠償，但是我覺得重點是我們要在法律的一開始，去納入他們的訴訟，當然這就要仰賴公司願不願意跟我們進行訴訟。如果他們在澳洲有註冊、有辦公室，通常會參與相關的法律訴訟。但即使訴訟過程順利，後續相關的執法，也會比較困難，如果有實體辦公室或註冊，就會簡單得多，也看到的是大概整個賠償金的金額是多少，救濟的內容是什麼；如果沒有，就會很困難，要看執法需要什麼樣的資源，有時候執法可能要求的是必須要刪除資料等。

另外一個例子是，澳洲電子安全委員(E Safety Commissioner)之前也曾試圖要求美國公司對特定網站進行地理封鎖（geo-blocking）。執法代表考量網頁快取(website caching)等技術問題，及數據可能分散儲存於不同地點，導致技術上難以執行。如此，法院可能就不想發布禁制令，因為他沒有辦法有效實施執行命令，不管是地理封鎖或資料刪除。這是一個非常複雜的問題，作為監管者，這當然不會影響我們執法，但確實也是我們必須要納入考量的。因為我們必須要考量的是，我們要投入多少的精力跟資源，最終是否會因為他是外國的性質，讓我們沒有辦法有效執行。

鄭瑋主任：

非常謝謝提問，確實在數位時代跨國監管跟控制是非常的困難跟模糊的。因為我們這個會議有晚大概五、六分鐘開始，我再蒐集兩個問題，臺上任何一位講者都可以回答。

觀眾四：

謝謝。我想要連結到第一個場次的主題，第一個場次，我想要問的問題，我想可能是大家都很有興趣的。就是在個人資料裡面，譬如位置追蹤（location tracking）上面，在臺灣去年有過一個青鳥行動的抗議者，他的位置可能被追蹤了，所以在一些其他的規範跟機制裡面，位置追蹤這件事情，要怎麼樣更好的透過個人資料保護法制來進行規範。

觀眾五：

同時也連結到上面的問題，在臺灣，很多人會擔心我們現在面對的嚴重的外內部挑戰，特別是我們在國際上的地位，同時還有我們民主程序的永續性，特別是針對中國來的挑戰。所以，我想要知道的是，以你的觀點來說，有沒有對於臺灣政府或者是公民社會，建議要怎麼樣去平衡人權及我們存在的保障？

鄭瑋主任：

非常謝謝兩位來賓的提問。兩位來賓的提問都有關臺灣最近的一些民主跟社會運動，這題我們請 David Kaye 先生回答好嗎，謝謝。

講者二 Jayantha Fernando：

我想先針對定位追蹤，去回應一下個人定位追蹤與實體定位追蹤。我想以法律的觀點來看，有一些國家他們的個資保護法 PDPA 是以權利為基準，也適用監管單位，不管是控制方、處理方。在應用的部分就是 Carly 剛剛回覆另外一個問題談到的，其實是很多國家遇到的問題就是控制方、處理方，他跟監管機關之間的權責界定怎麼劃分。如果控制方在那個國家沒有設立據點，但有在提供服務，政府的這個法律還會適用嗎？在斯里蘭卡，即便控制方在國內沒有實體業務，資料當事人可以去主張資料受到侵害，主張救濟。這也就是斯里蘭卡當初在法律起草階段之所以找很多的科技公司、社群媒體平臺，開始做一些公共諮詢，邀請他們一起來探討的原因之一。

跟資料當事人有關的位置追蹤，我覺得需要去做分析，因為在斯里蘭卡，這個資料當事人如果他資料受到侵害，他是可以去請求救濟。所以控制方他的行為，如果在我們的法律規範下，他是影響到資料當事人的，我們應該要有一個程序去決定，資料當事人有哪些權利，哪一些救濟可以去做。所以，當我們在判斷一位資料主體是否因某控制方的行為而受影響，且此行為是否受我們法律管轄時，定位技術（location tracking）也許可以成為一種幫助判定的工具。

但我也知道在這個領域其實有一些灰色地帶，需要進一步審慎檢討。我同意 Carly 說的，應該要有一些跨境的執法機關，或者是監管機關的合作。如果能夠針對這個議題來做討論，凝聚共識，也許可以促成定位追蹤相關法律技術使用的方式跟管轄範圍界定。

