行政院所屬各機關因公出國報告書

(出國類別：出席國際會議）

出席 2022 年 11 月
「全球 CBPR 論壇：實現我們的共同願景」
The Global CBPR Forum: Realizing Our Shared Vision
研討會暨相關工作小組會議

出國人員服務機關	職稱	姓名
國家發展委員會法制協調處	專門委員	吳欣玲
國家發展委員會法制協調處	專員	鄭美華
財團法人資訊工業策進會	專案經理	王德瀛

會議地點：韓國 首爾

會議時間：111 年 11 月 1 日至 11 月 4 日

完成報告：112 年 1 月 4 日

出席 2022 年 11 月「全球 CBPR 論壇：實現我們的共同願景」The Global CBPR Forum: Realizing Our Shared Vision 研討會暨相關工作小組會議

目錄

壹、 摘要

本次「全球 CBPR 論壇：實現我們的共同願景」研討會暨相關工作小組係由美國與韓國共同合辦，除舉行工作小組會議由澳洲、加拿大、日本、菲律賓、新加坡及我國等會員體針對全球 CBPR 論壇運作所需之相關基礎文件進行討論，並透過研討會向包括：巴西、智利、印尼、馬來西亞、泰國、英國、百慕達、杜拜金融中心等非會員國家／管轄權（jurisdiction），推廣 CBPR 跨境傳輸機制及進行相關能力建構，及與當責機構等相關利害關係人針對 CBPR 擴大工作之有關議題進行討論。

貳、會議情形

美國自 2020 年起積極推動「跨境隱私規則體系（CBPRs）」擴大工作，並於 2022 年 4 月 21 日推動成立全球 CBPR 論壇（下稱本論壇），我國為創始成員之一，迄今已有日本、新加坡、加拿大、墨西哥、韓國、菲律賓、澳洲等國加入。為持續與各會員體共同合作推動本論壇之運作，並汲取相關國家於國內推廣 CBPR 體系之經驗，爰由國家發展委員會法制協調處吳欣玲專門委員、鄭美華專員，及我國 CBPR 體系當責機構財團法人資訊工業策進會王德瀛經理共同參加本次會議，會議重點摘述如次：

■ 全球 CBPR 論壇工作小組會議【11 月 1 日】

本次工作小組會員會議，我國、美國、日本、韓國、加拿大、菲律賓、新加坡等實體出席，澳洲線上出席，墨西哥未出席；與潛在會員會議部分，除上述代表外，英國、百慕達及杜拜金融中心實體出席，馬來西亞線上出席。

一、 針對全球跨境隱私規則論壇未來應採取何種會員體制，以及應如何把關新成員加入的條件，新加坡與日本合作提出初步文件供與會人員討論。

二、 經工作小組會議討論後，對於是否要就利害關係人特別設置「觀察員」的會員體制或是一律作為一般非會員(non-participant)看待，尚無定論，爰先就會員與準會員條件為初步整理，以作為與潛在會員討論的基礎。

三、 針對上開會員體制設計，英國、杜拜金融中心(DIFC)、百慕達及馬來西亞等潛在成員意見重點如次:

1. 針對意向書應由資深技術官員或其他政治性代表等何種層級作成，英國建議可以混合方式作成，例如:由資深官員提供推薦信，並附上較低層級的技術性文件說明。

2. 英國及百慕達強調其國內隱私執法機關為獨立監理機關，與政府部門互不隸屬，故政府部門作成之意向書無法代為表達獨立監理機關之參與意願；反之亦然。

3. 美國認為準會員實際上係成為正式會員的暫時過渡機制，其目的係為讓提出申請加入者在獲准加入前即可參與本論壇會議討論的機制；惟英國表示此種概念實質上等同申請成為「正式會員」而非「準會員」，亦即必須在申請時候即符合申請加入隱私執法協議(CPEA)等所有條件，而非可先符合部分條件，待其他條件準備就緒後再申請成為正式會員，對於英國無法由政府部門代表國內獨立監理機關加入 CPEA 的情形，恐怕無法適用。

四、結論: 後續將考量潛在會員的相關意見後再修正文件。

■ 全球 CBPR 論壇研討會【11 月 2 日至 4 日】

一、全球 CBPR 論壇之更新（Update on the Global CBPR Forum）

美國商務部 Shannon Coe 簡介 CBPR 的發展歷史與近況，及 APEC 隱私綱領的相關原則，並表示發展 CBPR 體系可以作為企業展現其法遵能力的基礎，確保消費者的個人資料不論傳輸至何處均能受到保護。

二、分組會議及結論分享（Breakout Sessions）

（一） 第 1 組：關於如何建立 CBPR 程序（How to establish a CBPR Program: Ask the Experts）

本場次主要提供有興趣的潛在參與者，向當責機構(AA)與企業，透過問答的方式，詢問參與 CBPR 體系的相關問題，以作為非會員體及未設置 AA 會員體的參考。

本場次與談者包括二位企業代表（Cisco、APPLE），及五位 AA 代表（我國、新加坡、韓國、美國二位）。討論議題包括：

1. 提問：現在有 9 個會員，但只有 5 個 AA，是否各經濟體在設立 AA 上有任何的困難或阻礙？有無設立 AA 時應注意的事項或訣竅？

   答：AA 設立的標準和要求在各經濟體間都是一致的，有些經濟體正在研議設立中（如菲律賓），但有些因為還不具經濟規模（如加拿大），所以目前無設立的規劃。由於 AA 的工作非常的專業，且需確保獨立性，因此在人員的訓練、認證過程中獨立性或透明性的維持、以及如何在服務整體的表現取得顧客的信任等等都是應特別注意的事情。

2. 提問：擔任 AA 的適格主體、如何避免利益衝突問題，例如:企業是否會因 AA 於認證過程中發現有違失之情形，而承受 AA 向主管機關舉發的風險？

   答：在認證過中，AA 是在協助企業符合規範，建立能力等。尤其在亞州國家，大部分 AA 都是半官方色彩，甚至新加坡的 AA 就是由政府機構擔任，多是立於協助企業取得認證的角度提供協助。

3. 提問:除可符合部分國家內國法跨境傳輸限制的例外條件外，企業參與 CBPR 體系是否有其他好處？

   答：企業，尤其是中小企業，多難以掌握個資法規的內容，跨國的法規更是困難。透過 CBPR 認證的程序可使企業取得其就個資保護符合法規的證明，展現企業法遵及重視個人資料的保護，以進一步取得客戶的信賴。

4. 中小企業通常較無資源或經驗，其在取得認證過程中，可能面

臨什麼困難？如何提供協助？

答：CBPR 的規範及要求很明確，但通常中小企業無專人處理或了解認證過程，將可能造成認證流程中溝通或調整的困難，仍而中小企業可以選擇適合的認證階層以取得認證，在執行上應無太大問題。至於提供協助的部分，通常沒有足夠的資源或全職的人力去推動或接受訓練，是中小企業與大公司在推動認證過程中最大的不同，透過宣導或教育訓練，或如新加坡以提供經費或補助方式鼓勵 SME 參加，均為可採行的方式。

（二） 第 2 組：關於推動 CBPR 之更新（Updates on promoting CBPRs）

本場次主要針對如何促進 CBPR 體系參與進行互動討論，由美國商務部 Sarah Pham 擔任主持人，講者包括美國國務院 Geoff Gertz、新加坡資通訊媒體發展局資深經理 Shi Min Cheng，及當責機構代表美國 TRUSTARC(TRUSTe 母公司)全球隱私處處長 Noël Luke、財團法人日本情報經濟社會推進協會資深研究員 Mizushima Tsukumo。討論重點如次：

1. 目前當責機構在推廣 CBPR 體系時，經常遭遇企業可能對於 CBPR 體系可能有的誤會或問題包括如：企業一旦取得 CBPR 認證即等於其已符合所有亞洲地區的隱私法規；或是 CBPR 認證係由政府機關直接授予；以及對於跨國企業而言，應選擇在哪一個管轄權接受驗證程序等，顯現企業對於 CBPR 體系的認識仍有待加強。

2. 關於如何推廣 CBPR 體系，講者認為促進社會大眾對於 CBPR 的瞭解是重要關鍵之一，包括透過國際間、政府與當責機構共同合作等方式，促進企業對於 CBPR 體系的認識。此外，推廣策略上，建議著重 CBPR 認證為政府背書的國際隱私標章，並應提升企業對於 CBPR 認證能促進消費者對於該企業個資保

護能力信賴的認知。

3. 主持人另提及推廣期間降低認證費用或亦為可行的策略之一，例如韓國當責機構韓國訊息安全局(KISA)即在今年推廣期間豁免相關費用。然部分講者表示其實降低費用對於企業申請數量的提升並無顯著效果，認為重點恐怕還是在認知推廣上，必須加強說明 CBPR 能如何增進消費者對企業信賴。

4. 日本目前的隱私標章分為兩種，其一為 CBPR 認證，另一為 PMARK 標章。前者是瞄準國際傳輸，取得者為大型企業；後者則屬於國內的隱私標章，多適用於非瞄準國際市場的中小企業。至於為何中小企業較少申請 CBPR 認證，講者表示可能是基於成本的考量，無國際傳輸的需求即無申請 CBPR 認證的誘因；另有觀眾補充，也可能是因為 PMARK 在日本國內推廣已久，較為民眾孰悉之故。主持人對此表示，透過國內法與 CBPR 體系要求的比對，CBPR 標準其實也具有協助企業遵循國內法的功能，建議未來或可結合二者。

三、CBPR 認證軟體演示（CBPR certification software demo）

美國商務部 Shannon Coe 展示並說明由美國開發完成的 CBPR 認證軟體，將免費提供 AA 及受認證的企業使用。並宣布將與我國當責機構資策會展開測試合作。另程式碼亦將對外公開，可由下載的使用者自行依其需求進行調整。現在已有沙盒（sand box）供大家測試，如果有任何問題或建議，歡迎提供我們參考改進。

四、監理者圓桌會議（Regulator Panel）

本場次由菲律賓法務部副部長 Geronimo Sy 主持，並由相關監理者代表針對執法合作、如何透過 CBPR 體系促進法遵與跨境傳輸信任，以及

CBPR 體系如何協助跨國公司及法規制定者確認各國資料保護法體系等議題進行討論，各講者發言重點如次:

（一） 墨西哥國家資訊透明與個資保護局 Louise 表示墨西哥「保護私人持有個人資料的聯邦法律 (Federal Law on Protection of Personal Data Held by Private Parties) (LFPDPPP)」是在 2010 年 7 月發佈，規範由個人或私營部門之合法實體所執行的個人資料處理，此外，工會聯盟核准各項法規，規範了資料隱私權，其中包含「保護義務方持有個人資料的一般法律 (General Law on Protection of Personal Data Held by Obligated Parties) (LGPDPPSO)」，其規範公共部門的個人資料處理。可存取個人資料的資訊和保護的「國家透明度組織 (The National Institute of Transparency，INAI)」，是墨西哥的自治憲法機構，負責確保法律及相關法規之合規審查。2019 年 1 月美加墨自由貿易協定(USMCA)第 19 章數位貿易已承認 CBPR 體系為有效的跨境傳輸保護機制，相較於 GDPR 是更具彈性的跨境傳輸機制，且對非 APEC 會員開放參與，將可使以數位傳輸做為全球發展為趨勢的情況下，適用於更多管轄權。

（二） 巴西國家資料保護署(ANPD)Ailana Linhares de S. Medeiros 簡介「巴西一般資料保護法」("LGPD")巴西個資法的發展歷史及憲法定位，並說明該署如何執行其跨境傳輸法規。LGPD 是巴西為保護個人資料所採用的主要規範，於 2018 年 8 月 14 日通過，並於 2020 年 8 月 16 日生效，雖在此之前有類似消費者保護法中有規劃個人資料保護，但都不全面。

LGPD 適用於公共或民營部門的個人或法律實體對個人資料的處理，而無論其使用什麼處理方式或控制者或資料位於哪個國家，只要其符合以下條件：1、 在巴西境內處理資料，2、 處理的目的在於提供產品或服務，或者在於處理身處巴西的個人的資料，又或者

3、 在巴西境內收集個人資料，就必須遵守 LGPC 的規定。

LGPD 建立了有關處理個人資料的原則和規範。組織必須能夠展現出採取措施以證明其符合個人資料保護規則的能力，包括此類措施的效能，從而促使制訂並實施適用於個人資料處理的合規性政策。依照 LGPD，控制者和處理者 須採取技術與管理措施，防止未經授權存取個人資料或者此類資料在意外或非法情形中被損壞、遺失、變更、流傳，或者任何形式的不當或非法處理。另外，LGPD 授予巴西國家資料保護機構 (ANPD) 建立由控制者和處理者實施的最低技術標準的權力。

（三） 杜拜金融中心(DIFC)資料保護委員長辦公室法務與資料保護副處長 Lori Baker 介紹該中心特殊的自由區(Free zone)起源與定位，包括以普通法(common law) 作為體系基礎、以英文為主要語言，享有自治法權。又 DIFC 於設立時即參考歐盟 1995 年個資保護指令訂定個資法，並於 2020 年進行修正，修正時並非僅借鏡 GDPR，尚參考包括如美國加州隱私法(CCPA)和其他國家的規範。個資法的保護在 DIFC 是個很重要的議題，尤其是在金融科技如 Blockchain、fintech 等重要運用的前提下，作為世界金融中心之一，如何確保資料以及個人資料及運作體系的完整非常重要，企業尤其希望在進行跨國資料傳輸時能有更明確且可信任的機制供他們在實際操作時參考，我們亦有提供相關規範指引及建議供企業使用。我們對於如何在安全及明確的前提下進行全球資料傳輸非常的關心，也在思考未來規劃方向，包括是否設立 AA?或採用新加坡模式等，希望能多參與並與大家交流。

（四） 日本個人情報保護委員會(PIPC)國際研究處處長 Junichi Ishii 強調跨境執法合作在高度數位化時代的重要性，並表示 PIPC 確有碰到一些個案，比如對於伺服器架設於境外的違法者，面臨無法直接調

查的困境，必須透過跨境執法合作才能解決，這樣的情形未來勢必更加頻繁發生，而如可透過透過研討會可以學習如何使用 CPEA 等跨境合作的機制，應可以有效解決相關問題。

（五） 菲律賓國家隱私委員會法務處律師 Josefina E. Mendoza 表示菲律賓《2012 年資料隱私權法 (PDPA)》已於 2012 年 9 月 8 日生效。這項法案連同最終實施規則及規範 (IRR) 是菲律賓管理資料隱私權的法律依據。PDPA 中闡明資料控管者與資料處理者的義務，並將特定權利延伸至資料當事人。此外，該法律也授予負責執行及監管法律的國家隱私權委員會 (NPC) 制定規則的權力。菲律賓個資法與 APEC 隱私綱領原則高度相仿，因此 CBPR 體系可有效協助該國企業展現其執法能力。另菲律賓高度仰賴境外企業的投資，因 CBPR 體系的跨境執法合作機制亦具有重要性，可以縮短不同管轄權內監理者之間的差距，並有助於增加民眾對於跨境傳輸的信賴，菲律賓目前已兩度運用 CPEA 機制，尤其是主要企業體在海外的情況；另規劃將設置境內 AA，刻正由 NPA 進行審查程序。

五、處理者隱私認證（PRP）案例分享（The Case for the Privacy Recognition for Processors）

HP 全球隱私策略長暨歐盟資料保護長 Jacobo Esquenazi 分享 HP 藉由 PRP 體系以符合供應商盡職調查(vendor due diligence)要求之旗艦計畫。其表示鑒於 CBPR 體系自願性機制的本質，導致即使 HP 願意對合作廠商提供補助費用，願意參與計畫者的企業仍寥寥可數。在最初針對高風險且最相關的行銷廠商（marketing vendor）進行計畫推動，但僅 2 家廠商參加。我們有大約 150 家廠商，其中有 6 家願意但還未進行申請，而 9 家已提出申請的廠商，亦僅 2 家完成。因此若非強制要求恐怕自願參加者不多，他們多反應沒有時間、資源以及一年後的再認證及後續維持認證多影響其參與意願。目前該計畫將繼續延長一年，但由於計畫結束

後廠商仍需自行負擔每年認證更新費用，因此應該思考降低認證費用，以及如何擴充 CBPR/PRP 體系爭取更多監理者背書，充分展現此體系為企業法遵及社會責任的實現，以及企業可因此獲得的益處等，如此才可能有效提升其參與意願。

現場來賓問及針對已通過認證的二家廠商，有無任何的意見反應或經驗可與大家分享？以及促使他們願意參與認證的誘因為何？E 氏表示其中一間是只有 2 人的小公司，雖然他們無多餘人力專責處理認證事宜，但透過計畫顧問提供改善建議，協助取得認證，從他們的經驗看來取得認證應非難事。雖然 HP 並未強制其參加，但由於通過認證可以證明其公司在隱私保護的重視，增加與其合作企業的認同度，應為其願意參與認證的主要考量。

六、CBPR 體系與內國法圓桌討論會議（Panel Discussion on CBPRs and Domestic Law）

本場次由百慕達隱私委員會委員 Alexander White 主持，主要針對如何於國內法律體系內運作 CBPR 及 PRP 體系，及與其他跨境傳輸機制之比較等議題進行討論，各講者發言重點如次:

（一） 國際隱私專家協會華盛頓特區管理處長 Cobun Zweifel-Keegan 說明 CBPR 體系建立的基礎源於美國無一般性的聯邦個資法，係由聯邦貿易委員會(FTC)依聯邦交易委員會法起訴違反自願性承諾而不法侵害消費者隱私的企業。CBPR 體系在美加墨協議中已被承認是有效的個資跨境傳輸機制，希望能逐步推廣為全球性的機制。相較於歐盟 GDPR 採取由監理者由上而下的確認規範內容並管理企業，CBPR 採取由下而上的企業自願性承諾機制更具彈性，並可在欠缺個資法的情況下保障消費者隱私。

（二） 加拿大創新科學經濟發展部資深政策顧問 Jill Paterson 表示加拿大

很早就認知到在貿易及數位經濟時代，資料傳輸及資料保護的重要性並做了規範和限制。為了避免資料在跨境傳輸時受到不必要的限制，加國制訂政策鼓勵企業取得認證，尤其是可透過類似 CBPR 等體系取得一個廣泛且一致性的認證，此外我們也提供企業諮詢以協助他們採行適合的機制，但在個資保護委員會的人力及資源有限，而任務日漸多元的情況下，我們也正在思考調整機制，近期並規劃修法納入 CBPR 認證，主要是考量 CBPR 體系在美加墨協議中已被承認是有效的個資跨境傳輸機制；此外，加拿大的個資保護委員會對於調查處理案件具有廣泛的裁量權，我們也建立一定的規範和流程以進行企業遵守隱私保護行為之調查。我們認為有效證機制的設立可有效確保企業在通過認證後即減少被控為侵害個資保護的風險。例如，企業如取得有效認證，即便有發生個資事件，如果其經認證已採行必要的個資保護措施，應可被認為非故意（not intent）或非有意為之，而不違法，委員會得不對該企業施加行政處罰。如此應可以創造企業申請認證並強化其個資法令遵行的強大誘因，並可平衡機關在調查處理個資侵害事件的負擔，我們希望能在一年內完成修法。

加拿大亦已取得歐盟 GCPR 的適足性認證。適足性認證與 CBPR 體系最大的不同就是適足性認證是由政府為主體去進行，責任非常重大也須投入極大的人力及物力，相較於 CBPR 是由企業或組織自行認證，CBPR 的方式是比較有彈性的，也有助於企業盡早完成後續安排。未來如 CBPR 可以順利推展為全球化的認證及傳輸機制，將可對企業於資料傳輸流通及安全的防護有極大助益。

（三） 英國數位文化媒體體育部(DCMS)資料政策處處長 Hattie Davison 表示英國原則禁止跨境傳輸，但有多種機制可以構成合法例外，包括: 適足性認定、標準契約條款(SCC)、企業拘束性準則(BCR)、行為準則與認證(尚在發展中)等。在英國，DCMS 為政府部門負責發展政

策，個資保護監理者則為資訊委員辦公室(ICO)(線上參加)，沒有當責機關(AA)。英國刻正進行修法，目前正在議會審理階段，盼能確保資料流通的價值、規劃清楚可預見性的法規，並尊重各國的隱私文化。

（四） 日本經產省國際數位政策協調處處長 Makiko Tsuda 簡介經產省針對跨境傳輸機制與資料在地化的最新研究成果。該報告比較各認證機制，包括國際規則（CBPR/PRP）、法規、跨境傳輸機制和其他數據保護機制。雖然每個系統都獨立於其他系統，但它們相互影響，並且近年來，於 OECD 以及 APEC 等國際組織隱私原則的發展多有共同點，此外許多國家或地區都已制訂自己的規則，且越來越多國家採取類似於 GDPR 的法規。此外根據每個國家/地區的法規，亦有多種認證機制且多具有共通性。此外，跨境轉輸機制亦非常多元，且各種個人數據保護工具所需的內容列表幾乎相同，即使在沒有 GDPR 類似法規的國家（例如中國），採行標準契約條款（Standard Contractual Clauses，SCC） 也越來越受歡迎，並已在許多國家/地區採用。由於相關保護工具間共通性逐漸提高，各國均逐步提高並改進其間的連接性和互操作性。例如在韓國，已整合其國內個人資料保護相關的認證；台灣亦可同時獲得個人數據保護認證（dp.mark）和 CBPR。該報告之完整內容將於明年 3 月上網公開(目前僅日文版)，提供各界參考。

（五） 日本個人情報保護委員會國際研究處處長 Junichi Ishii 表示 CBPR 是日本納為個人資料跨境傳輸一個很重要的機制，日本 2015 年個資法修正後所納入的三種個資傳輸機制，包括:各國或區域間適足性認定、安全維護措施、當事人同意等。CBPR 體系在日本被承認為安全維護措施其中一種，不論是在境內的資料傳輸或是境外，但源自歐盟的個資不能透過CBPR認證再傳輸至日本以外的國家。CBPR體系雖可使國際間的資料傳輸更為安全且便利，但是否可以被有效

