出國報告（出國類別：開會）

出席 IAPP 2019 年亞洲隱私論壇
出國報告書

服務機關：國家通訊傳播委員會

姓名職稱：伍科長麗芬、羅科員郁文

派赴國家：新加坡

出國期間：108 年 7 月 14 日至 7 月 17 日

報告日期：108 年 10 月 1 日

出國報告摘要

國際隱私權專家協會（International Association of Privacy Professionals，IAPP）致力於透過產業交流、訓練及論壇等方式促進國際相關領域專家間對於個人資料及隱私保護法規執行或實務操作的經驗分享及互動。

本次亞洲隱私論壇由 IAPP 在新加坡假濱海灣金沙會議中心，於 2019 年 7 月 15 日及 16 日舉辦。開幕嘉賓香港個人資料私隱公署的專員 Stephen Kai-yi Wong 及新加坡個人資料保護委員會的主委 Tan Kiat How 均強調從法規遵循到課責建立的個資與隱私保護責任之演進；閉幕致詞則由菲律賓的國家隱私委員會主委 Raymund Liboro 分享關於菲律賓國家隱私委員會處理個人資料申訴事件及當事人權利行使之經驗。

而在為期兩天的議程中，IAPP 匯集超過 450 位隱私專家，透過 16 場專題講座分享關於 GDPR 施行一年的發展、亞太區個人資料保護的現狀、中國相關資料保護法規、個人資料治理、供應商管理、資料在地化問題、兒童資料處理、人工智慧的隱私議題、企業的課責性建立，以及個資管理系統的全新國際標準等法規內容與實務經驗等。

目次

壹、目的

歐盟於 107 年 5 月 25 日起實施的個人資料保護規則(European Union General Data Protection Regulation），對於個人資料保護規範更嚴格，影響層面更廣，各國均在數位轉型過程中加速調整因應。面對數位經濟及新技術發展，如何建構安全、可信任及有效的數位環境，同時做好個人資料及隱私保護，這是各行各業都將面臨的挑戰，尤其近來產業變動及競爭相當激烈，惟有掌握先機，事先做好準備，才能開創新局，引領世界潮流。本會作為我國通訊傳播事業於個人資料保護法的中央目的事業主管機關，藉由參加相關個資及隱私保護論壇，了解各國個資保護政策與業界實務操作經驗以作為本會通傳監理政策之參考。

國際隱私權專家協會（International Association of Privacy Professionals , IAPP）成立於西元 2000 年，為由個人資料及隱私保護與資訊安全專家組成之協會，透過產業間的交流、訓練及論壇的方式促進國際專家間對於個人資料及隱私保護法規執行或實務操作的經驗分享及互動。本次論壇為 IAPP 於 2019 年舉辦的亞洲隱私論壇，在為期兩天的議程中共計 16 場的專題座談，內容包含 GDPR 施行一年的發展、亞太區個人資料保護的現狀、中國相關資料保護法規、個人資料治理、供應商管理、資料在地化問題、兒童資料處理、人工智慧的隱私議題、企業的課責性建立，以及個資管理系統的全新國際標準介紹等，並邀請來自各方的學者、實務工作者、研究人員及業界代表參與各專題分享。

本會希望經由本次 IAPP 亞洲隱私論壇適度瞭解國際上的個人資料與隱私保護趨勢及業界關注焦點，並掌握比較法規的發展現況與企業的法遵執行方式，

將可借鏡作為我國法規或政策調整的方向評估，且可協助輔導通傳業者落實法規遵循的具體策略。

貳、 論壇資訊

一、 會議時間：2019 年 7 月 15 日至 7 月 16 日

二、 會議地點：新加坡濱海灣金沙飯店會議室

三、 出席人員：伍科長麗芬、羅科員郁文

圖 1 IAPP 2019 年亞洲隱私論壇地圖

參、論壇內容

一、 議程

(一) 7 月 15 日

時間	議程
08：15	報到

09：30	開幕大會 新加坡個人資料保護委員會專員　Tan Kiat How 香港個人資料私隱專員 Stephen Kai-yi WONG
11：00	● GDPR 實施一年後，數據外洩受害者與資安專家之經驗分享 GDPR (1 Year Later): Lessons From Data Breach Victims and Security Professionals (蘭花主宴會廳 4203) 主持人：IAPP 香港區域負責人 Jason Wai King Lau ➢ 資安專家分享關於 GDPR 實施一年後的經驗，包括數據洩露實務和符合 GDPR 隱私規範之策略 與談人： Kudelski Security 區塊鍊安全主管 Scott Carlson 香港 Baptist 大學 教授 Chung Kei Dorothy Chau Twitter 副總法律顧問　Damien Kieran 澳新銀行 總經理 Robinson Roe
11：00	● 亞太區的資料保護 The Data Protection Landscape in APAC (蘭花主宴會廳 4206) ➢ 亞太區的資料保護規範迅速發展，各國立法及執法策略 與談人： Nymity 策略研究負責人 Paul Breitbarth Morrison&Foerster 法律事務所合夥人 Daniel Levison 中央大學 政策學副教授 Hiroshi Miyashita
13：30	管理第三方供應商數據風險 Are Suppliers Your Biggest Data Breach Risk? Managing Third Party Vendor Risk

	(蘭花主宴會廳 4203) 主持人：OneTrust 總經理 ANZ Rob Roe ➢ 組織在管理第三方供應商風險時面臨的驅動因素和挑戰，及隱私專家實際處理案例分享 與談人： Grab 區域資料保護長 Wijaya Abori Agoda 資料治理長暨資深資料顧問 Brendan Pat
13：30	資料在地化的崛起：我們如何安全導航? The Rise in Data Localisation: How Can We Navigate Safely? (蘭花主宴會廳 4206) ➢ APEC 跨境隱私規則，多邊協議認證系統落實 ➢ 資料在地化和數據流機制的最新發展 與談人： Bird & Bird 合夥人 Michelle Chan 亞洲商法研究所 資料隱私主管 Clarisse Girot Refinitiv 亞洲區隱私主管 Sandra Liu 北京大學法律與發展學院 資深顧問 Hong Yan Qing
14：45	中國的資料法規發展及對企業的影響 Developments of China’s Data Regulations and the Impacts for Businesses (蘭花主宴會廳 4206) ➢ 中國的資料法規體系介紹 與談人： Norton Rose Fulbright 律師事務所合夥人 Barbara Li
14：45	人工智慧的隱私問題及降低風險的策略

	Privacy Implications for the Use of AI and Strategies to Mitigate Risks (蘭花主宴會廳 4203) ➢ 人工智慧的常見用途，及對隱私影響和相關風險 與談人： 新加坡 個人資料保護委員會 副主任 Lanx Goh Facebook 亞太區隱私及公共政策代表 Arianne Jimenez 亞洲雲端運算協會 執行長 May-Ann Lim Rajah & Tann 電信及數據隱私主管 Steve Tan
16：30	亞洲資料保護治理的演進 Evolving Data Protection Governance in Asia (蘭花主宴會廳 4203) ➢ 亞洲數據保護格局演變的過去、現在和未來 與談人： IAPP 創始人 Rahul Sharma 新加坡國立大學 貿易與經濟政策教授 Amitendu Infosys 全球隱私個資保護負責人 Srinivas Poosarla
16：30	為兒童著想：處理兒童資料的關鍵挑戰 Think of the Children — Key Challenges to Processing Children's Data (蘭花主宴會廳 4206) ➢ GDPR 對於歐盟兒童數據處理的影響，及實例解析 與談人： Wilson Sonsini Goodrich & Rosati 律師 Laura Brodahl TotallyAwesome 首席營運長 Marcus Herrmann 樂高亞太區資深顧問 Patrica Lee 方達律師事務所 合夥人 Jianyuan Yang

(二) 7 月 16 日

時間	議程
08：15	報到
9：00	閉幕大會 菲律賓國家隱私委員會 主委 Raymund Liboro 印度政府電子和科技部 秘書 Gopalkrishnan S.
10：05	◆ 從理論到實踐-雲端資料治理 From Theory to Practice — Data Governance in the Cloud (蘭花主宴會廳 4206) 主持人：亞洲雲端運算協會 執行長 May-Ann Lim ➢ 組織資料治理策略和營運模型 與談人： Google 亞太區雲端公共政策代表 Yam Ki Chan DBS 銀行 法遵與隱私部門代表 Joey Pang
10：05	◆ 當 GDPR 與中國資料保護法規遵循相遇 When the GDPR Meets Chinese Data Protection Compliance (蘭花主宴會廳 4203) ➢ GDPR 執行趨勢，及中國最新資料保護法律規範 與談人： L'Oréal China 資料保護長 Shawn Xiaosheng Li EY 會計師事務所合夥人 Fabrice Naftalski 華為 全球資安與個資法副總裁 Kevin Wang