講者一 David Kaye：

我盡量簡短，我覺得這兩個問題都非常有意思。位置追蹤，從資料保護的觀點我可能沒有辦法回答，其他的與談人可以回答。

我覺得這兩個問題都談到說，有時候我們表面上看到的問題本身

就會覺得這個就是某某議題，但實際上可能是資料保護的議題，或者是隱私的問題。定位追蹤其實也跟言論自由有關，這是一個身分識別的問題，這個人他是一個社運人士，是一個記者還是誰，都會跟身分有關。所以，今天要去回答這個問題，可以從資料保護法，也可以從人權跟言論自由的觀點來去回應。

這個又連接到我們這整場座談會，臺灣要研擬第二部「國家人權行動計畫」，必須明確訂出規則，要有一些規則來講在表面上我們明顯看不出來的狀況下，有哪些規則適用，譬如，單位需要請求位置資訊的時候應該怎麼做？或是電信商要去請求資訊的時候，我們的標準是什麼？從隱私請求的原由我們要怎麼去評估？

這兩個問題我覺得真的是需要另外一場研討會來去深入的討論，不是一兩句就可以回答的，但是我認為有這樣的，像是「國家人權行動計畫」，有工具、有原則標準來依循，然後去明確清楚的訂定。當然一部分是為了保護人權，另外也要去列出說針對外國勢力的介入，我們怎麼樣去因應，策略是什麼？處理原則是什麼？這其實就是這些人權法規想要我們去做到的，不只是一些原則概括性的方針訂定，而是具體要怎麼做，有哪些工具，應該要遵循的程序、原則是什麼？然後制定必要且適當的規範，來回應這些挑戰。

「如何保護國家生存」這麼宏大的問題，我無法直接回答，所以我覺得我會用這些來回答你的問題，這是我思考這類議題的方式。

講者三 Carly Kind：

回到資料保護，我很同意 David 說的，我的想法也一樣，就是必要性、比例原則，這些人權相關的原則也適用在資料保護領域。我覺得也非常的實用，是很好的基礎。

回覆您的問題，我覺得也可以把它想成，國安、科技之間的互動。我們近期針對臉部辨識技術做的一個判定，就被問到這個有必要嗎？這個有用嗎？會成功嗎？能夠達到你的目標嗎？在這個例子裡面，零售業用的臉部辨識，我們要去思考到底有沒有必要，是否能達到我們想要的目的。不只是要去想它好不好操作？好不好執行？便不便利？而是真的能夠達到目的嗎？所以，這個是人權跟資料保護的交會點，我們能夠來思考的。

我們現在看到越來越多的定位追蹤，真的到處都是，現在很多的服務商品，都是在應用程式上面預設有位置追蹤，跟剛剛栗原先生談到隱私非常的重要，如此就能夠拿到使用者的位置資訊，然後來販售、來推銷。我們看到現在很多的申訴都是跟位置追蹤相關，我們也要去思考資料最小性原則，例如銀行的應用程式就會合理化位置追蹤的說法，如果有拿到這些數據，就能提供更個人化的服務等等。但是我覺得都還是要跟必要性、比例原則來做平衡，我們也需要去思考這個整個設計，是不是有以隱私為本。

鄭瑋主任：

非常謝謝，栗原先生可以給我們作個簡短的結語嗎？謝謝。

講者四栗原宏平：

關於公民行動，我覺得也是一個非常重要的要素，因為人權對大家來講都很重要。每個國家也都面臨不同的人權議題，重點是我們要互相交流、合作，這個很重要，公民運動也是很重要一個力量。在亞洲我覺得隱私、個資保護都是重要的關鍵字，我們要透過互相合作、意見交流去找到未來的方向。所以從公民的觀點，我們去分享、去溝通，去分享我們面臨的挑戰跟擔憂，然後一起去思考，集思廣益怎麼

樣去解決。開源的精神就是這樣子，我也有參加一些開源社群，是促進我們共同打造更美好社會的一個很棒的方式。

鄭瑋主任：

非常謝謝 4 位講者，看似其實是社會運動或是隱私追蹤的問題，其實跟言論自由還有侵犯人權也息息相關。最後各位講者說到，這些問題以及課題其實都難以分離，需要大家一起有共識並且進行對話，然後持續演進。非常謝謝今天各位與會者的耐心，也非常謝謝 4 位演講者帶來精彩及深刻的見解，我們這個會議就到這邊結束，謝謝大家。