運用就取決於是否能有更多經濟體加入，我們應該共同來思考如何推動並擴充參與經濟體的可能性。

（六） 南韓個人資料保護委員會(PIPC)國際合作處長 Jungsoo Byun 表示南韓目前就個資保護有二套機制，其一為國際的傳輸保護機制，另一則為國內內的認證機制 ISMS-P。南韓的個資法的跨境傳輸機制以當事人的知情同意作為合法傳輸條件，惟因國際傳輸需求日增，並為符合國際標，PIPC 已提出第二次修法草案，除當事人同意外，並將納入包括適足性認定（如歐盟 GDPR）等傳輸機制。並簡介 2018 年韓國 PIPC 與科學資訊技術部(MSIT)合作推動的國內隱私認證機制 ISMS-P。

（七） 現場來賓問及依據歐盟最近的判決，似乎取得適足性認定的國家或經濟體並不能保證就可通行無阻，而是認為個別企業在為跨境傳輸時，仍須盡到審慎注意（due diligent）。在 CBPR 的情況下，是否當企業如與其往來的企業亦取得 CBPR 認證時即足以認為其已盡到審慎注意？或是仍應有其他的要求？與談者多認為此問題很難回答，且非如科學問題可被印證，恐怕得看各國實務及個案情況而定。

（八） 現場來賓問及目前除了新加坡及日本外，並未有國家或經濟體於法規中明定 CBPR 是被承認的機制，此與須透過政府取得適足性的 GCPR 有很大的不同，也會使 CBPR 是否可被採為有效的機制產生很多的不確定性。與會者表示於各國法規中明定多須要花很多時間，有相當的困難性，且亦會失去彈性，亦有與會者認為 CBPR 也是 GDPR 中所定的一種認證方式，再者 GDPR 第 46 條亦規定如可有安全維護措施亦為一種方式，重點是確認相符性，與是否於各國的法規明定應無影響。

七、英國數位文化媒體體育部國際資料傳輸處副處長 Joe Jones 致詞（Keynote remarks）

Joe Jones 表示，本次代表英國政府前來，主要為達成三項任務：第一是向外發展，因為單一個國內法規體系可做的極其有限，一個獨立於外的體系將失去其存在的意義；第二是與他人學習及合作，因為其他國家的傳統歷史、採用方法，可以帶來新的啟發及異中求同；第三是針對資料傳輸的框架、解決方案及挑戰做出貢獻，以達成如本次研討會主題—「實現我們共同的願景」。數位科技讓世界變得更小、更為緊密，並深化企業與國家之間的國際關係，個人資料現已成為產品的核心，高度連結的世界日益仰賴個人資料的流通與跨境使用，其不僅帶來經濟成長、提升生產力、解放科學進步、協助執法、促進公共服務的提供，故做好相關的工作具有史無前例的重要性。然即便我們意識到其重要性，現今仍存在破碎化、保護主義政策的威脅，全球市場對於如何展現對資料跨境使用的信賴亦存在著鴻溝。透過本論壇的創意與領導力，能夠發揮影響力以發展、設計一套足以擴大與可信賴的機制。英國自豪於其歷史悠久的高度資料與隱私保護規範，包括從 1970 年起探討資料保護的概念、成為 108 號公約的首輪締約國，並在近年的英國及歐盟 GDPR、執法指令等扮演主動角色，持續致力與其他管轄權合作制定嚴格的個人資料保護標準。因此，參與本論壇並共同發展足以擴大與可信賴的機制，對於英國而言是重要的機會。

八、如何展現法遵並接軌 CBPR（How to demonstrate CBPR Requirements and Mapping）

（一） 全球隱私與資料智庫—資訊政策領導中心（Centre for Information Policy Leadership, CIPL）副主任及資深政策顧問 Markus Heyder 過去在美國聯邦貿易委員會（FTC）工作期間曾代表該會參加 APEC 會議，並從 2005 年開始參與 CBPR 體系的相關工作，2014 年起任職於 CIPL。Heyder 表示，任何一個欲參與 CBPR 體系的經濟體，都必須將其國內法規與 CBPR 體系進行比對，以判斷是否能於境內

執行 CBPR 相關要求、檢視其間的落差，並決定如何處理該等落差。

執行 CBPR 體系要求有兩種可能做法，其一係透過執行與 CBPR 要求相當的國內法規，以間接落實 CBPR 體系；抑或是如美國，由國內的不正交易主管機關 FTC 針對企業對大眾所為的欺罔行為（例如：宣稱遵守 CBPR）進行執法。在後者的情形下，經濟體只要指出該執法機關即可。如果比對的結果是國內法規較 CBPR 體系要求嚴格，則取得認證的企業必須再額外符合國內法規的要求，但該經濟體無須採取其他措施，蓋 CBPR 的規則及程序明定取得認證的企業必須遵循 CBPR 體系要求及額外的國內規範，因此國內規範恆為 CBPR 體系的一部分，即便 CBPR 認證不適用於國內法規。倘比對的結果是 CBPR 體系要求比國內法規嚴格，則經濟體必須決定相關落差是否重要，並採取如修法或尋找替代機制等措施，以加入 CBPR 體系。

CIPL 在去年針對 APEC CBPR 體系、歐盟－美國隱私盾及 UK GDPR 之異同進行比較研究，以下即就該研究成果之重點進行說明，以作為 CBPR 潛在申請者評估其加入可能性之參考：

1. APEC CBPR 體系與 UK GDPR 相關規定的重疊率達 61%；歐盟－美國隱私盾與 UK GDPR 相關規定的重疊率則有 67%。值得注意者，與 UK GDPR 沒有相同的規定並不意味其保護水準較低，特別是在討論適足性（adequacy）方面，蓋被認為具有適足性的隱私盾與 UK GDPR 的重疊率只有 67%，因此可以推論與 UK GDPR 具有 61%重疊率的 CBPR 體系，亦可如個資法一般，被認為具有一定程度的 GDPR 適足性。

2. 要針對使用不同定義、觀念的法體系進行比較分析具有一定的困難性，必然需容有一定的爭議性與不同意見，為盡可能達到正確性，本研究因此使用「直接符合」、「間接符合」及「不

符合」等用語來表達其間的重疊性。而隱私盾在「直接符合」的比率上較 CBPR 體系更低，但卻也被認為具有適足性，因此適足性其實並非指完全一致，而是指大致相當。

3. 要檢視符合性，並應進一步比對具體的規範內容，及判斷相關內容的保護水準，其中可以發現一些 CBPR 體系要求較 GDPR 更為嚴格的部分，例如 CBPR 體系並無公共利益或正當利益之合法事由，僅以當事人同意作為處理個人資料之合法性基礎，而當事人同意被許多專家學者認為是更嚴格的標準，因此雖然具爭議性，但在或可說 CBPR 體系在這部分顯現較 GDPR 更高的保護水準；又或如與監理機關合作方面，CBPR 體系除有相仿規定外，並更詳載取得認證的企業應如何與監理機關或執法機關進行合作，因此在這方面亦與 GDPR 直接相符。

4. 至於 GDPR 有但 CBPR 體系沒有的規範，不意味 CBPR 體系的保護就比較低，例如以圖示作為透明性工具、公告資料保護官（DPO）相關資訊等，就 CBPR 整體透明性、專責人員的要求來看，即使沒有如 GDPR 上開鉅細靡遺的規範，也並非保護較低；或如行政罰鍰部分，CBPR 體系保留由國內法規或 AA 提供消費者相關的救濟措施，因此即便未作規定，仍然存在與 GDPR 相當的保護水準，其他如從設計保護隱私、資料轉傳等情形亦同。

5. 另 CBPR 與 GDPR 不相符的部分，包括如：不適用於已公開的資料、就兒童資料或兒童同意未有相關規範、欠缺敏感性資料的概念、間接蒐集資料無須告知、無個資侵害事故通知或個資影響評估之要求，及缺乏多種當事人權利（例如：自動化決策），是 CBPR 被認為保護水準較 GDPR 低的部分。但即便如此，值得注意的是，隱私盾亦未納入上開規定，卻仍被認為具

有適足性，因此即使不具備該等規定，亦未必表示不具有適足性。

（二） 美國聯邦貿易委員會國際消費者保護與隱私顧問Michael Panzera先介紹FTC為消費者保護主管機關，對隱料與資料安全有廣泛的管轄權，其下設隱私、執法等專責部門，並另有研究與調查部門，以便在涉及新興科技利用資料時，協助隱私或執法部門瞭解相關情形。FTC運用美國法下「不公平與欺罔行為（unfair and deceptive conduct）」此一廣泛的法律概念，起訴在隱私脈絡下有詐欺（misrepresentation）行為的企業，包括無理由對消費者造成重大損害者、對消費者可能造成損害的資料處理行為等。此外，FTC也負責執行各個部門性的隱私法，包括涉及兒童線上保護、金融資料、信用資料等。關於涉及CBPR部分，FTC的職責主要在於確保宣稱取得CBPR認證的企業名實相符，曾經針對軟體供應商、行銷公司等謊稱取得認證的企業執法，未依和解協議改正的企業並會受到民事懲罰；針對在隱私權政策內謊稱參與CBPR體系的企業，FTC得發送警告信函，限期該公司採取法遵措施，或刪除相關陳述。否則亦將面臨執法行動。

（三） Panzera另針對加入CBPR之先決條件—跨境隱私執法協議（Cross-border Privacy Enforcement Arrangement, CPEA）進行介紹：

1. CPEA 旨在監理者之間建立自願性的合作網絡，以協調跨境執法或協助國內執法。透過參與經濟體的隱私執法機關、資料保護監理機關間的資訊分享，以建立有效的跨境合作機制，包括通報、併行或共同調查等。此外，CPEA亦鼓勵與框架以外的主管機關進行資料分享及合作。

2. 關於跨境合作，CPEA 建立可供參與經濟體間互相請求協助的體系，請求分享與調查中案件或執法行動有關的資訊。CPEA亦容許經濟體獨自或共同依照案件的優先性（例如隱私侵害行為

的嚴重性、實際造成的損害等）進行安排。CPEA 並針對跨境合作交換資訊的使用訂有具體規範，供請求及被請求機關依據個案情形共商，以確保資訊的使用符合相關國內規範。

3. 值得注意的是，任何參與的執法機關均有權拒絕接受合作請求，或限制合作的範圍，因此提出請求不代表對方即負有合作的義務，被請求的機關可能基於與國內法規不符、非職權範圍內、資源有限等考量因素拒絕請求，並可將拒絕的理由以書面通知請求機關（非義務）。CPEA 並規定參與的執法機關得將可能的個資違法行為，通知另一個參與的執法機關，以供其採取適當作為。

4. CPEA 的保密規定亦具有關鍵重要性，即分享的資訊必須保密不得對外揭露，取得資訊的執法機關必須盡最大努力保持其機密性，並尊重提供方所尋求的任何保護措施。如果有公民（團體）依如政府資訊公開法等國內法規要求揭露資訊，應注意 CPEA 並未禁止請求方依其國內法規向第三人揭露該等資訊，因此在揭露之前，請求方必須先說明依法在何種情形下必須揭露該等資訊。請求方**有義務**在揭露的 10 天以前，將任何形式的揭露告知提供方；此外，請求方必須竭力依其國內法規拒絕對第三人揭露，不能僅是毫無作為。

5. CPEA 有關安全及保存的規定亦值得留意，執法機關應採取適當措施避免依照協議取得的資料滅失、遭非法取用等；資料保存亦不得逾法定或必要期限。另為避免聯繫上的困難，協議亦包含各執法機關的聯繫窗口，及其實務、政策及活動說明，以利其他參與者瞭解該經濟體內的情況，並可向正確的窗口遞交請求。CPEA 亦包括人員交流、訓練事宜。關於合作所需的費用方面，CPEA 原則上盼能各自負擔，但亦不排除雙方得依照個案

情形，針對費用負擔部分自行協商。最後，CPEA 並提供制式表格供請求方使用。

九、重新檢視 CBPR 程序要求（Review of CBPR Program Requirements）

（一） 本場次主要延續前次夏威夷研討會討論的基礎，針對先前當責機構們檢視 CBPR 計畫要求之成果進行進一步的討論，並由美、新等國當責機構代表及企業針對 CBPR 計畫要求之內涵與形式進行討論。本場次引導討論的代表包含：新加坡資訊通信媒體發展局（主管機關且同時為該國當責機構）Evelyn Gho、美國當責機構 Truste 代表 Joanne Furtsch、美國當責機構 Schellman 代表 Chris Lippert、美國當責機構 BBB National Programs 代表 Dona Fraser 以及企業代表美國 Stripe 公司 APAC 隱私長 Willem Balfoort 等。

（二） Truste 代表Joanne Furtsch 分享此前各國當責機構之工作成果，表示已經將 CBPR 計畫要求（program requirement）由原先問卷方式改為要求標準的形式，以符合一般驗證活動之常態。此一改變獲得無論來自當責機構或企業界的代表及其他與會者之同意，咸認此種方法有助於消除業者對於標準之困惑，也避免問卷形式可能造成不當的引導效果，導致評估失準。

（三） 除確認前階段工作成果外，與會者亦討論於下一階段調整要求事項時，可以考慮的內容。較具有共識的項目包含個資事故通知等目前大部分國家規範均有，但 CBPR 沒有之項目。其中，有關增加事故通知規範部分，係由新加坡個資主管機關代表 Evelyn Gho 所提出，其主要依據為多數 CBPR 會員國內國規範已有此類事故通知之規定，且亦為國際間通用作法，應加入 CBPR 規範中，以強化其實之保護效果。此外，Stripe 公司 APAC 隱私長 Willem Balfoort 建議於下一階段調整時，可以將「政府要求近用資料時的處理方式」以及新技術（如資料探勘等）的管理規範等議題納入思考的範圍。亦有與會

者建議可以探索資料可攜權等規範之可能性。在程序面上，則有與會者建議考量受驗證單位之負擔，及確保驗證品質的實際需要，或許不需要強制要求每年進行驗證，可適度延長驗證的週期。

（四） 在計畫要求修正的程序上，與會者建議在計畫要求修正時，應強化與不同利害關係人之溝通，並與（包含現有論壇成員及潛在有興趣成員在內的）管制者討論。在確定修正後，也應預留一定的轉型期，以使相關企業有時間調整因應。在後續計畫要求的運作上，Evelyn Gho 等與會者特別建議，可以考慮針對計畫要求中的部分內容（如「安全維護措施」的具體內容等），可以考慮以新論壇的立場，以指引等方式提供更進一步之說明。

十、非會員參與可能性圓桌會議（Panel for non-CBPR participants on possibilities for engagement）

本場次邀請非 CBPR 體系會員體，包括英國、百慕達、印尼、智利及巴西等政府或監理機關代表，分享其管轄權內目前關於個資保護、跨境傳輸規範的最新發展情形，及其評估國內參與 CBPR 的主要需求及加入可能面臨的挑戰為何：

（一） 英國

英國脫歐以後將 EU GDPR 調整為 UK GDPR，並據此與歐盟監理機關建立跨境傳輸的機制。從相關經驗我們認知到，適足性認定是一個耗費相當多資源、相當具挑戰性的過程，而可資運用的監理工具是單邊性或雙邊性，因此具有侷限性而難以擴大。我們曾針對英國的數位產業進行調查，並令人驚訝地發現世界上有約 70 個國家仿效歐盟採取適足性認定（或類似版本）作為跨境傳輸之工具，而這樣的現象可能造成重複性、破碎化的風險。英國在不知情的情況下受到其他國家的評估，由於該國家的資料可以傳輸到英國，或許是好事，但要瞭解整體市場全貌卻面臨重大的鴻溝。英國對於認證、

行為準則等資料隱私或跨境傳輸之工具並不熟悉，因此藉此探索、向其他國家學習這些我們過去未善加利用的工具，是很好的機會。

關於挑戰方面，可能是一旦有愈多的國家加入，要找到共同點就會更加的困難，相同的困境亦可見於 OECD、WTO。尤其個資保護基本上反映該國家的價值、文化與傳統，如果全面性地執著，便很難有所進展。因此如果能聚焦於結果，並接受各自有不同的做事方法，不論是透過法律、行為準則、市場機制等，以不同的方式達成相同的結果，則有可能克服相關的困境。

（二） 智利

基於對資料流通保持開放的立場，智利對於參與 CBPR 體系有高度的興趣。在智利與美國間的自由貿易協定（FTA），談論到包括資料自由流通、禁止計算機設備在地化等議題，在我們看來皆與 CBPR 體系的精神一致。此外，智利的貿易對象包括美國、歐洲及亞洲，因此我們主要的目標是在各個體系之間取得平衡，特別是促進不同體系之間的相容性，例如 CBPR 體系與 GDPR，以支持智利的中小企業。近 5 年來，智利持續在討論修法議題，但因此議題並非具有優先性，所以推動相當不易；但如果是與 CBPR 體系的相容性，由於智利已經有國內關於電子商務信賴標章的經驗，故評估要在國內推動 CBPR 標章應不構成問題，只要有資料保護主管機關可以加入 CPEA，就可以著手進行相關審查程序。

關於挑戰部分，或許是如何建立一個可以容納發展中國家、有特殊情形國家的體系等關於包容性的問題，包括針對如原住民等特殊族群的個資保護，也許未來也可以被納入CBPR體系或甚至是GDPR。

（三） 印尼

印尼今年 9 月甫通過個資保護法（PDP Bill），目前仍面臨的挑戰是監理機關的建立。在 PDP Bill 舊法訂有 跨境傳輸之規範，並課予

資料中心相關義務，資料跨境傳輸必須要履行報備義務。我們相信任何的傳輸機制都有相同的目標，亦即鼓勵企業實施良好的個資保護治理，特別是在進行負責任的跨境傳輸時。要加入 CBPR 體系，印尼尚須經過幾個階段，包括將 PDP Bill 與 CBPR 要求進行比對，如果評估結果是 CBPR 體系要求比較高，可能必須先退一步思考後續應採取的措施。

作為一個甫施行個資法的國家，最大的挑戰是如何從多個跨境傳輸模式中尋找最適合印尼的機制，而同時關切個資保護與跨境傳輸的 CBPR 體系為其中之一。現階段印尼必須確保 CBPR 體系等傳輸機制與 PDP Bill 相符，並確保相關國際傳輸協定例如標準契約條款能獲得普遍的實踐。

（四） 百慕達

百慕達是英國海外領地，但擁有自己的議會及法律，故一般而言，英國法令並不直接適用於百慕達。百慕達的法律片面承認 CBPR 體系的原因與其以保險（尤其是再保險）為主要事業的特性有關，全球有 40%的保險金流會經過百慕達，對百慕達的隱私法規發展具有重要影響。百慕達對於多種金融領域的國際認證相當熟悉，包括洗錢防制、保險清償能力監理等，因此對於參與國際機制並不陌生；此外，百慕達是位處於大西洋的小國，一半資料向東流向歐洲；另一半資料則西流至北美，因此我們無法只是二選一的選擇單一傳輸機制而忽視另外一邊，而是必須找出能同時運作兩種體系的方法。百慕達的個資法是最近才有的發展，2020 年才開始起草新的標準及指引，而我們認為最佳標準應該是放諸四海皆準的，因此要求企業遵循一套全新的百慕達標準並無道理；而且現實是百慕達是一個小國，如果訂的標準與其他國家完全不同，要求跨國企業遵循顯然是不切實際的。此外，百慕達也盼能取得適足性認定，但誠如多位講者所提及，該過程相當的費時耗力，因此如果能透過多邊機制解決

個別的雙邊評估或談判，將對百慕達有非常大的幫助。

百慕達關於跨境傳輸有三項規範：1.不論資料傳輸至何處組織都應負責;2.組織必須評估接收者是否能確保資料受到相當程度的保護;3.該評估標的為（接受者）管轄權的法律是否具有相符性。而 CBPR 係一傳輸及認證體系，取得認證的企業也許可以作為其具有相當保護程度的佐證，但恐仍無法免除該組織仍負有盡職調查的義務（due diligence）。因此 CBPR 體系未來可以再努力的地方包括，提升一般大眾對其的熟悉度，讓大眾可以瞭解 CBPR 認證含括及未含括的項目。關於百慕達面臨的挑戰，主要是境內保險產業欲與美國的保險公司進行資料傳輸，而由於美國採取部門式的監理方式，該傳輸主要受到美國州層級的金融機關監管，因此我們認為應該將該等機關納入 CBPR 體系，方能使 CBPR 體系對百慕達發揮最大的效益。

（五） 巴西

巴西在 2018 年通過個資保護法，刻正致力於推動該法的全面落實，同時與其他國家進行數個自由貿易協定的談判，其中並有專章規範數位經濟與電子商務，而相關貿易與資料流通具有交集。巴西在世界貿易組織（WTO）中對於參與相關條文的談判一直相當積極，包括：資料交換解決方案、國家體系的相互操作性、資料自由流通、開放政府資料、隱私與個資保護等議題，我們相信透過參與多邊、雙邊貿易談判有助於提升消費者信心，達成與 CBPR 體系相同的目標。

關於巴西加入 CBPR 體系的主要挑戰，除其他講者已經提到的部分外，主要涉及巴西國內工作的順序，首先是推動新法的落實，次者是相關權責機關的組織改造，最後是與公民社會及產業團體溝通。

十一、 CBPR 會員體參與近況更新（Updates from CBPR Participants）

本場次由澳洲、加拿大、日本、南韓、菲律賓、新加坡、我國及美國分享參與 CBPR 體系的最新情形

（一） 澳洲(線上參與)

澳洲在 2018 年加入 APEC CBPR，並在今年 8 月加入本論壇，持續支持 CBPR 體系在國際間的擴展。儘管澳洲為 CBPR 體系成員之一，但由於目前國內正在大幅修正相關隱私規範，草案甫提交國會審議，故尚未完全落實 CBPR 體系，其中有幾項由澳洲法務部長在今年 10 月提出的修正，乃是為了回應近期於澳洲國內發生的重大個資外洩事故，包括大幅提高罰鍰以提升企業法遵意願及採取有效措施保護所蒐集的個資；加強監理者權力以針對網路安全事故進行有效執法。另一部分則涉及廣泛的隱私規範審視，該部分的修正並徵詢產業有關實施CBPR體系的意見,今年初蒐集的意見多屬正面,並顯現如果愈多企業加入將會提升企業參與的意願。後續澳洲政府將參考相關意見於國內推動 CBPR。