11：30	隱私保護下的資料治理 Data governance for privacy (蘭花主宴會廳 4206) ➢ 消費者隱私與資料治理 與談人： Informatica 資料隱私部門副總裁 Russell Feldman Deloitte 資料分析部門代表 Chris Lewin
11：30	亞太區的隱私規範回應 Tackling Privacy Requirements in the APAC Region (蘭花主宴會廳 4203) ➢ 消費者隱私及亞太區資料監理政策發展 與談人：Sony 亞太地區隱私長 Joyce Chua
13：30	課責性之實踐：隱私治理的現在與未來 Implementing Accountability: Privacy Governance Approaches for Today & Tomorrow (蘭花主宴會廳 4203) 主持人：Access Partnership 美國及亞洲負責人 Christopher Martin ➢ 問責制度融入全球隱私框架的方式 與談人： Hunton Andrews Kurth 資訊政策領導力中心總裁 Bojana Bellamy Mastercard 資深管理顧問 Yi Lin Seng SAS 歐洲及亞洲隱私策略長 Kalliopi Spyridaki Google 亞太區隱私長 Angela Xu
13：30	ISO 27552 管理與認證隱私制度介紹 Managing and Certifying Privacy Operations With the

	New ISO 27552 (蘭花主宴會廳 4206) ➢ 了解新的 ISO / IEC 27552 標準和 ISO / IEC 27001 標準 與談人： EY 亞太地區數位法律負責人 Alec Christie Microsoft 認證政策部門主管 Alex Li 北京大學 法律與發展學院資深顧問 Hong Yan Qing
15：00	歐盟與日本的自由資料流動：在相互適足認定之後 Free Flow of Data Between the EU & Japan: After Major Mutual Adequacy Decisions (蘭花主宴會廳 4206) ➢ 歐盟與日本關於跨境數據流動政策 與談人： 亞洲商務法律研究所 資深研究員 Clarisse Girot Mori Hamada & Matsumoto 律師事務所合夥人 Atsushi Okada Bird & Bird 法律事務所合夥人 Takeshige Sugimoto
15：00	企業法務團隊如何處理全球隱私議題 How an In-House Legal Team Takes Privacy Global (蘭花主宴會廳 4203) ➢ 美國/亞洲內部法務團隊處理全球電子商務環境複雜的隱私問題 與談人： Airbnb 全球副法務長 Paul Nikhinson Airbnb 全球隱私法務長 Bernadine Seet Airbnb 美國副法務長 Derek Smith
16：00	論壇結束

二、 論壇重點摘要

（一） GDPR 實施一年後，數據洩漏受害者和資安專家的實務分享

作為本次論壇首場座談，主辦單位共邀請來自香港Baptist 大學、Twitter、區塊鏈資安公司 Kudelski Security、個資評估工具大廠 OneTrust 以及國泰航空，分享有關資料外洩受害者與資安專家之實務經驗。

網路時代下，科技使得相關應用及服務跨越國界迅速傳播中，社群傳播媒體在網路時代下，應負起保護用戶及使用者個人資料的義務。Twitter 副總法律顧問 Damien Kieran 表示該公司的全球性隱私政策，已清楚揭露個人資料之蒐集利用處理的規範，並於取得使用者同意後才會開始進行。該公司內部設立專業個資保護長(DPO)，並強化個資的保護措施避免外洩。

香港 Baptist 大學教授 Chung Kei Dorothy Chau 認為 GDPR 實施一年後，除了企業內部改革組織內部規範及流程以遵守新規定外，社會及教育界也提高對於隱私教育(Privacy education)的重視。

Kudelski Security 區塊鍊安全主管 Scott Carlson 認為在服務創新與資料保護間不存在衝突，越是對於個資隱私有完善保護機制，越是能強化使用者接近高科技及新興服務的信心，進而推升服務創新。

與會專家以漫談之形式，各自表達了他們對 GDPR 實施一年來之觀察，包含 GDPR 再次提升了歐盟公民之隱私權意識，但 GDPR 很多規定並不明確，也造成業者遵循時之困惑，專家們也提到原本預期與 GDPR 一起實施之歐盟電子隱私法案（ePrivacy）尚未能通過，區塊鏈科技是否可能運用於個人資料保護等探討。

（二） 亞太區的資料保護

本場次由 Nymity 的策略研究負責人 Paul Breitbarth 主持，由 Morrison & Foerster 法律事務所的合夥人 Daniel Levison 及 Chuo University 的政策研究系助理教授 Hiroshi Miyashita 一同與談。

講者指出，亞太區的資料保護情形在短短幾年大幅度趨向成熟，各國政府也都更加重視個人資料（及營業秘密）的保護。

Paul Breitbarth 認為，作為亞太區資料保護的借鏡，需留意個人資料保護法規往往與網路安全法規緊密相關；此外，歐盟在跨境傳輸個人資料的適足性決定標準仍不明確，如何將歐盟與亞太區的個資保護法律體系介接以促進雙邊個人資料的自由傳輸，仍有待實務發展。

Daniel Levison 也補充指出，跨境傳輸個人資料的合規性應是企業的巨大挑戰，但目前企業尚難了解如何落實各地資料隱私法規，亦多未認知有關跨境傳輸個人資料的法規遵循問題。

最後，Hiroshi Miyashita 分享日本經驗，日本對於個資傳輸至第三方係採取「原則禁止、例外許可」之立法。區域性隱私個資體系制度，日本除了已加入 APEC 之 CBPR（Cross-Boarder Privacy Rules）跨境隱私規則體系外，更於 2019 年 1 月與歐盟通過相互承認的跨境傳輸個人資料機制，即日本已列入歐盟個資保護適足性的白名單，接下來應由日本政府將適足性決定的內涵納入各事業的特別法規。

（三） 資料在地化的崛起：我們如何安全導航？

本場次內容較為豐富且受關注，主持人 Michelle Chan 首先介紹了越南、印度、印尼之資料在地化立法，接下來重點則在於討論中國網絡安全法（以下稱「網安法」）。

越南正在立法要求國內外網路服務提供者（Online service providers），包含：電信業、網路資料分享或儲存業、電子商務、線上支付、社交網路、社群媒體、線上遊戲以及電子郵件服務等，必須將越南人民之個資儲存於越南當地，並應政府要求提供給越南政府。

印度正透過資訊科技法、個資保護法案、草擬電子商務政策等方式，要求線上資料和個人資料必須在地化，目前存在較大之爭議為敏感個人資料之定義（包含：密碼、財務資料等）似乎過廣，且關鍵個資（critical personal data）定義不明，但又要求關鍵個資必須在當地處理。

印尼依據為 2008 年之電子資訊與交易法，採註冊及特許制，目前正草擬修法。

中國網安法由參與該法及其子法草擬之北京大學教授 Hong Yan Qing 講述：

1、 適用範圍：網安法第 31 條對關鍵資訊基礎設施之定義「國家對公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域，以及其他一旦遭到破壞、喪失功能或者資料洩露，可能嚴重危害國家安全、國計民生、公共利益的關鍵資訊基礎設施，在網路安全等級保護制度的基礎上，實行重點保護。關鍵資訊基礎設施的具體範圍和安全保護辦法由國務院制定。」而關鍵資訊基礎設施之定義相當廣泛，因此可能影響非常多的企業。

2、 資料在地化：網安法第 37 條「關鍵資訊基礎設施的運營者在中華人民共和國境內運營中蒐集和產生的個人資訊和重要資料應當在境內存儲。」關於個人資訊和重要資料之定義與安全評估程序正在討論中。

3、 跨境傳輸：網安法第 37 條「因業務需要，確需向境外提供的，應當按照國家網信部門會同國務院有關部門制定的辦法進行安全評估。」此「個人資訊出境安全評估辦法」正在對公眾徵求意見中。

4、 如執法機關要求，必須提供資料予執法機關。中國網安法之相關子法正快速制定與討論中，下圖整理近期子法之立法狀態：

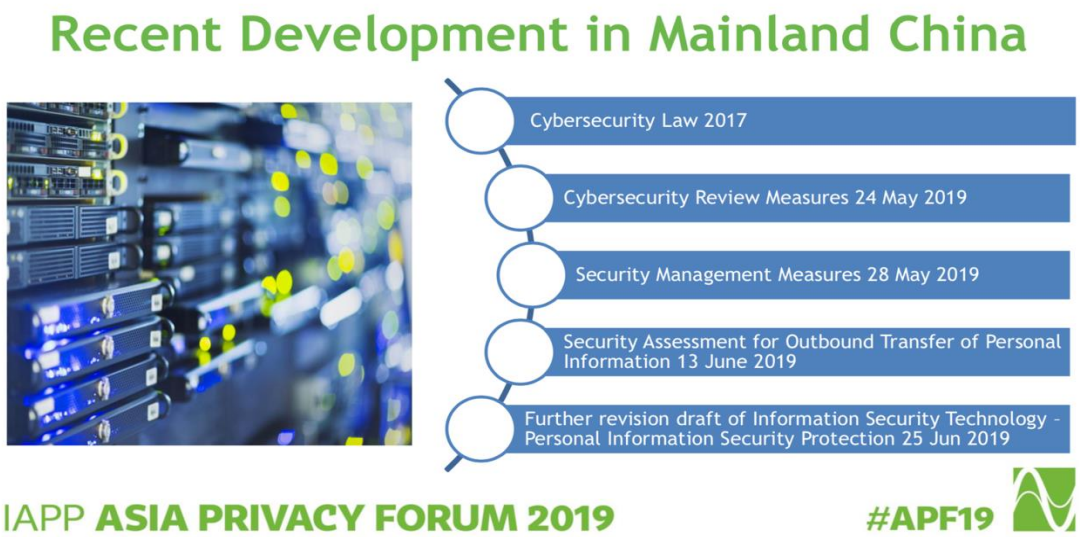

圖 2　中國網絡安全法發展進程(講者簡報第 9 頁)

