全球跨境隱私規則（GLOBAL CBPR）
驗證規則

公告日期：2026 年 4 月 1 日

本文件旨在說明全球跨境隱私規則（Global Cross-Border Privacy Rules, Global CBPR）體系的基本要求，協助全球 CBPR 論壇認可之當責機構對申請組織進行審查，並確保審查流程的一致性。

當責機構負責接收申請組織提交的自我評量文件及相關佐證資料，查證其是否符合全球 CBPR 體系要求，並在適當情況下協助申請組織調整隱私政策與作業流程，以確保符合規範。符合基本準則的申請組織將由當責機構予以認證，並由當責機構依據評估標準負責監督其持續遵守全球 CBPR 體系。

本文件應與【全球 CBPR 自我評量問卷】一同檢視，以協助申請組織評估其是否符合規範之情形。

預防危害（Q1~5） 1
告知（Q6~9） 7
告知例外情形 17
限制蒐集（Q10~12） 19
個人資料利用（Q13~18） 25
當事人自主選擇（Q19~27） 37
當事人自主選擇機制例外情形 54
個人資料完整性（Q28~32） 56
安全維護（Q33~42） 62
近用及更正（Q43~45） 81
近用及更正機制例外情形 87
責任（Q46~57） 88

預防危害（Q1~5）

評估目的－*確保申請組織之個人資料保護制度係為了避免個人資料遭到濫用導致侵害個人權益而設計。此隱私原則認知，非法蒐集或濫用某些類別之個資種類（包含兒童個資）可能導致更嚴重的侵害，因此需要更完善之保護程度。本規則要求申請組織評估其所蒐集之個資之風險，並採取與個資濫用可能性及嚴重性相稱的安全維護措施。最後，若個資發生外洩，申請組織應通知當事人並提供相關資訊，使其能夠採取措施避免個資遭濫用。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
1. 對於機敏個人資料，是否已識別並採取適當之保護措施？如是，請說明。	若申請組織回答為「**是**」，當責機構應查證其提供之書面政策及程序。符合以下要求： ● 已盡適當注意義務； ● 判斷所蒐集之資料是否屬於機敏資料或應受特別保護之資料； ● 判斷是否涉及處理由外部組織移轉而來之機敏個資； ● 依法採取較對其他類型個人資訊更嚴謹之保護措施。 若申請組織回答為「**否**」，當責機構應通知申請組織必須符合本題之要求以遵循告知原則。		**TPIPAS 2021：8.4.7. 特種個人資料之蒐集、處理及利用限制** 組織針對病歷、醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料， 其程序應符合下列要求： (1) 組織人員原則禁止蒐集、處理及利用特種個人資料之要求。 (2) 例外得蒐集、處理或利用特種個人資料時，係屬合乎法律要求。 (3) 保存前二款相關紀錄。 (4) 必要時，額外之風險管控措施。 **TPIPAS 2021：8.7. 安全管理措**

			施 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資 料被竊取、竄改、毀損、滅失或洩漏之必要且適當之安全管理措施。如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。
2. 是否依據個資法及相關法規採取評估您所蒐集、處理及利用之個人資料是否屬於兒童個資之措施？	若申請組織回答為「**是**」，當責機構應查證其提供之書面政策及程序。符合以下要求： ● 評估組織蒐集、處理或揭露之個資，是否屬於個資法及相關法律所定義之兒童個資。 若申請組織回答為「**否**」，當責機構應通知申請組織必須符合本題之要求以遵循告知原則。		**TPIPAS 2021：11.5. 當事人同意** 組織於取得當事人同意時，宜注意當事人同意給予之真摯性、自主性、任意性、 具體特定且受充分告知。 組織於當事人撤回同意時，其當事人撤回同意之方式宜與給予同意之方式等同便利。 **TPIPAS 2021：11.7. 未成年人之保護** 組織於蒐集、處理或利用未成