（二） 加拿大

加拿大雖然為 CBPR 體系的成員之一，且從該機制發展之初即已參與，惟其國內尚未完全落實 CBPR 體系，因為宣布加入當時國內市場並未有任何機構有意願擔任當責機構的角色。此外，加拿大自當時起也開始展開國內隱私改革計畫(目前正在國會審議中，盼能於 2023 年通過)，為了在比對 CBPR 要求時以最新的隱私規範為比對對象，避免比對完舊的規範以後又必須重新比對新的規範，因此暫時未完成相關工作。

在隱私改革計畫後的下一步，加拿大已開始針對不同型態的當責機構進行評估，雖然相關規劃尚待進一步徵詢利害關係人意見，但目前傾向於設置私法人組織型態的當責機構，蓋加拿大為雙語系國家，如果要使用其他市場的當責機構在符合語言要求上恐怕較為困難。

此外，如果可行的話，未來並希望將 CBPR 認證與國內法相關認證程序結合。

（三） 韓國

韓國在今年 5 月開始啟動 CBPR 體系認證，並針對企業辦理多場說明會，其中平台業者、遊戲業者及內容業者均多對 CBPR 體系表達高度興趣，大部分的企業都需要取得認證以加強其在全球事業的可信賴力。程序上，第一步必須先進行初步審查程序，該程序主要係檢驗相關 CBPR 標準是否皆已符合；第二步是檢視針對相關缺失採取的措施是否具有適當性；最後，透過由外部專家組成的委員會做成最後的決定。目前已有三家企業通過初步審查，有一家企業正在等待委員會的決定程序，倘無意外，預計有數家企業可於今年底順利取得 CBPR 認證。至於費用部分，到明年上半年均豁免相關費用，估計明年會有更多企業展現對 CBPR 體系的興趣；另亦提供國內隱私標章 ISMS-P 資深審查員相關教育訓練，盼能在推動上更為順利。

（四） 日本

日本代表繼續介紹有關經產省針對跨境傳輸機制與資料在地化的最新研究成果，表示該報告針對 16 家業者進行訪問調查，對象涵蓋廣泛的產業領域，並彙整相關企業對各傳輸機制優缺點的意見。就結論而言，從勞力及時間成本而言，拘束性企業準則(BCR)取得的難度較高，但一旦實施即具有高度公信力；標準契約條款(SCC)在成本上具有優勢，因為屬於定型化契約，簽署後企業只需要配合調適，但在簽署過程及契約變更上對於大型企業集團會造成相當負擔，因為集團內部有過多主體；至於 CBPR 則具有一定程度的公信力，但缺點是因為不若 SCC 或 BCR 具有拘束力，因此對於取得及維持認證有效性所需付出的成本較不明確。此外，有意見認為由於當責機構數量不多、取得認證的企業規模較小，因此 CBPR 體系的影響

力亦有所不足。

（五） 菲律賓

菲律賓在 2020 年 3 月加入 CBPR 體系後就遇上疫情爆發，疫情期間針對當責機構之申請制定相關內部指引，目前並依該指引審查相關申請者之資格，菲律賓個資保護委員會並計畫成立內部委員會處理相關當責機構之申請與提名程序，並由副主任委員擔任召集人。菲律賓在CBPR推動上主要透過發布相關串流影音及網路文章進行推廣，如果本論壇有製作相關宣傳素材，個資保護委員會也會將該等資料於國內網站或是社群媒體上推播。菲律賓目前在推動 CBPR 體系上遭遇的最大困難仍為國內認知有所不足，為解決此一困境，個資保護委員會嘗試與國內其他機關合作，並盼能透過個資保護長的機制，就相關訊息及活動進行推廣。

（六） 新加坡

新加坡近期修正關於驗證機構的申請程序，機構現在可以隨時提出申請，截至目前為止已指定七家驗證機構。自上次進度更新以來，新加坡新增各 1 家 CBPR 及 PRP 認證企業，共計 7 家 CBPR 認證企業及 4 家 PRP 認證企業，並有數家企業目前正在進行不同階段的認證程序。由於認證程序包括現場審查，過去兩年因為疫情的關係，對當責機構及企業而言都相當不易，盼透過相關規定的鬆綁，未來能看到更多當責機構及企業加入。

（七） 臺灣

我國由吳專門委員欣玲分享我國參與 CBPR 情形，說明我國係於 2018 年正式加入 APEC CBPR 體系，在 2021 年 6 月並由財團法人資訊策進工業會(下稱資策會)獲得認可成為我國第 1 個、全球第 9 個當責機構。資策會與我國隱私執法機關共同合作發展策略以有效

推動 CBPR 體系，並於今年 9 月 14 日正式宣布展開認證程序，目前國內已有金融、醫療及航空產業向資策會接洽申請認證的可能性，後續臺灣將持續與其他經濟體共同合作推動 CBPR 體系。

（八） 美國

從 APEC 隱私綱領、CBPR 體系發展以來，美國一直都主動參與相關推動程序，是第 1 個參與 CBPR 體系、設置當責機構的經濟體，自 2018 年起並已新增 4 家當責機構；目前參與 CBPR 及 PRP 的企業也多為美國企業。此外，美國透過參與聯合監督小組(JOP)，也持續在 CBPR 體系的監督管理上扮演重要的角色並投入相當資源。

美墨加協議已認可 CBPR 體系為有效的跨境傳輸機制，美國亦盼能在印度-太平洋經濟架構(Indo-Pacific Economic Framework, IPEF)中納入相仿規定，並透過本論壇向 IPEF 夥伴進行相關能力建構。此外，近期美國與英國發布聯合聲明將共同合作透過本論壇等多邊倡議推動受信賴的資料流通，美國商務部長亦於本論壇成立同日發表類似聲明，展現美國政府最高層級對此承諾的重視。美國將致力於透過與夥伴共同舉辦研討會、發展認證軟體及教育訓練影片等相關活動，以提升各界對 CBPR 體系的認知，擴大本論壇的會員體。

十二、 從產業角度看 CBPR（CBPRs from an Industry Perspective）

本場次由國際隱私專家協會(IAPP)華盛頓 DC 管理處長 Cobun Zweifel-Keega 擔任主持人，並有 LINE 隱私長 Hee-Jun LIM、Stripe 的 APAC 隱私長 Willem Balfoort、AWS 數位政策及東協事務主任 Annabel Lee 及新加坡 Keppel Data Centres Holding 執行長 Wai Meng WONG 等參與。其發言重點如下：

（一） AWS 數位政策及東協事務主任 Annabel Lee 認為 CBPR 是一個「信任服務」，在於提供消費者、企業及管制者信任。目前其認為 CBPR

對於「企業對企業」的資料流動較具有吸引力，對於消費者而言由於其對 CBPR 熟悉程度不高，因此發展相對受限。

（二） LINE 隱私長鑑於該公司設於韓國，但日、台等國皆為其重要市場的發展現狀，由於其須因此安排不同的隱私規劃，造成成本提高，因此若 CBPR 可以協助企業降低法遵成本，將對其有高度興趣。

（三） Stripe 的 APAC 隱私長則強調，CBPR 有別於 GDPR，是亞太地區對隱私見解的呈現，其發展有助於全球領域討論隱私議題時，不再只是集中於「歐洲視角」

（四） 新加坡 Keppel Data Centres Holding 執行長則建議 CBPR 應強化民眾的認識。其表示根據該公司研究，有近半數民眾不認識 CBPR。

總體而言，儘管企業認同 CBPR 體系對於其開展國際業務、降低跨國法遵成本有所助益，且可在全球隱私法領域規範發展的競逐中展現「亞太觀點」。但企業們也提醒，要使 CBPR 體系獲得進一步發展，仍須進一步提升一般常民對於 CBPR 的認識，才能真正發揮其價值。

十三、 CBPR 會員體與非會員體之討論會議

（一） 對於未來研討會的建議

1. 加拿大表示每次的研討會都能從中學習到新的知識，尤其對於不甚熟悉 CBPR 體系的人來說，每次研討會都是很好的學習機會，因此即便內容略有重複亦無大礙。另鑒於時程上希望在明年 4 月本論壇成立屆滿週年時完成一定工作，加拿大期盼能增加召開實體工作小組會議，以促進本論壇相關基礎工作的推動。

2. 美國亦認同實體會議相較線上會議有更佳的討論成效，提議除預定於 4 月再次舉辦的研討會外，討論在 2023 年初再次安排實體工作小組會議的可能性。

3. 新加坡表示要再明年研討會之前再安排其他的實體會議可能會過於緊湊。針對未來的研討會，建議或可考慮將 2 天的研討會濃縮為 1 天至 1 天半，並可增加與 AA、產業及潛在會員等利害關係人分組討論的機會。

（二） 會員體制與加入條件

新加坡依據 11/1 工作小組及潛在會員的意見，針對本論壇的會員體制與加入條件提出簡報說明，供會員體再次討論：

1. 修正後的會員體制與加入條件規劃（草案）重點略以：

   新增「準會員（Associate Member）」體制，供新成員在成為正式會員以前，先行取得參與本論壇相關會議討論之地位，有權針對相關議案與文件表達意見，但無最終決定作成或參與表決之權限。欲取得準會員資格之管轄權必須提出意向書表明意願，並表達加入 CPEA 的興趣，及符合下列條件之一：(1)說明 CBPR 程序要求與其管轄權內法制的相符性；或(2)確認管轄權內法制承認全球 CBPR 體系。取得準會員資格後並應於一定期限內申請成為會員，否則失去準會員資格。

2. 美國表示考量部分國家如果要同時由政府與監理機關（regulator）兩方參與可能有相當困難，建議在準會員階段或可以只由政府或監理機關其中一方提出意向書並描述國內有 PEA 的角色即可，並透過準會員階段進行相關能力建構，讓 PEA 可以共同參與。

3. 加拿大表示贊同美國意見，並說明其監理機關—加拿大隱私委員辦公室（Office of the Privacy Commissioner of Canada, OPC）完全獨立於政府部門，且 OPC 將本論壇視為政府部門領導的倡議，儘管願意共同合作，但在本論壇確立以前不會作成任何參與決定，政府部門亦無法代表 OPC 作成任何承諾。

4. 菲律賓表示本論壇的重點應係盡可能地擴大參與，讓更多經濟體擁護 CBPR 體系，故初期應僅設定最低標準，讓潛在成員得透過參與論壇研討會等相關活動與會員體交流，進而瞭解、並比對自己國內法規與 CBPR 體系標準。

5. 新加坡表示，依 APEC CBPR 體系規範，國內必須要有 PEA 加入 CPEA，這是 APEC CBPR 體系的重要加入條件；另 CPEA 非僅針對 CBPR 體系的運作，尚包括執法調查、資訊分享等合作，故加入 CPEA 應不意味對於 CBPR 體系提供背書，對於準會員而言應非難以達成的條件。

（三） 與非會員之意見交流

巴西、智利、杜拜金融中心(DIFC)、百慕達、泰國(線上)、馬來西亞(線上)、英國等非會員體針對 CBPR 體系說明其興趣與建議，並針對新成員加入條件表示意見：

1. 巴西表示 CBPR、PRP 體系可以提升法明確與國家競爭力，並營造有利投資的環境，此外，亦有助於協助企業向消費者、合作夥伴、執法機關展顯其法遵能力，增進信賴。巴西最近才開始針對國際傳輸進行監理，明年將發展相關國際傳輸工具，包括標準契約條款(SCC)、企業拘束性準則(BCR)、適足性認定，及行為準則等。

2. 馬來西亞表示本次的研討會提供相當豐富、實用的資訊，該國目前正在申請加入 CBPR 的第一階段，即申請加入隱私執法協議(CPEA)，待通過以後應分享相關資訊，並期待在本論壇有更多的參與；智利表示國內開始有企業對 CBPR 體系有興趣，樂見相關發展；泰國表示該國今年 6 月甫施行個資法，並開始對跨境傳輸進行監管，東協有標準契約條款(Model Contractual Clauses, MCC)作為跨境傳輸的工具，樂見 CBPR

體系成為區域經濟體間的跨境傳輸機制，泰國也盼未來能夠加入。

3. 杜拜金融中心表示其視 CBPR 體系為相當重要的法遵要求，可以協助其管轄權內的企業以非常簡單且有效率的方式完成法遵，另外建議未來也許可以成立次級小組，每季或每月一次讓成員及非成員進行交流，以保持聯繫並分享最新的隱私保護動態；百慕達則建議除成員、當責機構的分組會議外，盼未來也能增加針對執法機關的分組會議。

4. 至於英國則對於新會員體制針對「準會員」要求於兩年內申請成為正式會員的規劃，表示盼能有其他可能性，蓋倘涉及修法，就英國的情形而言，兩年期限恐怕有時仍有所不足；又正式會員能夠享有完整的權利，準會員應會積極想要取得正式會員的資格，故應無須設定兩年的期限避免準會員遲遲不申請成為正式會員。

十四、 當責機構協調聯繫會議

（一） 本次會議計有美國 TrustArc、BBB、日本 JIPDEC、韓國 KISA 及我國資策會代表實體出席，美國 Schellmen 及新加坡 IMDA 則線上參與。當責機構們討論彼此之驗證範圍及驗證方法、對於驗證頻率及當責機構重審頻率之看法、共同識別符號的想法，以及對於 CBPR 要求事項修正進一步進展的看法。

（二） 在驗證範圍上，我國及日本主要以內國企業為驗證範圍（但我國擴及企業位於外國的辦事處），韓國、新加坡及美國，則以當地企業為驗證對象，且將驗證範圍擴及海外的關係企業。在驗證方法上，我國、日本、新加坡及韓國的國內驗證機制（ISMS-P）的當責機構除書面審查外，亦納入實地審查（日本僅第一年實施實地審查，其後

則視狀況而定)，實地審查之方法類似，但依照抽樣的強度而有 0 差異（日本僅有 3 人、半天，韓國則與我國類似)，對於企業的海外組織，新國則無實地審查之計畫。而美國的當責機構們多因幅員廣大，因此多以線上、書面審閱證據方式驗證，並無實地審查要求。

（三） 在驗證頻率上，與會的當責機構普遍同意以 2 年為頻率，並加入期中的查核機制的作法較為適當，或將建議政府端考慮修改相關文件。而在當責機構的重審頻率，也建議調整為 3 年，以平衡監管需求及負擔。

（四） 在 CBPR 驗證制度的共同識別符號議題上，考慮不同當責機構間的識別問題，當責機構們建議以「共同識別」加上「各自象徵」的方法處理 CBPR 識別標示，以強化 CBPR 的全球識別性。對於 CBPR 要求事項修正進一步進展上，與會當責機構同意在視政府單位就第一階段成果的反應後，再做思考，且現階段應以強化各界對 CBPR 認知為重。

（五） 此外，資策會代表就當責機構申請文件的修正向在場其他當責機構請教意見。當責機構代表建議可以加入要求新當責機構加入當責機構聯盟，以強化驗證品質統一及跨國合作。

十五、 論壇成員與當責機構會議

（一） 論壇會員及當責機構分別針對其閉門討論會議結果進行報告與交流。全球 CBPR 論壇會員計畫於未來增加實體會議之頻率，以期能加速轉型的進程，期望能於明年 4 月論壇成立 1 週年時取得部分里程碑成果。惟因接下來北美及亞洲將分別進入年度長假，具體時間仍尚需後續以電子郵件方式確認。針對本次工作會議及論壇的進展上，論壇會員認為全球 CPBR 論壇會員制度設計仍需進一步討論，目前尚未取得共識，預期將成為短期內主要之討論項目。

（二） 當責機構由美國 Truste 公司 Joanne Furtscht 代表發言，認為在計畫要求已經初步完成形式轉換後，短期內之重心應非更新其實質內容，建議可以更著重強化大眾對 CBPR 體系認知，期待監管機構能公開表達對 CBPR 體系的支持。同時，亦希望能針對 CBPR 體系發展提供更清楚之路線圖，已協助當責機構像企業說明後續之轉變。

參、會議觀察與後續應辦事項

一、本次會議美方表示美墨加協議已將CBPR體系之境傳輸機制納入規範，並盼能在印度-太平洋經濟架構(IPEF)中納入相仿規定，顯示美方對於擴大 CBPR 體系的規劃並非僅著眼於個資保護或隱私權等基本人權保障，而係與數位經濟發展息息相關，故我國未來在推動雙邊與多邊國際貿易協定上，亦需密切關注此議題之後續發展，以確保個資保護與數位經濟發展得以相輔相成。

二、透過與各會員體及非會員體之交流，可觀察各國國內個資保護法規之發展，對於 CBPR 體系之參與亦有相當影響。以 CBPR 會員體澳洲、加拿大為例，其近年對於國內相關個資保護規範之改革，對於其加入後國內 CBPR 體系機制之落實具有關鍵影響；至於非會員體則有如巴西、印尼等，雖已完成國內個資法規之立法程序，但亦有待針對新法與CBPR 體系相關要求做進一步比對。此亦可為我國未來修法時之借鏡，於修法過程中即將相關機制納入考量，或可縮短新法與 CBPR 機制之間之調適期間，以降低對於我國推動及參與 CBPR 體系之影響。

三、鑑於全球 CBPR 論壇之運作尚有賴各會員體持續參與相關基礎文件之修訂與討論，我國未來亦將配合論壇工作小組之規劃，積極參與相關會議並做出貢獻。

肆、附件

【研討會議程】

The Global CBPR Forum: Realizing Our Shared Vision

Multistakeholder workshop: November 2-3

Government/Accountability Agent meetings: November 4

Day 1: Wednesday, November 2

9:00-9:20: Opening Remarks by Hosts

- US
- Korea

9:20-9:35: Keynote by PIPC

9:40-10:00 Update on the Global CBPR Forum

- **Shannon Coe**, International Trade Administration, U.S. Department of Commerce

10:00-11:00: Breakout Sessions

Session One: How to establish a CBPR Program: Ask the Experts

This session will provide an opportunity to ask Accountability Agents and companies about participating in the CBPR System. This session is best for non-CBPR participant economies and CBPR participants without an Accountability Agent.

Moderator: **Shannon Coe**, International Trade Administration, U.S. Department of Commerce

Leads:

- Accountability Agents

- **Joanne Furtsch**, Director, Privacy Intelligence Development, Truste, United States
- **Evelyn Goh**, Director International Policy & Strategy at Infocomm Media Development Authority, Singapore
- **Dona Fraser,** BBB National Programs, United States
- **Suyeun Chae**, KISA, South Korea
- **Te Ying Wang,** Project Manager, Institute of Information Industry, Chinese Taipei

- Certified company

- **Harvey Jang**, Vice President and Chief Privacy Officer, Cisco
- **Huey Tan,** APAC Head of Privacy and Law Enforcement, Apple

Session Two: Updates on promoting CBPRs

This session will include an interactive discussion on how to promote uptake of the

CBPR System. This session is best for CBPR members and other participating stakeholders.

Moderator: **Sarah Pham**, International Trade Administration, U.S. Department of Commerce

Leads:

- CBPR participants
  - **Geoff Gertz**, State Department, United States
  - **Infocomm Media Development Authority,** Singapore **(tbc)**
- Accountability Agents
  - **Noël Luke,** Director, Global Privacy, TrustArc (TRUSTe), United States
  - **Mizushima Tsukumo**, Senior Researcher, JIPDEC, Japan
  - **Personal Information Protection Commission,** Korea **(tbc)**

11:00-11:30: Break

11:30-12:00: Breakout session leads to share outcomes with broader group

12:00-12:15: CBPR certification software demo

- **Shannon Coe**, International Trade Administration, U.S. Department of Commerce

12:15-12:30: GROUP PHOTO

12:30: Lunch

2:00-3:00: Regulator Panel

This panel will bring together regulators to discuss enforcement cooperation and how CBPRs can facilitate compliance and trust in cross border transfers. This panel will discuss how the CBPR System can help global companies and regulators identify commonalities and divergence in data protection law.

Moderator: **Geronimo Sy**, Undersecretary of the Department of Justice, Philippines

Speakers:

- **Ailana Linhares de S. Medeiros,** General Coordination of Institutional and International Relations-CGRII, National Data Protection Authority (ANPD), Brazil
- **Lori Baker**, VP, Legal & Director of Data Protection, Office of the Commissioner of Data Protection, Dubai International Financial Centre
- **Junichi Ishii**, Director and Head of International Research, Personal Information Protection Commission, Japan
- (**Speaker tbc**) National Institute for Transparency, Access to Information and Personal Data Protection (INAI), Mexico

- **Josefina E. Mendoza,** Attorney IV, Legal Division, National Privacy Commission, Philippines

3:00-3:15: Break

3:15-3:45: The Case for the Privacy Recognition for Processors (PRP)

This panel will provide an update on HP's pilot program using the PRP System to meet vendor due diligence requirements and discuss lessons learned.

LEAD: Jacobo Esquenazi, Global Privacy Strategist & EU DPO, HP

3:45-5:00: Panel Discussion on CBPRs and Domestic Law

This panel will discuss how the CBPR and PRP Systems work within their legal systems, how the Systems can be effectively utilized under domestic frameworks and how the Systems compare with other cross-border transfer and compliance mechanisms.

Moderator: **Alexander White**, Privacy Commissioner, Bermuda

Speakers:

- **Cobun Zweifel-Keegan,** Managing Director for Washington DC, International Association of Privacy Professionals
- **Jill Paterson**, Senior Policy Advisor, Innovation, Science and Economic Development, Canada
- **Hattie Davison,** Data Policy Directorate at the Department for Digital, Culture, Media and Sport, United Kingdom
- **Makiko Tsuda,** Director for Coordination on International Digital Policy, Ministry of Economy, Trade and Industry, Japan
- **Junichi Ishii**, Director and Head of International Research, Personal Information Protection Commission, Japan
- **(Speaker tbc),** Personal Information Protection Commission, South Korea

5:00: Close

<u>Day 2: Thursday, November 3</u>

9:00-9:10: Keynote remarks

- **Joe Jones**, Deputy Director, International Data Transfers at the Department for Digital, Culture, Media and Sport, United Kingdom

9:10-10:00: How to demonstrate CBPR Requirements and Mapping

This session will discuss how a prospective member can demonstrate that it meets the requirements to participate in the CBPR and PRP Systems, including joining mechanisms that allow the regulators to cooperate, like the Cross Border Privacy

Enforcement Arrangement (CPEA), and mapping domestic law to the CBPR program requirements.