HERITAGE PARTNERS

ATTORNEYS-AT-LAW

PERSONAL DATA PROTECTION ACT, NO. 09 OF 2022

BY:

Jayantha Fernando, Partner – Heritage Partners, Attorneys-at-Law

Chairman, Sri Lanka PDPA Drafting Committee (2018 – 2022); Director Sri Lanka CERT & DP Authority

Background and Process

- Article 14A of the Constitution of Sri Lanka

- Legal frameworks considered
  - OECD Privacy Guidelines
  - APEC Privacy Framework
  - Convention 108
  - General Data Protection Regulation
  - Personal data protection laws of UK, Singapore, Mauritius and India
  - 2nd Additional Protocol to the Budapest Cybercrime Convention (2021) – Art 14

- Seven stakeholder consultations + sectoral reviews
  - CSSL, FITIS, SLASSCOM, Ceylon Chamber & others
  - All version changes to Bill published online from 16th June 2019 onwards

OBJECTIVES OF THE PDPA

To regulate the processing of personal data.

To strengthen the rights of data subjects in terms of their personal data.

The establishment of the Data Protection Authority to enforce the provisions of the Act.

Date of operation
Not before 18 months and not after 36 months.

Preamble

"*..facilitate growth and innovation in the digital economy, whilst ensuring the protection of personal data..*"

"*..improve interoperability among personal data protection frameworks as well as to strengthen cross-border cooperation among enforcement authorities*".

Broad sphere of application

Includes: entities offering goods and services in Sri Lanka, monitors behaviour of data subjects, etc.

Excludes: personal data processed purely for domestic or household purposes by an individual and data that is not "personal data"

HERITAGE PARTNERS

ATTORNEYS-AT-LAW

PDPA: KEY TERMS

PERSONAL DATA

Any information that can identify a **data subject**, directly or indirectly by reference to an identifier or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person. Includes ***special categories*** of personal data.

DATA SUBJECT

An identified or identifiable natural person, alive or deceased, to whom the personal data relates.

PROCESSING

Any operation performed on personal data, including but not limited to collection, storage, preservation, alternation, retrieval, disclosure, transmission, making available, erasure, alignment, combination or carrying out of logical or arithmetical operation on personal data.

CONTROLLER

Any natural or legal person, public authority, public corporation, non-governmental organization, agency or any other body or entity which alone or jointly with others determines the purposes and means of the processing of personal data.

PROCESSOR

A natural or legal person, public authority or other entity established by or under written law, which processes personal data on behalf of the controller.

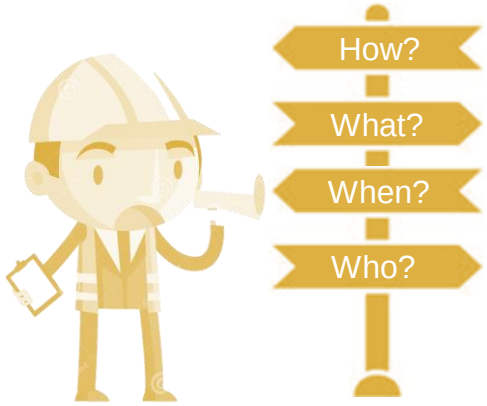
SPECIAL CATEGORIES OF PERSONAL DATA

The personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, personal data relating to offences, criminal proceedings and convictions, or personal data relating to a child;

HERITAGE PARTNERS

ATTORNEYS-AT-LAW

Controller



Natural or legal person who decides the purposes and means of processing

Insurance providers storing customer data profiling to provide value added services.

Cloud Service Providers providing storage services to banks.

Public corporations engaged in public service with XXX employees.

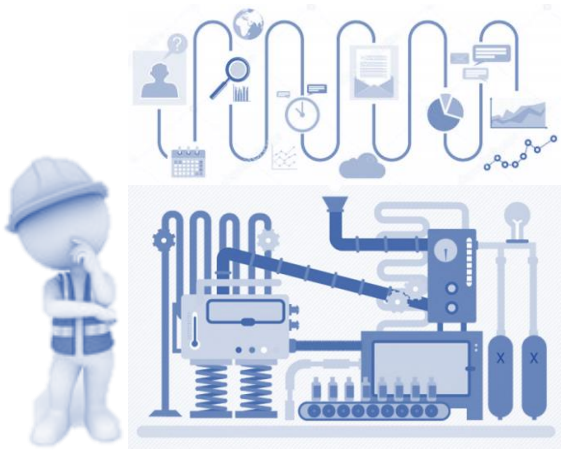
Department of Registration of Persons which issues NICs.