			年人個人資料時，宜有較高之注意義務與安全管理措施，並應確認已採取措施足辨識未成年之法定代理人已有效代為同意，或足辨識具其他符合法律規定之特定情形。
3. 如蒐集兒童個資，是否已採取措施驗證父母或監護人之同意之真實性？是否對兒童個資，或由資料來源之第三方組織標示為兒童個資者採取適當保護措施，確保具備合法的法律依據？	若申請組織回答為「**是**」，當責機構應查證其提供之驗證父母或監護人同意之機制。 當責機構應要求申請組織就蒐集兒童個資之其他適當法律依據，提供具體說明，以證明其處理兒童個資時，已具備相應之程序。 若申請組織回答為「**否**」，當責機構應通知申請組織，倘其有處理兒童個人資訊之情事，必須符合本題之要求以遵循告知原則。		**TPIPAS 2021：11.5. 當事人同意** 組織於取得當事人同意時，宜注意當事人同意給予之真摯性、自主性、任意性、具體特定且受充分告知。組織於當事人撤回同意時，其當事人撤回同意之方式宜與給予同意之方式等同便利。 **TPIPAS 2021：11.7. 未成年人之保護** 組織於蒐集、處理或利用未成年人個人資料時，宜有較高之注意義務與安全管理措施，並應確認已採取措施足辨識未成年之法定代理人已有效代為同意，或足辨識具其他符合法律規定之特定情形。

4. 是否採取相關機制，以識別並評估在資料處理過程中可能因濫用而對個人造成潛在損害之風險？是否依據潛在損害發生的可能性和嚴重程度採取相應措施，以降低損害風險？	若申請組織回答為「**是**」，當責機構應查證其提供之相關程序或機制。符合以下要求： ● 識別並評估因個資被濫用而可能產生損害的風險； ● 採取合適的保護措施以降低損害； ● 記錄風險評鑑結果； ● 在必要時實施保護措施。 若申請組織回答為「**否**」，當責機構應通知申請組織必須符合本題之要求以遵循告知原則。		**TPIPAS 2021：6.3. 因應風險之規劃** 組織於規劃個人資料管理制度時應將內外部議題、利害關係人需求與相關本制度規範納入考量，規劃風險管理之原則、框架及過程，辨識相關風險與因應管 控措施，並得適時採納從設計與預設階段著手隱私保護（Privacy by design and default）之概念。 **TPIPAS 2021：6.3.1. 個人資料隱私衝擊風險評鑑** 組織應建立與維持個人資料相關之風險分析與評估程序，風險分析與評估程序應包含以下事項： (1) 建立與維護個人資料風險準則，包括風險接受準則與實施個人資料風險分析與評估之準則。 (2) 確保重複之個人資料風險分析與評估產生一致、有效及可比較之結果。

			(3) 識別個人資料風險與風險擁有者。 (4) 分析個人資料風險，包括風險實現時可能導致之潛在後果、風險發生之實際可能性與決定風險等級。 (5) 評估個人資料風險，包括比較風險分析結果與訂定已分析風險之風險處理優先次序。 (6) 所識別風險應包含組織與當事人之影響。 **TPIPAS 2021：6.3.2. 風險管控措施** 組織應考量個人資料隱私衝擊風險評鑑結果，決定適當之個人資料風險管控措施，並確保符合附表A所列必要管理措施。
5. 是否已建立相應流程，當發生個資事故，且可能對受影響之個人造成重大損害時，能在合理延遲的情況下通知受影	若申請組織回答為「**是**」，當責機構應查證其提供之書面政策和程序，是否得在不造成不合理延遲的情況下通知受影響的個人。通知受影響個人的內容應包括： ● 外洩事件的性質和範圍；		**TPIPAS 2021：8.10. 事故之緊急應變** 為避免事故可能產生之不利益及影響，組織應訂定並落實事故緊急應變措施。相關措施應至少包括：

響的個人？如是，請說明。	● 涉及的個資類型； ● 受影響個人可採取保護自己免受潛在傷害之步驟； ● 簡要說明申請組織採取之行動，如：調查外洩事件； ● 減輕損害和防止進一步外洩； ● 申請組織個資窗口的聯絡資訊。 若申請組織回答為「否」，當責機構應通知申請組織必須符合本題之要求以遵循告知原則。		(1) 知悉事故時於適當時機及方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 採取即時有效之應變措施，防止事故之擴大，及記載相關事實、影響、已採取之因應措施，並保存相關紀錄。 (3) 避免類似事件再次發生之方法。 (4) 將事故即時通報主管機關及其他依組織所識別之法令應通報之政府機關。 (5) 將事故即時通報授證機關。 組織應將通知或通報之內容、方式、時限與通報範圍、應變措施及紀錄保存，以供備查。

