出國報告（出國類別：研討會）

在資訊當道的時代下，日本新資料隱私規範及其如何促使跨境資料流通、創新及隱私保護（Japan’s New Data Privacy Regime and How it Will Enable Cross-Border Data Flows, Innovation and Privacy Protections in the Modern Information Age）

服務機關：國家發展委員會
姓名職稱：衛漢君科員
派赴國家：日本東京
出國期間：**2017** 年 **5** 月 **10** 日至 **12** 日
報告日期：**2017** 年 **5** 月 **23** 日

摘要

本次研討會係由 Centre for Information Policy Leadership（CIPL）舉辦，共有日本、韓國、台灣、美國等各官方及產業界代表與會。討論共分為三個主題，分述如下：

第一場會議係「**日本新修訂的隱私法如何促進跨境數據流通、數據驅動經濟以及個人數據的創新和保護**」（**How does Japan's Amended Privacy Law Enable Cross-Border Data Flows, the Data Driven Economy, Innovation and Protection of Personal Data**），小組成員討論日本的隱私法變更和新的實施細則與指引。在跨境數據流動和數據驅動創新方面，有何新的法律要求可同時保護個資？新法律應如何進一步解釋與運用以遵守數據使用的責任、實現大數據及分析的效益，並因應物聯網、雲計算或機器學習的挑戰？相關權責組織在訂定與實施企業隱私計畫方面的責任是什麼？監管機構在鼓勵最佳做法方面的角色是什麼？等內容。

第二場會議係「**跨境數據流動與亞太經濟合作組織跨境隱私規則制度**」（**Cross-Border Data Flows and the APEC Cross-Border Privacy Rules System**），小組成員討論日本關於跨境數據流動的新規定，特別是亞太經合組織跨境隱私規則（CBPR）制度。包括 CBPR 在日本的作用為何、隨著 CBPR 在亞太地區日趨重要，CBPR 的認證對組織與監管機構的好處，以及作為全球解決跨境數據流動治理模式的潛力為何等內容。

第三場會議係「**對大數據分析、機器學習與人工智慧適用之新法制要求**」（**Applying New Legal Requirements to Big Data and Analytics, Machine Learning and AI**），小組成員討論數位經濟和新技術的效益與挑戰。包括隱私風險評估、透明度、合法利益處理、匿名化及個人權利等，對於實現有效的數據保護、數位成長與創新方面可以發揮什麼作用、監管機構如何實現這些目標等內容。

目錄

壹、會議目的 5

貳、會議過程 5

（一） 第一場會議（日本新修訂的隱私法如何促進跨境數據流通、數據驅動經濟以及個人數據的創新和保護） 6

（二） 第二場會議（跨境數據流動與亞太經濟合作組織跨境隱私規則制度） 7

（三） 第三場會議（對大數據分析、機器學習與人工智慧適用之新法制要求） ..10

參、心得 12

附件 14

壹、會議目的

本次研討會共有三個探討議題，分別為「日本新修訂的隱私法如何促進跨境數據流通、數據驅動經濟以及個人數據的創新和保護」（How does Japan’s Amended Privacy Law Enable Cross-Border Data Flows, the Data Driven Economy, Innovation and Protection of Personal Data）、「跨境數據流動與亞太經濟合作組織跨境隱私規則制度」（Cross-Border Data Flows and the APEC Cross-Border Privacy Rules System）以及「對大數據分析、機器學習與人工智慧適用之新法制要求」（Applying New Legal Requirements to Big Data and Analytics, Machine Learning and AI），希冀透過本次會議取得第一手資料，並藉由官產學各界專家交流與互動的過程中，瞭解及學習國際間關於個資隱私保護、大數據分析與人工智慧等最新的法制框架與規範及其相關做法。

貳、會議過程

首先由 CIPL 的副總兼顧問 Markus Heyder 開場，歡迎各位與會嘉賓並介紹 CIPL 組織以及致力於隱私保護的任務與願景。接著由引言人[1]分別發言，簡要談及資訊共享與流通、建立與國際接軌的基本框架、數據的透明度等等的重要性，尤其是在無國界的網路時代，國際間不應該禁止資訊的流通而是應該去想如何負 embassy 責任地使用它，因此效益與風險兩者之間的管理及衡平就顯得格外重要。在歷經了農業社會與工業社會後，網際網路以及數據將我們帶進了數位經濟的時代，此刻面臨的是繼網際網路社會後的第四個產業革命：數據社會（data society），必須開始思考其所帶來的諸如互相連結（always connected）、數據的處理（data processing）以及轉型經營模式（transformation of business models）等的社會改變。而「數據」作為此階段產業革命的核心，它是經濟及創新的關鍵推動力，也是企業及政府的重要資產，更為社會帶來廣泛的好處[2]。對此，值得信賴的數位時代隱私新架構必須被建立起來，它包含了企業的數位責任框架（corporate digital responsibility/ accountability frameworks）[3]、風險管理（risk management）[4]、

[1] 分別為 Andrew Wylegala（Minister Counselor for Commercial Affairs, Embassy of the United States, Tokyo）、Mr. Takuya Hirai（House of Representatives/Chairman, Special Mission Committee on IT Strategy）、Ms. Mari Sonoda（Secretary General, PPC）與 Bojana Bellamy（President, CIPL）。

[2] 例如透過數據的使用以保護環境（environmental protection）、取得流行疾病的訊息（pandemic disease information）、預防犯罪（crime prevention）等增進社會利益；或提升智慧運輸系統（intelligent transports systems）、緊急預先定位服務（pre-positioning emergency services）等提升服務的效益；或發展智慧城市（smart cities）、智慧農業（smart agriculture）等因應世界的改變並促進政府的服務及目標。

[3] 例如涉及隱私管理計畫、跨境隱私規則、行為準則與標準等等。

賦予同意之外的個人權力（empowering individuals beyond consent）[5]以及隱私原則演變的詮釋（evolved interpretation of privacy principles）[6]等四個面向，以強化個人數位授權與信任，同時促進社會的數位成長、創新與包容。

（一）第一場會議（日本新修訂的隱私法如何促進跨境數據流通、數據驅動經濟以及個人數據的創新和保護）

首先由與談人「個資保護委員會」（Personal Information Protection Commission, PPC）顧問 Kuniko Ogawa 女士介紹日本新通過的個資保護法（The Amended Act on the Protection of Personal Information, APPI）[7]，隨著 ICTs（Information and Communications Technologies）的進步，加劇個人資訊的運用及多樣化，帶來了諸如擴大個資的灰色地帶、大數據的運用以及因應全球化的環境轉變，APPI 的修法目的係試圖在「個人權益的保護」（the protection of an individual's rights and interests）以及「個人資訊的利用」（the utility of personal information）之間尋求平衡。主要內容包括成立 PPC（個資保護委員會）、明確定義個人資訊、建立一個促進個資積極使用的法律框架（尤其是對於匿名處理資訊的規範）、因應全球化（尤其是跨境資料的傳輸）、措施響應所謂的「交易者名單」（Name List Trader）（強制履行應確保與第三方有關的個人數據紀錄之義務）、選擇退出程序（opt-out procedure）應通知 PPC 等規範。此外，PPC 亦已加入 GPEN（Global Privacy Enforcement Network）、APPA（Asia Pacific Privacy Authorities）等國際執法合作框架，致力與國外執法當局積極建立合作關係。Kaori Ishii 教授則介紹修法的概念與發展，相關環境的改變，例如擴大個資用於大數據、物聯網和雲計算服務的效益；對匿名資料處理的挑戰；機器學習（machine learning）所帶來的不可預見性等，都顯示了個資保護的方面需要一套更全面及廣泛的觀點。包括個資的範圍、對同意的詮釋、匿名處理資訊、洩漏數據、揭露個人數據予第三方的要件等，由 PPC 發佈指導原則，並擴大跨境數據流對國外實體的應用。值得一提的是，日本情報經濟社會促進協會（JIPDEC）於 2016 年成為 APEC－CBPR 體系下的問責機構（Accountability Agent, AA），處理申訴、與 PPC 分享資訊並適當教育對新法有更好的理解。日本 Yahoo!的顧問 Naoya Bessho 先生介紹新修的個資保護法之目的、PPC 的功能與期待、匿名資訊的處理、對消費者所可能引發的不安、洩漏資訊的相關罰則等。並表示大數據的利用絕對是將來關注的焦點，日本 Yahoo!密切關注個人隱私的保護，於 2016 年 6 月修訂了隱私政策，依據法

[4] 即對個人傷害的「風險」以及對個人、組織或社會的「利益」之間的衡平。
[5] 例如以使用者為中心的透明度；有權取得、修改、拒絕或刪除；或申訴與補救措施等。
[6] 例如合法利益的處理、公平的處理、對個人的風險或傷害、新的透明度機制等。
[7] 日本 APPI 亦有譯為「個人情報保護法」，惟本報告將"personal information"統一稱為「個人資訊（個資）」、"data"統一稱為「數據」，合先敘明。

律妥善處理個人數據並完善對消費者的保護[8]，詳細可參考日本雅虎隱私指南（Yahoo! JAPAN Privacy Guide）。Naoko Mizukoshi 律師：面對新法的實施，許多公司已開始調整相關作為並致力於新的數據政策，但仍有缺乏相關法律上資源的困境，造成對新法的誤解。新法將於（今年）5 月 30 日實施，我們將持續努力教育及宣導其他公司、消費者以及產業以利共同良好的運作。