5、 眾所關注之「個人資訊出境安全評估辦法」第二版徵求意見稿，待解決之重要議題如下：

(1) 適用範圍與法律文字定義需進一步釐清

(2) 跨境傳輸之程序

(3) 未經同意之跨境傳輸例外

(4) 安全評估報告之內容（特別是安全維護措施可能是企業之高度機密）

(5) 境外公司之境內代表或代理人之角色

(6) 資安認證和執行業務守則之角色

最後，香港講者 Sandra Liu 說明香港個人資料私隱專員公署尚未執行跨境傳輸限制，因為香港乃世界金融中心之一，個資流通有助於交易和資金流通，建議應基於正當利益與比例原則，建立一個有助於資料合法流通之法律架構。

（四） 中國的資料法規發展及對企業的影響

本場次由 Norton Rose Fulbright 法律事務所的合夥人 Barbara Li 分享中國的（個人）資料相關法規，包含中國的網安法、有關兒童個人資料保護及跨境資料傳輸安全評估等規範的草案，以及 2019 年 5 月發布，將於 12 月 1 日施行，將雲端運算、大數據、物聯網、自動化技術均納入規範的網路安全等級保護制度 2.0 標準等。

中國於 2017 年實施「網絡安全法 (Cybersecurity Law)」規範的對象可分為 Network operaters、Administrators 與 Service providers，受規範者不是只有電信業者，也包含了提供網際網路服務的企業，同時不限於中國本地業者，外國業者也在規範範圍內。

《網絡安全法》除了規範大陸境內的個人、組織、網路運營者和關鍵資訊基礎設施的運營者，有些規定更涉及境外業者，重要條文內容如下：

1. 要求向公安、國安機關提供技術支持和協助（第 28 條）。

2．特定公司通過國家安全審查（第 35 條）。

3．在大陸儲存使用者和經營數據（第 37 條）。

4．境外的機構、組織、個人的處罰（第 76 條）。

講者亦介紹了屬於中國國家建議性標準的個人信息安全規範，以及正在進行中的密碼法、個人信息保護法、數據安全法等，並建議在中國營業之企業應密切注意近 12 個月來中國關於（個人）資料保護法規的快速進展演變，隨時注意企業的法規遵循落查，並適時採取新興技術妥為因應。

中國制訂網絡安全法之初時，已經引起國內外企業高度矚目及擔憂，相關資安及個資隱私法規陸續實施，將對外國營業組織在中國境內經營業務，產生廣泛影響。建議臺商赴陸投資時，應審慎評估可能的風險、資訊安全及商業秘密保護等問題，以免觸法。

（五） 人工智慧的隱私問題及降低風險的策略

本場次由亞洲雲端運算協會執行長 May-Ann Lim 主持，邀請了包含 Facebook 等三位業界代表演講。

隱私專家 Steve Tan 首先說明了 AI 對個資保護之挑戰：

1、 首先是在當事人未表達同意，甚至不知情之情形下的個資自動化蒐集，例如：有人臉辨識功能之監視器（CCTV）、智慧門鎖、智慧電視、商店之感測器等。

2、 由於 AI 之複雜性，AI 之決策過程像黑箱作業，並不透明，應如何描述 AI 之演算法？

3、 大數據分析時，資料之利用可能與蒐集時之特定目的不同，大數據分析之結果甚至可能為資料利用目的帶來新的方向和洞見，這使得「明確同意」成為個資保護之一大挑戰。

臉書代表 Arianne T. Jimenez 則介紹臉書如何透過資料選擇（例如：資料類型與範圍、去識別化、組成代表檢查、加密、刪除等方法），以及風險評估、安全維護措施、演算法之公平性評估（Fairness Assessment）等措施，保護 AI 時代下之個資運用。

最後，新加坡個資主管機關代表 Lanx Goh 則說明新加坡政府對 AI 之態度，希望能以不斷進步之立法，在個資保護與創新之間取得平衡，建立可信賴之環境。並提醒業界於利用 AI 科技時，應特別注意「告知、同意、目的限制、正確性、保護性、保存期限、資料移轉限制、當事人近取權和更正權、透明性」等九個重點。他也提醒企業應注意第三方合作夥伴揭露個資之合法性，並應進行個資同意範圍之盡職調查（Due diligence investigations）。

（六） 亞洲資料保護治理的演進

本場由印度 IAPP 創辦人 Rahul Sharma 先生主持，邀請新加坡國立大學 Amitendu Palit 教授、Grab 公共政策與研究負責人 Marian Panganliban 以及 Infosys 全球隱私個資及個資保護副總裁 Srinivas Poosarla 等三位專家與談。

Palit 教授首先表達對近年來亞洲國家紛紛提出「資料在地化」之立法表示關切，他認為亞洲各國之資料在地化立法會阻礙資料流通，進而阻礙亞洲國家間之經貿發展。

另二位與談人則進一步談到 APEC 之 CBPR（Cross-Boarder Privacy Rules），但與談人對於 CBPR 是否可緩和資料在地化之立法，進而促進亞洲各經濟體間之資料流通，均表示較為保守之觀點，與談人特別談到：雖然亞洲各國之資料在地化立法目的都是為了進一步保護個資，實際上卻含有政治監控之目的，因此 CBPR 可能無法完全解決資料在地化之問題。

現階段 GDPR 與 CBPR 暫時無法完善解決資料在地化問題，不過我們可以思考的是如何使資料的運用合於規範，讓各區域都建立隱私保護的架構，並在此架構下落實個資保護規範，並進而達到不同制度與法律之間應該如何融合溝通的最終目的。

（七） 為兒童著想—處理兒童資料的關鍵挑戰

本場次由 Laura Brodahl 主持，講者包含方達律師事務所的合夥人 Jianyuan Yang、樂高亞太區資深顧問 Patrica Lee，以及 TotallyAwesome 的營運長 Marcus Herreman。

主持人 Laura Brodahl 首先介紹 GDPR 關於兒童個資保護的具體規範，強調 GDPR 的管制重點在於針對直接對兒童提供之服務下的行銷與使用者人格剖析等行為，同時為聽眾提出下列建議：

1、 先確認處理兒童個資的適當法律依據。

2、 導入必要的年齡驗證工具。

3、 在隱私權聲明中使用易於理解的文字語言。

4、 針對兒童採取隱私保護設計（by-design）及預設（by-default）。

5、 針對兒童資料採取額外的安全維護措施。

Jianyuan Yang 接著介紹中國在 2019 年 5 月 31 日提出的兒童線上隱私保護法草案，該特別法強調家長的明示同意、鼓勵產業採取自律規範、強化透明性、要求嚴格的保護措施、提升兒童的資料權利，並課予營運者較重的內部控管義務。Jianyuan Yang 並分享中國識別兒童身分的幾種方式，包含臉部辨識、實名認證，以及利用政府資料。

來自樂高的 Patrica Lee 則分享實務經驗，表示由於樂高為跨國企業，適用包含美國兒童線上隱私保護法（COPPA）及歐盟 GDPR 在內的各國法規，因此樂高集團於政策上即特重並內化對於兒童的個人資料及隱私保護，例如嚴格遵守資料最少蒐集原則（data minimization）、於各項服務中規劃隱私與安全設計，並控管在其網站、行動裝置應用程式及其他數位服務中均能有效揭露其隱私權政策。

Patrica Lee 強調，樂高的宗旨是一切以兒童權利優先，該公司甚至將網站及應用程式入口區分為「家長版」及「兒童版」，進入兒童版瀏覽商品或使用各項功能時，將完全不會收到任何形式的廣告追蹤或投遞（Advert Free）。

最後，TotallyAwesome 的營運長 Marcus Herreman 說明根據調查，每天有 17 萬名兒童第一次進入網路世界、有 79%的兒童喜歡網路勝過電視、有 77%的兒童偏好使用網路的裝置為手機。

而該公司為亞太區第一的兒童安全數位媒體公司，非常重視兒童的隱私保護，特別在廣告方面，TotallyAwesome 提供了即時廣告過濾機制，可在廣告追蹤或投遞過程中移除未滿 13 歲兒童的個人識別資訊，並可阻擋對於兒童裝置的不當廣告追蹤，且所有廣告均需通過該公司的技術審查以百分百確保兒童的安全。

（八） 從理論到實踐—雲端資料治理

本場次由亞洲雲端運算協會執行長 May-Ann Lim 主持，邀請 Google 亞太區負責雲端公共政策的 Yam Ki Chan 及新加坡星展銀行的 Joey Pang 分別從雲端服務提供者及使用者的角度分享經驗。

講者認為，資料類型及來源的多元化將促使企業更加重視資料存取、安全、治理及法規遵循，且如要打造資料驅動（data-driven）的企業文化，就更需要雲端運算的協助。

雲端服務具備了五個特點，包括：隨需求自助式服務 (On-demand Self-service)、多元網路接取 (Broad Network Access)、資源池存取模式 (Resource Pooling)、快速且具彈性 (Rapid Elasticity)，以及可量測服務使用狀況 (Measured Service)。

講者提及在雲端運算不同的服務型式之間，其安全風險彼此間是有相互依賴性的，舉例來說，如果有一個雲端服務廠商所提供的服務內容為軟體服務（SaaS），這項服務建置在某一個雲端開發平台之上（PaaS），而開發平台背後採用了另一家廠商的雲端基礎架構（IaaS）服務，此時，在資料安全、風險管理方面都會彼此相互影響繼承的。