Telecommunication or service providers onboarding customers.

Private schools collecting information regarding parents and children.

A supermarket chain engaging a third party to manage their customer loyalty program.

Processor



Natural or legal person who process on behalf of the controller

PRINCIPLES OF PROCESSING

LAWFULNESS

Processing is lawful only if it is in accordance with Schedules I-IV.

PURPOSE SPECIFICATION

The purpose for processing should be specified, explicit and legitimate.

DATA MINIMIZATION

The personal data processed should be adequate, relevant and proportionate to the corresponding purpose of processing.

ACCURACY

The personal data processed should be accurate and updated.

HERITAGE PARTNERS
ATTORNEYS-AT-LAW

PRINCIPLES OF PROCESSING

STORAGE LIMITATION

Personal data should be stored only for a time as may be necessary or for as long as it is required for the purpose for which it is processed.

INTEGRITY AND CONFIDENTIALITY

Appropriate technical and organizational measures are to be implemented to prevent the unauthorized / unlawful processing of personal data, or the loss, destruction or damage of personal data.

TRANSPARENCY

Provide data subject with information:

- referred to in Schedule V; and
- regarding any decision taken with respect to the exercise of a data subject's rights.

ACCOUNTABILITY

Maintaining a Data Protection Management Programme.

LAWFUL PROCESSING

Processing Personal Data
(SCHEDULE I)

- Consent (Schedule III)
- Contractual performance
- Controller's legal obligation
- Necessary to respond to the emergency or safety of the data subject
- Public interest or official authority of Controller prescribed by law
- Legitimate interest of controller

Processing Special Categories of Personal Data
(SCHEDULE II)

- Consent
- Employment, social security, public health, prevention of communicable diseases
- Data manifestly made public by the data subject
- Threat to life, health or safety of data subject
- Establishment of legal claims before a court of law
- Substantial public interest as prescribed by law
- Occupational medicine, medical diagnosis, treatment or management of health-care services
- Archiving, scientific or historical research, statistical purposes

DATA PROTECTION MANAGEMENT PROGRAMME

- The draft DPMP Guidelines stipulate various components which are to be included in a DPMP.
- A controller is required to maintain duly catalogued records on the implementation of personal data processing principles.
- The DPMP must be designed on the basis of the structure, scale, volume, and sensitivity of the controller's processing activities.
- A tiered approach is to be implemented in adopting internal controls and procedures.
- Devise a mechanism to receive complaints and conduct inquiries.
- Consist of mechanisms to identify personal data breaches.
- Periodic monitoring and continuous assessments.
- Facilitate the exercise of a Data Subjects' rights.
- Controllers must monitor and assess their systems regularly and make updates as required to ensure continuous improvement.
- Carry out Data Protection Impact Assessments as appropriate (*Refer* - Draft Regulations on Personal Data Protection Impact Assessments under the Personal Data Protection Act No. 9 of 2022).

HERITAGE PARTNERS
ATTORNEYS-AT-LAW

RIGHTS OF DATA SUBJECTS

Access Section 13	Withdraw consent Section 14(1)	Right to object Section 14(2)	Rectification Section 15	Erasure Section 16
• Right to access personal data processed by the Controller. • Obtain confirmation on the personal data processed. • Information on matters set out in Schedule V.	• Right to withdraw consent if the processing is based on consent. • Withdrawal shall not affect the lawfulness of prior processing.	• Object to the further processing of personal data, if such processing is either based on public interest or legitimate interest.	• Request the rectification of inaccurate data or the completion of incomplete data. • Subject to the controller's right to: (i) maintain such data for evidentiary purposes; or (ii) refuse such request under section 17 of the PDPA.	• If the processing is in contravention with the principles of processing. • If the data subject withdraws his / her consent. • If it is required by written law or an order of court.

CONTROLLER'S RIGHT TO REFUSE A REQUEST BY A DATA SUBJECT

- Grounds:
  - National Security;
  - Public order;
  - Any inquiry, investigation or procedure conducted under any written law;
  - Prevention, detection, investigation or prosecution of criminal offences;
  - Requirement to process data under any written law;
  - Technical and operational feasibility of the Controller to act on the request of Data Subject.