（二）第二場會議（跨境數據流動與亞太經濟合作組織跨境隱私規則制度）

首先由 Jacobo Esquenazi 介紹各位與談人，然後小組成員進行交流及分享。日本經濟產業省國際事務辦公室主任 Shinji Kakuno 介紹了促進 APEC 跨境隱私規則制度（Cross-Border Privacy Rules system）的重要性，APEC/CBPR 欲建立消費者、企業與監管機構信任的個資跨境流動發展，透過認可的問責機構（Accountability Agent, AA）評估企業或組織的隱私政策是否與 APEC 隱私保護框架與規則的要求相符，目前參與 CBPRs 的經濟體有美國、墨西哥、日本與加拿大，通過認可的問責機構（AA）有美國的 TRUSTe 與日本的 JIPDEC，而目前日本有一家經認證的機構[9]，期許將來有更多的經濟體加入 CBPRs。資訊的自由流通係促進全球經濟與社會發展的基礎，同時數據與隱私的保護也相當重要，為了避免各國的隱私保護政策造成資訊流通的阻礙，CBPRs 建立一套國際的隱私框架以確保個資跨境傳輸的安全，即成為有利的解決機制。2016 年 APEC 宣示了 CBPRs 的重要性，目前 APEC 經濟體當中，韓國[10]與菲律賓有意願加入 CBPRs，而澳大利亞、香港、俄羅斯、新加坡與越南等亦在考慮中，值得一提的是，最近一次 APEC/ECSG 會議中，台灣、新加坡與菲律賓表達了加入 CBPRs 的興趣。加入 CBPRs 的好處是透過一個全球標準的隱私保護政策，增加各方的「可信度」（credibility），在資料或數據的取得、處理及儲存的過程中能夠依照一套國際通用的可靠標準進行，尤其是如果通過 CBPRs 的認證將有助於新修正的 APPI 關於跨境傳輸資料予國外第三方的適用。因此，持續擴展並讓更多的國家或經濟體加入 CBPRs 有其必要性，惟目前 CBPRs 僅適用於 APEC 成員國之間，將來更期許能建立與 GDPR 的互通性（interoperability）或全球系統（global system），以因應全球化的效應。

PPC 顧問 Tsuzuri Sakamaki 提及跨境數據傳輸（Cross-Border Data Transfers）的問題，這是本次修法的一項全新規定，第 24 條（對外國第三方提供資訊之要件）、第 75 條（APPI 執行於國外事業亦適用之範圍）及第 78 條（請求國外主管

[8] 諸如數據的收集、利用或提供予第三方等皆有規範。

[9] IntaSect Communications, Inc.於 2016 年 12 月 20 日經認證符合 CBPRs 標準，這是日本第一個案例。

[10] 韓國已於去年 12 月提交了加入 CBPRs 的申請。

機關協助執行)的內容,如何確保國外第三方亦具備與日本相等的隱私保護架構,係由 PPC 負責訂定規則並進行判斷,但事實上在隱私保護方面,每個國家有不同的法規範,甚至並不是所有國家都有 DPA(Data Protection Act),為了確保執行上的可行性,促進個人資訊/數據隱私保護的統一法制框架就很重要,這也是為什麼我們如此迫切需要 CBPR 系統,它讓我們在適用不論是第 24 條或是第 78 條時,提供了國外執法當局是否亦建立安全機制或相當的隱私保護架構之判斷基礎。

日本總務省(Ministry of Internal Affairs and Communications, MIC)主任 Yoichi Iida 提及資訊的自由流通在許多國際論壇中備受關注,最近像是 2017 年 4 月的 G20 Digital Ministers' Declaration 重申了對 ICT 政策的支持,促進跨境資訊流並且讓網路使用者都能夠合法地依其選擇而取得線上訊息、知識與服務,同時承認個人數據與隱私保護、智慧財產權都被認為是強化數位經濟信心與信任之核心。數位化及數據驅動社會帶來了創新經濟的成長,而「信任」(trust)是提升數位服務的重要元素,其認為如何提升消費者資料提供的意願並促進流通與使用是很值得關注的部份。在此方面,提出了所謂「數據信任銀行」(Data Trust Bank)以及「數據交換市場」(Data Exchange Market)的概念。此外發展認證機制,對於提升消費者的信任亦有其必要,以促進數位經濟的成長。

韓國內政部個資保護政策(Personal Information Protection Policy)副主任 Suhee Kim 介紹韓國個資保護法制體系以及 CBPR 對韓國或亞太地區的重要性。韓國係由個資保護委員會(Personal Information Protection Commission, PIPC)負責監管個資保護政策及相關機構,在 ICT 方面有 KCC(Korea Communications Commission)的資通信網絡利用及信息保護法(The Act on Promoting of Information and Communications Network Utilization and Information Protection , Network Act)、在財政方面有 FSC(Financial Services Commission)的信用資訊使用及保護法(Credit Information Use and Protection Act)、在公共/非營利產業方面有 MOI 的個資保護法(Personal Information Protection Act, PIPA)。思考兩個部分,其一是個資的保護,其二係數據的傳輸,前者係 PIPA 欲處理的部分,由 MOI 來執行且適用於公共或非營利部門,因此 MOI 所關注的政策係針對於消費者而非私人公司,其致力於個資的保護,而不在於促進數據傳輸或產業之使用目的;因此對於數據傳輸的保護,MOI 則開始思考 CBPR 作為一種補強的工具。韓國倘成功加入 CBPR 後,接連的規劃包括由 MOI 指定問責機構(Accountability Agent, AA)、由 KCC 獲得 APEC ECSG DPS(JOP)之認可,建立一套 APEC/CBPR 運作系統(operating system)、修正與數據傳輸相關的法規,像

是 PIPA 以及 Network Act 修正允許通過 CBPR 等認證進行數據傳輸。CBPR 對於韓國及亞太地區的重要性，在政府與個人方面，增加了監管當局跨國合作的信心並創造一種讓亞太地區擁有更好的隱私保護政策之協同效應（synergy effects）；在企業方面，（尤其是國外的企業）將受益於跨境數據傳輸，且通過 CBPR 的認證制度可視為 GDPR 第 46 條的適當安全措施（appropriate safeguard），將有利於降低法規障礙。

日本情報經濟社會推進協會（Japan Institute for Promotion of Digital Economy and Community ,JIPDEC）主任 Masataka Saito 首先提到目前 JIPDEC 在 2016 年 1 月成為日本第一個經認可的 APEC/CBPR 問責機構（AA）[11]，JIPDEC 於該年 6 月開始運作 APEC/CBPR 問責機制，而 IntaSect 通訊公司在該年 12 月 20 日通過了 JIPDEC 的檢驗與認證。問責機構（如日本的 JIPDEC）的任務係審查申請機構的隱私保護政策或程序的自我評估是否符合 CBPR 系統之要求、處理投訴並向 APEC 提交匿名的案件說明及投訴的統計數據，且持續監督已獲得認證的公司或企業是否改變其隱私保護處理方式，以判斷是否進行額外的審查或是停止或取消認證。取得 CBPR 認證的好處在於它可宣示其所引用的個資處理政策符合 APEC 的隱私保護原則或標準，這將對於跨境交易的發展有所助益。申請認證的過程大致可分為申請（application）、審查（review（documentation/on-site））、審查委員會（board of review）及註冊（registration）4 個部分。

TRUSTe 國際法規事務主任 Josh Harris 提及隱私保護是一條漫長的路，而 CBPR 為跨境資訊流通提供一個重要的開始，目前應關注的是它的可擴展性（scalability），讓更多的小型企業加入並提供共通的應用系統，另外互通的認證制度也很重要；Apple 全球隱私權高級總監 Jane Horvath 認為應善用 APEC/CBPRs 的整合與認證功能解決跨國資料傳輸的問題，國際間的運作框架如何達成相互的認可（mutual recognition）——例如日本與歐盟之間的承認——也是關注的方向。當 iphone 的功能不再只是聯繫，它還連結了你每天去了哪裡、你的健康數據或付款的資訊等，數據流的安全顯得更加重要，因此必須建立更加強而有力的數據隱私保護政策；GOOLE 隱私法務主任 Keith Enrigh 則認為應樂觀看待數據，當我們運用越多的數據就獲得越多的創造力及價值，數據可以告訴我們很多事情，只要能夠在利益與可能的傷害之間找到平衡，數據可以解決很多人類基本的問題，而 GOOLE 對於跨境資料傳輸採取支持 CBPR 框架的態度，在通用的框架之下促進安

[11] 根據日本新修法 APPI，個資保護認證組織（Authorized Personal Information Protection Organizations）係由政府依法進行認可，而 CBPR 認證亦屬該認可運作的一環。