Leads:

- **Markus Heyder**, Vice President and Senior Policy Counselor, The Centre for Information Policy Leadership (CIPL)
- **Michael Panzera**, Counsel for International Consumer Protection and Privacy, U.S. Federal Trade Commission

10:00-11:00: Review of CBPR Program Requirements

This discussion will focus on developing recommendations for updating the program requirements building on the recommendations from previous workshops. The session will also include opportunity to discuss with all stakeholders the process for making any changes.

Leads:

- **Joanne Furtsch**, Director, Privacy Intelligence Development, Truste, United States
- **Evelyn Goh**, Director International Policy & Strategy at Infocomm Media Development Authority, Singapore
- **Chris Lippert**, Senior Manager, Schellman, United States
- **Dona Fraser,** BBB National Programs, United States
- **Willem Balfoort**, APAC Privacy Lead, Stripe, United States

11:00-11:30: Break

11:30-12:30: Panel for non-CBPR participants on possibilities for engagement

Jurisdictions will discuss progress on engagement in the CBPR System and how the CBPR System could be leveraged under their domestic frameworks.

Moderator:

Panelists:

- **Joe Jones**, Deputy Director, International Data Transfers at the Department for Digital, Culture, Media and Sport, United Kingdom
- **Piero Guasta Leyton**, Services and Digital Economy Division, Chile
- **ANPD or Economia, Brazil**
- ~~**Ministry of Foreign Trade and Tourism, Peru (tbc)**~~
- **Rajmatha Devi,** Ministry of Communication and Informatics Indonesia

12:30: Lunch

2:00-3:00: Updates from CBPR Participants

Each CBPR participant will provide an update on participation in the CBPR System.

- Australia
- Canada
- Japan
- Korea
- Mexico
- Philippines
- Singapore
- Chinese Taipei
- United States

3:00-3:30: Break

3:30-5:00: CBPRs from an Industry Perspective

Current certified companies and prospective participants will share the business case for the CBPR System.

Moderator: **Cobun Zweifel-Keegan,** Managing Director for Washington DC, International Association of Privacy Professionals

Panelists:

- **Hee-Jun LIM,** Chief Privacy Officer, LINE, South Korea
- **Willem Balfoort**, APAC Privacy Lead, Stripe, United States
- **Annabel Lee,** Director, Digital Policy (APJ) and ASEAN Affairs, AWS
- **Wai Meng WONG**, CEO, Keppel Data Centres Holding, Singapore (tbc)
- **Derek Ow,** Great East Life Insurance (tbc)

5:00: Wrap up and Concluding remarks

<u>Day 3: Friday, November 4</u>

9:00-10:00: CBPR Participants

10:00-11:00: All government officials participating in the workshop

11:00-11:30: Break

11:30-12:30: CBPR Participants and Accountability Agents

In a separate room:

9:30-11:00: Accountability Agent coordination

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

APEC Cross-Border Privacy Rules Requirements and EU-U.S. Privacy Shield Requirements Mapped to the Provisions of the UK General Data Protection Regulation

This document presents a comparison of the APEC Cross-Border Privacy Rules (CBPR) Requirements and the EU-U.S. Privacy Shield Requirements to the requirements of the UK General Data Protection Regulation (GDPR). For purposes of this analysis, the Centre for Information Policy Leadership (CIPL) at Hunton Andrews Kurth LLP analyzed relevant documents pertaining to participation in both the CBPR and Privacy Shield certification system.[1]

Below we present key recommendations, as well as the main findings from the results of this analysis, followed by two pie charts demonstrating the percentage overlap of the requirements of the CBPR and Privacy Shield Requirement to the UK GDPR. Following this is a detailed table containing the analysis.

This map does not refer to any additional data protection requirements found in the UK Data Protection Act of 2018 (DPA). Relevant DPA provisions that do not appear in the UK GDPR relate to the following issues:

- Special categories of personal data, criminal convictions data, etc.
- Automated decisions required or authorized by law.
- Conditions applicable to reliance on exemptions under Article 23.
- Processing for archiving, research and statistical purposes.
- Enforcement.
- Prohibitions and criminal offences.

[1] See Cross Border Privacy Rules System Documents available at http://cbprs.org/documents/. In particular, this analysis considered the CBPR Program Requirements, Intake Questionnaire, Policies, Rules and Guidelines and the Accountability Agent Application, and the Requirements of Participation in the Privacy Shield Program, available at https://www.privacyshield.gov/article?id=Requirements-of-Participation.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Main Findings from the Results of this Analysis

1. The requirements of the APEC CBPR System and the EU-U.S. Privacy Shield overlap significantly with the requirements of the UK GDPR at 61% and 67%, respectively. This overlap comprises requirements of the UK GDPR that appear either directly or indirectly within each system.

2. In cases where the requirements of the APEC CBPR System and the EU-U.S. Privacy Shield do not match to the requirements of the UK GDPR, this does not necessarily mean those instruments provide a lower level of protection with respect to such provisions/processing scenarios. Furthermore, in cases where there is a non-match with a GDPR provision that provides lesser protection to individuals (e.g. exemptions to obligations - see point 4. a. below), such non-matches may not need to be bridged with the CBPR system.

3. **CBPR matches and non-matches providing a higher level of protection.** With respect to some CBPR non-matches, the CBPR requirements actually provide a higher level of protection than that included in the GDPR. For example:

    a. ***Legitimate and public interest (GDPR Article 6(1)(e) and (f)) [CBPR non-match to GDPR]***: The CBPR do not include public interest or legitimate interests as legal bases for processing, unlike the GDPR. This has the effect of creating a more restrictive standard for processing under the CBPR that will not have to be augmented through any add-on requirements for purposes of bridging the requirements of the CBPR with those of the UK GDPR.

    b. ***Cooperation with the Commissioner (GDPR Article 31) [CBPR match to GDPR]***: The CBPR requires organizations to have procedures in place to respond to judicial or other government subpoenas, warrants or orders. In the context of cooperation with the Commissioner under Article 31 GDPR, the CBPR goes further with respect to responding to such requests by mandating specific procedures be put in place.

4. **CBPR non-matches that are not less protective.** Other CBPR non-matches do not necessarily indicate substantively less protection than that provided by the GDPR.

    a. ***Exemptions to notice to individuals where data has not been collected directly from them (GDPR Article 14)***: The CBPR do not contain notice requirements for organizations that collect information about individuals from sources other than

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the individuals themselves. Consequently, the CBPR does not contain exemptions to this requirement. However, the lack of exemptions here does not mean that this non-match must be bridged with the GDPR.

b. ***Icons (GDPR Article 12(7))***: There is no match to the GDPR transparency provision allowing icons but the absence of this does not mean that existing transparency requirements under the CBPR provide substantively less transparency when compared to the standards under the GDPR.

c. ***Exemption from obligation to maintain records (GDPR Article 30(5))***: There is no match to the GDPR provision exempting certain organizations from maintaining records. However, the absence of such an exemption does not mean that the CBPR provides less protection.

d. ***Publishing DPO contact details (GDPR Article 37(7))***: There is no match to the GDPR requirement to publish the contact details of the DPO and communicate them to the Commissioner but this does not necessarily mean that the CBPR is less protective. Under the CBPR applicants must still provide a "Contact Point" – regardless of whether this is a DPO or not.

e. ***Position of the DPO (GDPR Article 38)***: The GDPR requirements concerning the position of the DPO do not fully match with the requirements contained in the CBPR. Although some of the technicalities of the DPO position are spelled out in the GDPR, the CBPR still requires applicants to provide a "Contact Point" and to have an individual responsible for compliance, and the absence of the technicalities listed in the GDPR do not necessarily indicate that the CBPR is less protective in this regard.

f. ***Tasks of the DPO (GDPR Article 39)***: The GDPR spells out specific tasks that the DPO is responsible for. This list of tasks does not fully match with the requirements contained in the CBPR. However, this does not necessarily mean that the "Contact Point" or individual responsible for compliance under the CBPR will not undertake such obligations. As a result, the lack of these requirements in the CBPR does not necessarily mean that it provides less protection than the GDPR.

g. ***Administrative fines and penalties (GDPR Articles 83 and 84)***: Administrative fines and penalties as described in the GDPR are subject to the domestic law of the participating CBPR country and are enforceable by privacy enforcement authorities in those jurisdictions. As a result, such remedies are not specified in the CBPR program requirements.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

However, under the CBPR, the official DPAs in participating jurisdictions can impose their own set of sanctions, including administrative fines under their legal framework, including redress in court.

5. **CBPR non-matches that are less protective.** At the same time, other CBPR non-matches indicate lesser protection. In some cases, the CBPR does not include specific concepts contained in the GDPR (e.g. data portability), while in others the difference in protection results for different approaches to concepts contained in the GDPR.

    a. ***Publicly available data***: The CBPR generally do not apply to publicly available data that was made available to the public by the individual or that appears in public government records, journalistic reports or information required by law to be public.

    b. ***Children's data (GDPR Article 8)***: The CBPR does not contain requirements around obtaining parental consent for processing the data of children under a certain threshold age.

    c. ***Sensitive data (GDPR Article 9)***: The CBPR do not prohibit processing of sensitive data unless a special condition exists.

    d. ***Processing related to criminal convictions and offences (GDPR Article 10)***: The CBPR do not provide restrictions on processing data related to criminal convictions and offences.

    e. ***Notice to individuals where data has not been collected directly from them (GDPR Article 14)***: The CBPR do not contain notice requirements for organizations that collect information about individuals from sources other than the individuals themselves. Under the CBPR, individuals receive notice from controllers that collect their information directly and subsequently if the controller discloses that information for unrelated purposes.

    f. ***Informing other controllers that the data subject has requested erasure (GDPR Article 17(2))***: The CBPR do not require the communication of erasure requests to other third parties except in the limited circumstances whereby the controller is communicating a correction request to third parties, which might include deletion under the CBPR.

    g. ***The right to restrict processing (GDPR Article 18)***: The CBPR do not contain a right to restrict processing with respect to the specific scenarios outlined in the GDPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

h. ***The right to data portability (GDPR Article 20)***: The CBPR do not contain a right to data portability.

i. ***The right to object (GDPR Article 21)***: The CBPR do not contain a right to object to specific processing.

j. ***The right not to be subject to automated-decision making (GDPR Article 22)***: The CBPR does not contain a right not to be subject to solely automated-decision making producing legal or similarly significant effects.

k. ***Joint controllers (GDPR Article 26)***: The concept of joint controllers is not included in the CBPR.

l. ***Breach notification to the Commissioner (GDPR Article 33)***: There is no requirement to notify breaches to a supervisory authority under the CBPR.

m. ***Breach notification to individuals (GDPR Article 34)***: There is no requirement to notify breaches to individuals under the CBPR.

n. ***Data Protection Impact Assessment (DPIA) (GDPR Article 35)***: There is no requirement to carry out a DPIA under the CBPR.

o. ***Prior consultation (GDPR Article 36)***: There is no requirement to consult a supervisory authority where DPIAs indicate processing would result in a high risk (including because there is no requirement to conduct DPIAs in the first instance).

6. **CBPR non-matches that achieve the same objectives as the GDPR.** There are also some cases where CIPL considers there is a non-match/indirect match between the requirements of the CBPR and the UK GDPR that accomplishes the same goal as the provisions of the GDPR. In other words, the match does not correspond in the CBPR to every detail contained in the GDPR or the requirement may be expressed differently but the spirit of the law and outcome is the same:

   a. ***The right to erasure (GDPR Article 17)***: The right to erasure exists in the CBPR. However, the scope of this right is broader and more restrictive in the GDPR. The exceptions to the right to erasure contained in the GDPR are not expressly listed in the CBPR but the exceptions to providing correction (and by extension deletion under the CBPR) are similar in spirit to the GDPR exceptions for the right to erasure.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

b. ***Notification obligation regarding rectification/erasure/restriction (GDPR Article 19)***: The CBPR contains an obligation to communicate corrections to third parties to whom personal information was transferred/disclosed. This achieves the same objective as Article 19 of the GDPR with respect to rectification and, in limited ways, erasure. There is no right to restriction under the CBPR.

c. ***Restriction of obligations and rights (GDPR Article 23)***: The CBPR provides qualifications to the provision of certain obligations and rights which achieves a similar outcome to Article 23 of the GDPR. However, the GDPR is broader in this regard as it is the Secretary of State who has discretion to impose further restrictions on obligations/rights.

d. ***Privacy by Design (GDPR Article 25)***: There is no explicit privacy by design or by default requirement in the CBPR. However, the CBPR accountability and security safeguards and provisions around uses of personal information overlap with the spirit of the GDPR privacy by design provisions.

e. ***Commitment to confidentiality regarding processor contracts (GDPR Article 28(3)(b))***: Under the CBPR, any confidentiality obligations that are included in processor contracts will attach to persons authorized to process data by the processor entity which achieves the same outcome as Article 28(3)(b) of the GDPR.

f. ***Subprocessor agreements (GDPR Article 28(4))***: Under the CBPR, protections generally flow with the data. For example, an applicant must limit the use of collected information to the intended purpose, including when disclosing data to third parties for processing. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations on processing apply to the processor, who, in turn, is bound by them and cannot onward transfer without these protections. Moreover, under the CBPR, the Applicant may require a processor to obtain the controller's consent to subprocessing. In such cases, the applicant will likely require that sub-processor to adhere to the same requirements as the processor the applicant initially engaged. This achieves the same outcome as Article 28(4) of the GDPR.

g. ***Provision of records to enforcement authority (GDPR Article 30(4))***: Under the CBPR, certified organizations must participate in any dispute resolution requested by a consumer or the Accountability Agent and presumably provide records in the process. Moreover, certified organizations are subject to the jurisdiction of the Privacy Enforcement Authority in the jurisdiction in which they were certified and must respond to document requests from the Privacy

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Enforcement Authority in the context of an investigation. This achieves the same objective as the obligation to make records available to the Commissioner on request under the GDPR.

h. ***GDPR Onward Transfer Requirements (See GDPR Articles 44, 45 and 46)***: While the CBPR requirements do not map to the general cross-border transfer requirements in the GDPR (because the CBPR are a transfer mechanism) the CBPR directly and implicitly provide onward transfer safeguards that achieve similar protections as the GDPR.

i. ***Fines (GDPR Article 83)***: While the CBPR does not spell out levels of fines or circumstances under which they apply, the Accountability Agent has a range of options in enforcing the CBPR program requirements where the certified organization has failed to remedy a violation as ordered by an Accountability Agent, including by issuing a "monetary penalty". This provides the same enforcement remedy as under the GDPR (see note on enforcement under CBPR below).

7. Some elements of the EU GDPR are contained in the CBPR but not in the EU-U.S. Privacy Shield. For example:

a. ***Notification obligation regarding rectification/erasure/restriction (GDPR Article 19)***: The CBPR contains an obligation to communicate corrections to third parties to whom personal information was transferred/disclosed. The Privacy Shield does not contain such a requirement.

b. ***DPO Appointment (GDPR Article 37)***: There is no requirement to appoint a DPO under the Privacy Shield. Under the CBPR, applicants must provide a "Contact Point" and designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles, including as described in its Privacy Statement.

8. APEC also developed a **Privacy Recognition for Processors (PRP)**. It is a streamlined certification for processors with respect to the security safeguards and accountability measures that enable processors to process personal data on behalf of controllers consistent with applicable CBPR obligations and/or the requirements specified by the controllers. The security and accountability measures largely track the corresponding requirements in the CBPR, but are expressly articulated from the processors perspective and more detailed. The PRP system is not part of the CBPR and only two of the CBPR countries are also participating in the PRP. While processors can and do currently certify to the CBPR, processor-specific requirements are more clearly articulated in the PRP and many CBPR requirements simply would not be relevant to processors and certified processors would not have to implement or comply with them.

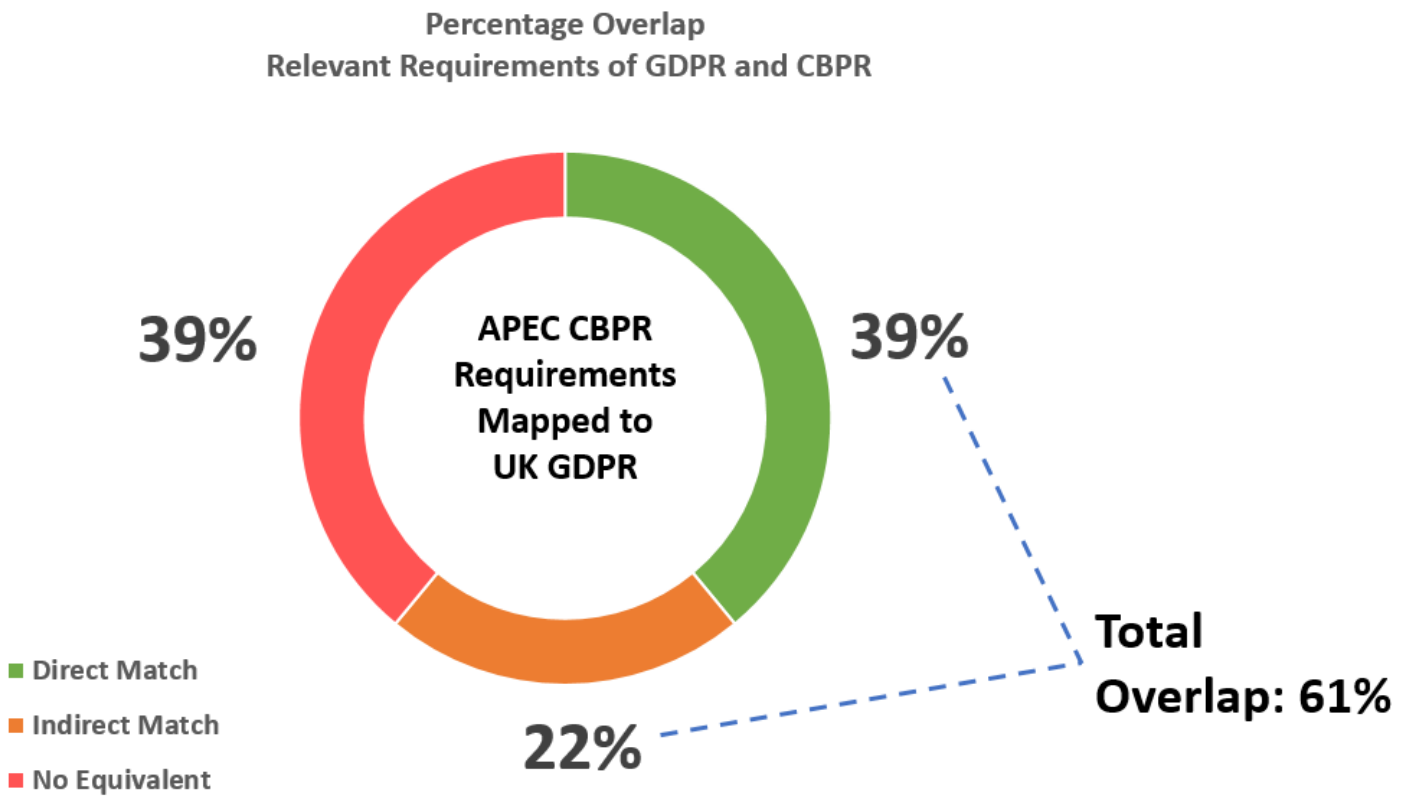
This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Note on the Enforceability of the APEC CBPR System

Once an organization joins the system and is certified by a third-party Accountability Agent under the CBPR Program Requirements, the certification becomes legally enforceable by the Privacy Enforcement Authority (PEA) in the economy in which the organization has been certified. To join the CBPR system, APEC economies must demonstrate that the CBPR are enforceable under their laws and by their PEA. Enforcement of the CBPR is currently provided by APEC-based Privacy Enforcement Authorities that have joined the APEC Cross-Border Privacy Enforcement Arrangement (CPEA). If the CBPR were to be globalized, the CPEA would have to be expanded to allow participation by PEAs from non-APEC economies. Organizations can certify to the CBPR only if they are subject to the enforcement jurisdiction of the PEA in the economy in which they seek certification.

With respect to the sanctions and fines for violations, as mentioned above, administrative fines and penalties as described in the GDPR are subject to the domestic law of the participating CBPR country and are enforceable by privacy enforcement authorities in those jurisdictions. As a result, such remedies are not specified in the CBPR program requirements. Under the CBPR, judicial redress and administrative fines and remedies are left to the individual jurisdictions. The PEAs in the participating jurisdictions can impose their own set of available sanctions, including any administrative fines provided under their legal framework.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

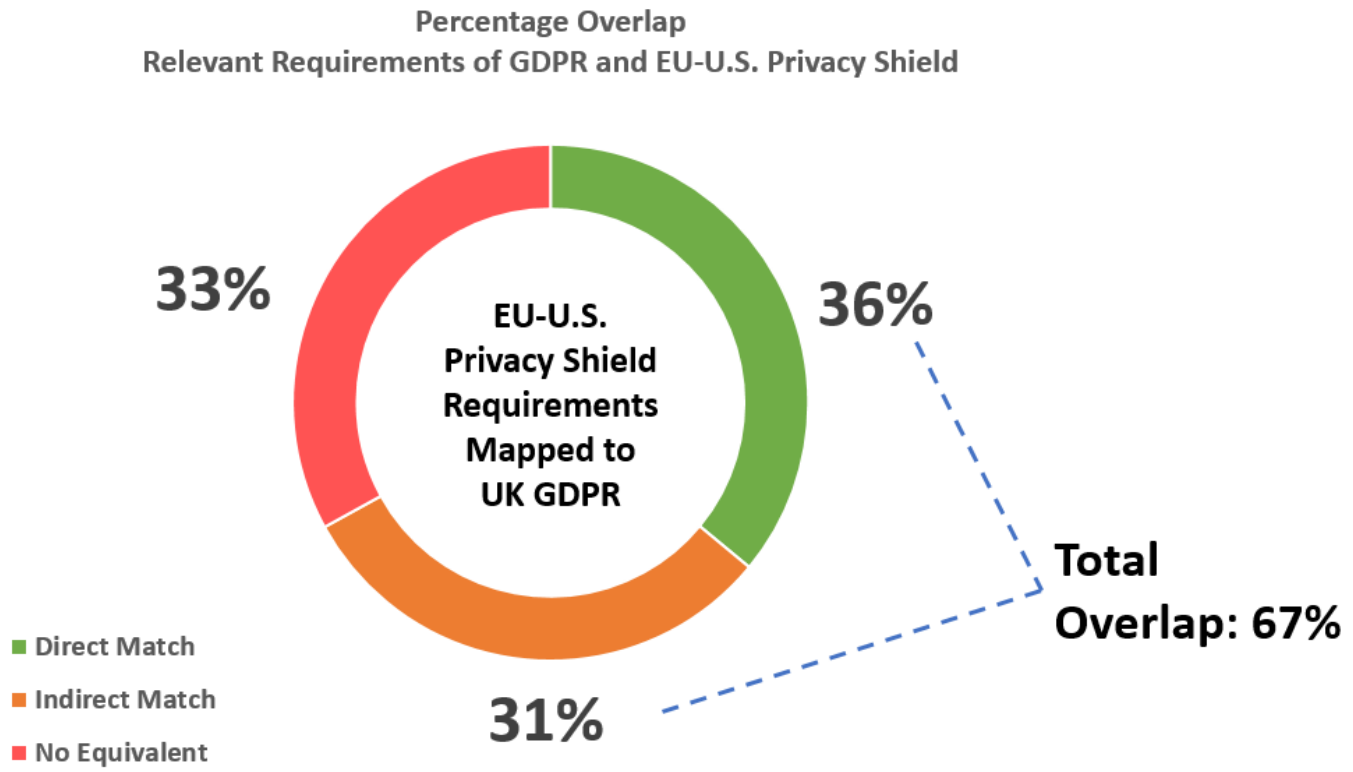


This chart compares 138 relevant GDPR requirements against the requirements of the APEC Cross-Border privacy rules.