- Appeal to the Data Protection Authority and thereafter to the Court of Appeal.

HERITAGE PARTNERS

ATTORNEYS-AT-LAW

DATA PROTECTION OFFICER

[*Refer*: Draft Regulations on the Appointment of the Data Protection Officer under Section 20 of the Personal Data Protection Act No. 9 of 2022]

MANDATORY APPOINTMENT

A ministry, government department or public corporation, except for judiciary acting in their judicial capacity.

If a controller processes personal data that (i) regularly and systematically monitors data subjects or (ii) processes special categories of personal data, according to a prescribed scale and magnitude.

A controller's processing resulting in a risk of harm to the rights of data subjects.

QUALIFICATIONS

Prescribes academic and professional qualifications.

Academic background, knowledge & technical skill on data protection.

Competency and capacity to implement strategies and mechanisms to respond to inquiries and incidents.

RESPONSIBILITIES

Advise controllers and its employees on the requirements under PDPA.

Ensure compliance with the Act on behalf of the Controller.

Capacity building of staff.

Advise on Data Protection Impact Assessments.

Cooperate with the DPA regarding instructions and directives

CROSS-BORDER DATA FLOW

LIMITED LOCALIZATION

- Limitations only on public authorities - ministries, departments, provincial councils, local authorities, etc.
- No limitations on controllers who are banks, telcos and other regulated businesses.

CONTROLLERS OTHER THAN A PUBLIC AUTHORITY

- Processing can be done either based on an "adequacy decision" or in any country, provided the Controller complies with the safeguards under the Act.
- Compliance under section 26 (3) through "instruments" specified by the DPA - Binding Corporate Rules, Standard Contractual Clauses, etc.
- In the absence of an adequacy decision or safeguards, a controller or processor may still process personal data outside Sri Lanka under Section 26(5) of the PDPA, if:-
  - The consent of the data subject is obtained.
  - The transfer is necessary for the performance of a contract between data subject and the controller.
  - It is on the basis of public interest.
  - Other conditions prescribed by Regulations

DATA PROTECTION AUTHORITY

1. Regulate the processing of personal data in accordance with the provisions of the PDPA.
2. Safeguard the privacy of the data subjects from any adverse impact arising from the digitalization of the procedures and services in the public and private sector.
3. Provide for mechanisms to ensure the protection of personal data of data subjects engaged in digital transactions and communications.
4. Ensure the regulatory compliance with the provisions of this Act to facilitate the growth and innovation in the digital economy.

DIRECTIVES AND PENALTIES

The DPA may issues directives to controllers or processors, where the DPA determines that such controller or processor (a) is engaged in, or is about to engage in, any processing activity which is in contravention with the Act; or (b) has contravened or failed to comply with the provisions of the Act, any rule, regulation, instruction, directive or order given under the Act or any other written law which, in the opinion of the Authority, relates to processing of personal data.

Penalties (Section 38)

- Where a controller/processor fails to comply with a directive issued by the DPA. Liability is extended to directors of body corporates and partners of firms.
- Maximum penalty - Ten Million Rupees for *each* non-compliance.
- Subsequent failures will result in additional penalties.
- Failure to pay a penalty may result in the DPA making an *ex-parte* application to the Magistrate Court, for the recovery of the relevant sum.
- The imposition of a penalty does not preclude the DPA from implementing other regulatory measures (e.g: suspension the controller's / processor's business, cancellation of a license, etc.)
- An aggrieved party has 21 days to appeal to the Court of Appeal against a decision of the DPA.
- **Mitigatory factors** - prior to the imposition of penalties, the Authority will consider: the nature, gravity, duration of the contravention; mitigatory action taken by the controller/processor; effectiveness of the data protection management programme; previous non-compliances by the controller/processor; etc.