全的傳輸，同時讓整個社會認識到數據自由流通的效益與好處。很期待更多的持續對話。

（三）第三場會議（對大數據分析、機器學習與人工智慧適用之新法制要求）

本研討會最後一場會議係由 CIPL 總裁 Bojana Bellamy 開場並介紹與談人。Susumu Hirano 教授聚焦於兩項主題：其一係人工智慧研發原則（AI R&D Principles）、其二係人工智慧網絡（AI Networking）的影響與風險評估。針對前者其提出了 9 項原則，分別為（1）協作原則（Principle of Collaboration）[12]、（2）透明度原則（Principle of Transparency）[13]、（3）安全原則（Principle of Security）[14]、（4）可控性原則（Principle of controllability）[15]、（5）人身安全原則（Principle of Safety）[16]、（6）隱私原則（Principle of Security）、（7）倫理原則（Principle of Ethics）[17]、（8）用戶協助原則（Principle of User Assistance）[18]、（9）責任原則（Principle of Accountability）[19]。而前述原則對於 AI 網路的功能，「原則（1）」主要係促進其健全成長與效益、「原則（2）至（7）」主要係限制其風險、「原則（8）」則是補充了前述的兩項功能，而「原則（9）」則係期待對利益關係者完成前項各種原則的可能。

日本 PPC 顧問 Kuniko Ogawa 除了延續上半場的內容外，於第三場會議主要提到大數據的效益以及個人數據的保護。APPI 建立了一個新的「匿名資訊處理」（anonymously processed information）法制框架，在處理個資時使用一種方式讓它無法識別出特定個人的訊息，並且去識別化後不允許該個資重建，對於這種匿名處理的個資之流通或使用可採取比較寬鬆的管制。PPC 對於匿名資訊處理的方法有訂定相關標準：（1）刪除足以識別特定個人的描述（description）[20]（2）刪除個人識別碼（individual identification codes）[21]（3）刪除互相連結的其他資訊（linking mutually plural information）之號碼[22]（4）刪除特質描述（idiosyncratic

[12] 注意對於 AI 系統的互連性與互相操作性。
[13] 注意對於 AI 系統行為的認證或解釋能力。
[14] 這裡的安全指的是 AI 網絡系統本身的健全與可靠性，例如避免網絡系統運作失控或通信故障等等。
[15] 注意對於 AI 系統的可控制性，且適當地努力提供相關的資訊。
[16] 這裡的安全指的是避免造成生命或身體的傷害。
[17] 尊重人性尊嚴（human dignity）或個人自主權（individual autonomy）
[18] 考慮到 AI 系統可以幫助用戶、適當地為用戶提供選擇的機會並努力提供相關資訊。
[19] 努力完成對於用戶或相關利益關係人的責任。
[20] 刪除部分或全部特定個人諸如名字、地址、生日或性別等之描述。
[21] 刪除全部個人識別碼，諸如臉部識別數據（face authentication data）、指紋識別數據（fingerprint identification data）、個人號碼或駕照號碼（individual number or driver's license number）等。
[22] 例如對於身分管理（management ID）所連結到的電話號碼、電子信箱等個人訊息。

descriptions）[23]（5）其他基於個資資料庫（personal information database）的必要處理作為[24]。PPC 訂定的匿名訊息處理標準於今年 2 月 27 日發布，提供了處理的指導原則，以期在自律規範（self-regulation rule）下完善大數據的利用以及隱私的保護。

日本 MIC 高級研究員 Satoshi Narihara 討論了 AI 網絡社會（AI Network Society）進展的階段：（1）獨立運作（2）不同 AI 系統互相合作（3）強化人類的能力[25]（4）人類與 AI 共生共存。並分享 MIC 今年在東京舉辦了「AI Network Society 國際論壇」，來自美國、歐盟與日本的官產學界互相交流了關於 AI 網絡的社會、經濟、倫理與法制等相關意見，同時也討論了 AI R&D Guidelines，認為指導方針雖然不具有法律上的拘束力，但可在國際間提供一套跨部門或領域的基本框架。

CISCO 全球隱私與數據保護總監 Harvey Jang 提及對於數據的使用以及個人權利的保護的關注，數據使用的安全及效益極大化、大數據的分析等都需要持續的訓練與教育，因為可能在你還無法確定會需要蒐集什麼樣的資訊時，所有的資訊或數據就已經存在大數據資料庫裡面了，只要經過工程師的篩選或分析，資訊或情報就隨時可能產生，而隱私的風險就這樣出現了。大數據的利用對社會或個人所造成的影響，必須透過持續訓練以茲因應，但關鍵不在於如何設計相關計畫（program），而是如何讓它發揮實際的功效，否則都只是空談，而這是一項重要的任務與挑戰。

J.J. Pan 博士談及關於大數據的新的法律要求，在「數據使用的必然性」與「信用的缺乏」之間，我們必須找出數據使用的責任與倫理界線。有什麼責任制度與措施是我們所需要的？責任的基本要素是什麼？——管理風險及公平對待所有利害關係者：諸如承諾致力於內部政策、建立讓這些政策發揮作用的機制、內部監督確保該機制的運行、重視個人參與的透明度及同意以及在必要時隨時向監管機關表明相關計畫要求或補救；再者，如何實施數據使用的操作倫理？——其責任與衡量標準：諸如企業責任、員工個人責任（釐清公司所有人（包括公司領導人、

[23] 有些關於特別的事實或可能顯現某種重要差異而得以識別出特定人的描述，例如在日本只有兩位超過 116 歲的人，像這樣的資訊必須刪除或者使用其他的表達方式（像是「超過 90 歲」這樣的描述方式或之類的）來代替。

[24] 除了前述 1 至 4 項作為外，在個人資訊的大資料庫當中所蒐集到的資訊，例如移動資訊（movement history）可能識別到住家或辦公場所；消費者極其有限的購物資訊（purchase history）可能識別到某些消費者，依其屬性刪除之。

[25] 例如透過感應器（sensors）或執行器（actuators）連結人類的大腦或身體，增加人類的各種潛在能力。

工程師、所有公司的利害關係人等等）的權責）、對客戶進行合法實體與合法權益的認證或透過數據等方式篩選供應商、實施隱私影響評估及建立相關的評價機制等。

參、心得

隨著網路與科技的發展，時代的進步與更迭將人們從農業革命、工業革命一路帶領到現今的數位時代，經濟或產業的發展更加無遠佛屆，其影響的層面及強度亦為過去所無法匹敵。在個人資訊或數據的部分，不論是大數據分析或跨境傳輸，皆亟需面對如何在有效的運用、鼓勵創新以及足夠的隱私保護間互相權衡的問題。本次研討會受益良多，「信任」（trust）的元素在許多環節的討論中都扮演重要的腳色，因為當「信任」在整個信息體系中建立起來，才能夠提升消費者提供資訊的意願，進而促進使用與流通，並且在跨境傳輸部分順利推展。而「信任」作為整個信息系統中的核心部分，對它的提升與強化，可以降低數據使用的不確定性以及企業的成本，因此如何健全個人資訊或數據的隱私保護架構，尤其是一套符合國際趨勢的法制環境或保護框架，以期創造資訊利用的最大效益同時又能進行完善的保護，已成為刻不容緩的思考方向。

首先，在法制環境方面，綜觀國際上的個資保護趨勢，越來越多國家傾向於設立專責機關[26]，並完善相關的法律規範。像是日本修法 APPI 在個資的定義、匿名資料處理（去個人識別化基準或程序、放寬管制標準等）或國際傳輸等皆有更明確的規範，本會議中亦於跨境傳輸的部分進行不少的討論[27]，對於個資傳輸至境外第三方，日本採取「原則禁止、例外允許」的立法，與國際上許多國家採取相同的規範模式，亦可供我國參考。

此外，在保護框架方面，加入 CBPRs 的重要性逐漸提升，會議中亦積極鼓勵各經濟體加入，對於發展認證機制、增加各方的「可信度」（credibility）以及確保國外第三方是否亦具備相同的隱私保護架構等方面皆有所幫助。再者，對於日本的「個資保護認證組織」（Authorized Personal Information Protection

[26] 例如英國的資訊委員辦公室（Information Commissioner's Office）、日本的個人情報保護委員會（Personal Information Protection Commission, PPC）、韓國的個人資料保護委員會（Personal Information Protection Commission, PIPC）、新加坡的個人資料保護委員會（Personal Data Protection Commission, PDPC）、香港的香港個人資料隱私專員公署（Office of the Privacy Commissioner for Personal Data, Hong Kong，縮寫：PCPD）、菲律賓的國家隱私委員會（National Privacy Commission, NPC）等。

[27] APPI 第 24 條、第 75 條與第 78 條內容的討論。

Organizations）制度，一方面立基於 PPC 的隱私保護規範基礎，另一方面提倡企業的自律空間，亦有持續關注其發展及相關規範動態之重要性。

最後，面對大數據的分析以及人工智慧的運用，我們面臨的是一個數據幾乎無所不在（near-ubiquitous）的嶄新時代，新型態的隱私保護議題逐漸開展，政府應重新思考傳統信息的管理方式，推動與時俱進的監管措施，並持續透過研習、教育或輔導積極鼓勵企業進行隱私影響評估或訂定隱私保護政策，持續對話並與國際接軌。

附件

（圖）會場畫面

4 May 2017

Centre for Information Policy Leadership
Hunton & Williams LLP

Centre for Information Policy Leadership

Japan's New Data Privacy Regime and How it Will Enable Cross-Border Data Flows, Innovation and Privacy Protections in the Modern Information Age

