APEC CBPR 驗證機制要點

公告日期：2023 年 6 月 30 日

0. 依據

本要點係依據「臺灣個人資料保護與管理制度維運規章」與「亞太經濟合作（Asia Pacific Economic Cooperation, 以下稱「APEC」）跨境隱私規則體系（Cross Border Privacy Rules System, 以下稱「CBPRs」）」之相關規範所訂定。

1. 目的

為明確組織申請 CBPR 驗證及當責機構執行驗證之程序及其他相關事項，特訂定本要點。

2. 定義

本要點用語定義如下：

(1) 個人資料管理制度：指組織針對所持有個人資料所訂定之政策、內部管理組織及其規則、風險管控措施、應變處理程序及教育訓練計畫之整體管理體系。

(2) 組織：指任何主要營業據點設立於我國之自然人以外之非公務機關。

(3) CBPR 驗證：指以 2016 年臺灣個人資料保護與管理制度規範、個人資料保護法、APEC Privacy Framework、APEC Cross Border Privacy Rules System Program Requirements Map 等 APEC 認可文件為驗證標準，所進行之驗證。

(4) 更新驗證：指於組織之 CBPR 驗證有效期間屆滿前，為瞭解組織就 CBPR 與個人資料管理制度落實之情形，經組織提出申請後所執行之更新驗證。

(5) 當責機構：指財團法人資訊工業策進會，為 APEC 認證之我國當責機構，負責我國 CBPR 驗證、維運與推行之機構。

(6) 驗證機構：指經當責機構認可並登錄、公告之驗證機構，執行 CBPR 驗證。

(7) 受證組織：指通過 CBPR 驗證，經當責機構授予通過證明之組織。

(8) 書審：指 CBPR 驗證的第一階段；由當責機構或驗證機構針對申請組織之 CBPR 與個人資料管理制度相關文件進行初步審閱。

(9) 實審：指 CBPR 驗證的第二階段；由當責機構或驗證機構至所擇定之申請組織營運或業務執行場所審查其作業流程及個人資料管理制度文件與制度實際執行狀況。

(10) CBPR 驗證爭議：指對據以認定書審、實審驗證結果之事實所生之爭議。

(11) 事故：指組織之個人資料外洩、滅失、毀損、竄改及其他侵害；或其他違反個人資料保護相關法令規範之情事。

3. 執行原則與保密

執行驗證，應秉持專業知識，避免利益衝突之情形並以獨立、公正、負責之態度為之；除因法令或本制度各規範所要求者外，對因執行驗證相關業務所知悉之組織之機密資訊應予保密。

4. CBPR 驗證申請

4.1. CBPR 驗證申請資格

(1) 當責機構接受組織申請 CBPR 驗證，如有下列情形之一者，當責機構得駁回其申請，或暫緩 CBPR 驗證執行：

(a) 申請組織曾接受實審而未通過，其期間尚未屆滿六個月者。

(b) 申請組織受暫停使用 CBPR Seal 之處置，其期間尚未屆滿者。

(c) 申請組織於一年內曾受終止 CBPR Seal 使用之處置者。

(d) 申請組織於一年內曾受行政處分或法院判決，認定其因故意或過失，而導致個人資料遭洩漏、竊取、竄改、毀損、滅失或其他非法利用；且處分或判決尚未經撤銷、廢止或廢棄。

(e) 申請組織，其負責人、代表人、經理人、執行業務董事或其他有代表權人，曾因違反個人資料保護相關法令而受刑罰之處罰，而其刑期或刑罰之執行尚未結束，或自執行結束之翌日起，尚未屆滿三年者。

(2) 組織於提出 CBPR 驗證申請時，須據實聲明是否有 4.1(1)之情形，如組織虛偽陳述或嗣後經發現陳述內容與事實不符者，當責機構得駁回其申請或暫緩驗證之執行；如組織已經驗證，當責機構得認定驗證程序無效，組織所繳交之文件與費用不予退回；如組織已獲授證，當責機構得認定授證程序無效，組織所繳交之文件與費用不予退回，當責機構得公告無效之事由。

(3) 當責機構應審查申請組織與當責機構間有無利益衝突之情事，並依財團法人資訊工業策進會「執行 APEC CBPR 問責機構職責之利益衝突迴避管理程序」處理。

4.2. 文件繳交

組織於提出 CBPR 驗證申請時，須依當責機構要求繳交 CBPR 驗證相關文件。

5. CBPR 驗證

(1) CBPR 驗證與更新驗證應通過書審與實審程序。

(2) 當責機構接受 CBPR 驗證申請並收訖費用後，書審階段即可展開，並由當責機構初步審查申請組織文件是否符合 CBPR 驗證要求，於審查完成後將結果以書面通知申請組織；審查結果如為未通過者，應載明未通過之理由。

(3) 申請組織通過書審，與當責機構就實審之相關事項完成協議，即進入實審階段。

(4) 當責機構應於實審完成後，將實審結果以書面報告通知申請組織。

(5) 實審之結果為未通過者，書面報告應載明未通過之理由，並要求申請組織

於當責機構所指定之期限內，或於申請組織接獲書面報告之翌日起二個月內完成改善；就不符合事項採取矯正措施（corrective actions），當責機構將確認申請組織是否完成矯正措施，若申請組織屆期未完成矯正措施，則視為實審不通過。