Implementation Challenges

- Implementation Strategy
  - Phased-out implementation
  - Raising stakeholder awareness & capacity building
  - Identify suitable organizational structure for DPA
- Establish an Independent Data Protection Authority (DPA)
  - Ensure financial and administrative independence within the limits of Sri Lankan legal framework
  - Ensure coordination between DPA and other sectoral regulators to ensure smooth implementation of the Data Protection Act
- Formulation of Rules and Regulations under the new Law
  - Facilitate public-private consultations prior to promulgation
- Training & capacity building
  - Ensure the officials of DPA possess the requisite technical knowledge and skill to perform the duties and functions
  - Attract and retain skilled personnel for the staff of DPA
  - Provide nation-wide stakeholder training and capacity building for government sector and private sector
- Developing industry norms/standards - sectoral

HERITAGE PARTNERS

ATTORNEYS-AT-LAW

THANK YOU

JFDO@HERITAGE-PARTNERS.COM

Training of Professionals in Personal Data Protection

Kohei Kurihara - Privacy by Design Lab

Introduction

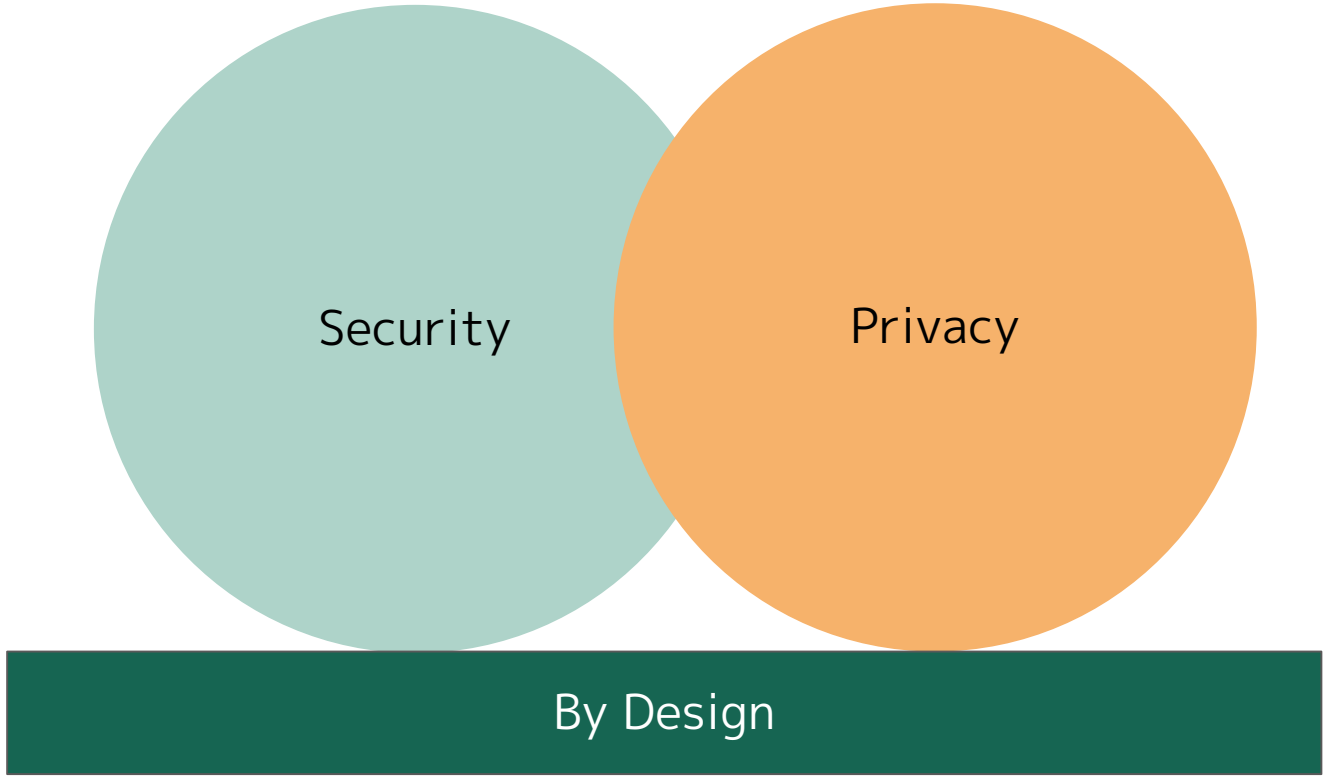
Kurihara Kohei
Privacy by Design Lab

Kohei is Co-Founder of Privacy by Design Lab, a leading data privacy culture and society community. As a not-for-profit, the organization was originally established as a privacy oriented corporate structure program and policymaking. We collaborate with multi-stakeholders, public affairs, government, companies and civic organizations, and international watchdogs to enhance fundamental privacy culture. He has spoken at many international conferences such as UNESCO and participated in open-source projects as a data privacy and blockchain expert. He also has extensive experience with education and non-profit organizations, and working with the secretaries of local politicians around the world creating and developing public policy.