也就是說，雲端服務提供商（SaaS），除了要維護應用程式的安全性和可用性之外，同時也要確保所使用的開發工具沒有安全漏洞（PaaS），而且在運作過程中要確保運算、網路、儲存設施的安全（IaaS），本身就必須要負起相對較多的安全責任。而使用軟體服務的使用者，則是要在服務水準、安全控制措施、法規遵循等，也要在合約之中明確要求，以釐清相關的管理責任。

在此同時，企業除應慎選雲端服務提供者之外，也應就雲端資料治理建立一套可有效執行的策略與操作模式。更重要的是，雲端運算將無可避免涉及資料在地化的法規議題，企業在使用雲端服務時務必瞭解所應適用的管轄法律關於資料在地化的具體規範。

（九） 當 GDPR 與中國資料保護法規遵循相遇

本場主持人為 EY 會計師事務所合夥人 Fabrice Naftalski，講者包含 EY 法律事務所合夥人 Zhong Lin、華為全球資安與個資法副總裁 Kevin Wangke，以及萊雅中國個資保護長 Shawn Li。

Zhong Li 先簡短介紹 GDPR 之規定與架構，然後特別提醒聽眾：要研究中國之個資保護，僅瞭解中國網安法是不夠的，還要注意中國一般法律（如刑法、民法）、各產業之特別法規、與資料相關之法規、各種官方制定之標準和指引等。

華為代表接下來分享華為公司為符合 GDPR 所做之努力，他領導之團隊共有 400 人，其中 200 人為工程師。他的團隊依據 GDPR 建置了一套個資生命週期管理與運作機制之方法論，其立體之思考框架相當值得臺灣企業參考。

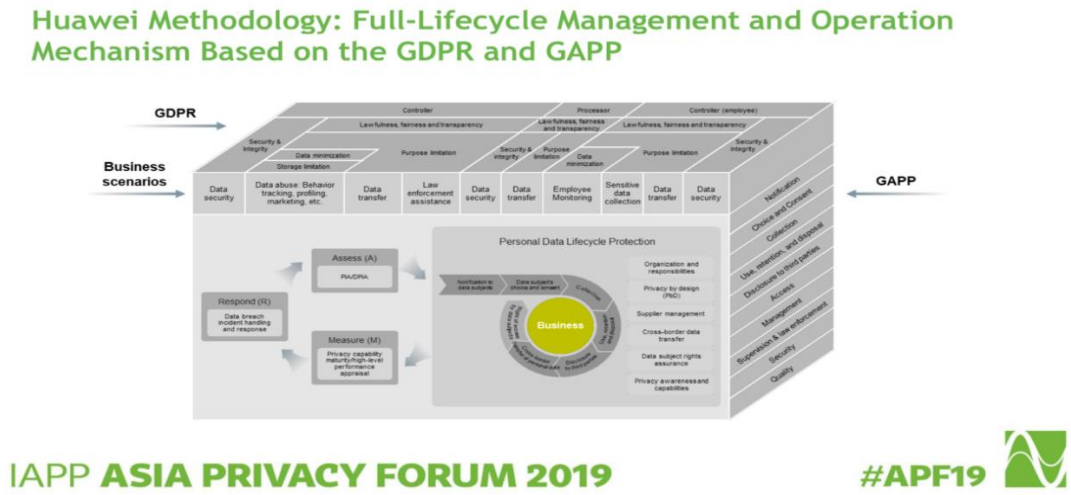

圖 3　華為公司個資生命週期管理方法論（講者簡報第 10 頁）

華為代表分享該公司為確保個資保護之合規性，各部門如何協調合作分工，以及整個華為產品隱私預設設計（Privacy by Design）之流程。華為代表也特別提到他們採用第三方之個資評估工具（PIA tools，例如在會場設攤位展示之 OneTrust 產品）輔助達成 GDPR 合規之目標，此亦值得臺灣有符合 GDPR 需求之企業參考。

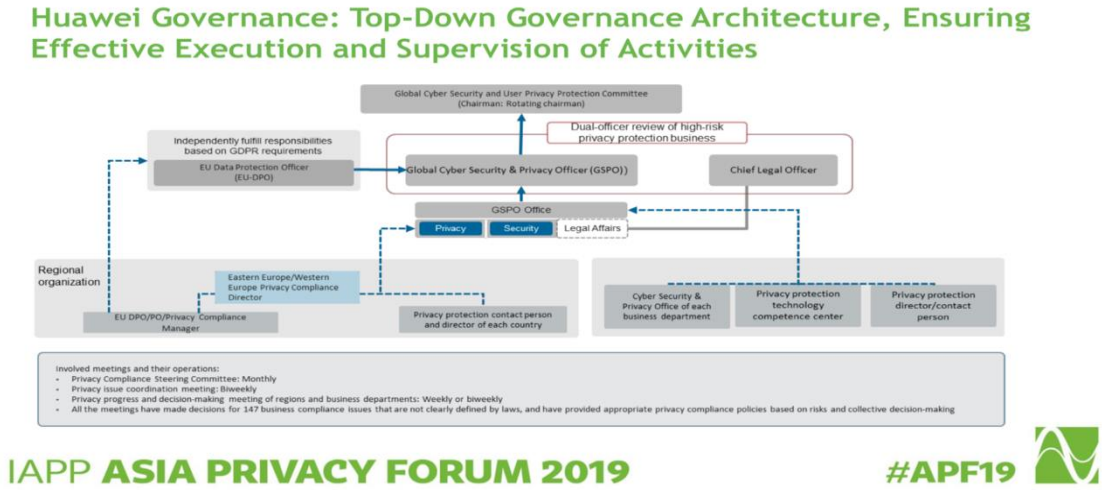

圖 4 華為公司隱私治理架構（講者簡報第 11 頁）

（十） 亞太區的隱私規範因應

本場議程由 Sony 亞太區隱私長蔡麗卿（Joyce Chua）分享 Sony 如何因應亞洲各國不同之隱私保護法律要求，內容相當值得臺灣政府與企業參考。

GDPR 實施一年後，開罰金額已高達 5600 萬歐元，主關機關接獲案件超過 20 萬件，民眾超過 94000 次之申訴，以及超過 64000 次個資外洩通知。其中 Google 在 2019 年 1 月被法國開罰 5000 萬歐元，新加坡個資主管機關 PDPC 也因駭客攻擊導致資料外洩而開罰 IHiS 和 SingHealth 二家公司共 100 萬新加坡幣，因此企業應該要特別重視個資之法規遵循。

Sony 先研究世界各國個資法，例如：敏感資料、個人資料和機密資料之區別、管轄權、控管者與受託運用者之角色等，然後將外部法律要求轉成內部法遵要求，並制定出「公司隱私管理計畫」（Corporate Privacy Management Program）。

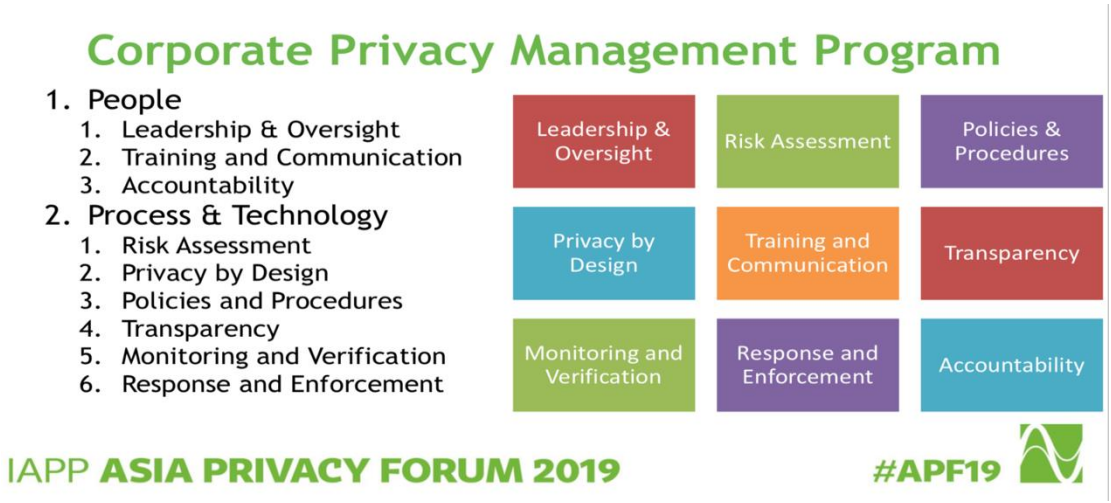

圖 5 sony 公司隱私管理計畫（講者簡報第 10 頁）

Sony 並盤點出目前亞洲已有之個資法，包含澳洲、韓國、香港、馬來西亞、紐西蘭、菲律賓、新加坡、臺灣等，以及正準備立法或修法之國家，例如：印尼、印度、新加坡（資料可攜、強制資料外洩通知）、泰國、越南、南非等。Sony 也仔細比對了 OECD 隱私原則和 GDPR，認為二者之原則與架構相當。

講者並以電子商場 E-MALL 為例，從「蒐集、利用、分享、刪除」之資料生命週期，分析企業最常碰到的挑戰，包含：未經授權之蒐集；不安全之資料傳輸；稽核紀錄不足；過度信任第三方夥伴；永久保存個資；未及時刪除；未完整刪除；未提供清楚的當事人申訴管道；當事人拒絕行銷後仍寄送行銷 email；不合理的申訴收費等。