5.1. CBPR 更新驗證

CBPR 驗證之效力為一年。組織於通過 CBPR 驗證滿八個月至一年間，應接受當責機構之更新驗證。

5.2. 授證

(1) 組織 CBPR 驗證通過後，當責機構就 CBPR 驗證結果進行審核，並將審核結果通知組織；審核結果為不通過者，上述通知應以書面附理由為之。

(2) 通過 CBPR 驗證之組織，當責機構將授予通過 CBPR 驗證之證明，作為受證組織之證明。

(3) 當責機構得於網站上公布受證組織之相關資訊（包括但不限於組織名稱、網址、驗證範圍或驗證有效期間）。

6. 受證組織之監督

(1) 當責機構為確保受證組織符合 CBPR 之要求，在 CBPR 驗證有效期間，當責機構得要求受證組織就其個人資料管理制度之狀況提出書面報告或相關資料，當責機構認為必要時並得對受證組織實施定期或不定期之實地檢查。受證組織應配合當責機構為執行本條所提出之相關要求，且實地檢查之費用由受證組織負擔。

(2) 受證組織有下列情形時，應立即以書面通知當責機構，並依當責機構要求提供相關文件：

(a) 受證組織之個人資料管理制度出現重要變更或有重要變更之計畫時。

(b) 組織所經營業務有變更時。

(c) CBPR 驗證申請文件所載受資料有變更時。

(3) 發生個資事故時，受證組織應即通知當責機構，並於查明後儘速向當責機構提出書面報告，說明事故之原因、損害狀況及處理之情形，必要時當責機構得派員查明事故。

(4) 任何人認為受證組織有違反 CBPR 要求時，得以電話、電子郵件或網站等方式向當責機構提出申訴，當責機構並應依「臺灣個人資料保護與管理制度紛爭解決機制運作要點」進行處理。

(5) 如受證組織任何不符合 CBPR 要求之情形，當責機構得要求受證組織於時限內改善，在受證組織未能證明其符合前述要求之前，當責機構有權暫停、終止受證組織關於 CBPR 驗證之效力或其他適當處置。

7. 受證組織之處置

7.1. 處置之發動

當責機構得視監督與檢查之結果、組織所通知或報告之內容或組織違反通知或報告義務之情形，依「處置等級標準暨裁定表」（附件）為以下之處置，並附理由以書面通知組織：

(1) 向該組織提出警告。
(2) 具體要求組織進行改善。
(3) 暫停組織對 CBPR Seal 之使用，暫停期間為一年以下。
(4) 終止組織對 CBPR Seal 之使用。

7.2. 對處置之異議

(1) 組織得於接獲處置通知之翌日起，五個工作日內，以書面具體申明理由向當責機構提出處置異議。
(2) 當責機構應就處置異議做出決定，並以書面通知組織。
(3) 在當責機構就處置異議做出決定前，原處置之效力不受影響。

7.3. 處置之公告

當責機構得公告組織受處置之內容。

8. 爭議處理

(1) 就 CBPR 驗證爭議事項，組織應按下列規定，向當責機構提出；如未依規定提出，視為無爭議：
   (a) 如為書審爭議，組織應於收受書審結果之翌日起五個工作日內以書面方式附理由提出。
   (b) 如為實審爭議，組織應於實審之閉幕會議上提出，如未能於閉幕會議解決爭議，組織應先請求當責機構，於通知實審結果之書面上載明或註記爭議項目，並於舉行閉幕會議之翌日起，五個工作日內以書面方式附理由提出。
(2) 當責機構應就爭議做出決定，並以書面通知組織。
(3) 組織對於前款之爭議如有疑義時，得向當責機構提出申訴。
(4) 爭議做出決定前，原書審或實審結果不受影響。

9. 費用之實施

當責機構如就 CBPR 驗證相關事項收取費用時；其收取項目或數額，由當責機構公告後實施，修訂時亦同。

10. 要點之實施

(1) 本要點由當責機構公告後實施，修訂時亦同。
(2) 本要點如經修正並公告實施後，應遵守修正實施後之規定。

附件：處置等級標準暨裁定表

一、處置等級標準

當責機構依規定，判斷嚴重程度據以採取相應於其等級的處置。

(1) 依事實按事故類型分類

(2) 判斷發生事實的原因，評斷組織有無責任。

(3) 對於事實發生的原因判斷為企業應負責任時，再考量事故的影響。

(4) 將嚴重程度區分為 1 至 10，依事故類型、原因及影響判斷等級。

分類發生的事實（事故類型）	判斷事實的原因（評斷有無責任）	事故的影響	嚴重程度等級
①. 竊取 ②. 竄改 ③. 毀損 ④. 滅失 ⑤. 洩漏 ⑥. 違法蒐集、處理或利用 ⑦. 違法目的外利用 ⑧. 違法行銷 ⑨. 違法國際傳輸 ⑩. 違法進行或不進行當事人權利行使	故意 （組織故意）	不考量	10
	過失 （制度運作不完備、設備不周全、監督責任等）	□洩漏或其他類型事故的個人資訊的內容（特種個人資料等） □涉及個人資料數量 □本人受害的發生狀況 □對社會的影響或對隱私標章制度的影響 □過去的發生事故經歷	根據事實內容個別判斷 1 至 10
	不可抗力	不考量	0

二、處置裁定

依嚴重程度等級，判斷處置裁定類型。

處置等級	處置內容		
	取得標章組織	CBPR 驗證中的組織	準備申請中的組織
10	終止組織對 CBPR Seal 之使用	中止 CBPR 驗證（一年內不得申請）	一年內不得申請
8、9	暫停組織對 CBPR Seal 之使用	相當於暫停 CBPR Seal 使用期間內中止驗證	相當於暫停 CBPR Seal 使用期間內不得申請
5 至 7	具體要求組織進行改善	繼續 CBPR 驗證	可申請
1 至 4	向該組織提出警告	繼續 CBPR 驗證	可申請
0	不採取任何處置	繼續 CBPR 驗證	可申請