Office Building 1 of the House of the Representatives, International Conference Room
Nagata-cho 2-1-1,
Chiyoda-ku, Tokyo, Japan
11 May 2017 | 10:00-17:00

WORKSHOP AGENDA

10:00 **Registration**

10:30 **Welcome and Introduction**

- Markus Heyder, Vice President and Senior Policy Counselor, Centre for Information Policy Leadership

10:35 **Special Remarks**

- Andrew Wylegala, Minister Counselor for Commercial Affairs, Embassy of the United States, Tokyo

10:40 **Special Opening Keynotes**

- Mr. Takuya Hirai, Member, House of Representatives/Chairman, Special Mission Committee on IT Strategy, Liberal Democratic Party
- Ms. Mari Sonoda, Secretary General, Japan Personal Information Protection Commission (PPC)

11:05 **Scene Setting Remarks**

- Bojana Bellamy, President, Centre for Information Policy Leadership

11:20 **Session 1: How does Japan's Amended Privacy Law Enable Cross-Border Data Flows, the Data Driven Economy, Innovation and Protection of Personal Data**

Panelists will discuss Japan's privacy law changes and the new implementing regulations and guidelines. What are the concepts of the new law that enable cross-border data flows and data driven innovation, while protecting individuals and their data? How should the new law be interpreted and developed further to allow responsible uses of data, to realize the benefits of Big Data and analytics and to respond to the challenges and opportunities in the IoT, cloud computing and machine learning? What are the responsibilities of accountable organizations in building and implementing corporate privacy programs and what is the role of regulators in encouraging best practices?

***Please note that simultaneous translation will be available at the workshop**

Centre for Information Policy Leadership
Hunton & Williams LLP

Moderator:

- Manuel Maisog, Partner, Hunton & Williams

Panelists:

- Kuniko Ogawa, Counselor, Japan Personal Information Protection Commission (PPC)
- Kaori Ishii, Associate Professor at the Faculty of Library, Information and Media Science, University of Tsukuba
- Naoya Bessho, General Counsel, Yahoo! Japan
- Naoko Mizukoshi, Attorney-at-Law, Endeavour Law Office

12:35 **Lunch**

14:05 **Session 2: Cross-Border Data Flows and the APEC Cross-Border Privacy Rules System**

Panelists will discuss the new rules in Japan on cross-border data flows and, particularly, the APEC Cross-Border Privacy Rules (CBPR) system. What is the role of the CBPR in Japan, their increasing importance in the Asia-Pacific region, the benefits of CBPR certifications for organizations and regulators, and their potential to serve as a model for global solutions to the governance of cross-border data flows?

Moderator:

- Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.

Panelists:

- Shinji Kakuno, Director, International Affairs Office, Japan Ministry of Economy, Trade and Industry (METI)
- Tsuzuri Sakamaki, Counselor, Japan Personal Information Protection Commission (PPC)
- Yoichi Iida, Director for International Research and Policy Coordination, Global Strategy Bureau, Japan Ministry of Internal Affairs and Communications (MIC)
- Suhee Kim, Deputy Director, Personal Information Protection Policy, Ministry of the Interior, Korea
- Masataka Saito, Director, Accredited Personal Information Protection Organization Office, Japan Institute for Promotion of Digital Economy and Community (JIPDEC)
- Josh Harris, Director of International Regulatory Affairs, TRUSTe
- Jane Horvath, Senior Director of Global Privacy, Apple
- Keith Enright, Director, Global Privacy Legal, Google

15:35 **Session 3: Applying New Legal Requirements to Big Data and Analytics, Machine Learning and AI**

Panelists will discuss the benefits and challenges of the digital economy and new technologies. What can be the role of privacy risk assessment, transparency, legitimate interest processing, anonymization, and individual rights in enabling

Please note that simultaneous translation will be available at the workshop

Centre for Information Policy Leadership
Hunton & Williams LLP

both effective data protection and digital growth and innovation? What is the role of regulators in enabling both goals?

Moderator:

- Bojana Bellamy, President, Centre for Information Policy Leadership

Panelists:

- Susumu Hirano, Professor of Law, Faculty of Policy Studies/Graduate School of Policy Studies, Chuo University
- Kuniko Ogawa, Counselor, Japan Personal Information Protection Commission (PPC)
- Satoshi Narihara, Senior Researcher, Policy Research Department, Institute for Information and Communications Policy (IICP), Japan Ministry of Internal Affairs and Communications (MIC)
- Harvey Jang, Director, Global Privacy and Data Protection, CISCO
- Dr. J.J. Pan, Chief Privacy Officer and Director of Public Policy, Acxiom Asia Pacific Corp.

16:45 **Closing Remarks**

17:00 **End of Workshop**

Please note that simultaneous translation will be available at the workshop

Centre for Information Policy Leadership
Hunton & Williams LLP

A GLOBAL PRIVACY AND SECURITY THINK TANK

BRIDGING REGIONS
BRIDGING INDUSTRY & REGULATORS
BRIDGING PRIVACY & DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

50+
Member companies

5+
Active projects & initiatives

20+
Conferences, workshops & events annually

15+
Principals & advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank.
- Based in Washington, DC, Brussels and London.
- Founded in 2001 by leading companies and Hunton & Williams LLP.
- CIPL works with industry leaders, regulators and policy makers to develop global solutions and best practices for privacy and responsible use of data to enable the modern information age.

Bojana Bellamy
President
bbellamy@hunton.com

Markus Heyder
Vice President & Senior Policy Counselor
mheyder@hunton.com

Michelle Marcoot
Director, Business Development
mmarcoot@hunton.com

twitter.com/the_cipl

linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Avenue
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

Centre for Information Policy Leadership
Hunton & Williams LLP

CIPL GDPR Project at a Glance

The project aims to establish a forum for an expert dialogue between industry representatives, DPAs, the European Data Protection Supervisor (EDPS), the EU Commission, Member States' representatives and academic experts through a series of workshops, webinars and white papers with the following specific objectives:

- Informing and advancing **constructive and forward-thinking** interpretations of key GDPR requirements;
- Facilitating **consistency in the interpretation** of the GDPR across the EU;
- Facilitating **consistency in the further implementation** of the GDPR by Member States, EU Commission and EDPB;
- Examining **best practices**, as well as **challenges**, in the implementation of the key GDPR requirements;
- **Sharing industry experiences and views** to benchmark, coordinate and streamline the implementation of new compliance measures; and
- Examining how the new GDPR requirements should be interpreted and implemented to **advance the European Digital Single Market strategy and data-driven innovation**, while protecting the privacy of individuals and respecting the fundamental right to data protection.

85+ Industry Participants

10+ White Papers & Consultations

10+ Workshops, Webinars & Calls/Year

Project Priorities

- **Data Protection Officer (DPO)**
- **Certifications**
- **Smart Data Protection**
- **Core Principles:**
  - Consent
  - Legitimate Interest
  - Transparency
- **Data Portability**
- **One-Stop Shop**
- **ePrivacy Regulation**
- **New User Rights:**
  - Restrictions on Processing
  - Right to object
  - Rights related to automated decision taking
- **Risk**
- **Innovation Drivers:**
  - Historical/Statistical Research exemption
  - Anonymisation/
  - Pseudonymisation

White Papers & Consultations Include:

Response to EU Commission's Consultation on ePrivacy Directive	Submitted on 5 July 2016
GDPR Survey Report	Released on 7 November 2016
Data Protection Officer (DPO) Paper	Released on 17 November 2016
One-Stop-Shop Paper	Released 30 November 2016
Risk Paper	Released 21 December 2016
CIPL Comments on WP29 DPO Guidance	Submitted on 24 January 2017
CIPL Comments on WP29 Lead Supervisory Authority Guidance	Submitted on 15 February 2017
CIPL Comments on WP29 Data Portability Guidance	Submitted on 15 February 2017
Certifications Paper	Submitted on 12 April 2017
Smart Data Protection Paper	In Progress – Plan to Submit Q2 2017

For more information about the project, visit www.informationpolicycentre.com

CIPL Japan Workshop Panel

Cross-Border Data Flows and the APEC Cross-Border Privacy Rules System

11 May, 2017

Yoichi IIDA
Global ICT Policy Strategy Bureau
Ministry of Internal Affairs and Communications

Free flow of information in International Fora

Free flow of information and privacy protection are parallel priorities in policy talks.

G7 ICT Ministers' Declaration (2016.4)

We continue to support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to access online information, knowledge and services of their choice. We oppose data localization requirements that are unjustifiable taking into account legitimate public policy objectives

G20 Hangzhou Summit (2016.9)

We support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to lawfully access online information, knowledge and services of their choice. At the same time, the G20 recognizes that applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy.

G20 Digital Ministers' Declaration (2017.4)

We reaffirm support for ICT policies that preserve the global nature of the Internet, promote the flow of information across borders, and allow Internet users to lawfully access online information, knowledge and services of their choice. At the same time the G20 recognizes that applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy.