In terms of the percentage overlap:

- **61% of requirements (84 requirements) contained in the GDPR appear either directly or indirectly within the CBPR system.**
- **39% of GDPR requirements (54 requirements) do not appear in the CBPR. This figure does not indicate that the CBPR requirements are 31% less protective as explained above.**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.



This chart compares 141 relevant GDPR requirements against the requirements of the EU-U.S. Privacy Shield.

In terms of the percentage overlap:

- **67% of requirements (94 requirements) contained in the GDPR appear either directly or indirectly within the Privacy Shield.**
- **31% of GDPR requirements (54 requirements) do not appear in the Privacy Shield. This figure does not indicate that the Privacy Shield requirements are 31% less protective as described above.**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Detailed Mapping Analysis

Table Legend:

	Table Headings
	UK GDPR provision has an equivalent match in the APEC CBPR / EU-U.S. Privacy Shield
	UK GDPR provision does not have an equivalent match in the APEC CBPR / EU-U.S. Privacy Shield
	UK GDPR provision has a similar/implied but not direct equivalent match in the APEC CBPR / EU-U.S. Privacy Shield
	UK GDPR provision
	Overarching UK GDPR provision (e.g. Article 5) with sub-provisions following in the chart (e.g. 5(1)(a))
	UK GDPR provisions that are not relevant to this mapping exercise
	EU GDPR provisions that have been deleted from the UK GDPR (as indicated by the UK GDPR Keeling Schedule)
FFD	FFD = For further discussion. Indicates areas of overlap that might be subject to multiple interpretations

Note that for purposes of the APEC CBPR Requirements, "**applicant**" means the data controller (although it may also include the data processor as such entities can also certify to the CBPR system). For purposes of this mapping exercise, we use the term applicant to mean the controller.

EU-U.S. Privacy Shield Requirements	UK GDPR Article		APEC CBPR Requirements	Comments
EU-U.S. Privacy Shield Framework Overview • *Lays down the rules relating to the protection of personal data transferred to the U.S. from the EU.*	1	**Subject matter and objectives** • *Lays down rules relating to the protection of personal data.*	**Intake Questionnaire; General (iv.) personal information** • *Applicant must specify what type(s) of personal information it is applying for certification? (customer, employee, prospective*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			customer/employee or other).	
EU-U.S. Privacy Shield Framework Overview • *Privacy Shield applies to U.S. organizations that self-certify their adherence to the Privacy Shield Principles.*	2	**Material scope** • *Applies to automated/structured processing of personal data.* • *Sets out exceptions to which the Regulation does not apply.*	**Intake Questionnaire; General (i) & (ii);** • *CBPR certification applies to applicant organization and listed subsidiaries/affiliates* • *Publicly available information is not covered by the CBPR (see Qualifications to the Provision of Notice and Choice Mechanisms in the intake questionnaire).* • *CBPR certification only applies to commercial information – by inference, CBPR does not apply to law enforcement or intelligence activities or processing conducted for purely personal or household activities.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Framework Overview *In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the U.S. FTC, U.S. Department of Transportation, or another statutory body that will effectively ensure compliance with the Principles; (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement the Principles.*	3	**Territorial scope** • *Sets out scenarios regarding the jurisdictional scope and extraterritorial reach of the Regulation.*	**Intake Questionnaire; General** • *Applicant must specify which economies it or its affiliates/subsidiaries collect or anticipate collecting and transfer or anticipate transferring personal information to be certified under the CBPR.*	
EU-U.S. Privacy Shield I. Overview • *"Personal data" and "personal information" are data about an identified or identifiable*	4	**Definitions** • *"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable*	**Definitions in the APEC Privacy Framework** • *The CBPR were developed specifically to implement the Privacy Principles of the APEC Privacy*	Note that the CBPR generally do not apply to publicly available data that was made available to the public by the individual or that appears in public government records,

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form. • *"Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.* • *"Controller" means a person or organization which, alone or jointly with others, determines*		*natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.* • *"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,*	*Framework. The relevant definitions for the CBPR (e.g. "personal information", "personal information controller") are found in the APEC Privacy Framework.* • *"Personal information" is defined under Part II of the Framework as any information about an identified or identifiable individual.* • *"Personal information controller" is defined as a person or organization who controls the collection, holding, processing or use of personal information.*	journalistic reports or information required by law to be public.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the purposes and means of the processing of personal data.		*restriction, erasure or destruction.* • *"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.* • *See the full text of the UK GDPR for the many other definitions contained in Article 4.*		
	5	**Principles relating to processing of personal data**		
EU-U.S. Privacy Shield Framework Overview • *Consistent with the goal of enhancing privacy protection, organizations should strive to implement the Privacy Shield Principles fully and transparently,*	5(1)(a)	*Lawfulness, fairness and transparency* • *Personal data shall be processed lawfully, fairly and in a transparent manner.*	**CBPR Program Requirements; Assessment Criteria 7** • *Applicant must collect personal information by lawful and fair means, consistent with the requirements of the jurisdiction that governs*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

including indicating in their privacy policies where exceptions will apply on a regular basis.			*the collection of such personal information.*	
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Personal information must be limited to the information that is relevant for the purposes of processing.* • *An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.*	5(1)(b)	*Purpose limitation* • *Personal data shall be collected for specified, explicit and legitimate purposes and not further incompatibly processed.*	**CBPR Program Requirements; Assessment Criteria 6, 8, 10, 12 & 13** • *Applicant must limit the use of collected personal information to those purposes for which the information was collected or for other compatible or related purposes.* • *If applicant discloses personal information to other personal information controllers, the disclosure must be limited to the purpose of collection of compatible or related purposes unless new purposes of processing have been consented to by the individual, it is*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfers • *Where data is transferred to a third party acting as a controller, the transferring organization must enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it*			*necessary to disclose the data to provide a service or product requested by the individual or disclosure is compelled by law.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

can no longer meet this obligation.				
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Personal information must be limited to the information that is relevant for the purpose of processing.*	5(1)(c)	*Data minimization* • *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*	**CBPR Program Requirements; Assessment Criteria 6** • *Applicant must limit the amount and type of personal information collected to that which is relevant to the stated purpose. Proportionality may be a factor in determining what is relevant (see assessment purpose).*	
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *An organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current.*	5(1)(d)	*Accuracy* • *Personal data shall be accurate and, where necessary, kept up to date.*	**CBPR Program Requirements; Assessment Criteria 21 and 22** • *Applicant must take steps to verify that the personal information it holds is up to date, accurate and complete, including by having a mechanism for correcting inaccurate, incomplete and outdated personal information to the extent necessary for purposes of its use.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Personal information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a (Purpose Limitation – see above).*	5(1)(e)	*Storage limitation* • *Personal data shall be kept no longer than necessary.*	**No Direct Equivalent in CBPR**	Indirectly implied via requirement 31 – applicant must implement a policy for secure disposal of information. A storage limitation period may form part of a secure disposal policy. Moreover, the nature of an end to end data security requirement implies that data should not be held in perpetuity unless there is a significant reason for doing so.
EU-U.S. Privacy Shield Principle 4. Security • *Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking*	5(1)(f)	*Integrity and confidentiality* • *Personal data shall be processed in a manner that ensures appropriate security of the personal data.*	**CBPR Program Requirements; Assessment Criteria 30(b)** • *Applicant must implement safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of information and the context in which it is held through information systems and management, including network and software*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

into due account the risks involved in the processing and the nature of the personal data.			*design, as well as information processing, storage, transmission and disposal.*	
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles. This can be done either through self-assessment or outside compliance reviews, both of which are described in further*	5(2)	*Accountability* • *The controller shall be responsible for, and be able to demonstrate compliance with, the processing principles.*	**CBPR Program Requirements; Assessment Criteria 39** • *Applicant must have measures to ensure compliance with the CBPR program requirements (i.e. internal guidelines or policies, contracts, compliance with applicable industry or sector laws and regulations, compliance with self-regulatory applicant code and/or rules, other measures)*	Note that there is a reference error in requirement 39 as the question asks what measures does the applicant take to ensure compliance with the APEC Information Privacy Principles. The principles in reference in requirement 39 refer to the principles listed in the CBPR program requirements as noted in the assessment purpose of the accountability section. Although these principles correspond with the APEC Information Privacy Principles, the CBPR do not include the principle of preventing harm. APEC will likely fix this in a

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

detail. Also, organizations must keep records concerning their implementation of their Privacy Shield obligations.				subsequent update to the Program Requirements.
	6	**Lawfulness of processing**		
EU-U.S. Privacy Shield Principle 2. Choice • *An organization must offer individuals the opportunity to choose (opt-out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available*	6(1)(a)	*Consent*	**CBPR Program Requirements; Assessment Criteria 9(a), 13(a), 14, 15 & 16** • *Use of data for unrelated purposes requires express consent or must be compelled by law. Disclosure of data to other controllers for purposes unrelated to the original purpose, or transfer of data to processors for purposes other than the original purpose, requires express consent, or must be necessary to provide a requested service or product, or must be compelled by law.*	The aggregate effect of the CBPR "Use" and "Choice" Assessment Purposes and Assessment Criteria is that data can be used without choice or consent if the data is used for the purpose for which it was collected and/or related/compatible uses. The fundamental criterion in determining whether a purpose is compatible with or related to the states purposes is whether the extended usage stems from or is in furtherance of such purposes.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

mechanisms to exercise choice.			• *Applicants must ensure individuals are provided with a mechanism to exercise choice in cases where choice would be appropriate. A choice mechanism is not required where the consent would be implied or where an applicable qualification (exception) is identified – this includes "obviousness" or circumstances whereby consent can be inferred from the provision of information by the individual. It also includes all uses related to the original purpose based on the "use" assessment criteria above.*	
EU-U.S. Privacy Shield Principle 2. Choice • *Under the EU-U.S. privacy shield, a consumer has the ability to exercise a choice where the*	6(1)(b)	*Contractual Necessity*	**Intake Questionnaire; Choice & CBPR Program Requirements; Assessment Criteria 13(b)** • *Applicants do not need to provide a mechanism for choice where consent can*	The Choice section of the Intake Questionnaire seems to indicate that choice can be inferred where an individual provides information in connection with a product or service they requested – this may

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

information is to be disclosed to third parties or to be used for materially different purposes. It can be implied that where information is provided by a consumer to engage in a transaction, the organization can process that data without consent (i.e. similar to the basis of contractual necessity under the GDPR).			*be inferred from the provision of the individual's information (see (i) "Obviousness" under Qualifications to the Provision of Choice Mechanisms in the intake questionnaire).* • *Applicants can further process data for purposes incompatible with the original where necessary to provide a service or product requested by the individual.*	well be in the context of a transaction or to enter into a contract and is similar to the contractual necessity ground for processing under the UK Regulation.
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is necessary for the establishment of*	6(1)(c)	Compliance with a legal obligation	**Intake Questionnaire; Choice & CBPR Program Requirements; Assessment Criteria 9(b) and 13** • *Applicants do not need to provide a mechanism for choice where disclosure is made (1) to law enforcement agencies for certain investigation purposes; (2) to third parties pursuant to a*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

legal claims or defenses. **EU-U.S. Privacy Shield Supplemental Principles 16. Access Requests by Public Authorities** • *Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.*			*lawful form of process (e.g. discovery requests); (3) for purposes relating to investigations regarding violations of codes of conduct, breaches of contract or contravention of domestic law (see (v), (vi) and (vii) under Qualifications to the Provision of Choice Mechanisms in the intake questionnaire).* • *Applicants do not need to provide a mechanism for choice for further processing unrelated to the original purpose where such processing is compelled by applicable laws.* • *Applicants do not need to provide a mechanism for choice to disclose personal information to third party controllers or processors for further processing*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			unrelated to the original purposes where such disclosure is compelled by applicable laws.	
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is in the vital interests of the data subject or another person.*	6(1)(d)	*Protection of vital interests*	**Intake Questionnaire; Choice** • *Applicant does not need to provide a mechanism for choice in emergency situations that threaten the life, health or security of an individual.*	
No equivalent in EU-U.S. Privacy Shield	6(1)(e)	*Public interest*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	6(1)(f)	*Legitimate Interest*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *An organization may not process personal*	6(4)	*Compatible Purposes*	**CBPR Program Requirements; Assessment Criteria 8 & 12** • *Applicant must only use or disclose personal information it collects to*	Under the CBPR, applicants can process data for further incompatible purposes if such processing is based on express consent or if compelled by applicable

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. • *Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.*			*fulfill the original purpose of collection or another compatible or related purpose.*	laws (See CBPR Program Requirements' Assessment Criteria 9 and 13). Under the GDPR, if the processing is deemed incompatible after taking into account the factors listed in Article 6(4) GDPR, then a new legal basis to conduct the processing may be required. This could include consent or necessity for compliance with a legal obligation.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

	7	**Conditions of consent**		
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must retain their records on the implementation of their Privacy Shield privacy practices (see Supplemental Principle 7(e)).* • *Organizations must have in place internal procedures for periodically conducting objective reviews of compliance. This impliedly includes records of consumer choices where choice is made on an opt-in basis (e.g. in the context of sensitive data processing).*	7(1)	*Demonstrable* • *Controller must be able to demonstrate that the data subject has consented to processing.*	**No Direct Equivalent in CBPR**	Indirectly implied via CBPR Program Requirements; Assessment Criteria 20. • Applicant must have policies or procedures in place specifying how preferences expressed through choice mechanisms are honored in an effective and expeditious manner. Having a choice mechanism in place and enabling preferences to be honored implies that such consent would be recorded and demonstrable by the applicant.
EU-U.S. Privacy Shield Principle 2. Choice	7(2)	*Distinguishable*	**CBPR Program Requirements; Assessment Criteria 17, 18 and 19**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.*		• *Controller must present the request for consent in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.*	• *Applicant's choice mechanism must be (1) displayed in a clear and conspicuous manner; (2) clearly worded and easily understandable; and (3) easily accessible and affordable.*	
No equivalent in EU-U.S. Privacy Shield	7(3)	*Withdrawal of consent*	**CBPR Program Requirements; Assessment Criteria 9(a), 13(a), 14, 15 & 16** • *In cases where obtaining express consent is required under the CBPR (i.e. for uses of data for unrelated purposes or disclosures of data to other controllers or transfers of data to processors for purposes other than the original purpose), the choice mechanisms facilitating such consent should provide an opportunity for individuals to withdraw consent. For example, via preference/profile pages;*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			email as well as other means.	
No equivalent in EU-U.S. Privacy Shield	7(4)	*Services conditional on consent to processing of personal data*	**No Equivalent in CBPR**	
	8	**Conditions applicable to child's consent in relation to information society services**		
No equivalent in EU-U.S. Privacy Shield	8(1)	*Age of consent* • *In relation to the offer of information society services, where a child is under the age of 13, processing is only lawful where consent is given or authorised by the holder of parental responsibility over the child.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	8(2)	*Parental consent verification* • *The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child.*	**No Equivalent in CBPR**	
	9	**Processing special categories of personal data**		
EU-U.S. Privacy Shield Principle 2. Choice	9(1)	*Special categories of data*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *For sensitive information, organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice.* • *Sensitive information is considered personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or*		• *Processing of data regarding race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation shall be prohibited unless an exception applies.*		

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

information specifying the sex life of the individual • *Organizations should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.*				
EU-U.S. Privacy Shield Principle 2. Choice • *For sensitive information, organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the*	9(2)(a)	*Explicit consent*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

individuals through the exercise of opt-in choice.				
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is necessary to carry out the organization's obligations in the field of employment law.*	9(2)(b)	*Obligation under employment and social security and social protection law*	**Intake Questionnaire; Choice & CBPR Program Requirements; Assessment Criteria 9(b) and 13** • *Applicants do not need to provide a mechanism for choice where disclosure is made to third parties pursuant to a lawful form of process.* • *Applicants do not need to provide a mechanism for choice for further processing unrelated to the original purpose where such processing is compelled by applicable laws.* • *Applicants do not need to provide a mechanism for choice to disclose personal information to third party*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			controllers or processors for further processing unrelated to the original purposes where such disclosure is compelled by applicable laws.	
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is in the vital interests of the data subject or another person.*	9(2)(c)	*Vital interests*	**Intake Questionnaire; Choice** • *Applicant does not need to provide a mechanism for choice in emergency situations that threaten the life, health or security of an individual.*	
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with*	9(2)(d)	*Legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim*	**No Equivalent in CBPR**	Note that it is unlikely that CBPR certified entities will be confronted with such processing scenarios as foundations, associations and other not-for-profit body with a political, philosophical, religious or

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

respect to sensitive data where the processing is carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.				trade union aim cannot certify under the CBPR system. As a result of the point above, for purposes of this mapping exercise, we are counting this provision as not relevant. To the extent that certifying organization engages in such activities, it can process sensitive data where the activity comprises the primary purpose of processing or a related purpose. If the activity constitutes processing that is unrelated to the original purpose, then the **CBPR is more privacy protective than the GDPR in this context as choice must always be given for such processing** (unless an appropriate qualification to choice applies).

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is related to data that are manifestly made public by the individual.*	9(2)(e)	*Data publicly disclosed by data subject*	**No Equivalent in CBPR**	Publicly available information is not covered by the CBPR (see Qualifications to the Provision of Notice and Choice Mechanisms in the intake questionnaire).
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is necessary for the establishment of*	9(2)(f)	*Establishment, exercise or defense of legal claims*	**Intake Questionnaire; Choice** • *Applicants do not need to provide a mechanism for choice where disclosure is made (1) to law enforcement agencies for certain investigation purposes; (2) to third parties pursuant to a lawful form of process (e.g. discovery requests); (3) for purposes relating to investigations regarding violations of codes of*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

legal claims or defenses.			*conduct, breaches of contract or contravention of domestic law (see (v), (vi) and (vii) under Qualifications to the Provision of Choice Mechanisms in the intake questionnaire).*	
No equivalent in EU-U.S. Privacy Shield	9(2)(g)	*Reasons of substantial public interest*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for reasons of substantial public interest under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				appropriate qualification applies.
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is required to provide medical care or diagnosis.*	9(2)(h)	*Purposes of preventive or occupational medicine*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for purposes of preventive or occupational medicine under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an appropriate qualification applies.
No equivalent in EU-U.S. Privacy Shield	9(2)(i)	*Public health*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				reasons of public interest in the area of public health, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an appropriate qualification applies.
No direct equivalent in EU.U.S. Privacy Shield; however, Privacy Shield Supplemental Principles 14. Pharmaceutical and Medical Products provides that: • *Where personal data collected for one research study are*	9(2)(j)	*Research or statistical purposes*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for research or statistical purposes under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. • *It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where*				the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an appropriate qualification applies.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.				
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with*	9(3)	*Processing for purposes of preventive or occupational medicine by or under the responsibility of a professional subject to the obligation of professional secrecy*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for purposes of preventive or occupational medicine by or under the responsibility of a professional subject to

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

respect to sensitive data where the processing is required to provide medical care or diagnosis.				the obligation of professional secrecy under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is for a purpose unrelated to the original purpose. In such cases, **the CBPR is more privacy protective than the GDPR in this context as choice must always be given for such unrelated processing** unless an appropriate qualification applies.
No equivalent in EU-U.S. Privacy Shield	10	**Processing of personal data relating to criminal convictions and offences**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	11	**Processing which does not require identification** • *Controller shall not be obliged to process or acquire further information to identify a data subject for the sole purpose of complying with the regulation.*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as CBPR requirements only relate to personal information (i.e. information that is personally identifiable).