International Conference
- Aspen Institute Italia　Aspen Seminars for Leaders
- My Data Global　MyData Online 2022 conference

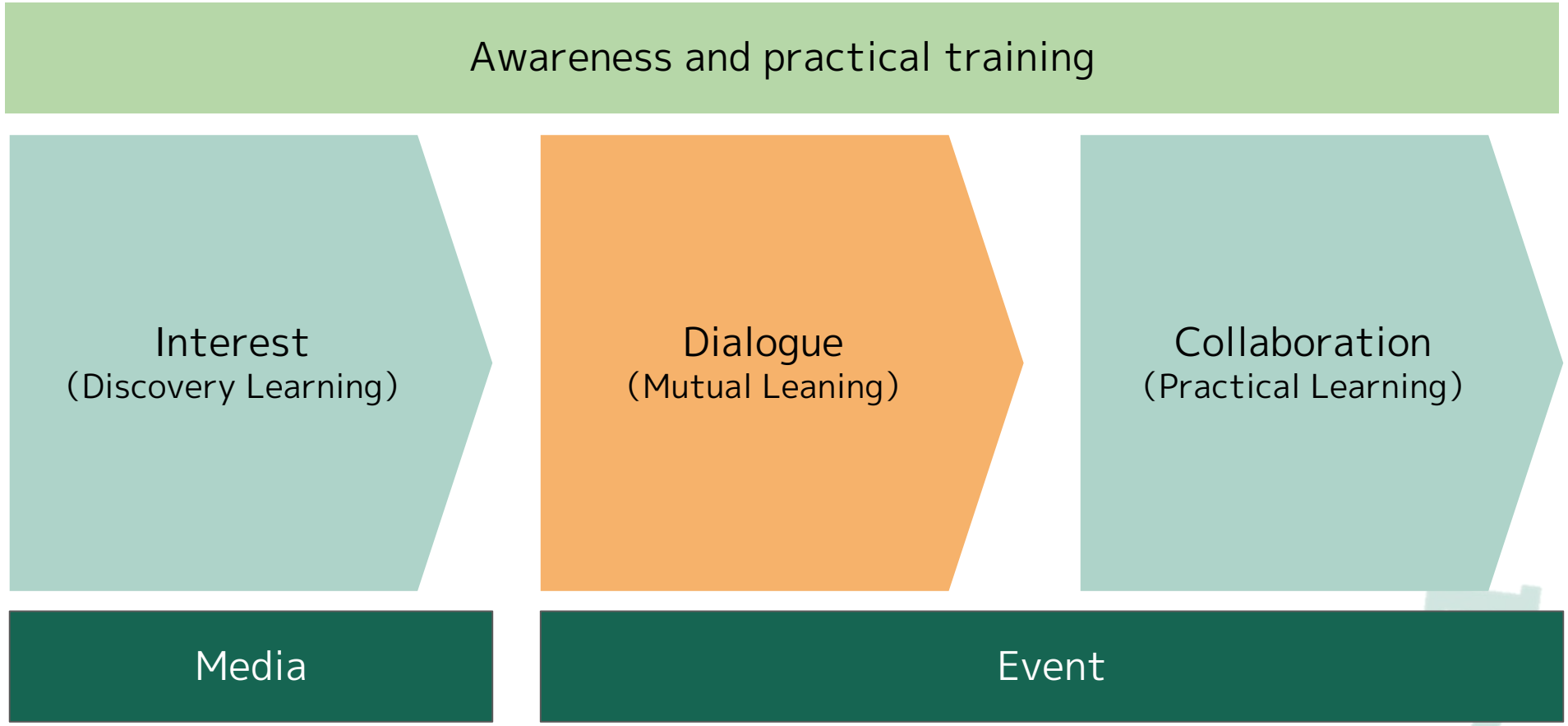
Why is “Privacy Awareness” indispensable with cybersecurity?

To implement fully secure and privacy infrastructure, both of elements have to be embedded altogether, and it is necessary to design into our digital infrastructure.