Promoting Data Driven Society and Data Flow

Digitalization and Data-driven society bring ;

→ boosting economic growth via innovation
GDP increase appx. 30 Trillion Yen (260-270 Billion US$) estimate in White Paper 2016

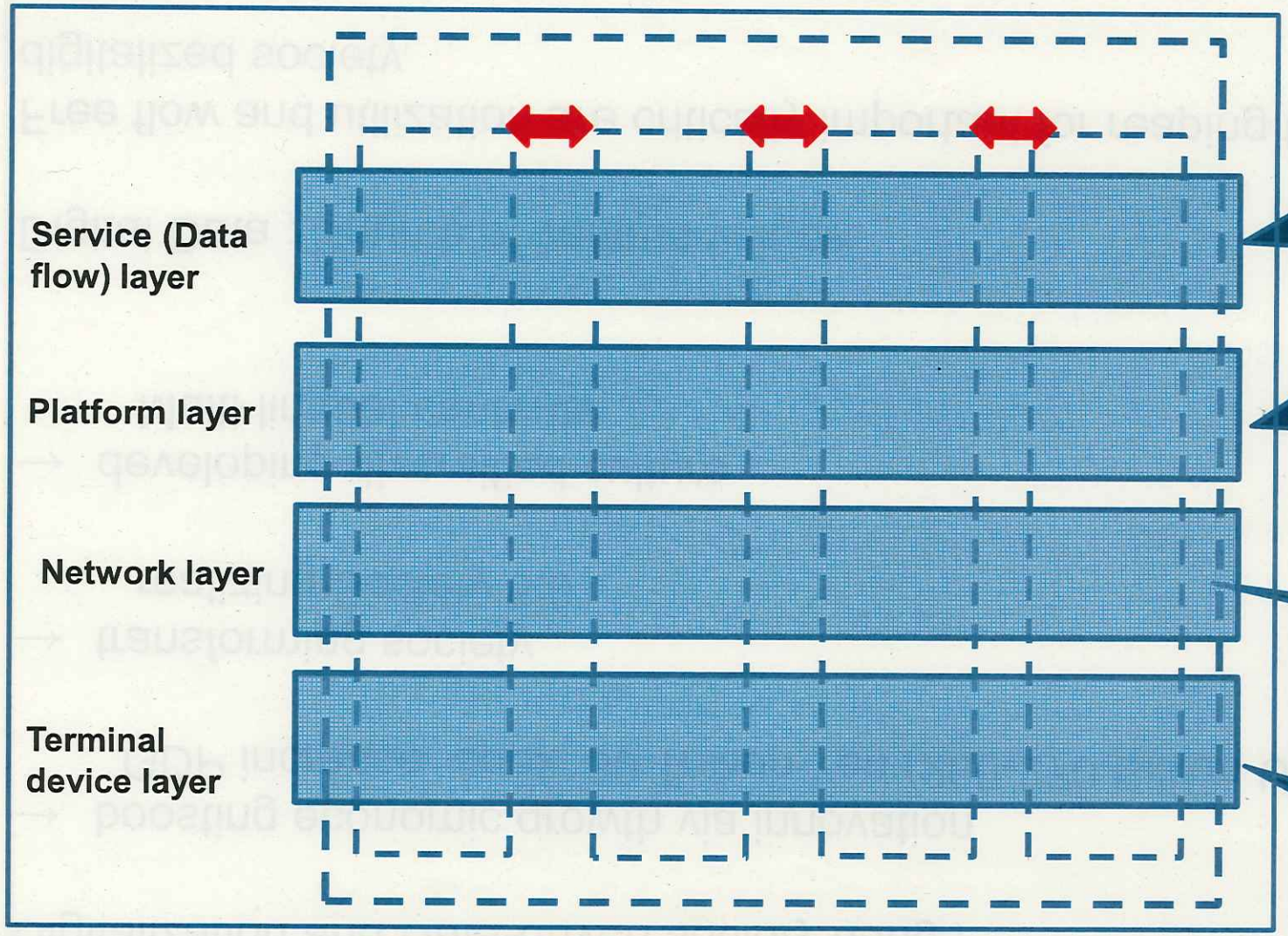
→ transforming society
realizing Society 5.0

→ developing diversified culture
Multi-lingual contents

Digital Data ; Source of various values

Free flow and utilization are critically important for reaping the benefits of digitalized society.

Structure of ICT/Digital services and promotion measures



Measures

- framework and rules to promote data utilization
- establishment of data exchange market
- enabling environment for cross sector interaction

- accreditation infrastructure
- persona data controllability
- systemic risk management

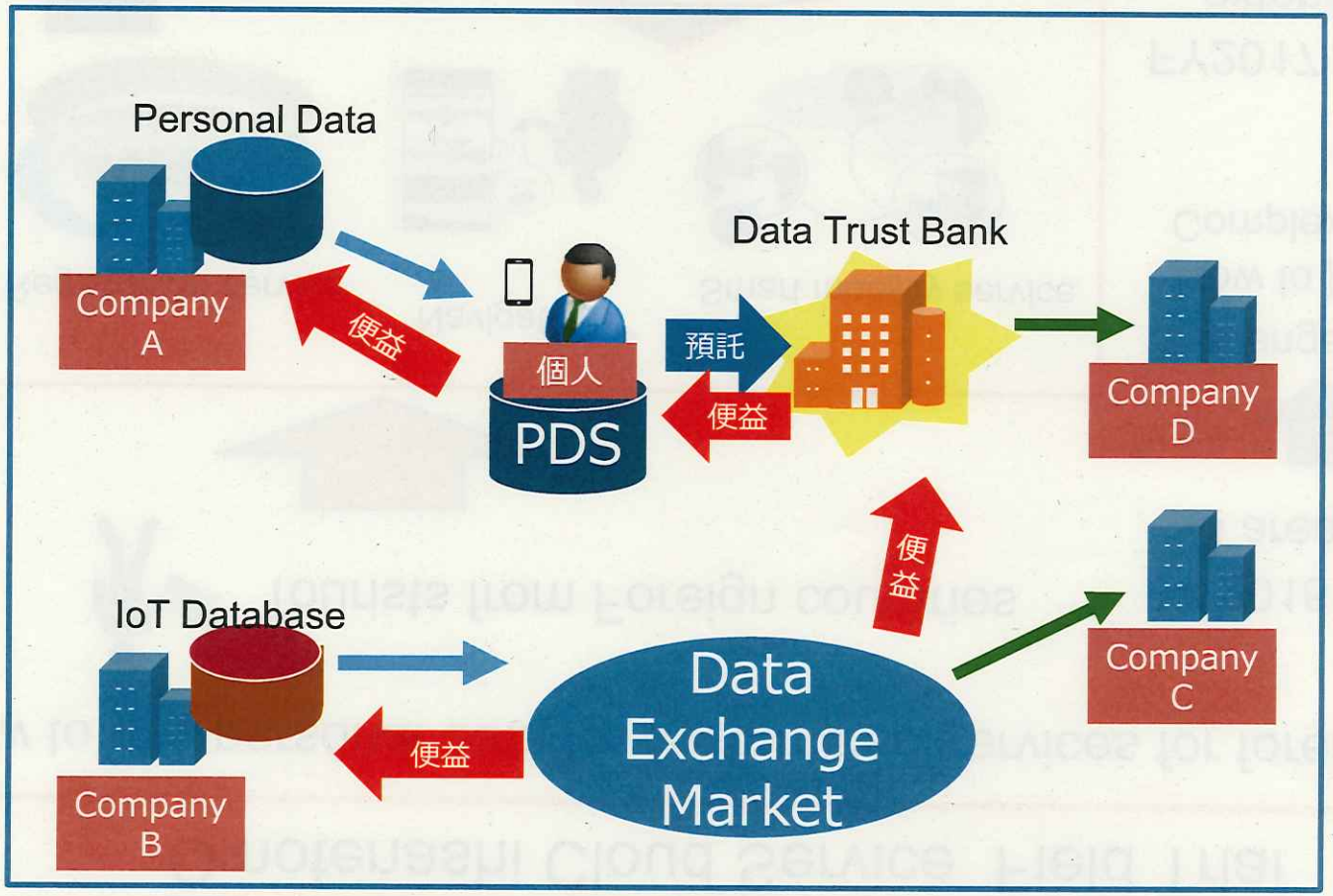
- deployment of SDN/NFV
- realization of 5G mobile network
- capacity building in network experts

- effective management of IoT terminal devices
- development and deployment of next generation AI

Concept of Data Exchange Market and Data Trust Bank

- framework and rules to promote data utilization
- establishment of data exchange market
- enabling environment for cross sector interaction