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		• *The rights under Articles 15 to 20 of the GDPR shall not apply except where the data subject provides additional information enabling his or her identification for the purpose of exercising such rights.*		
	12	**Transparent information, communication and modalities for the exercise of the rights of the data subject**		
EU-U.S. Privacy Shield Principle 1. Notice • *An organization must inform individuals of the information listed in (a)(i)-(xiii), which includes information about the right of individuals to access their personal data and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data.*	12(1)	*Transparent information and form* • *The controller shall provide information, communications and the modalities for the exercise of rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language.*	**CBPR Program Requirements; Assessment Criteria 1 and 38(a)** • *Applicant must provide clear and easily accessible statements about its practices and policies that govern the personal information* • *Applicant must provide access and correction mechanisms in a clear and conspicuous manner.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable.*				
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*	12(2)	*Facilitating data subject rights* • *The controller shall facilitate the exercise of rights and not refuse to act on a request to exercise such rights unless it is not in a position to identify the data subject.*	**CBPR Program Requirements; Assessment Criteria 22, 36 and 37** • *Applicant must have mechanisms in place to enable individuals to access or correct their personal information.* • *Applicant must grant access to any individual to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.*	Note that the CBPR does not include inability to verify the identity of an individual as a qualification to the provision of access and correction. The qualifications listed in the CBPR include where providing access or correction would result in a disproportionate burden on the personal information controller, where information cannot be disclosed due to legal or security reasons or to protect confidential commercial information or where provision of access

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access.* • *Organizations must make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific.* • *An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity*				or correction would infringe the privacy rights of other persons.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

of the person making the request.				
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.* **EU-U.S. Privacy Shield Supplemental Principle 8. Access** • *Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form*	12(3)	*Responding to exercise of rights* • *The controller shall provide information on action taken on a request to exercise rights to the data subject without undue delay and in electronic form if the request was made by such means.*	**CBPR Program Requirements; Assessment Criteria 36, 37(b), (d) and 38(d)** *Form* • *In responding to an access request, applicant must provide information in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc.)* *Information on Action Taken* • *In responding to an access request, the applicant must provide confirmation of whether or not it holds personal information about the requester (unless an applicable qualification applies)* • *In responding to a request to exercise correction*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

that is readily intelligible to the individual.			*rights, applicant must provide a copy of the corrected personal information to the individual or confirmation that the data has been corrected or deleted.* *Timing* • *Applicant must provide access within a reasonable timeframe following an individual's request to access their data.*	
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a*	12(4)	*Controller not taking action* • *If the controller does not take action on a request to exercise rights, it shall inform the data subject without delay.*	**CBPR Program Requirements; Assessment Criteria 38(e)** • *If access or correction is refused, applicant must provide the individual with an explanation of why access or correction will not be provided, together with the contact information for further inquiries about the denial of access or correction.*	The CBPR provides the following qualifications to the provision of access and correction: (1) where providing access or correction would result in a disproportionate burden on the personal information controller, (2) where information cannot be disclosed due to legal or security reasons or to protect confidential commercial information or (3) where provision of

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

contact point for any further inquiries. • *An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.*				access or correction would infringe the privacy rights of other persons.
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *An organization may charge a fee that is not excessive.* • *Charging a fee may be justified (e.g., where requests for access are manifestly excessive, in particular because of their repetitive character).*	12(5)	*Applicable fees* • *Information and communication and actions regarding requests to exercise rights shall be provided free of charge unless where requests are manifestly unfounded or excessive.*	**Intake Questionnaire; Access and Correction & CBPR Program Requirements; Assessment Criteria 37(e)** • *Applicant does not need to provide access and correction where the expense of doing so would be unreasonable (e.g. where claims for access are repetitious or vexatious).*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Access may not be refused on cost grounds if the individual offers to pay the costs.*			• *If applicant charges a fee for providing individuals access to their data, it must describe the basis for the fee and how it ensures the fee is not excessive.*	
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.*	12(6)	*Identification of requestor* • *The controller may request additional information necessary to confirm the identity of the data subject.*	**CBPR Program Requirements; Assessment Criteria 36 and 37(a)** • *Applicant must grant access to any individual to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. Applicant must take steps to confirm the identity of the individual requesting access.*	
No equivalent in EU-U.S. Privacy Shield	12(7)	*Icons* • *Information to be provided under the Regulation may be provided in combination with standardized icons.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

	13	**Information to be provided where personal data are collected from the data subject**		
EU-U.S. Privacy Shield Principle 1. Notice • *An organization must inform individuals of the information listed in (a)(i)-(xiii), which includes, e.g., the types of personal data collected; the purposes for which the organization collects and uses personal information; how an individual can contact the organization with any inquiries or complaints; the type of third parties to which the organization discloses personal information, and the purposes for which it does so; the right of individuals to access*	13(1)	*Information to be provided* • *The controller must provide at the time when personal data are obtained the information listed in Article 13(1) at the time of collection to the data subject, where personal data is collected directly from the data subject. These include the identity and contact details of the controller and DPO, the purpose and legal basis for processing, the recipients of the personal data, the categories of data concerned, the intention to transfer data to a third country or international organization, the legal basis for the intended international transfer and the legitimate interests of the controller if the processing is conducted on that basis.*	**CBPR Program Requirements; Assessment Criteria 1(a)-(f), 2, 3 and 4** • *Applicant must provide statements about its practices and policies that govern personal information, including how personal information is collected (including types of data, and whether data is collected directly or through a third party or agent and the categories or specific sources of collected data), the purpose of collection, whether personal information is made available to third parties and for what purposes, the name of the applicant's company and location, including contact*	Note that unlike the GDPR, the CBPR does not include the concept of legitimate interest and as a result does not contain a transparency requirement for the use of such a basis to process data.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

their personal data; and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data. • *This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information, or as soon thereafter as is practicable.*			*information, information about the use and disclosure of an individual's personal information and how an individual can access and correct their data.* • *Applicant must provide at the time of collection of personal information (whether directly or through the use of third parties acting on its behalf) notice that information is being collected.*	
EU-U.S. Privacy Shield Principle 1. Notice • *Either when first collecting the personal information or as soon thereafter as practicable, an organization must inform individuals of the information listed in (a)(i)-(xiii), which*	13(2)	*Further information for fair and transparent processing* • *The controller must provide at the time when personal data are obtained further information enumerated in Article 13(2) to the data subject to ensure fair and transparent processing. These include the period for which the data will be stored or*	**CBPR Program Requirements; Assessment Criteria 1(f), 2** • *Applicant must provide information regarding whether and how and individual can access and correct their personal data.* • *Applicant must provide at the time of collection of*	Note that while the CBPR includes a requirement mandating certain further information to be provided to the data subject on top of those enumerated in Article 13(1), the CBPR only requires information about the existence of the right to request access to and rectification of personal data when compared

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

includes, e.g., how an individual can contact the organization with any inquiries or complaints; the right of individuals to access their personal data; and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data.		*criteria to determine the storage period, the existence of the right to request access, correction, erasure, restriction or objection to the processing data, as well as portability, the existence of the right to withdraw consent and lodge a complaint with the Commissioner, whether the provision of personal data is a statutory or contractual requirement or necessary to enter into a contract and meaningful information about the logic involved in some types of automate decision-making.*	*personal information (whether directly or through the use of third parties acting on its behalf) notice that information is being collected.*	against the requirements of Article 13(2) GDPR (e.g. there is no requirement to provide information about the right to lodge a complaint to the Commissioner, provide information about the existence of automated decision-making, other rights such as data portability etc.)
EU-U.S. Privacy Shield Principle 1. Notice • *Notice must be provided before the organization uses the information for a purpose other than that for which it was originally collected or processed by the*	13(3)	*Further processing* • *Prior to further processing of data for purposes other than that which the data was collected, the controller must provide to the data subject information about that further purpose of processing.*	**CBPR Program Requirements; Assessment Criteria 9 and 13** • *Applicant may further use, disclose or transfer personal information it collects for purposes other than which the data was collected if it bases such further processing on consent or in order to fulfill*	Note that if further processing data on the basis of separate consent or to provide a service or product requested by the individual, the applicant will need to communicate such further processing purposes to individuals when seeking consent or in the context of

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

transferring organization or discloses it for the first time to a third party.			*a legal obligation. In the case of disclosure or transfer, further processing is permitted to provide a service or product requested by the individual.*	the transaction to provide products or services.
EU-U.S. Privacy Shield Supplemental Principle 15. Public Record and Publicly Available Information • *It is not necessary for an organization to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the*	13(4)	*Exception* • *The information requirements of Article 13 do not apply if the data subject already has the information.*	**No Equivalent in CBPR**	Note that while this specific exception to the requirement to provide notice does not appear in the CBPR, if an individual already has the information then the CBPR notice requirements may not apply as a matter of practice (see (i) "Obviousness" under Qualifications to the Provision of Notice in the intake questionnaire).

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

relevant jurisdiction are respected. • *It is generally not necessary for an organization to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends.*				
	14	**Information to be provided where personal data have not been obtained from the data subject**		
EU-U.S. Privacy Shield Principle 1. Notice • *The Privacy Shield notice principle appears*	14(1)	*Information to be provided* • *The controller must provide the information listed in Article 14(1) to the data*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 1(a)-(f), 2, 3 and 4**	The CBPR limits the provision of notice to the individual where personal data has not been obtained from the data subject to

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

to apply regardless of whether information is collected directly or through a third party. • *See Privacy Shield criteria corresponding to Article 13(1) GDPR above.*		*subject, where personal data has not been obtained from the data subject. These include the identity and contact details of the controller and DPO, the purposes of the processing and legal basis, the categories of personal data, the recipients, intention to transfer personal data to a third country or international organizations and the basis for transfer.*	• *Under the CBPR notice requirements, the applicant must identify in the privacy statement whether personal information is made available to third parties and for what purpose.* • *Disclosure of data to other controllers for purposes unrelated to the original purpose requires express consent, or must be necessary to provide a requested service or product, or must be compelled by law. For cases, where express consent is required, the individual will be notified of the new purpose of processing.* • *However, the recipient of the data is not obligated to provide notice to the individuals at or before the time of the collection (see*	notice stemming from the applicant that shared the data rather than from the recipient (as envisaged under Article 14(1) of the GDPR). This may be in the form of notice provided at the initial point of collection which specifies with whom the data may be shared and for what purpose or when the information is shared for unrelated purposes and express consent is sought from the individual.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			Qualifications to the Provision of Notice in the Intake Questionnaire).	
EU-U.S. Privacy Shield Principle 1. Notice • *An organization must inform individuals of the information listed in (a)(i)-(xiii), which includes, e.g., how an individual can contact the organization with any inquiries or complaints; the right of individuals to access their personal data; and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data.*	14(2)	*Further information for fair and transparent processing* • *The controller must provide further information enumerated in Article 14(2) to the data subject to ensure fair and transparent processing. These include the period for which the data will be stored or criteria to determine the storage period, the fact that processing is based on legitimate interests, the existence of the right to request access, correction, erasure, restriction of, or objection to, the processing data, as well as portability, the existence of the right to withdraw consent and to lodge a complaint with the Commissioner, the source of the data and meaningful information about the logic*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 1(a) and (f)** • *Applicant must report the specific sources of all categories of personal information collected.* • *Applicant must provide information regarding whether and how and individual can access and correct their personal data.*	The CBPR limits the provision of notice to the individual where personal data has not been obtained from the data subject to notice stemming from the applicant that shared the data rather than from the recipient. Note that while the CBPR includes a requirement mandating certain further information to be provided to the data subject on top of those enumerated in Article 14(1), the CBPR only requires information about the existence of the right to request access to and rectification of personal data as well as the source from which the personal data originate when compared against the requirements of Article

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		involved in some types of automate decision-making.		14(2) GDPR (e.g. there is no requirement to provide information about the right to lodge a complaint, provide information about the existence of automated decision-making, other rights such as data portability etc.)
EU-U.S. Privacy Shield Principle 1. Notice • *Notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable.* • *Notice must be provided before the organization uses such information for a purpose other than that for which it was originally collected or*	14(3)	*Timing for provision of information* • *The controller must provide the information enumerated in Articles 14(1) and (2) within either a reasonable period after obtaining the data, at the time of first communication with the data subject (if the data is obtained for such purposes) or at the time the personal data are first disclosed to another recipient.*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 2, 3 and 4** • *Applicant must provide at the time of collection of personal information notice that information is being collected.* • *Applicant must explain to individuals the purposes for which information is being collected and that their personal information will be or may be shared with third parties and for what purposes.*	Although there is a timing requirement for the provision of notice in the CBPR, the CBPR limits the provision of notice to the individual where personal data has not been obtained from the data subject to notice stemming from the applicant that shared the data rather than from the recipient.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

processed by the transferring organization or discloses it for the first time to a third party.				
EU-U.S. Privacy Shield Principle 1. Notice • *Notice must be provided before the organization uses personal information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.*	14(4)	*Further processing* • *Prior to further processing of data for purposes other than that which the data was obtained, the controller must provide to the data subject information about that further purpose of processing.*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 9 and 13** *Applicant may further use, personal information it collects (including indirectly) for purposes other than which the data was collected if it bases such further processing on express consent or in order to fulfill a legal obligation.* *In the case of disclosure to third parties or transfers to processors, further processing is permitted on the basis of express consent, to provide a service or product requested by the individual or to fulfil a legal obligation.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			In cases of express consent or to provide a service or product requested by an individual, applicant will need to provide notice about the further purposes of processing.	
EU-U.S. Privacy Shield Supplementary Principle 4. Performing Due Diligence and Conducting Audits • *The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles in certain circumstances (see below).* • *Investment bankers and attorneys engaged in due diligence, or auditors conducting an*	14(5)	*Exceptions* • *The information requirements of Article 14 do not apply if the data subject already has the information, the provision of such information proves impossible or would involve a disproportionate effort, or provision of the information would render impossible or seriously impair the achievement of the objectives of processing, obtaining or disclosing the information is expressly laid down in domestic law or the data is subject to an obligation of professional secrecy.*	**No Equivalent in CBPR but consider Intake Questionnaire; Notice** • *Applicants do not need to provide notice do not need to provide notice under certain circumstances (see (v) under Qualifications to the Provision of Notice in the intake questionnaire) – disclosure to a third party pursuant to a lawful form of process.*	Note that the exception to providing notice where collection of information is laid down in law maps to the CBPR qualification to notice of disclosure to a third party pursuant to a lawful form of process. However, the other exceptions laid down in Article 14(5) GDPR do not seem to have a direct equivalent in the CBPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

investment bankers or auditors.				
	15	**Right of access by the data subject**		
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.* **EU-U.S. Privacy Shield Supplemental Principle 8. Access** • *Individuals must have access to personal information about them that an organization*	15(1)	*Scope* • *The data subject has the right to obtain confirmation of and information about the data processing and a copy of his or her data from the controller.*	**CBPR Program Requirements; Assessment Criteria 36** • *Applicant must provide confirmation of whether it holds personal information about a requesting individual and must grant access (unless it identifies an applicable qualification) to personal information collected or gathered about that individual upon confirming the individual's identity.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

holds, including the purposes of the processing, the categories of personal information concerned, and the recipients or categories of recipients to whom the personal information is disclosed.				
No equivalent in EU-U.S. Privacy Shield	15(2)	*Transfers to third countries or international organizations* • *The data subject also has the right to be informed of appropriate safeguards for the transfer of his or her data to a third country or international organization.*	**No Equivalent in CBPR**	**FFD**
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Access can be provided in the form of disclosure of the relevant personal information by an*	15(3)	*Fees and form of delivery* • *The controller shall provide a copy of personal data undergoing processing and may charge a reasonable fee for further requested copies. Where the access request is*	**CBPR Program Requirements; Assessment Criteria 37 (d) and (e)** *Fee* • *If applicant charges a fee for providing individuals access to their data, it*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

organization to the individual and does not require access by the individual to an organization's data base. • *Charging a fee may be justified (e.g., where requests for access are manifestly excessive, in particular because of their repetitive character).* • *Access may not be refused on cost grounds if the individual offers to pay the costs.*		*made by electronic means, the information shall also be provided by such means unless otherwise requested by the data subject.*	*must describe the basis for the fee and how it ensures the fee is not excessive.* *Form* • *In responding to an access request, applicant must provide information in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc.)*	
Privacy Shield Supplemental Principle 8. Access • The right of access to personal information may be restricted in exceptional circumstances where	15(4)	*Third party rights* • *The right to obtain a copy of the data shall not adversely affect the rights and freedoms of others.*	**Intake Questionnaire; Access and Correction** • *Personal information controllers do not need to provide access where the information privacy of persons other than the individual would be*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the legitimate rights of persons other than the individual would be violated. • The right of access to personal information may be restricted where the legitimate rights or important interests of others would be violated			*violated (though it must provide access where the third party's personal information can be severed from the information requested after such third party's information is redacted) (see Qualifications to the Provision of Access and Correction Mechanisms – (iii) Third Party Risk – in the intake questionnaire).*	
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*	16	**Right to rectification** • *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data or the completion of incomplete personal data concerning him or her.*	**CBPR Program Requirements; Assessment Criteria 38 (b) and (c)** <u>*Right*</u> • *Applicant must make requested corrections or additions to personal information about an individual if that individual demonstrates the personal information held about them by the applicant is incomplete or incorrect.* <u>*Timing*</u>	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*			• *Applicant must make such corrections or additions within a reasonable timeframe following the request.*	
	17	**Right to erasure**		
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate,*	17(1)	*Applicability and cases for erasure* • *Data subject has the right to obtain from the controller the erasure of personal data where the data is no longer necessary, the data subject has withdrawn consent to processing based on consent, the individual objects to the processing and there are no overriding legitimate grounds*	**CBPR Program Requirements; Assessment Criteria 38** • *Applicant must permit individuals to challenge the accuracy of their information and have it deleted, where appropriate (subject to applicable qualifications).*	The CBPR requirements for access and correction provide a limited overlap with the GDPR right to be forgotten. Under the CBPR, deletion requests can be made where data held by the personal information controller is inaccurate.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

or has been processed in violation of the Principles. **EU-U.S. Privacy Shield Supplemental Principle 8. Access** • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*		*for processing, the data has been unlawfully processed, the data has to be erased by law or the data has been collected in relation to the offer of information society services directed to children.*		

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

No equivalent in EU-U.S. Privacy Shield	17(2)	*Informing other controllers* • *Where the controller has made the personal data public and is obliged to erase it, the controller shall take reasonable steps to inform controllers processing the personal data that the data subject has requested erasure of the data.*	**No Equivalent in CBPR**	In the context of a request to correct information (which may include deleting information under the CBPR), there is a requirement to communicate corrections to third parties which is a very limited match to the requirements of Article 17(2).
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *The right of access to personal information may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the*	17(3)	*Exceptions* • *Exceptions to the right of the erasure include where the processing is necessary for exercising the right of freedom of expression and information, compliance with legal obligations, reasons of public interest in area of public health, archiving purposes in the public interest or scientific, historical research and statistical purposes, and the establishment, exercise or defense of legal claims.*	**Intake Questionnaire; Access and Correction** *Personal information controllers do not need to provide correction (and by extension deletion per Assessment Criteria 38 in the CBPR Program Requirements) where information cannot be disclosure due to legal or security reasons.*	Note that the exception contained in the CBPR could in theory be read broadly to cover several of the GDPR exceptions, including, compliance with legal obligations, for reasons of public interest in the area of public health or the establishment, exercise or defense of legal claims.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

individual's privacy in the case in question. • *Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information.* • *Organizations can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

purposes, access may be denied. • *Other reasons for denying or limiting access are:* o *interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;* o *disclosure where the legitimate rights or important interests of others would be violated;*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

o *breaching a legal or other professional privilege or obligation;* o *prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or* o *prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

management, or in future or ongoing negotiations involving the organization.				
No equivalent in EU-U.S. Privacy Shield	18	**Right to restriction of processing**	**No Equivalent in CBPR**	**FFD**
No equivalent in EU-U.S. Privacy Shield	19	**Notification obligation regarding rectification or erasure of personal data or restriction of processing** • *The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the data have been disclosed unless this is impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if he or she requests it.*	**CBPR Program Requirements; Assessment Criteria 23, 24 and 46** • *Applicant must communicate corrections of personal information to personal information processors, agent, other service providers and other third parties to whom personal information was transferred/disclosed.* • *Applicant must also have mechanism in place with personal information processors, agents, contractors or other*	Note that correction in the CBPR includes deletion of data.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			service providers to ensure that the applicant's obligations to the individual will be met.	
No equivalent in EU-U.S. Privacy Shield	20	**Right to data portability**	**No Equivalent in CBPR**	
	21	**Right to object**		
• **No equivalent in EU-U.S. Privacy Shield**	21(1)	*Objection based on public interest and legitimate interests* • *The data subject shall have the right to object to processing based on public interest or legitimate interest, including profiling based on such provisions. The controller shall no longer process the data unless it demonstrates compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 12. Choice – Timing of Opt Out	21(2)	*Objection to direct marketing* • *The data subject shall have the right to object at any time*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Individuals should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective.*		*to processing of his or her personal data for direct marketing purposes.*		
EU-U.S. Privacy Shield Supplemental Principle 12. Choice – Timing of Opt Out • *Individuals should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization*	21(3)	*Cessation of processing for direct marketing* • *Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

time to make the opt out effective.				
EU-U.S. Privacy Shield Principle 2. Choice: • *Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.* **EU-U.S. Privacy Shield Supplemental Principle 12. Choice – Timing of Opt Out** • *An organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the*	21(4)	*Transparency* • *At the latest at the time of first communication with the data subject, the right to object to processing based on public or legitimate interest or for direct marketing purposes shall be brought to the attention of the data subject.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.				
EU-U.S. Privacy Shield Supplemental Principle 12. Choice - Timing of Opt Out • *Individuals may be able to exercise the opt out through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not*	21(5)	*Technical specifications* • *In the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.*	**CBPR Program Requirements; Assessment Criteria 14, 15 and 16** • *Applicant must ensure individuals are provided with a mechanism for individuals to exercise choice in relation to the collection, use and disclosure of their personal information (unless an applicable qualification is identified and justified). These mechanisms include any appropriate means to exercise choice, including online at the point of the collection, via email, via*	While a right to object does not exist under the CBPR, the CBPR enables the exercise of choices through electronic and other means. **FFD**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.			*preference/profile pages, via telephone, postal mail or other means.*	
No direct equivalent in EU-U.S. Privacy Shield. The Privacy Shield has a general opt-out provision, as listed above (Principle 2. Choice).	21(6)	*Objection to processing for research and statistical purposes* • *The data subject shall have the right to object to processing for scientific or historical research purposes or statistical purposes unless such processing is necessary for public interest reasons.*	**No Equivalent**	**FFD**
No equivalent in EU-U.S. Privacy Shield	22	**Automated individual decision-making, including profiling**	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Organizations can restrict access to information to the*	23	**Restrictions** • *The Secretary of State may restrict the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as*	**Intake Questionnaire; Notice, Access and Correction** • *Applicant does not need to provide notice, access or correction under certain circumstances (see*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. • *Other reasons for denying or limiting access are:* o *interference with the execution or enforcement of the law or with private causes of action, including the prevention,*		*Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22. When such restriction is necessary to safeguard: public security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, other important objectives of general public interest, in particular an important economic or financial interest, the protection of judicial independence and judicial proceedings, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the monitoring, inspection or regulatory function connected to the exercise of official authority, the protection of the data subject or the rights and freedoms of others, the*	*Qualifications to the Provision of Notice in the Intake Questionnaire, namely – (iv) Disclosure to a government institution which has made a request for the information with lawful authority; (v) disclosure to a third party pursuant to a lawful form of process; (vii) for legitimate investigation purposes; (viii) action in the event of an emergency; see also the Qualifications to the Provision of Access and Correction in the Intake Questionnaire – (ii) protection of confidential information, including where information cannot be disclosed due to legal or security reasons; (iii) third party risk (i.e. where providing access would violate the information*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

investigation or detection of offenses or the right to a fair trial; o *disclosure where the legitimate rights or important interests of others would be violated;* o *breaching a legal or other professional privilege or obligation;* o *prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and*		*enforcement of civil law claims.*	*privacy of persons other than the requester).*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

corporate re-organizations; or o *prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.*				
	24	**Responsibility of the controller**		
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must provide follow up procedures for verifying that the attestations and assertions they*	24(1)	*Accountability* • *The controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the Regulation and review and*	**CBPR Program Requirements; Assessment Criteria 39** *Applicant must have measures to ensure compliance with the CBPR program requirements (i.e. internal guidelines or policies, contracts, compliance with applicable industry or*	Note that there is a reference error in requirement 39 as the question asks what measures does the applicant take to ensure compliance with the APEC Information Privacy Principles. The principles in