至於公司實施個資保護之方法，Sony 建議依序執行「評估、設計、發現、執行、監督與改進」的步驟，分別檢視「建立、儲存、利用、分享、歸檔、刪除、當事人申訴管理」等七大個資生命週期階段，每階段均有許多執行細節，

以「建立」階段為例，至少要做到蒐集前之內部核准、制定標準隱私和安全條款、蒐集同意之管理、蒐集前之風險評估等工作，若以「利用」階段為例，則至少要做到委外監督、客戶資料之匿名化或假名化、貫徹特定目的內利用等細節。

最後，講者強調公司內部跨部門共同合作之重要性。Sony 成立隱私監督管理委員會，成員包含執行高層、隱私長、安全長、法務長、各事業單位隱私代表等，由隱私長直接與執行高層溝通，並和法務部門一起完成隱私政策、Cookies 蒐集聲明等工作，如此才能因應全球各地個資保護之挑戰。

（十一） 隱私保護下的資料治理

本場次由 Informatica 的 Russell Feldman 及 Deloitte 的 Chris Lewin 對聽眾介紹以隱私保護為目標的資料治理（Data Governance）方式。

講者指出，資料治理架構應包含：

1、 最高位階的指導性原則（Guiding Principles）

2、 第二位階的管理領導與課責（Leadership &Accountability）、技術與工具（Technology & Tools）、標準與架構（Standards & Architecture）及政策與程序（Policies & Processes）

3、 第三位階的遵循查核與持續改進（Compliance & Continuous Improvement）

講者亦指出，適當的資料隱私設計（Data Privacy by Design）可促成有效的資料治理，內涵包括：

1、 定義並管理資料治理政策

識別企業營運流程及相關系統，定義所蒐集之個人資料與其目的，並清查與第三方分享之資料，所著重關鍵在於建立組織內可執行的隱私政策。

2、 清查、分類個人資料

對個人資料進行盤點，確認保存位置及權責人員。

3、 識別身分

以技術方式自動識別個人資料當事人身分（不同國籍可能需遵循不同的法律要件，例如歐盟 GDPR 及美國加州消費者隱私法（CCPA）。

4、 分析資料風險、建置保護計畫

評估個人資料可能遭到的濫用或未獲授權存取之風險，並預先規劃因應措施及安全維護措施。

5、 保護資料安全、管理當事人權利及同意

在業務執行過程中保護個人資料，並持續研發、測試並評估安全措施的有效性；同時應尊重當事人權利的行使。

6、 評估、溝通並稽核成熟度

追蹤各項政策計畫的進行，並與相關角色人員持續溝通，且應有效稽核政策的遵循程度。

（十二） 課責性之實踐：隱私治理的現在與未來

本場次由 Access 美國及亞洲負責人 Christopher Martin 主持，與談人則包含 SAS 歐洲與亞洲隱私策略長 Kalliopi Spyridaki、Google 亞太區隱私長

Angela Xu以及Hunton Andrews Kurth資訊政策領導力中心總裁Bojana Bellamy等三位女士與談。

Bellamy 首先介紹課責性在個資保護上實扮演核心角色，她認為課責性由「領導力、風險評估、政策與程序、透明性、認知訓練、監督與驗證、反應與執行」等七大部分構成。她認為：公司的價值觀和道德觀能使課責性更健全，課責性並非靜態的觀念，而是動態反覆循環的過程，課責性將法律要求轉化成以風險為基礎、可驗證和可執行之公司實務作法，而組織必須要有能力對內（例如：執行高層、董事、股東等）和對外（例如：商業夥伴、立法者、社會、當事人等）證明課責性。

最後，另外二位與談人則分別口頭簡述Google和SAS如何透過取得ISO等標章或認證、制定公司隱私保護計畫、有拘束力之企業規則（BCR）、企業守則（Code of Conduct）以及加入APEC CBPR等方式，來執行並驗證公司已實質遵循隱私規範，並有能力證明課責性。與談者也提及，一般中小企業面對日趨嚴格的隱私規範及問責，尚難確悉落實的方法，且擔憂無法負擔法遵成本，因而建議各國個資隱私之主管機關，應盡速釋出相關指引文件，使企業內部得以設計處理資料的流程步驟。

（十三） 歐盟與日本的自由資料流動：在相互適足認定之後

本場次由 Bird & Bird 法律事務所（比利時）的合夥人 Takeshige Sugimoto 擔任主持人，與亞洲商務法律研究所（The Asian Business Law Institute）的資深研究員Clarisse Girot、Mori Hamada & Matsumoto律師事務所的合夥人Atsushi Okada、日本個人情報保護委員會的Junichi Ishii三位講者介紹日本與歐盟間的個人資料流動框架。

由於歐盟GDPR及日本個人情報保護法對於跨境傳輸個人資料均有類似「有主管機關」決定或指定可接受傳輸之國家白名單的規定，雙邊自 2017 年起開始就相互認可個人資料流動之法律框架展開對談，終於在 2019 年 1 月 23 日，由日本個人情報保護委員會指定歐盟為可跨境傳輸個人資料之接受國，由歐盟執委會作出承認日本的個資保護法規體系具備歐盟認可的適足性決定（即可由歐盟將個人資料跨境傳輸至日本），自此建構雙方互相傳輸個人資料的法律體系。

講者認為，在日本取得歐盟的適足性認定之後，雖然個人資料可由歐洲經濟區自由傳輸至日本，但受 GDPR 域外效力拘束的日本企業仍有諸多法規義務有待遵循。

此外，日本為爭取歐盟的適足性決定，以補充法規架接歐盟 GDPR 與日本個人情報保護法的落差，例如敏感個資的範圍、當事人權利的內容，以及將來自歐盟的個人資料再由日本傳輸至第三國的高保護義務等，凡此均是日本企業仍需留意之處。

最後，日本個人情報保護委員會的 Junichi Ishii 亦站在資料自由流動的立場，強調日本個人情報保護委員會推廣 APEC 跨境隱私規則（CBPR）體系的態度，認為 CBPR 可作為亞太地區各國自由傳輸個人資料的安全保護框架。

肆、心得及建議

網路科技日新月異及新興應用服務蓬勃發展，世界經濟發展重心已從實體經濟蛻變為虛實整合的數位經濟。巨量資料帶來嶄新的商機與機會，通訊傳播產業因提供服務而保有許多資料，其中有許多屬於個人資料，提升資料的有效利用及降低企業在經營上的法遵成本，及多面向跨業經營，是未來產業永續發展的重要議題。

資料跨境流通已為數位經濟不可或缺的一環，然而各區域經濟體間隱私保護規範有相當大之落差，如何有效建立安全可信賴的跨境資料流通機制，確保跨境資料自由流通、促進區域內電子商務活動的發展，並且平衡個人資料之保護，對於數位時代的全球經濟發展至為關鍵。

歐盟一般資料保護規範(GDPR)於 107 年 5 月 25 日實施，其個資保護之規定適用於新興科技業、人工智慧(Artificial Intelligence)、大數據(Big Data)、雲端(Cloud)、物聯網(Internet of Thing)、金融科技(Fintech)、電子商務、資訊、電腦、網通等領域之經營管理均受有影響，將潛在成為國際資料安全保護的基線，並影響其他區域法規協定。臺灣於 2018 年底申請歐盟適足性認定，若能獲得歐盟承認認可，將可建構雙邊跨境資料傳輸機制。

2018 年臺灣成為亞太經合組織（APEC）跨境隱私保護體系（Cross-Border Privacy Rules, CBPR）體系的成員，該體系成員包含美國、墨西哥、日本、加拿大、南韓、澳洲及新加坡。臺灣加入 CBPR 體系將有助於我國企業爭取海外商機，並協助國內企業及組織逐步建構個資保護制度，提高國際跨境隱私保護形象及創造跨國合作契機，形塑有利於推動跨境數位貿易的條件。本會為通訊傳播事業主管機關，積極協力我國加入 CBPR 體系之推動，協助企業取得 CBPR system 下相關問責機關（Accountability Agent, AA）的隱私認證，增加全球競爭力。

本次論壇邀集新加坡、菲律賓、日本及印度等國個資監理機關，並邀請國際企業、知名學者專家參與，共同討論 GDPR 施行一年的發展、亞太地區個人資料保護現狀、中國相關資料保護法規、資料在地化、雲端資料治理及企業課責性建立等議題。論壇各場次會後均開放現場人士提問，與會嘉賓熱烈響應，提問重點著重於資料在地化議題下，企業組織實務上應如何因應遵循各地資料隱私法規、降低法遵成本及風險。主辦單位亦表示審慎考慮於下次論壇中，設定企業組織實務上落實個資隱私操作方式之議程。

藉由參與本次國際性會議，充分蒐集國際及亞太地區資料隱私法規最新進展、中國資料隱私規範、雲端資料治理實踐、人工智慧的隱私管理等議題，了解各國個資保護政策與業界實務經驗，可做為本會因應大數據時代下隱私個資政策規劃及評估之參考。綜上，建議我國未來持續參加隱私個資相關國際會議或活動，與各國主管機關分享實務經驗，增加國際接軌及互動交流。