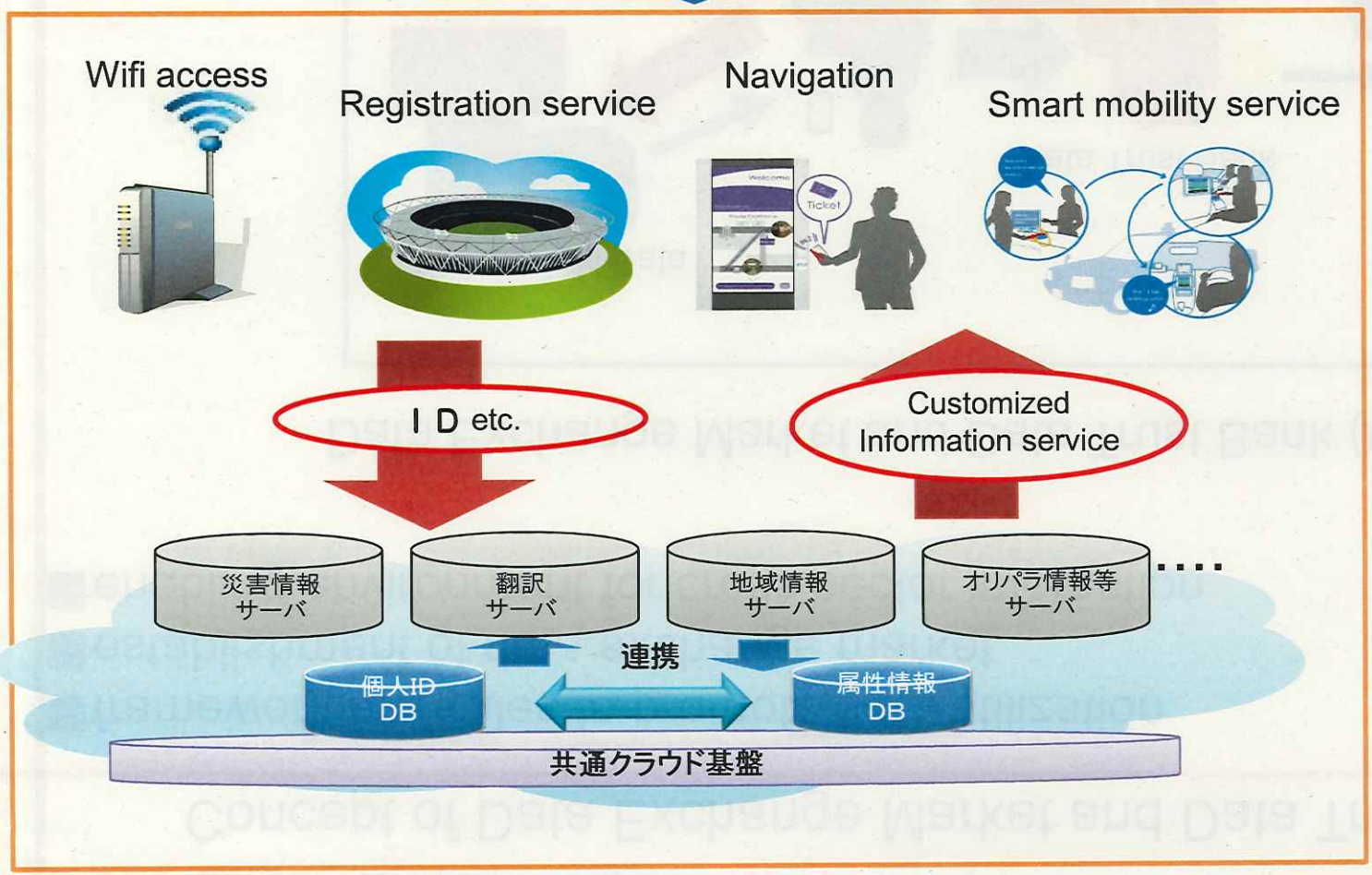
Data Exchange Market and Data Trust Bank (Concept)



Omotenashi Cloud Service Field Trial

Learn how to use personal data for customized services for foreign visitors

Tourists from Foreign countries



FY 2016
3 areas

Challenges;
How to judge credibility.
Complex procedure required.

FY2017
extended
(under planning)

Benefit of Big Data and Protection of Personal Data

Kuniko Ogawa

Counselor
Personal Information Protection Commission (PPC)

May 11 , 2017

The Amended APPI : Changes and Challenges

The Act on the Protection of Personal Information was enacted in 2003
(Fully enforced in 2005)

Changes of circumstances

As Information and Communications Technologies(ICTs) advanced, the utility of personal information became intensified and diversified beyond expectation

1. Enlargement of "gray areas" of personal information

So called "gray area" was enlarged, in which judgment of personal information was difficult

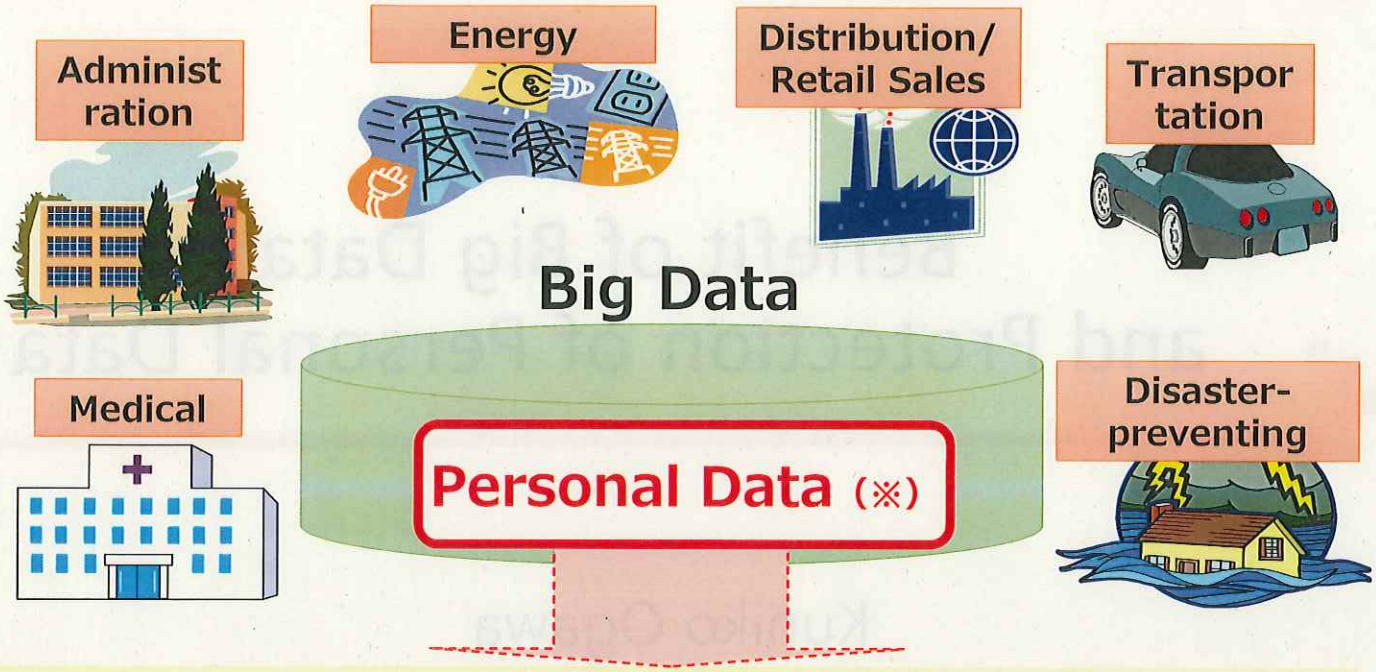
2. Correspondence for Big Data

To realize circumstances for appropriate usage of Big Data including personal data is necessary

3. Responses Globalization

As business operations are globalized, massive data flow goes beyond national border

Background of the Amendment



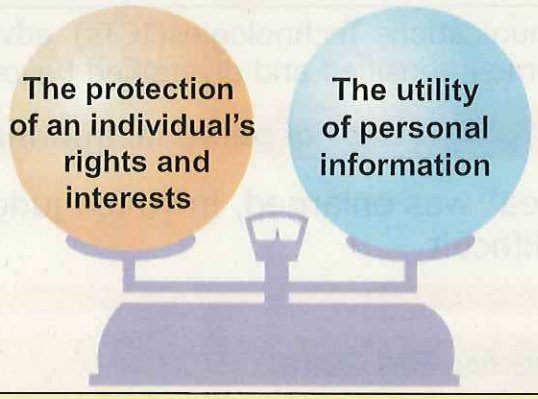
To realize circumstances for appropriate usage of Big Data including personal data is necessary

※ Personal data has a great deal of potential in utility of Big Data

Purpose of The Act on the Protection of Personal Information (APPI)

○The APPI aims to seek the balance between **the protection of an individual's rights and interests** and **the utility of personal information**.

○Besides the overall vision for the proper handling of personal information, this Act establishes obligations, etc. that a **personal information handling business operator** shall fulfil.



(Purpose of the Act)

Article 1 This Act **aims to protect an individual's rights and interests** **while considering the utility of personal information** including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan; by setting forth the overall vision for the proper handling of personal information, creating a governmental basic policy with regard to this, and establishing other matters to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities etc. of the central and local governments and establishing obligations etc. that a personal information handling business operator shall fulfill, in light of the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

○The Act on the Protection of Personal Information was amended in September 2015(To be fully enforced in May 30, 2017.)

The outline of the amendment

1.Establishment of the PPC

・Aggregation of the supervising authorities to the PPC, which are currently held by the relevant regulatory ministers toward personal information handling business operators under their respective supervision.

2. Clarifying the definition of personal information

(1) Clarifying the definition of personal information by stating partial bodily features etc. of a specific individual as personal information to cope with gray areas of personal information (individual identification codes)
(2) A principal's advance consent shall be obtained in principle in cases of acquiring or providing to a third party special care-required personal information (i.e., race, creed, medical record).

3. Establishment of a legal framework to enhance active use of personal information

Establishment of regulations concerning "anonymously processed information"(meaning information that has been produced by processing personal information in a way to make a specific individual unidentifiable and hence disallowing reconstruction of the personal information).