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles. This can be done either through self-assessment or outside compliance reviews. Also, organizations must keep records concerning their implementation of their Privacy Shield obligations.		*update such measures where necessary.*	*sector laws and regulations, compliance with self-regulatory applicant code and/or rules, other measures)*	reference in requirement 39 refer to the principles listed in the CBPR program requirements as noted in the assessment purpose of the accountability section. Although these principles correspond with the APEC Information Privacy Principles, the CBPR do not include the principle of preventing harm. APEC will likely fix this in a subsequent update to the Program Requirements.
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their*	24(2)	*Policies* • *Where proportionate in relation to processing activities, the measures for compliance shall include the implementation of appropriate data protection policies by the controller.*	**CBPR Program Requirements; Assessment Criteria 39** • *Appropriate measures for ensuring compliance with the CBPR program requirements include the implementation of internal policies.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.				
Not relevant to this mapping exercise as the EU-U.S. Privacy Shield is a certification.	24(3)	*Certification/Codes of conduct* • *Adherence to codes of conduct or approved certification mechanisms may be used to demonstrate compliance.*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as the CBPR is a certification.
	25	**Data protection by design and by default**		
EU-U.S. Privacy Shield Principles 4. Security, 5. Data Integrity and Purpose Limitation and Supplemental Principle 7. Verification • The principles of security, data integrity and purpose limitation and verification contemplate that the organization implement	25(1)	*Privacy by design* • *The controller shall implement appropriate technical and organizational measures which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the*	**CBPR Program Requirements; Security Safeguards (Assessment Criteria 26-35) and Accountability (Assessment Criteria 39-50)**	The CBPR security safeguards and accountability provisions contemplate that the applicant shall implement appropriate technical and organizational measures to meet the CBPR program requirements and protect the rights of individuals.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

appropriate technical and organizational measures to meet the requirements of the EU-U.S. Privacy Shield Principles.		*Regulation and protect the rights of data subjects.*		
EU-U.S. Privacy Shield Supplemental Principle 5. Data Integrity and Purpose Limitation • *Organizations must limit personal information to that which is relevant for the purposes of processing and must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current.*	25(2)	*Privacy by default* • *The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Such measures must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*	**No Direct Equivalent in CBPR**	While the CBPR program requirements do not require technical and organizational measures that, by default, ensure only personal data which are necessary for processing are processed, assessment criteria 9 requires that the applicant limit the amount and type of personal information collected to that which is relevant to the stated purpose.
Not relevant to as the EU-U.S. Privacy Shield is a certification.	25(3)	*Certification/Codes of conduct* • *An approved certification mechanism may be used to demonstrate compliance with*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as the CBPR is a certification.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		the requirements of data protection by design and by default.		
No equivalent in EU-U.S. Privacy Shield	26	**Joint controllers**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	27	**Representatives of controllers or processors not established in the United Kingdom**	**No Equivalent in CBPR**	
	28	**Processor**		
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfers • *Where personal data is transferred to a third party acting as an agent, organizations must take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles.*	28(1)	*Processors providing sufficient guarantees* • *The controller must only use processors providing sufficient guarantees to implement appropriate technical and organizational measures to comply with the requirements of the Regulation and ensure protection of the rights of the data subject.*	**CBPR Program Requirements; Assessment Criteria 27, 46, 47, 48 and 49** • *Applicant must take reasonable measures to require information processors, agents, contractors or other services providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of information.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			• *Applicant must implement mechanisms with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicants obligations will be met (such mechanisms include internal guidelines or policies, contracts, compliance with applicable industry or sector laws and regulations, compliance with self-regulatory applicant code and/or rules, other measures).* • *Applicant must require processors to provide self-assessments to ensure compliance with the applicant's instructions and/or agreements or contracts.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			• *Applicant must carry out regular spot checking or monitoring of processors to ensure compliance with the applicant's instructions and/or agreements or contracts (or explain why it does not spot check or monitor).*	
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor understands whether onward transfer is allowed. This might include a requirement to obtain written authorization of the controller before engaging a subprocessor.*	28(2)	*Subprocessors* • *The processor shall not engage another processor without prior specific or general written authorisation of the controller.*	**CBPR Program Requirements; Assessment Criteria 47** • *Applicant must impose restrictions on subcontracting unless the applicant provides consent to the subcontracting arrangement.*	
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer	28(3)	*Data processing agreements* • *Processing by a processor shall be governed by a contract or*	**CBPR Program Requirements; Assessment Criteria 46 and 47**	Note that the specific contractual requirements for processor contracts set out in the CBPR are not

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Where personal information is transferred to an agent, the organization must provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.* **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *When personal data is transferred from the EU to the U.S. only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.*		*other legal act under domestic law that sets out the subject matter and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.*	• *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicants obligations will be met.*	identical to those enumerated in Article 28(3) GDPR but the principle of having a contract in place exists within the CBPR. See the following columns for more information about each specific contractual requirement required by Article 28(3) GDPR and how they map to the CBPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Data controllers in the EU are always required to enter into a contract when a transfer for processing is made, and whether or not the processor participates in the Privacy Shield.*				
Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The purpose of the contract is to make sure that the processor acts only on instructions from the controller.*	28(3)(a)	*Controller instructions* • *Processor must process the personal data only on documented instructions from the controller unless required by domestic law.*	**CBPR Program Requirements; Assessment Criteria 47** • *Processor must follow instructions provided by the applicant relating to the manner in which its personal information must be handled.*	
Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers *The purpose of the contract is to make sure that the processor acts only on*	28(3)(b)	*Commitment to confidentiality* • *Processor must ensure that persons authorized to process the data have committed themselves to confidentiality or are under a statutory obligation of confidentiality.*	**CBPR Program Requirements; Assessment Criteria 47** *Processor must follow instructions provided by the applicant relating to the manner in which its personal information must be handled.*	Any confidentiality obligations that are included in processor contracts will attach to persons authorized to process data by the processor entity.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

instructions from the controller. Any confidentiality obligations that are included in processor contracts will attach to persons authorized to process data by the processor entity.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and*	28(3)(c)	*Security* • *Processor must take all applicable security measures pursuant to Article 32 GDPR.*	**CBPR Program Requirements; Assessment Criteria 35(a)** • *Applicant must require processors to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of information by implementing an information security program.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles. **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *The contract should make sure that the processor provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access, and*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

understands whether onward transfer is allowed.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent*	28(3)(d)	*Conditions for subprocessing* • *Processor must respect the conditions for engaging another processor.*	**CBPR Program Requirements; Assessment Criteria 47** • *Applicant must impose restrictions on subcontracting unless it provides consent to the subcontracting arrangement.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor understands whether onward transfer is allowed.*				
EU-U.S. Privacy Shield Supplemental Principle 9. Human Resources Data • *With respect to the application of the Access Principle, the Privacy Shield requires that an organization processing data in the U.S. will cooperate in providing such access either directly or through the EU employer.* **EU-U.S. Privacy Shield Supplemental Principle 10.**	28(3)(e)	*Providing assistance to controller (data subject rights)* • *Processor must assist the controller in fulfilling its obligation to respond to requests for the exercise of rights.*	**CBPR Program Requirements; Assessment Criteria 23, 24 and 25** • *Processors must update inaccurate, incomplete or out of date information when notified by the Applicant following a request to correct personal information. Similarly, processors must notify the applicant when they become aware of information that is inaccurate, incomplete or out of date.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.*				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide*	28(3)(f)	*Providing assistance to controller (risk, security and breach notification)* • *Processor must assist the controller in ensuring compliance with the GDPR's requirements on security, breach notification and communication of breaches, data protection impact assessments and prior consultation for high risk processing.*	**CBPR Program Requirements; Assessment Criteria 35** • *Applicant must require processors to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of information by implementing an information security program, notifying the applicant promptly when*	Note that the CBPR does not include requirements around data protection impact assessments and, as a result, Assessment Criteria 35 does not map to this prong of Article 28(3)(f) GDPR. The Harms Principle in the APEC Information Privacy Principles articles a risk-based approach to all privacy measures, but that was not made explicit or included in the CBPR program requirements.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the same level of protection as is required by the Principles; and (ii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing.			*they become aware of a breach and taking steps to correct/address the security failure which caused the breach.*	
No equivalent in EU-U.S. Privacy Shield	28(3)(g)	*End of service requirements* • *Processor must delete or return all the personal data to the controller after the end of the provision of services and delete existing copies unless domestic law requires storage of the data.*	**No Equivalent in CBPR**	Note the APEC Privacy Recognition for Processors (PRP) system contains a provision regarding disposal of information by processors following the end of the provision of services. Also, while the CBPR does not explicitly require processors to delete or return all personal data at the end of provision of services, the agreement under Assessment Criteria 47 requires processors to abide by the Applicant's APEC-complaint privacy policies and practices and

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				Assessment Criteria 31 requires a policy for the secure disposal of information.
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; and (ii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's*	28(3)(h)	*Processor accountability* • *Processor must make available to the controller all information necessary to demonstrate compliance with the processor obligations laid down in Article 28 GDPR.*	**CBPR Program Requirements; Assessment Criteria 48 and 49** • *Applicant must require processors to provide self-assessments to ensure compliance with the applicant's instructions and/or agreements or contracts.* • *Applicant must carry out regular spot checking or monitoring of processors to ensure compliance with the applicant's instructions and/or agreements or contracts (or explain why it does not spot check or monitor).*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

obligations under the Principles.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent*	28(4)	*Subprocessor agreements* • *Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act.*	**No Direct Equivalent in CBPR**	Note that under the CBPR, if the applicant consents to the use of a sub-processor, which under the CBPR is a precondition to sub-processing, the applicant will likely require that sub-processor to adhere to the same requirements as the processor the applicant initially engaged.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with the organization's obligations under the Principles. **EU-U.S. Privacy Shield Principle 7. Recourse, Enforcement and Liability** • *In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

proves that it is not responsible for the event giving rise to the damage.				
No equivalent in EU-U.S. Privacy Shield	28(5)	*Certification/Codes of conduct* • *Adherence of a processor to an approved code of conduct or an approved certification may be used to demonstrate sufficient guarantees as referred to in Article 28 GDPR.*	**No Equivalent in CBPR**	Note that the APEC Privacy Recognition for Processors (PRP) system is available for this function.
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.*	28(6)	*SCCs* • *The contract or other legal act reference in Article 28 may be based, in whole or in part, on standard contractual clauses.*	**CBPR Program Requirements; Assessment Criteria 46** • *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicant's obligations will be met.*	While GDPR standard contractual clauses are irrelevant in the context of the CBPR, the CBPR permits the use of contracts to govern relationships with data processors.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

N/A	28(7)	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	28(8)	*Adoption of SCCs* • *The Commissioner may adopt standard contractual clauses for the matters referred to in Article 28.*	**No Equivalent in CBPR**	Not relevant to this mapping exercise.
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the Privacy Shield.* • *In practice, such contracts will most*	28(9)	*Form of contract/legal act* • *The contract or other legal act reference in Article 28 shall be in writing, including in electronic form.*	**CBPR Program Requirements; Assessment Criteria 46** • *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicant's obligations will be met.*	Under the CBPR, the applicant can implement mechanisms with processors to ensure their obligations can be met. The mechanism will almost always be a contract. The Accountability Agent must verify the existence of each type of agreement described (i.e. the contract) and this implies there will be at least a written contract. It is highly unlikely that such contracts would not also be available in electronic form.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

likely be in written and electronic form.				
No equivalent in EU-U.S. Privacy Shield. In contrast, Privacy Shield Principle 7. Recourse, Enforcement and Liability states: • *In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization*	28(10)	*Liability* • *If a processor infringes the Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.*	**No Equivalent in CBPR**	Under the CBPR, liability for infringements by processors is governed by contract and local laws in participating economies determine legal liability for any misconduct associated with relevant processing activities. The CBPR itself does not provide legal protection however for the scenario envisaged by Article 28(10) GDPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

proves that it is not responsible for the event giving rise to the damage. **EU-U.S. Privacy Shield Supplemental Principle 3. Secondary Liability** • *The Privacy Shield does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.* **EU-U.S. Privacy Shield Supplemental Principle 9. Human Resources Data – Enforcement**				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Where personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU.*				
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *Where an organization engages a third party acting as an agent, the organization must implement a contract that should make sure the processor acts only on instructions from the controller.* • *Where an organization engages a third party*	29	**Processing under the authority of the controller or processor** • *The processor and any person acting under the authority of the controller or processor shall not process personal data except on instructions from the controller or if required to do so by domestic law.*	**CBPR Program Requirements; Assessment Criteria 12, 13, 46, 47, 48 and 49** • *If personal information is transferred to processors, such transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual or compelled by law.* • *Processors, agents, contractors or other*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

acting as a controller, the organization must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation.			*services providers must comply with the requirements of the applicant as set out under Assessment Criteria 46, 47, 48 and 49.*	
	30	**Records of processing activities**		

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the*	30(1)	*Types of records to be maintained by controller* • *Each controller and, where applicable, its representative, shall maintain a record of processing activities under its responsibility, including (a) name and contact details of controller, joint controller, representative and the DPO, (b) purposes of processing, (c) description of the categories of personal data and data subjects, (d) categories of recipients, (e) transfers of personal data to a third country/international organization, (f) envisaged time limits for erasure of categories of data, where possible and (g) a general description of the technical and organizational security measures under Article 32(1) GDPR or 28(3) of the UK Data Protection Act 2018, where possible.*	**CBPR Program Requirements; Assessment Criteria 6 & Assessment Purpose of "Integrity of Personal Information"** • *Accountability agent must require the Applicant to identify each type of data it collects, the corresponding state purpose of collection for each, all uses that apply to each type of data and an explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. By inference, the Applicant will need to retain records of such information.* • *The questions within the "Integrity of Personal Information" section of the CBPR are directed towards ensuring that the personal*	Note that while the CBPR program requirements impose a record keeping requirement, the specific types of information to be recorded are not identical to those enumerated under Article 30(1) GDPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Department relating to the organization's adherence to the Principles.			*information controller maintains the accuracy and completeness of records and keeps them up to date.*	
No equivalent in EU-U.S. Privacy Shield	30(2)	*Types of records to be maintained by the processor* • *Each processor and, where applicable, its representative shall maintain a record of processing activities carried out on behalf of the controller, containing (a) name and contact details of the processor and of the controller it acts on behalf of, (b) categories of processing carried out, (c) transfers of personal data to third country/international organization and (d) a general description of the technical and organizational security measures under Article 32(1) GDPR or 28(3) of the UK Data Protection Act 2018, where possible.*	**CBPR Program Requirements; Assessment Criteria 47 & Assessment Purpose of "Integrity of Personal Information"** • *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicants obligations will be met. Such an agreement must generally require such parties to implement privacy practices that are substantially similar to the applicant's policies or*	Under the CBPR, the applicant (i.e. controller) already has to maintain records and this obligation is passed on indirectly to processors as processors must implement privacy practices that are substantially similar to the applicant's policies or privacy practices by virtue of any contract entered into between the controller and processor.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			privacy practices (including the maintenance of complete and accurate records).	
No equivalent in EU-U.S. Privacy Shield	30(3)	*Form of records* • *Records of processing shall be in writing, including in electronic form.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 5. The Role of the Data Protection Authorities • *Organizations will implement their commitment to cooperate with EU supervisory authorities.* **EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer** • *Where an organization transfers personal data to a third party acting as an agent, the*	30(4)	*Making records available to Commissioner* • *Controller or processor shall make the record available to the Commissioner on request.*	**APEC CBPR Policies, Rules and Guidelines; CBPR Element 4 – Enforcement** • *Accountability Agents should be able to enforce the CBPR program requirements through law or contract.* • *The Privacy Enforcement Authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information*	Under the CBPR, certified organizations must participate in any dispute resolution requested by a consumer or the Accountability Agent and presumably provide records in the process. Moreover, certified organizations are subject to the jurisdiction of the Privacy Enforcement Authority in the jurisdiction in which they were certified and must respond to document requests from the Privacy Enforcement Authority in the context of an investigation.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

organization must provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request. **EU-U.S. Privacy Shield Supplemental Principle 7. Verification** • *Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for*			*consistent with the CBPR program requirements.* **Accountability Agent APEC Recognition Application; Recognition Criteria (Dispute Resolution Process and Mechanism for Enforcing Program Requirements)** • *An Accountability Agent must have a mechanism to receive and investigate complaints about Participants and to resolve disputes between complainants and Participants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents recognized by APEC economies when appropriate and where possible.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles. **EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement** • *Organizations, as well as their independent recourse mechanisms, must provide information relating to the Privacy Shield when*			• *Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC Cross-Border Privacy Rules System requirements has not been remedied within a reasonable time, so long as such failure to comply can be reasonably believed to be a violation of applicable law.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

requested by the Department.				
No equivalent in EU-U.S. Privacy Shield	30(5)	*Exceptions* • *The records of processing requirement shall not apply to an enterprise or organization employing fewer than 250 persons unless the processing is likely to result in a high risk to data subject, the processing is not occasional or the processing includes special categories of data.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 5. The Role of the Data Protection Authorities • *Organizations will implement their commitment to cooperate with EU supervisory authorities.* • *An organization commits to cooperate*	31	**Cooperation with the Commissioner**	**CBPR Program Requirements; Assessment Criteria 45** • *Organizations must have procedures in place for responding to judicial or other government subpoenas, warrants or orders.* **Accountability Agent APEC Recognition Application; Recognition Criteria**	The CBPR requires organizations to have procedures in place to respond to judicial or other government subpoenas, warrants or orders. In the context of cooperation with the Commissioner under Article 31 GDPR, the CBPR goes further with respect to responding to such requests by mandating specific procedures be put in place.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with EU supervisory authorities by declaring in its Privacy Shield self-certification submission to the Department of Commerce (see Supplemental Principle on Self-Certification) that the organization: ○ *elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with EU supervisory authorities;* ○ *will cooperate with EU supervisory authorities in*			• *Accountability Agents must have processes for ongoing monitoring, compliance reviews, annual recertification and dispute resolution in which certified organizations must participate and cooperate.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the investigation and resolution of complaints brought under the Privacy Shield; and ○ *will comply with any advice given by EU supervisory authorities where EU supervisory authorities take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, and will provide EU supervisory authorities with written*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

confirmation that such action has been taken. • *Organizations choosing the option for dispute resolution must undertake to comply with the advice of EU supervisory authorities.* • *An organization that wishes its Privacy Shield benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with EU supervisory authorities with regard to such data (see Supplemental Principle on Human Resources Data).*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *The Privacy Shield provides for the establishment of DPA Panels will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Privacy Shield. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with EU supervisory authorities for Privacy Shield purposes, while*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

encouraging and if necessary, helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer. **EU-U.S. Privacy Shield Supplemental Principle 9. Human Resources Data – Enforcement** • *A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the EU in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must commit to cooperate in investigations by and to comply with the advice of competent EU*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

authorities in such cases. **EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement** • *Organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs.*				
	32	**Security of processing**		
EU-U.S. Privacy Shield Principle 4. Security • *Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect personal information from loss, misuse and*	32(1)	*Security measures* • *The controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including pseudonymization, the ability to ensure the ongoing CIA and resilience of processing systems and services, the*	**CBPR Program Requirements; Assessment Criteria 26, 27, 28, 30 (c) and (d), 32 and 33** • *Applicant must implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use,*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.		*ability to restore the availability and access to personal data in a timely manner in the event of an incident and a process for regularly testing, assessing and evaluating the effectiveness of measures for ensuring security of processing.*	*modification or disclosure of information or other misuses and such safeguards must be proportional to the likelihood and severity of harm threatened, the sensitivity of information and the context in which it is held.* • *Applicant must implement measures to detect, prevent and respond to attacks, intrusions or other security failures and have processes in place to test the effectiveness of these measures.* • *Applicant must implement physical security safeguards.*	
EU-U.S. Privacy Shield Principle 4. Security • *In taking reasonable and appropriate measures to protect*	32(2)	*Risk assessment* • *In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in*	**CBPR Program Requirements; Assessment Criteria 27, 28 and 34** • *Applicant must implement physical, technical and*	Certification in this context – language in the assessment criteria. We assume this means as a result of a review by a