附錄一：研討會現場照片

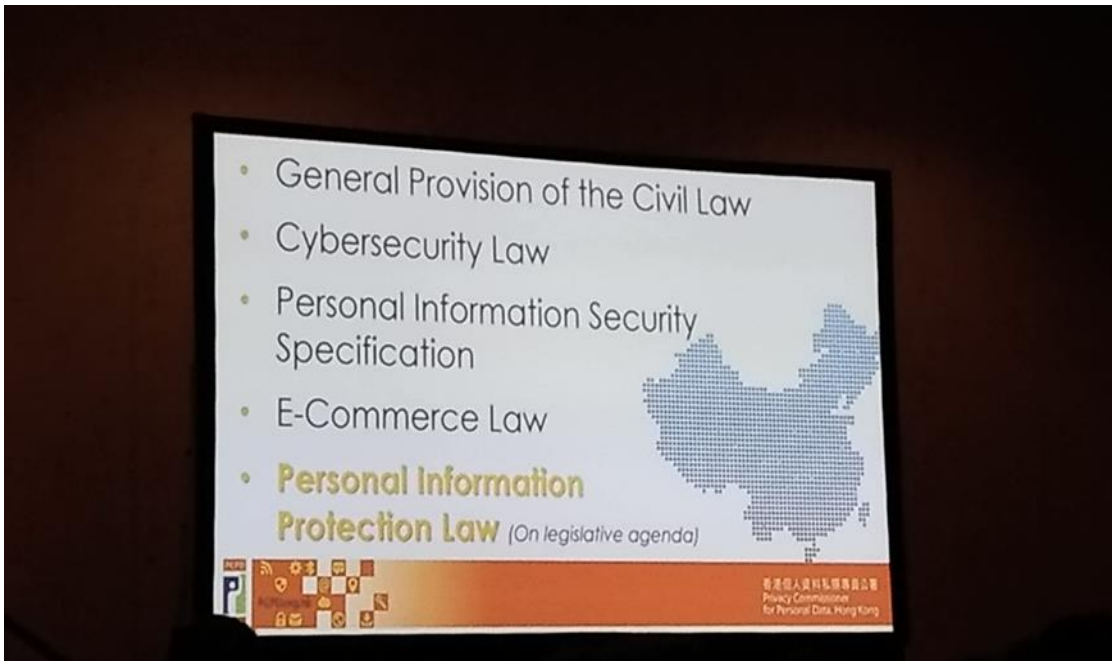

圖 6　開幕大會：香港個人資料私隱專員公署 現場報告照片

圖 7　議程：資料在地化的崛起-我們如何安全導航　會場討論照片

圖 8　議程：中國的資料法規發展及對企業的影響　講者與現場互動照片

圖 9　會場參展廠商照片

圖 10　閉幕大會：菲律賓國家隱私委員會主委 Raymund Liboro 發表演說照片

圖 11　議程：從理論到實踐-雲端資料治理 會場討論照片

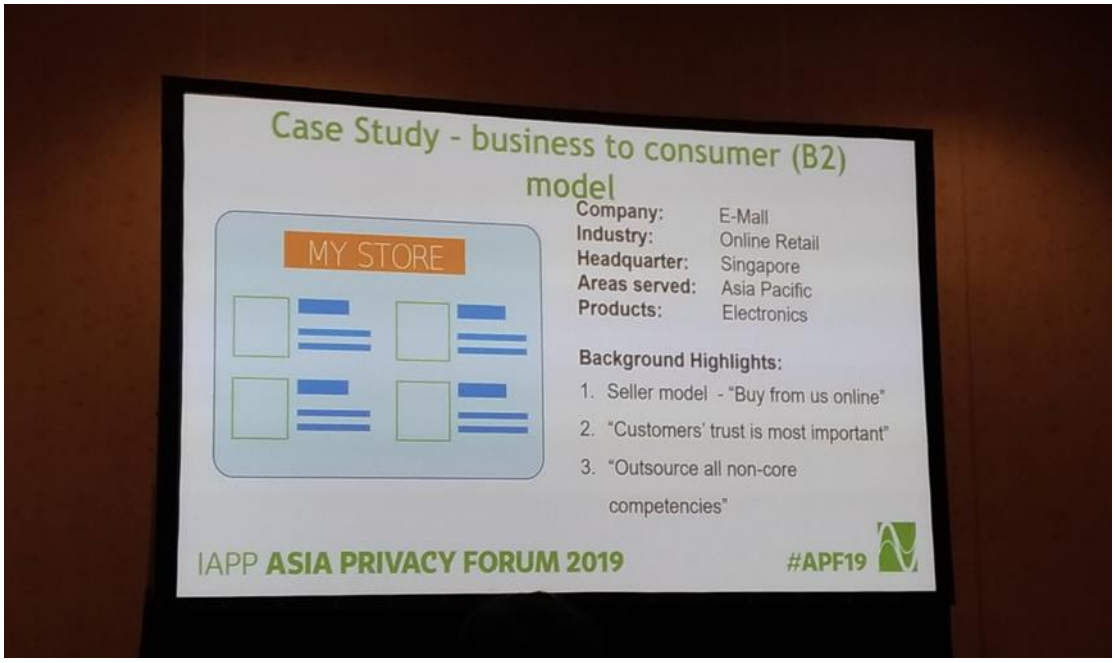

圖 12　議程：隱私保護下的資料治理 現場簡報照片

圖 13　議程：歐盟與日本的資料自由流動-在相互適足認定後 會場討論照片

・ 附錄二：研討會重點投影片資料

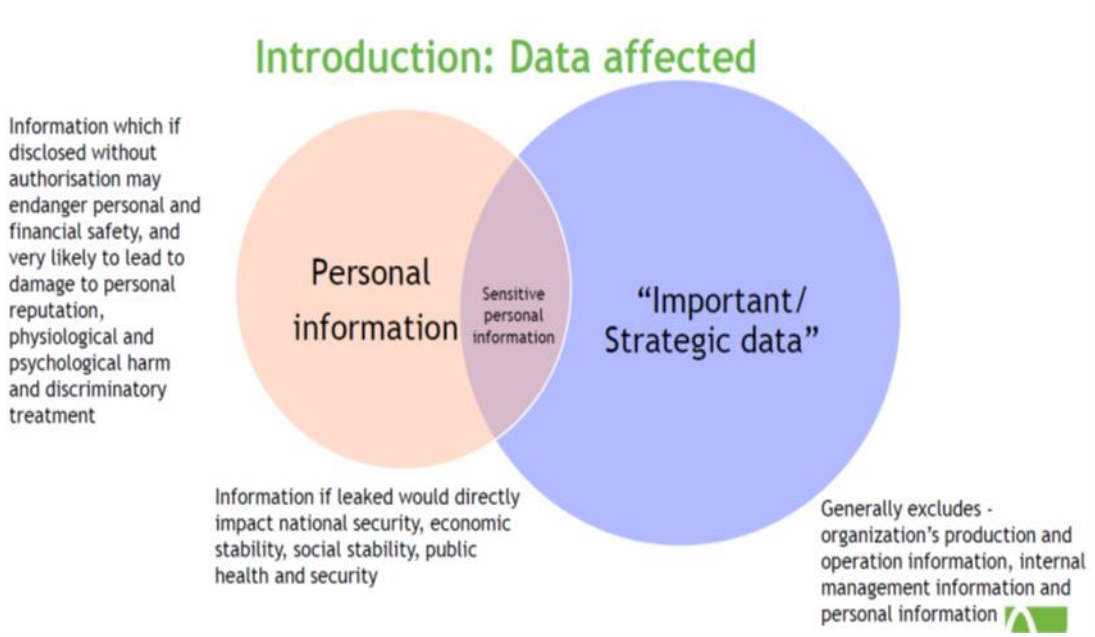

圖 14　議程：資料在地化的崛起-我們如何安全導航　簡報第 5 頁

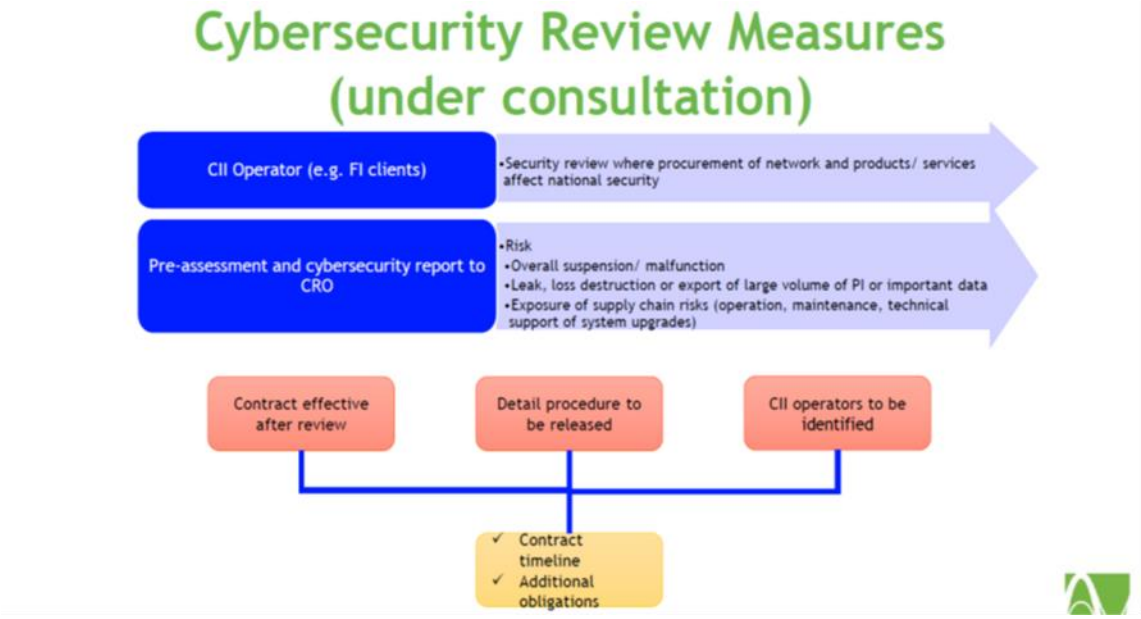

圖 15　議程：資料在地化的崛起-我們如何安全導航　簡報第 10 頁

圖 16　議程：中國的資料法規發展及對企業的影響 簡報第 11 頁

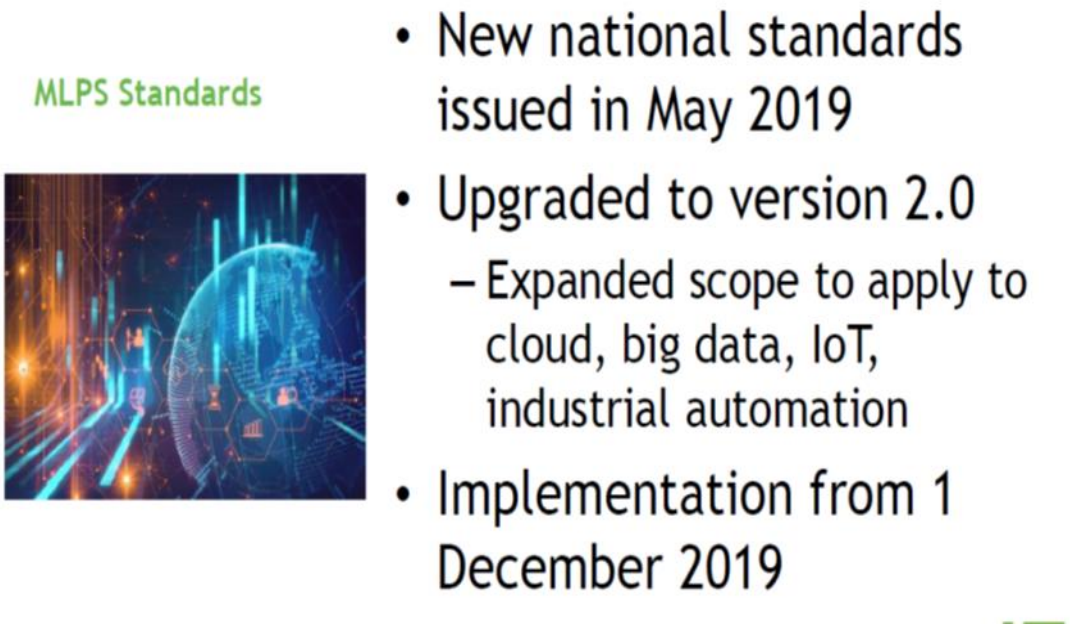

圖 17　議程：中國的資料法規發展及對企業的影響 簡報第 16 頁