4. Responses to globalization

(1)Introduction of a new legal provision for transferring personal data to a foreign third party
(2)Introduction of a new legal provision for extraterritorial application, and sharing information with the foreign enforcement authorities

5. Measures to Respond to a so-called "Name List Trader"

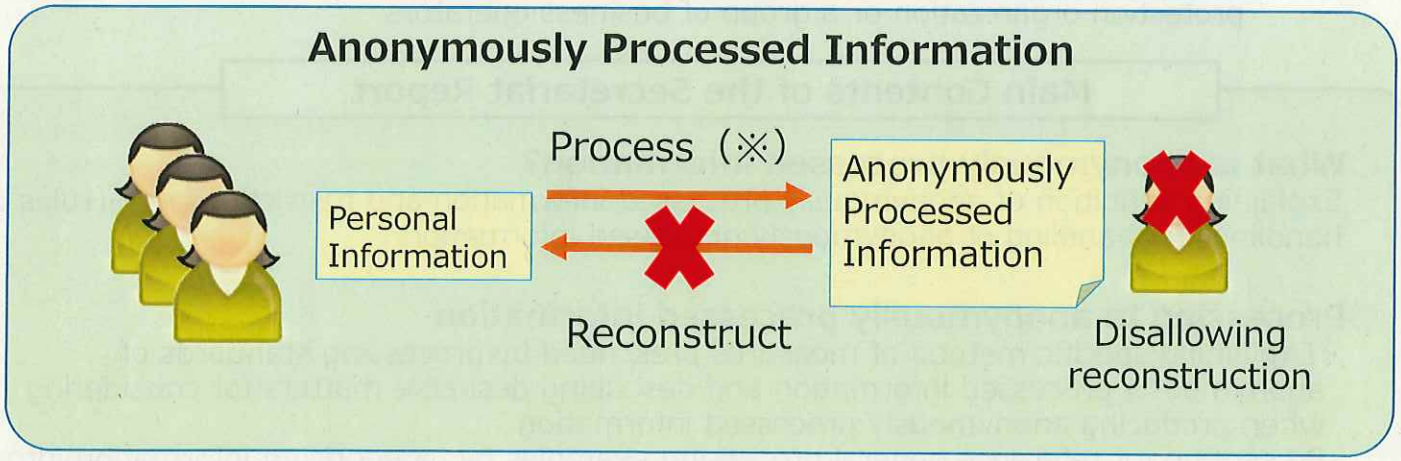
(1)Imposing new obligations to keep and confirm a record relating to a third-party personal data provision.
(2) An act of providing a third party with or stealing personal information database etc. for the purpose of earning illicit gains has become subject to criminal punishment as "the offense of providing personal information database".

6. Others

(1)Abolition of a system wherein a business operator handling personal information of 5,000 individuals or less may be excluded from the regulated subjects.
(2) A personal information handling business operator utilizing an opt-out procedure has become obligated to notify the Personal Information Protection Commission of certain legally required items.

Establishment of new legal framework of anonymously processed information 5

Establishment of regulations concerning **"anonymously processed information"**(meaning information that has been produced by **processing personal information in a way to make a specific individual unidentifiable** and hence **disallowing reconstruction of the personal information**), and enhance smooth circulation and utility under relaxed regulation compared with ordinally personal information



■ **Standards in the methods of producing anonymously processed information** (PPC Rules)

①Deleting a whole or part of those descriptions etc. which can identify a specific individual contained in personal information (e.g. name)(including replacing, same as below)
②Deleting all individual identification codes contained in personal information (e.g. my number, drivers license number)
③Deleting those code which link personal information and information obtained by having taken measures against the personal information
④Deleting idiosyncratic descriptions etc. (e.g. age 116)
⑤Besides action set forth in each preceding item, taking appropriate action based results from considering the attribute etc. of personal information database etc. such as a difference between descriptions etc. contained in personal information database etc.

Standards Related to Producing Anonymously Processed Information

For producing **anonymously processed information**, an appropriate processing needs to be done in accordance with standards prescribed by the PPC (**Standards prescribed by the PPC is a minimum standard**).

With regard to specific processing method based on characteristics of data and attribute of business, it is expected to be **appropriately developed by self-regulation of accredited personal information protection organizations or industry organizations** etc.

① **Deleting descriptions etc. which can identify a specific individual**	**Deleting a whole or part of descriptions etc. which can identify a specific individual** such as a name, address, date of birth or gender, or replace them with other descriptions etc.
② **Deleting individual identification codes**	**Deleting a whole individual identification codes (face authentication data, fingerprint identification data, individual number or driver's license number etc.)**, or replace them with other descriptions etc.
③ **Deleting codes linking mutually plural information**	**Deleting management ID** for seeking decentralized management etc. of obtained personal information in terms of security control **(including the case using telephone number or email address as an ID)**, or replace them with other codes
④ **Deleting idiosyncratic descriptions etc.**	**Deleting descriptions etc. relating to unusual fact or which have significant difference from other individuals (Example: 116 years old)**, or replace them with other descriptions etc. * "idiosyncratic descriptions etc." means the descriptions etc. which can identify a specific individual due to its idiosyncraticness.
⑤ **Other action based on the attribute of a personal information database etc.**	Further processing is necessary in **the case remaining the condition which can identify a specific individual or restore the original personal information** due to the characteristics of personal information database etc. even though the above-mentioned ①-④ process was taken * Cases mentioned in the Guideline: Movement history which can identify home or workplace, purchase history of merchandise which consumer is extremely limited, Disparity in the said personal information database

The PPC Secretariat Report on Anonymously Processed Information

Publication of the PPC Secretariat Report on Anonymously Processed Information
(February 27, 2017)

- Stating matters and aspects which are reference for considering voluntary rules related to producing anonymously processed information or actually producing anonymously processed information to an accredited personal information protection organization or a group of business operators

Main Contents of the Secretariat Report

○What is anonymously processed information?
Explaining definition of anonymously processed information and restrictions etc. (rules of handling) for handling of anonymously processed information

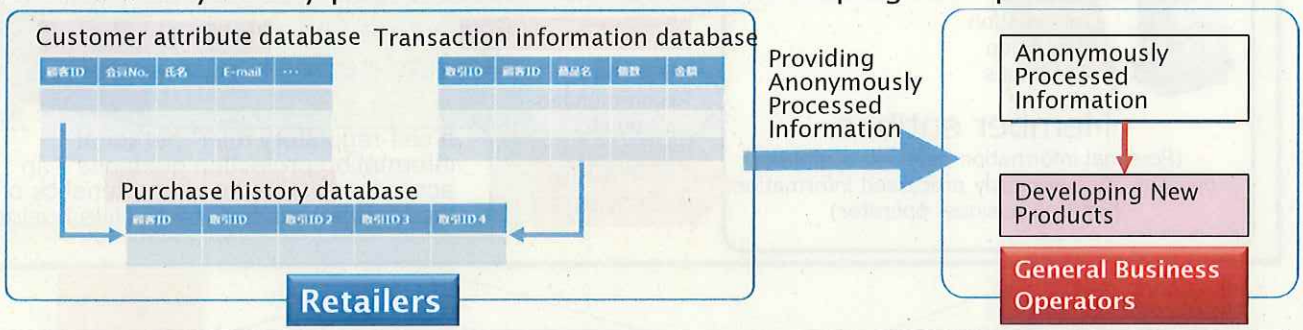
○Processing to anonymously processed information
- Explaining specific method of measures prescribed by processing standards of anonymously processed information and describing desirable matters for considering when producing anonymously processed information
- Presenting for reference general processing examples by categorizing information into **that belonging to an individual (a name, address) and history (purchase history)**, and in accordance with expected risk and basic aspects in each item of information

○Use case and example of processing of anonymously processed information
Introducing specific processing method, with expected use case in mind, of the case on purchase history, ridership history, movement history and electric usage history responding to matters and risks to be considered in respective item of information

Use Case and Example of Processing of Anonymously Processed Information① 8

○ Case of purchase history (ID-POS data)

- Processing purchase history (ID-POS data) held by retailers and providing a general business operator with processed data
- The said business operator utilizes consumer attribute and purchasing trend included in provided anonymously processed information for developing new products



Item	Example of Processing
① Member ID	Deleting or Replacing
② Name	Deleting
③ **Date of Birth**	**Replacing with year of birth**
④ **Gender**	**No processing**
⑤ **Address**	**Replacing with resident area**
⑥ Telephone No.	Deleting
⑦ **Retailer**	**No processing**
⑧ **Merchandise**	**Deleting information on merchandise which is extremely limited**