Why will “Privacy Awareness” become key factor of training?

To integrate the privacy and security, regardless of expert or non-expert, it needs to amplify the interest and encourage dialogues among the private and public practitioners.



What can Non-governmental Organization do for the awareness?

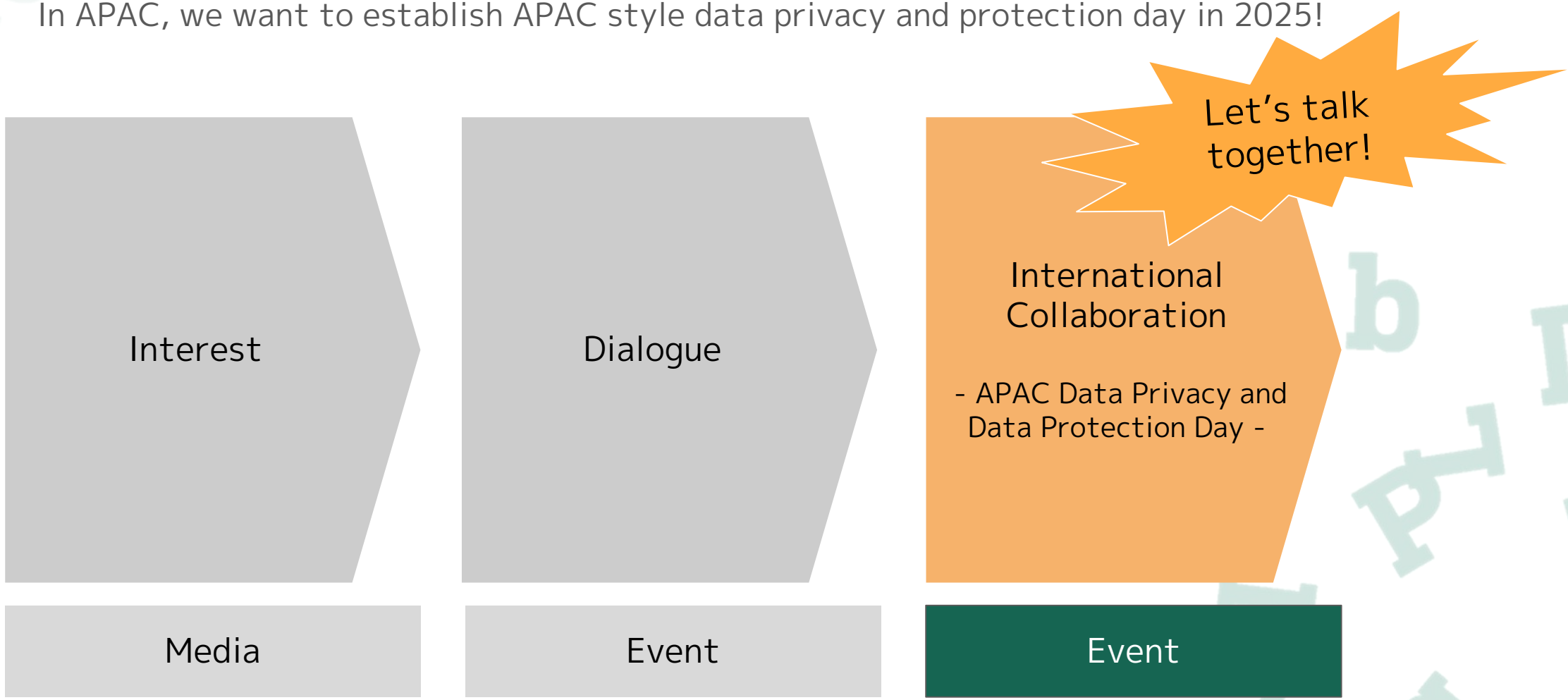
As a non-governmental organization, Privacy by Design Lab annually hosts the conference to celebrate data privacy and data protection day, sharing the experiences and idea for our digital future.

Media	Event
Talking with international privacy and security practitioners to share their practices	Participating from diverse backgrounds, government, private sectors, civil society, academics, talking about future issues related to privacy and security with societal themes together

Our next challenge by multi-stakeholder cooperation worldwide

Sharing the awareness movement, we envision international collaboration across countries.

In APAC, we want to establish APAC style data privacy and protection day in 2025!



Thank you!

Please Contact Me on Email