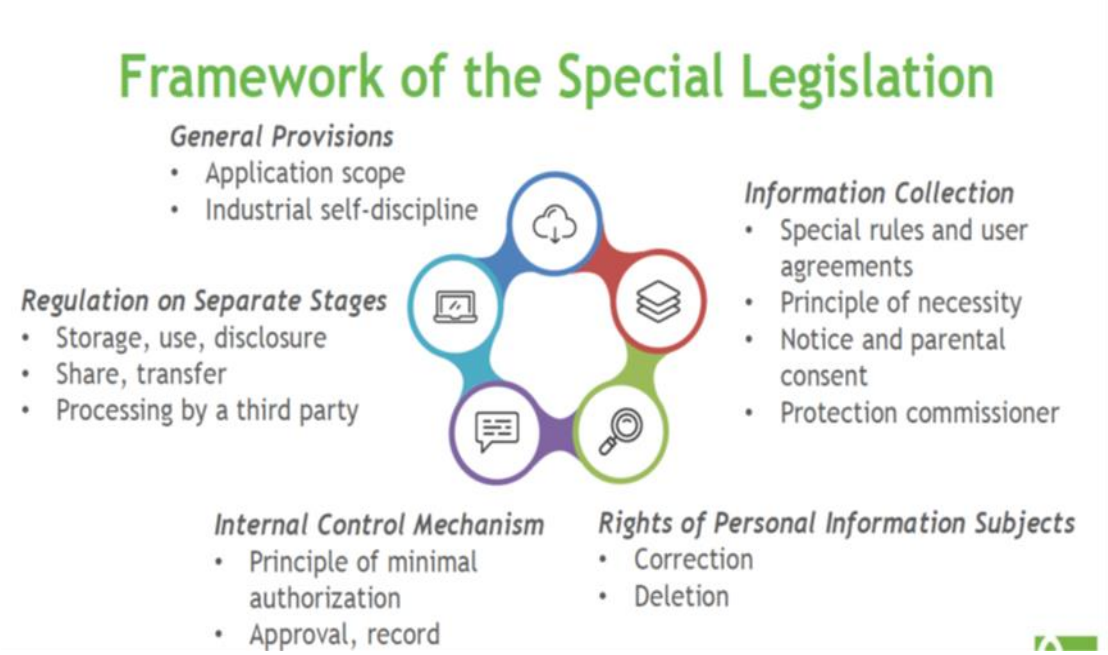

圖 18　議程：為兒童著想-處理兒童資料的關鍵挑戰 簡報第 14 頁

Highlights of the Special Legislation

Abstract	Description
• *Require Express Parental Consent*	• Collection, use beyond the agreed scope, joint use, transfer, substantive change in the notification matters
• *Encourage Industrial Self-discipline*	• Internet industrial organizations are encouraged to formulate industrial norms and code of conduct
• *Strengthen Transparency*	• Clear and easy-to-read special rules and user agreements • Parents shall be informed in a clear manner • Article 8 specifies the items that network operators shall include in the notice