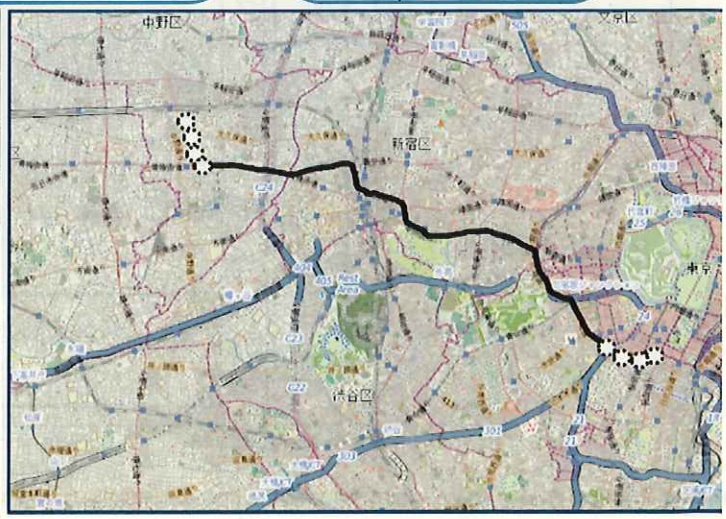
Use Case and Example of Processing of Anonymously Processed Information② 9

○ Case of movement history

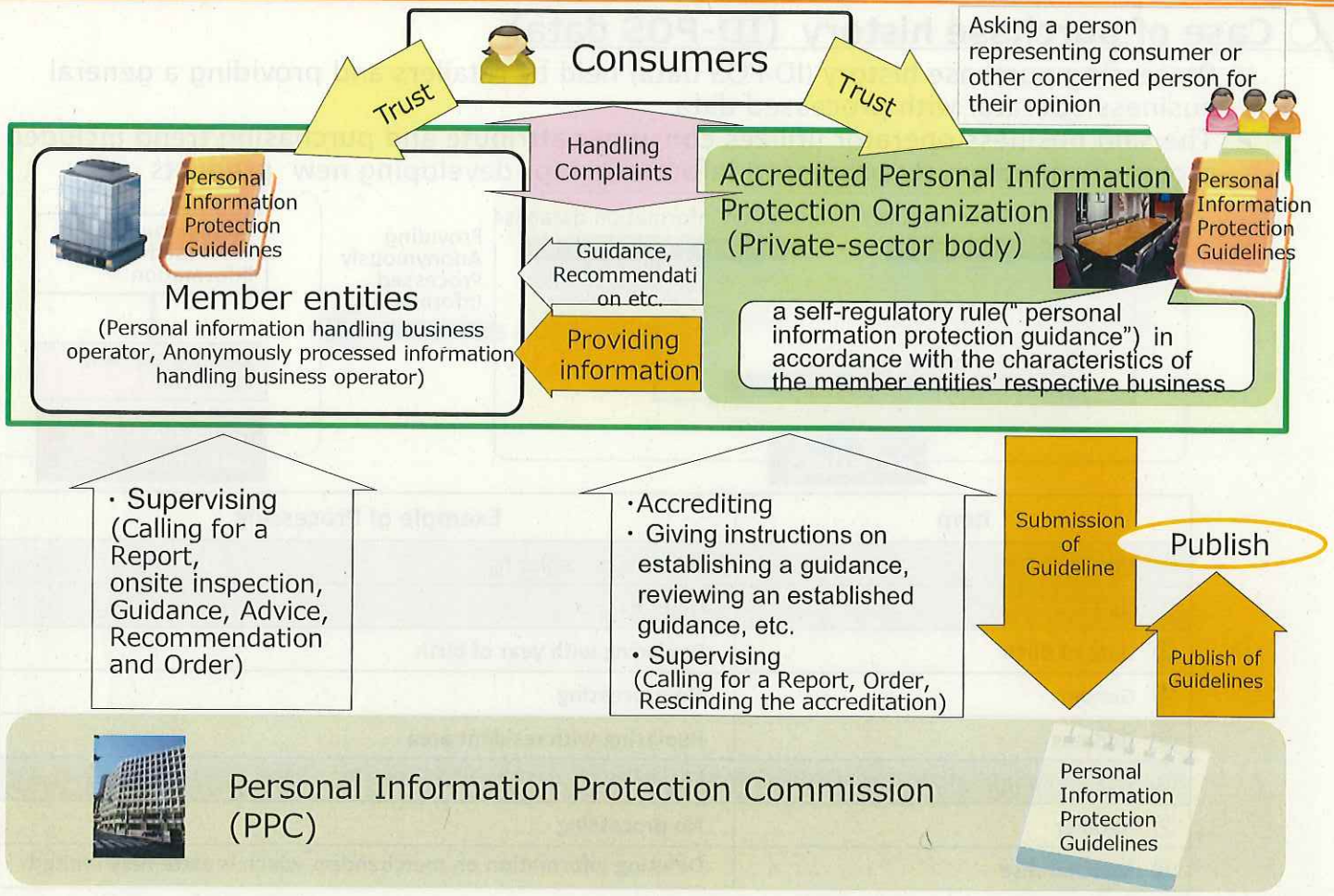
An auto manufacturer processes location information obtained through data communication module, and provide a general business operator (retailer) with processed information

The general business operator utilizes consumer attribute and moving history data included in provided anonymously processed information for store opening plan etc.

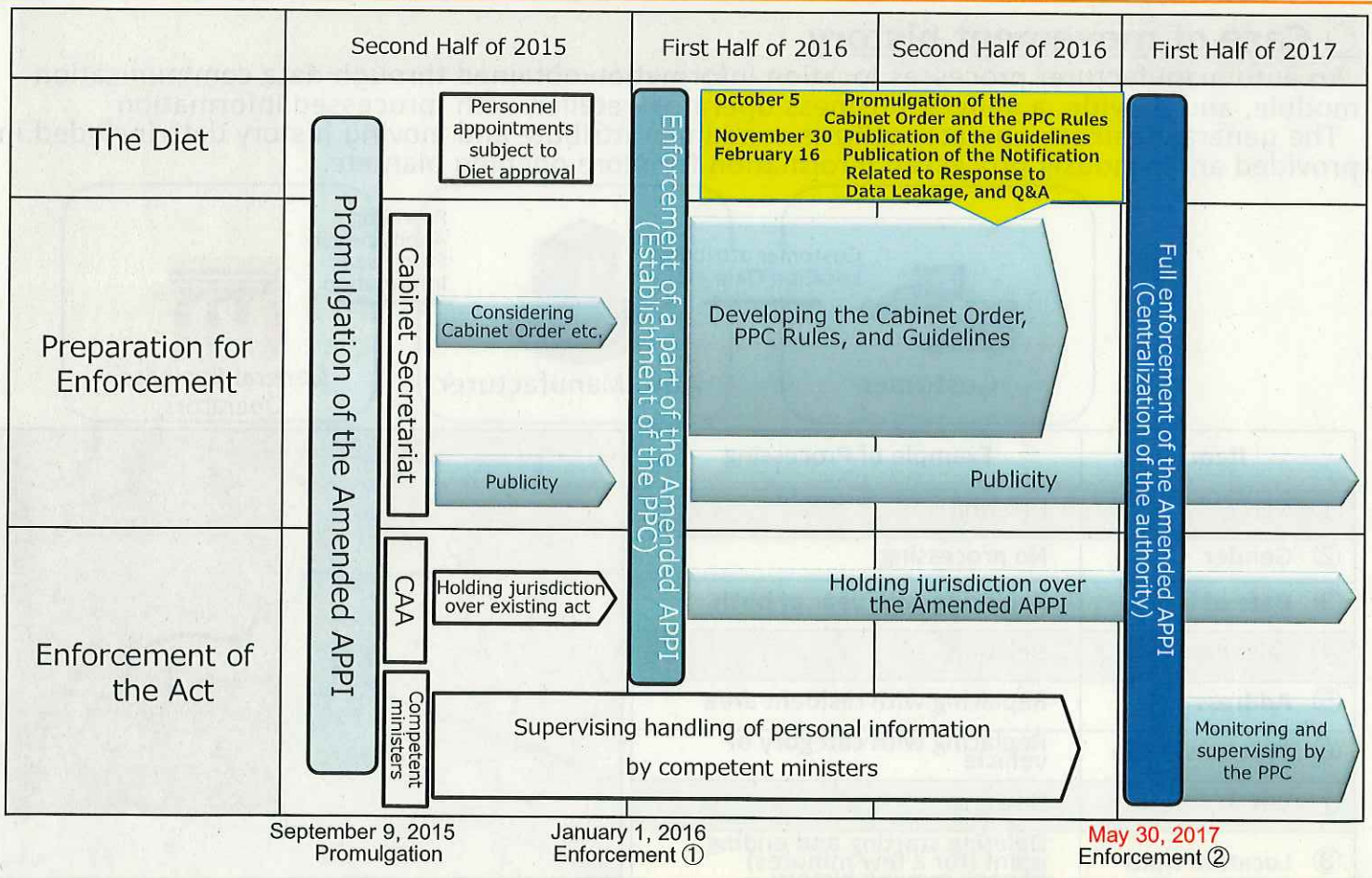
Item	Example of Processing
① Name	Deleting
② **Gender**	**No processing**
③ **Date of birth**	**Replacing with year of birth**
④ Telephone No.	Deleting
⑤ **Address**	**Replacing with resident area**
⑥ **Type of vehicle**	**Replacing with category of vehicle**
⑦ VIN	Deleting
⑧ **Location Data**	**Deleting starting and ending point (for a few minutes) of each moving history**



Accredited Personal Information Protection Organization



Schedule



Thank you !

Kuniko Ogawa
ogawa-k5pw@ppc.go.jp

Thank you !

Kuniko Ogawa
ogawa-k@ppc.go.jp