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

personal information, organizations must take into due account the risks involved in the processing and the nature of the personal data.		*particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*	*administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses and such safeguards must be proportional to the likelihood and severity of harm threatened, the sensitivity of information and the context in which it is held.* • *Applicant must adjust their security safeguards to reflect the results of certifications or risk assessments or audits.*	certification body/audit to adjust security.
Not relevant to this mapping exercise as the Privacy Shield is a certification.	32(3)	*Certification/Codes of conduct* • *Adherence to an approved code of conduct or certification mechanism may be used as an element by*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as the CBPR is a certification.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		which to demonstrate security of processing.		
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles.*	32(4)	*Security instructions to agents of controller/processor* • *The controller or processor must take steps to ensure that any natural person acting under the authority of the controller or processor does not process data except on the instructions of the controller unless required to do so by law.*	**CBPR Program Requirements; Assessment Criteria 29 and 30(a)** • *Applicant must implement employee security training and management.*	
No equivalent in EU-U.S. Privacy Shield	33	**Notification of a personal data breach to the Commissioner**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	34	**Communication of a personal data breach to the data subject**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	35	**Data protection impact assessment**	**No Equivalent in CBPR**	Note that the Harms Principle in the APEC Information Privacy Principles articles a risk-based approach to all

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				privacy measures, but that was not made explicit or included in the CBPR program requirements. However, note that there are some requirements to carry out risk assessments in the context of security under the CBPR.
No equivalent in EU-U.S. Privacy Shield	36	**Prior consultation**	**No Equivalent in CBPR**	
	37	**Designation of the data protection officer**		
No equivalent in EU-U.S. Privacy Shield	37(1)	*Designation of DPO* • *The Controller and Processor must designate a DPO in certain circumstances.*	**Intake Questionnaire; General (iii.) CBPR Contact Point & CBPR Program Requirements; Assessment Criteria 40** • *Applicant must provide a "Contact Point" for CBPR.* • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles,*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			including as described in its Privacy Statement.	
No equivalent in EU-U.S. Privacy Shield	37(2)	*Group of undertakings* • *A group of undertakings may appoint a single DPO provided that it is easily accessible from each establishment.*	**Intake Questionnaire; General (iii.)** **CBPR Program Requirements; Assessment Criteria 40** • *Applicant must provide a "Contact Point" for CBPR.* • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles, including as described in its Privacy Statement.*	Note that while the CBPR do not specify the scenario of appointing a single DPO for a group of undertakings, the CBPR allow for that.
No equivalent in EU-U.S. Privacy Shield	37(3)	*Single DPO for public bodies* • *A single DPO may be designated for several public authorities or bodies.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	37(4)	*Designation of DPO for representative associations* • *Controller/processor or associations and other bodies representing categories of*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		controllers/processors may designate a DPO.		
No equivalent in EU-U.S. Privacy Shield	37(5)	*Professional qualifications* • *DPO shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices and ability to fulfil the tasks outlined in Article 39.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	37(6)	*Staff or contractor as DPO* • *DPO may be a staff member of the controller/processor or a contractor.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplementary Principle 6. Self-Certification • *To self-certify to the Privacy Shield an organization must provide to the Department a contact office for the handling of complaints, access requests, and any other*	37(7)	*Publish DPO contact details* • *Controller/processor shall publish the contact details of the DPO and communicate them to the Commissioner.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

issues arising under the Privacy Shield.				
	38	**Position of the data protection officer**		
No equivalent in EU-U.S. Privacy Shield	38(1)	*Involve DPO in data protection issues* • *Controller/processor shall ensure the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	38(2)	*Providing resources and support to DPO* • *Controller/processor shall support the DPO in performing tasks by providing necessary resources and access to personal data and processing knowledge and in maintaining expert knowledge.*	**Intake Questionnaire; General (iii.) CBPR Contact Point & CBPR Program Requirements; Assessment Criteria 40** • *Applicant must provide a "Contact Point" for CBPR.* • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles,*	Although the CBPR do not explicitly require the Applicant to provide its appointed DPO with resources to carry out its tasks, it is clear that it will have to do so.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			including as described in its Privacy Statement.	
No equivalent in EU-U.S. Privacy Shield	38(3)	*Independence of DPO* • *Controller/processor must ensure the DPO does not receive any instructions regarding the exercise of its tasks and cannot dismiss or penalize the DPO for carrying out its tasks.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	38(4)	*Availability of DPO to assist with data subject requests to exercise rights* • *Data subjects may contact the DPO with regard to all issues related to the processing of their personal data and exercise of rights.*	**CBPR Program Requirements; Assessment Criteria 40, 41 and 42** • *Applicant must have in place opportune procedures to receive, investigate and respond to privacy-related complaints.* • *Applicant must have procedures in place to ensure individuals receive a timely response to their complaints.*	
No equivalent in EU-U.S. Privacy Shield	38(5)	*Secrecy and confidentiality*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		• *DPO shall be bound by secrecy or confidentiality concerning the performance of its tasks.*		
No equivalent in EU-U.S. Privacy Shield	38(6)	*Additional DPO tasks must not conflict* • *DPO may fulfil other tasks and duties but controller/processor must ensure such tasks and duties do not result in a conflict of interest.*	**No Equivalent in CBPR**	
	39	**Tasks of the data protection officer**		
No equivalent in EU-U.S. Privacy Shield	39(1)(a)	*Inform and advise* • *DPO must inform and advise the controller/processor and employees of their obligations under data protection law.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	39(1)(b)	*Monitor compliance* • *DPO must monitor compliance with data protection law and the data protection policies of the controller/processor, including the assignment of responsibilities, awareness-raising and training of staff*	**CBPR Program Requirements; Assessment Criteria 29, 30(a), 40 and 44** • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles,*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		involved in processing operations, and related audits.	*including as described in its Privacy Statement.* • *Applicant must have procedures in place for training employees with respect to its privacy policies and procedures.* • *Applicant must ensure that its employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight.*	
No equivalent in EU-U.S. Privacy Shield	39(1)(c)	*Provide advice on DPIAs* • *DPO must provide advice where requested as regards DPIAs*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	39(1)(d)	*Cooperate with Commissioner* • *DPO must cooperate with the Commissioner*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	39(1)(e)	*Point of contact for Commissioner*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		• *DPO must act as the point of contact for the Commissioner on issues relating to processing, including the prior consultation referred to in Article 36.*		
No equivalent in EU-U.S. Privacy Shield	39(2)	*Risk assessment* • *DPO must, in the performance of its tasks, have due regard to the risk associated with processing operations.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	40	**Codes of conduct**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	41	**Monitoring of approved codes of conduct**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	42	**Certification**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	43	**Certification bodies**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party*	44	**General principle for transfers**	**CBPR Program Requirements; Assessment Criteria 1(c), 1(e), 8, 9, 10, 12, 13; 50** • *Under the CBPR protections generally flow with the data. Applicant must limit*	Mostly not relevant to this mapping exercise as the CBPR themselves are a transfer mechanism or condition, but the onward transfer safeguards are relevant and the CBPR

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of			*the use of the information to the intended purpose, including when disclosing data to third parties. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations apply to the recipient who is bound by them and cannot onward transfer without these protections.* • *In cases of transfers to third parties where neither due diligence nor reasonable steps to ensure compliance with CBPR obligations are possible, the controller has to explain to the Accountability Agent why that is the case and how the information will <u>nevertheless be protected as required by the CBPR</u>. One option the controller*	directly and implicitly provide onward transfer safeguards.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request. **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *The contract should make sure that the processor understands*			*has is to obtain the consent of the individual and the controller must explain to the satisfaction of the accountability agent the nature of the consent and how it was obtained. Continued applicability of all CBPR protections can only be ensured if they apply to potential onward transfers.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

whether onward transfer is allowed.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent*	45	**Transfers on the basis of an adequacy decision**	**CBPR Program Requirements; Assessment Criteria 1(c), 1(e), 8, 9, 10, 12, 13, 50** • *Under the CBPR protections generally flow with the data. Applicant must limit the use of the information to the intended purpose, including when disclosing data to third parties. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations apply to the recipient who is bound by them and cannot onward transfer without these protections.* • *In cases of transfers to third parties where neither due diligence nor reasonable steps to ensure*	Mostly not relevant to this mapping exercise as the CBPR themselves are a transfer mechanism or condition, but the onward transfer safeguards are relevant and the CBPR directly and implicitly provide onward transfer safeguards.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.			*compliance with CBPR obligations are possible, the controller has to explain to the Accountability Agent why that is the case and how the information will nevertheless be protected as required by the CBPR. One option the controller has is to obtain the consent of the individual and the controller must explain to the satisfaction of the accountability agent the nature of the consent and how it was obtained. Continued applicability of all CBPR protections can only be ensured if they apply to potential onward transfers.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor understands whether onward transfer is allowed.*				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take*	46	**Transfers subject to appropriate safeguards**	**CBPR Program Requirements; Assessment Criteria 1(c), 1(e), 8, 9, 10, 12, 13, 50** • *Under the CBPR, protections generally flow with the data. Applicant must limit the use of the information to the intended purpose, including when disclosing data to third parties. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations apply to the*	Mostly not relevant to this mapping exercise as the CBPR themselves are a transfer mechanism or condition, but the onward transfer safeguards are relevant and the CBPR directly and implicitly provide onward transfer safeguards.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of			*recipient who is bound by them and cannot onward transfer without these protections.* • *In cases of transfers to third parties where neither due diligence nor reasonable steps to ensure compliance with CBPR obligations are possible, the controller has to explain to the Accountability Agent why that is the case and how the information will nevertheless be protected as required by the CBPR. One option the controller has is to obtain the consent of the individual and the controller must explain to the satisfaction of the accountability agent the nature of the consent and how it was obtained. Continued applicability of all CBPR protections can only be*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the relevant privacy provisions of its contract with that agent to the Department upon request. **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *The contract should make sure that the processor understands whether onward transfer is allowed.*			*ensured if they apply to potential onward transfers.*	
No equivalent in EU-U.S. Privacy Shield	47	**Binding corporate rules**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
N/A	48	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	49	**Derogations for specific situations**	**CBPR Program Requirements; Assessment Criteria 50** • *Applicant may disclose personal information to other recipient persons or organizations where due diligence and reasonable*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			steps to ensure compliance with the CBPR by the recipient is impractical or impossible by explaining why such due diligence and reasonable steps for accountable transfers are impractical and impossible to perform and the other means for ensuring that the information is, nevertheless, protected consistent with the APEC Privacy Principles.	
EU-U.S. Privacy Shield Framework Overview • *The U.S. Department of Commerce issued the Privacy Shield Principles under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with the European Commission,*	50	**International cooperation for the protection of personal data** • *Commissioner shall take appropriate steps to develop international cooperation mechanisms to facilitate effective enforcement of data protection legislation, provide mutual assistance in the enforcement of such legislation, engage stakeholder in discussion and activities aimed at furthering international cooperation in*	**The APEC Cross-border Privacy Enforcement Arrangement (CPEA)** was created to ensure cross-border enforcement cooperation of the CBPR among participating economies. It enables enforcement cooperation on all data protection and privacy-related enforcement matters, not just CBPR enforcement.	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union.		*enforcement and promote the exchange and documentation of personal data protection legislation and practice.*		
No equivalent in EU-U.S. Privacy Shield	51	**Monitoring the application of this Regulation**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	52	**Independence**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
N/A	53	Deleted from UK GDPR	N/A	N/A
N/A	54	Deleted from UK GDPR	N/A	N/A
N/A	55	Deleted from UK GDPR	N/A	N/A
N/A	56	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	57	**Tasks**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	58	**Powers**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	59	**Activity reports** • *Each supervisory authority must prepare an annual report that includes types of notified infringements and measures taken.*	**Accountability Agent APEC Recognition Application; Recognition Criteria [Dispute Resolution Process - 10(g) (Accountability Agent Complaint Statistics) and (h) (Accountability Agent Case Notes)]** • The Accountability Agents must prepare annual	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			complaint statistics and anonymized case notes on resolved CBPR complaints.	
N/A	60	Deleted from UK GDPR	N/A	N/A
N/A	61	Deleted from UK GDPR	N/A	N/A
N/A	62	Deleted from UK GDPR	N/A	N/A
N/A	63	Deleted from UK GDPR	N/A	N/A
N/A	64	Deleted from UK GDPR	N/A	N/A
N/A	65	Deleted from UK GDPR	N/A	N/A
N/A	66	Deleted from UK GDPR	N/A	N/A
N/A	67	Deleted from UK GDPR	N/A	N/A
N/A	68	Deleted from UK GDPR	N/A	N/A
N/A	69	Deleted from UK GDPR	N/A	N/A
N/A	70	Deleted from UK GDPR	N/A	N/A
N/A	71	Deleted from UK GDPR	N/A	N/A
N/A	72	Deleted from UK GDPR	N/A	N/A
N/A	73	Deleted from UK GDPR	N/A	N/A
N/A	74	Deleted from UK GDPR	N/A	N/A
N/A	75	Deleted from UK GDPR	N/A	N/A
N/A	76	Deleted from UK GDPR	N/A	N/A
EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement *Recourse Mechanisms for Individuals*	77	**Right to lodge a complaint with the Commissioner** • *Every data subject has the right to lodge a complaint with a supervisory authority.*	**CBPR Policies, Rules and Guidelines, paragraphs 22, 24, 25 and 26; Accountability Agent APEC Recognition Application; Recognition Criteria (Dispute Resolution Process - 9 and 10)**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Consumers have the ability to take complaints to independent recourse mechanisms (dispute resolution bodies), but Supplemental Principle 11 also states that consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms.* • *An arbitration option is available to an individual in the case of any residual claims not resolved by any of the other available mechanisms, if any. Arbitration may be used to determine whether a Privacy Shield organization has violated its obligations*		• *The supervisory authority must inform the complainant on the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78.*	• *For purposes of questions and complaints, the APEC CBPR Compliance Directory (www.cbprs.org) identifies and links to the relevant Privacy Enforcement Authority with jurisdiction over the Accountability Agent that certified the company that is subject of a complaint (Paragraph 22).* • *The CBPR must be enforceable by the Accountability Agents and Privacy Enforcement Authorities (Paragraph 24).* • *The CBPR system has an enforcement cooperation arrangement between the Privacy Enforcement Authorities in the participating countries (The Cross-border Privacy Enforcement Arrangement*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

under the Privacy Shield Principles as to that individual, and whether any such violation remains fully or partially unremedied. *<u>FTC Action</u>* • *The FTC reviews referrals alleging non-compliance with the Privacy Shield Principles received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated.* • *Non-compliance also includes false claims of adherence to the*			*(CPEA)) (Paragraph 25 and 26).* • *The Accountability Agent must have a mechanism to receive and investigate complaints and resolve disputes (Criterion 9)* • *The dispute resolution process must include a process, inter alia, for notifying the complainant of the complaint resolution (Criterion 10)*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Privacy Shield Principles or participation in the Privacy Shield by organizations, which either are no longer on the Privacy Shield List or have never self-certified to the Department.				
No direct equivalent in EU-U.S. Privacy Shield. The Privacy Shield contains independent recourse mechanisms for individuals, including binding arbitration (see Privacy Shield criteria corresponding to GDPR articles 77 and 82).	78	**Right to an effective judicial remedy against the Commissioner**	**No Equivalent in CBPR**	The availability of this remedy depends on the domestic law of the country in which the applicant is certifying to CBPR. **FFD**
No direct equivalent in EU-U.S. Privacy Shield. The Privacy Shield contains independent recourse mechanisms for individuals, including binding arbitration (see Privacy Shield criteria	79	**Right to an effective judicial remedy against a controller or processor**	**No Equivalent in CBPR**	The availability of this remedy depends on the domestic law of the country in which the applicant is certifying to CBPR. **FFD**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

corresponding to GDPR articles 77 and 82).				
No equivalent in EU-U.S. Privacy Shield	80	**Representation of data subjects**	**No Equivalent in CBPR**	The availability of this remedy depends on the domestic law of the country in which the applicant is certifying to CBPR. **FFD**
N/A	81	Deleted from UK GDPR	N/A	N/A
EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement and Annex I *<u>Arbitration</u>* • *In arbitration, the Privacy Shield Panel has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with*	82	**Right to compensation and liability**	**Not Equivalent in the CBPR but consider Accountability Agent APEC Recognition Application; Recognition Criteria (Mechanism for Enforcing Program Requirements - 13(e))** • *The Accountability Agent has a range of options in enforcing the CBPR program requirements where the certified organization has failed to remedy a violation as ordered by an Accountability Agent, including by issuing a "monetary penalty".*	Under the CBPR, it is not clear if monetary penalties by the Accountability Agent refers to penalties that may be awarded to individuals or only levied against the organization. **FFD**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

respect to the individual. • *In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.* • *Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.* *FTC Action*			• *The availability of Court ordered compensation would be subject to domestic law.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Consent order: If the FTC concludes that it has reason to believe that an organization violated Section 5 of the FTC Act, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect.* • *Civil penalty: The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order.*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

No direct equivalent in EU-U.S. Privacy Shield. However, in obtaining civil penalties for violations of consent orders, the FTC must show that the violator had "actual knowledge that such act or practice is unfair or deceptive and is unlawful" under Section 5(a)(1) of the FTC Act (*see* FTC Act Section 5(m)(1)(B), 15 U.S.C. Sec. 45(m)(1)(B)).	83	**General conditions for imposing administrative fines**	**No Equivalent in CBPR program requirements but consider Accountability Agent APEC Recognition Application; Recognition Criteria (Mechanism for Enforcing Program Requirements - 13(e))** *The Accountability Agent has a range of options in enforcing the CBPR program requirements where the certified organization has failed to remedy a violation as ordered by an Accountability Agent, including by issuing a "monetary penalty".*	Accountability agents can impose monetary penalties as deemed appropriate in their CBPR program. To our knowledge, no Accountability Agent has implemented that remedy to date. Note, however, that (outside of the CBPR program requirements) administrative fines and penalties as described in the GDPR are subject to the domestic law of the participating CBPR country and are enforceable by privacy enforcement authorities in those jurisdictions.
EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement • *If an organization persistently fails (as detailed in section (g)(ii)) to comply with the Principles, it is no*	84	**Penalties**	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

longer entitled to benefit from the Privacy Shield. The organization will be removed from the Privacy Shield List and must return or delete the personal information it received under the Privacy Shield.				
EU-U.S. Privacy Shield Supplementary Principle 2. Journalistic Exceptions • *Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.*	85	**Processing and freedom of expression and information**	**No Equivalent in CBPR**	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Privacy Shield Principles.*				
EU-U.S. Privacy Shield Supplemental Principle 15. Public Record and Publicly Available Information • *It is not necessary to apply the Access Principle to public record information as long as it is not combined with other*	86	**Processing and public access to official documents**	**No Equivalent in CBPR**	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.				
EU-U.S. Privacy Shield Framework Overview	86 A	**Processing and national security and defence**	**No Equivalent in CBPR**	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Adherence to the Privacy Shield Principles may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements.*				
N/A	87	Deleted from UK GDPR	N/A	N/A
N/A	88	Deleted from UK GDPR	N/A	N/A
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer*	89	**Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**	**CBPR Program Requirements; Assessment Criteria 26, 27, 28, 29, 39, 31, 32, 33, 34, 35 & 39** • *To the extent that CBPR certified companies engage in such data uses (i.e. processing for archiving purposes in the public interest, scientific or historical research purposes or statistical research purposes), the security safeguards and accountability requirements of the CBPR will apply.*	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision. **EU-U.S. Privacy Shield Framework Overview** • *Adherence to the Privacy Shield Principles may be limited: (a) to*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

such exceptions or derogations are applied in comparable contexts.				
N/A	90	Deleted from UK GDPR	N/A	N/A
N/A	91	Deleted from UK GDPR	N/A	N/A
N/A	92	Deleted from UK GDPR	N/A	N/A
N/A	93	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	94	**Repeal of Directive 95/46/EC**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	95	**Relationship with Directive 2002/58/EC**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	96	**Relationship with previously concluded Agreements**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
N/A	97	Deleted from UK GDPR	N/A	N/A
N/A	98	Deleted from UK GDPR	N/A	N/A
N/A	99	Deleted from UK GDPR	N/A	N/A

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

APPENDIX A: UK Data Protection Act 2018 – Provisions Not Appearing in the UK GDPR

Special categories of personal data and criminal conviction etc. data	S.10 and Schedule 1 Parts 1, 2 and 3 provide additional grounds for processing such data, subject to specified conditions and safeguards. S.11(1) applies further supplementary conditions to the processing of certain categories of such data.
Automated decisions required or authorized by law	S.14 applies obligations to notify data subjects of such decisions within a specified time and supplementary obligations in respect of re-considering the decision, giving further notice etc.
Conditions applicable to reliance on exemptions under Article 23	S.15 and Schedules 2, 3 and 4 implement exemptions permissible under Article 23 UK GDPR. Such exemptions are subject to certain supplementary conditions set out in the specific exemptions. Comment – the relevant point is that exemptions are specific and curtailed so they meet the criteria of being limited and specific. Broad or unrestricted exemptions would not be compatible with the UK DPA.
Processing for archiving, research and statistical purposes	S. 19 imposes additional safeguards in respect of such processing.
Enforcement	Part 6 S.142 to 164 implement the powers of the Commissioner to take enforcement actions (fines, notices, audits etc.). All the powers are subject to restrictions and conditions which impose procedural rules of fairness in the exercise of such powers. Comment – the relevant point is that a system which did not incorporate respect for proper procedures and the rights of those subject to enforcement action would not be compatible with UK DPA or UK standards more generally. The same applies to rights of appeal and other procedural matters.
Prohibitions and criminal offences	S.170 makes the unlawful obtaining or disclosure of personal data a criminal offence. S.171 makes the re-identification of de-identified data a criminal offence. S.173 makes the alteration of personal data to thwart disclosure under subject access a criminal offence. S.184 makes enforced subject access a criminal offence.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Notes

There are further obligations on the Commissioner which are not replicated in the APEC Framework or the Privacy Shield.

- In respect of codes of practice the Commissioner must prepare and issue codes covering Age Appropriate Design, Data Protection and Journalism, Direct Marketing and Data Sharing. Once such codes come into effect they are admissible in legal proceedings so, to that extent, operate as a "soft law" part of the UK regime.

- There are also obligations to maintain a register of national security certificates, provide guidance about the application of Police and Criminal Evidence codes of practice to the Commissioner's investigations, provide guidance on redress against media organization, provide assistance to data subjects, where appropriate, in cases related to journalism and issue guidance on regulatory action.