圖 19　議程：為兒童著想-處理兒童資料的關鍵挑戰 簡報第 15 頁

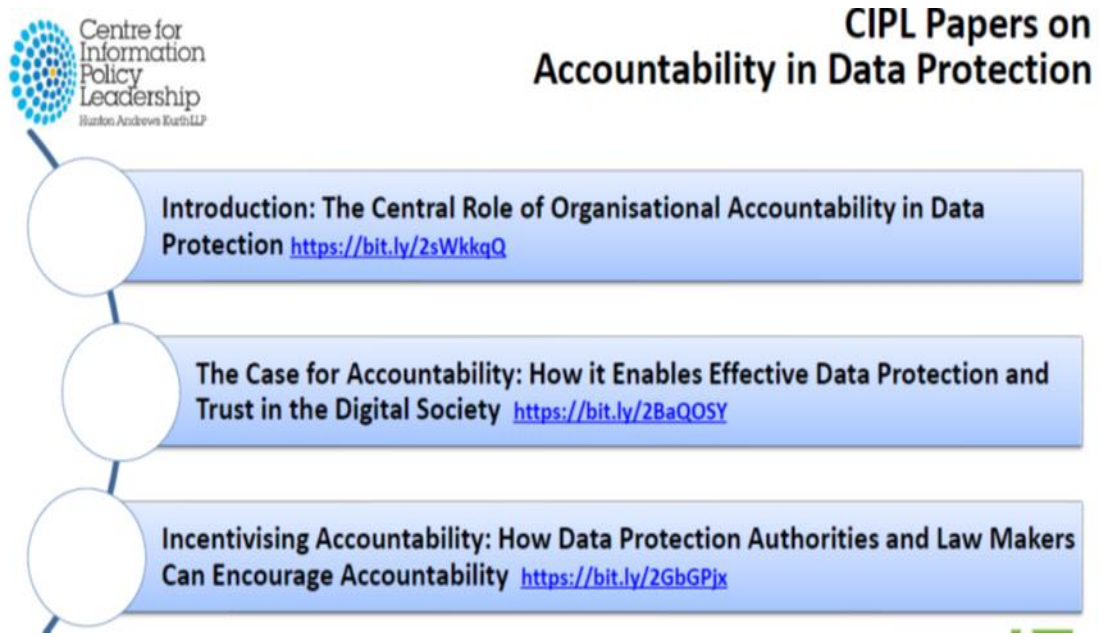

圖 20　議程：課責性之實踐-隱私治理的現在與未來　簡報第 5 頁

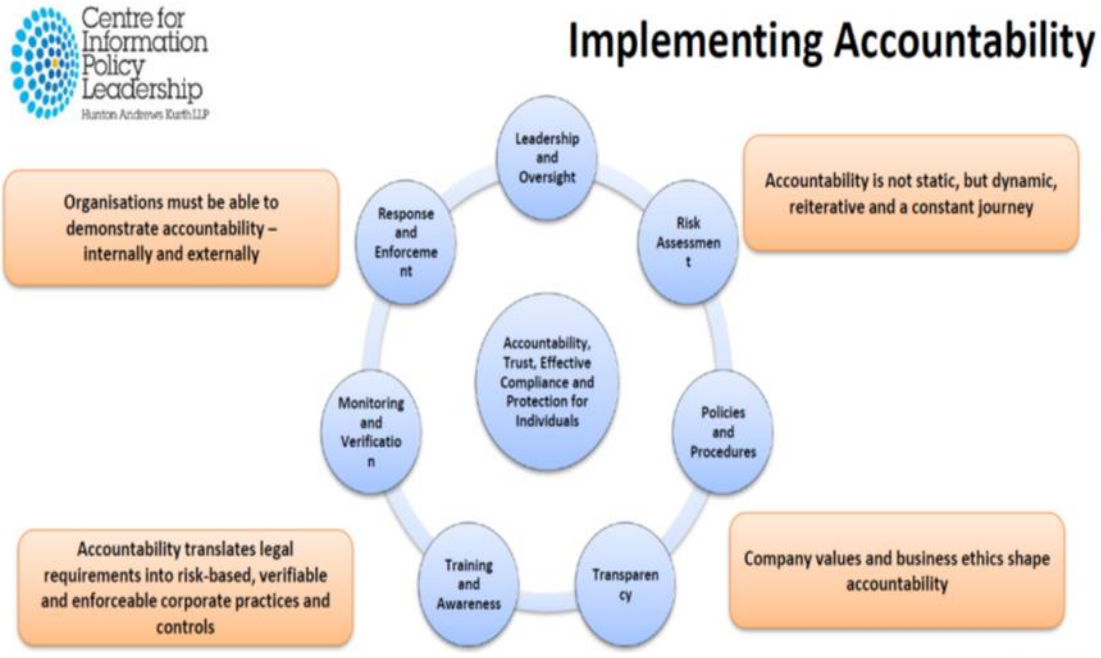

圖 21 議程：課責性之實踐-隱私治理的現在與未來　簡報第 6 頁

圖 22　議程：亞太區的隱私規範回應 簡報第 10 頁

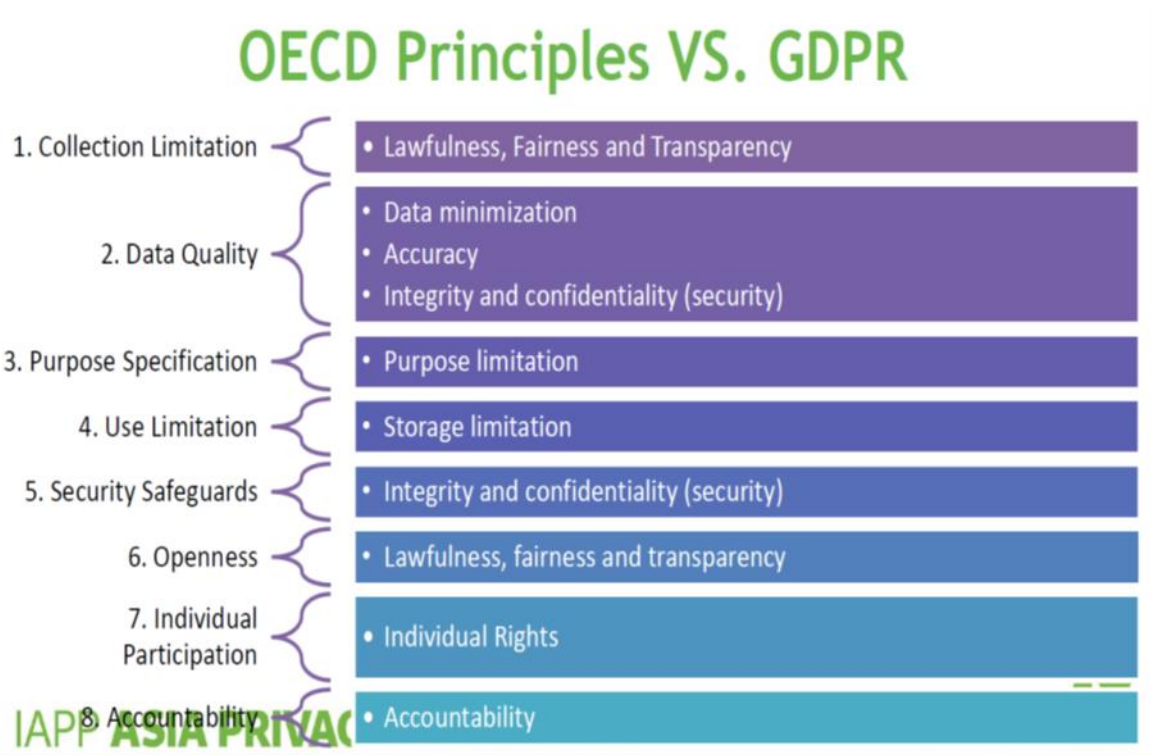

圖 23　議程：亞太區的隱私規範回應 簡報第 13 頁

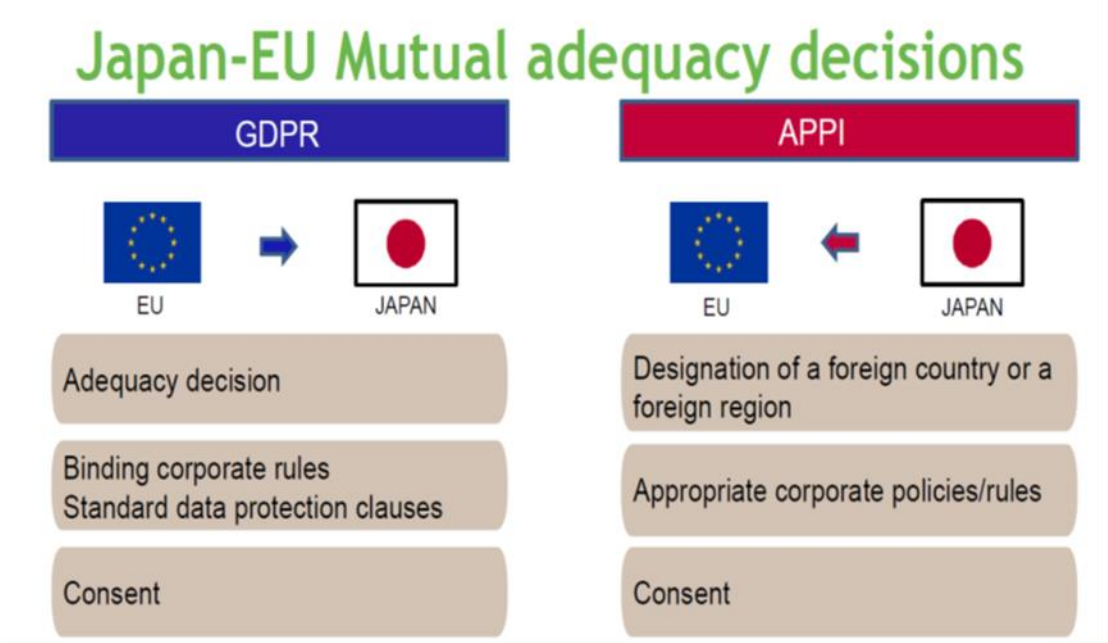

圖 24　議程：歐盟與日本的自由資料流動-在相互適足認定之後 簡報第 7 頁

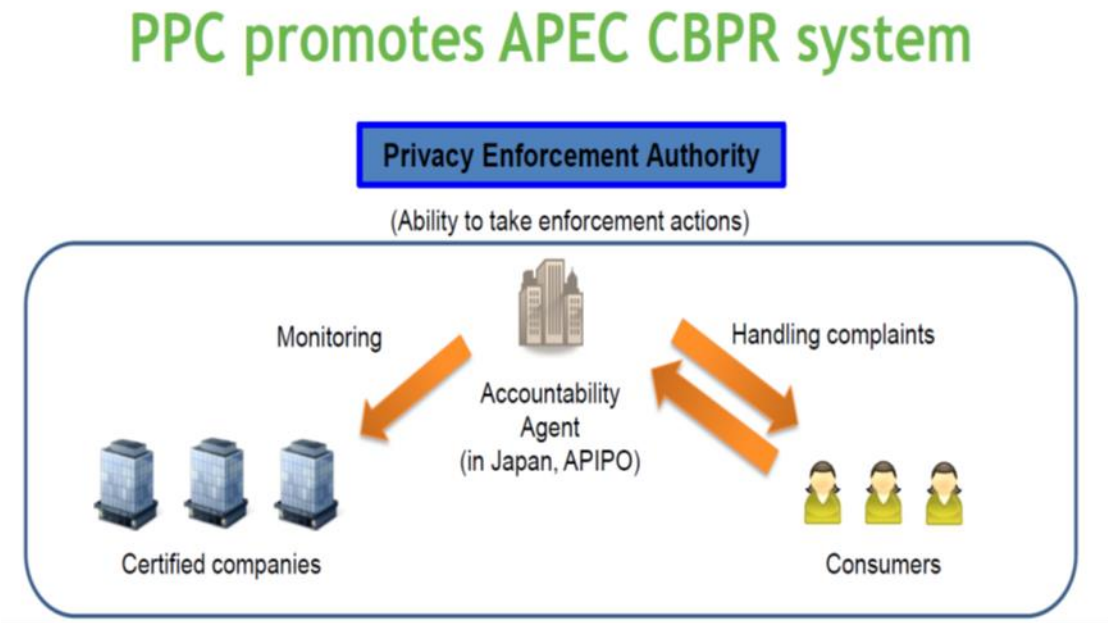

圖 25　議程：歐盟與日本的自由資料流動-在相互適足認定之後 簡報第 20 頁