告知（Q6~9）

評估目的－*確保資料當事人瞭解申請組織之個人資料政策以及免於告知例外情形，包括其個人資料於何時蒐集、傳輸至何人及其特定目的。參閱下方「告知例外情形」之說明。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
6. 是否提供隱私聲明，且內容清楚易懂、易於取得？若「是」，請提供隱私聲明文本及其超連結。	若申請組織回答為「**是**」，當責機構應查證其隱私政策及實務作法（或其他隱私聲明）符合以下要求： ● 可於申請組織網站上查閱，例如於網頁上張貼文字、網址連結、附件、彈跳視窗、涵蓋於問答集（常見問題）或者以其他方式呈現（必須具體說明）； ● 符合全球CBPR隱私綱領之基本原則； ● 易於尋找且可近用； ● 適用於所有線上或離線方式蒐集的個人資料； ● 載明其隱私聲明之生效日期。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須符合本題之要求以遵循告	**TPIPAS：2016 4.2. 個人資料保護管理政策** 組織應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。 **TPIPAS：2016 4.5.1.1. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 5.2. 個人資料保護管理政策** 最高管理階層應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。個人資料保護管理政策應包含以下事項： (1) 個人資料管理制度之目標。 (2) 承諾落實本制度規範要求事項與法令。 (3) 承諾定期檢視與持續改善。 **TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (4) 確認蒐集時具備特定目的，

	知原則。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。	**TPIPAS：2016 4.5.1.6. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **個人資料保護法第 8 條第 1 項** 公務機關或非公務機關依第十五條或第十九條規定向當事人	並符合法律規定之特定情形。 (5) 其他法令規定蒐集時應履行之義務。 (6) 保存前二款相關紀錄。 **TPIPAS：2021 8.4.8. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **TPIPAS：2021 8.5.2. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴

		蒐集個人資料時，應明確告知當事人下列事項： 一、公務機關或非公務機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 **個人資料保護法第 9 條第 1 項** 公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。	與諮詢之規則與流程並保存相關紀錄。
6(a) 是否於隱私聲明中說明蒐集個人資料的方法？	若申請組織回答為「**是**」，當責機構應查證： ● 其隱私聲明載明蒐集個人資料	同上。	

	的實務作法與政策且適用於所蒐集的所有個人資料； ● 其隱私聲明載明經直接蒐集、或經由第三方或代理人蒐集之個人資料類型，以及； ● 其隱私聲明載明所蒐集的所有個人資料之類別與特定來源。 若申請組織回答為「**否**」，當責機構應通知申請組織必須符合本題之要求以遵循告知原則。		
6(b) 是否於隱私聲明中說明蒐集個人資料之目的？	若申請組織回答為「**是**」，當責機構應查證其隱私聲明確實已告知資料當事人蒐集個人資料之目的。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織其隱私聲明必須包含蒐集個人資料之目的。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。	同上。	
6(c) 是否於隱私聲明中告知個人資料提供予第三方及其目的？	若申請組織回答為「**是**」，當責機構應查證其隱私聲明確實已告知資料當事人其個人資料將會或可能提供予第三方共享，**並列出第三方單位名稱或所屬產業別，以及其目的**。	同上。	

	若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須告知個人資料將會提供予第三方並載於隱私聲明。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。		
6(d) 是否於隱私聲明中公開組織名稱、地址，以及組織內部個人資料保護窗口之聯絡資訊？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證其隱私聲明確實提供其名稱、地址及**有效**電子郵件信箱。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須揭露相關資訊以遵循告知原則。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。	同上。	
6(e) 是否於隱私聲明中說明個人資料利用及揭露之情形？	若申請組織回答為「**是**」，當責機構應查證其隱私聲明包括如何利用與揭露所蒐集之個人資料。有關個人資料利用合規指引，參閱 Q8。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須提供相關資訊以遵循告知原則。若申請組織說明其適用「告知	同上。	

	例外情形」，當責機構應查證是否符合適用情形。		
6(f) 是否於隱私聲明中說明資料當事人如何近用及更正個人資料？	若申請組織回答為「**是**」，當責機構應查證其隱私聲明包含： ● 資料當事人（以電子或傳統非電子的方式）近用其個人資料的流程。 ● 資料當事人更正其個人資料的流程。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須提供近用及更正個人資料相關資訊（包括處理近用及更正請求的回應時間），以遵循告知原則。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。	同上。	
7. 是否於直接或間接蒐集個人資料時，完成告知義務？	若申請組織回答為「**是**」，當責機構應查證申請組織已告知資料當事人正在或已經蒐集個人資料**<u>並以合理方式向資料當事人進行告知</u>**。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須告知資料當事人正在蒐集	**TPIPAS：2016 4.5.1.1. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。	**TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。

	個人資料以遵循告知原則。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。	(3) 保存前二款相關紀錄。 **TPIPAS：2016 4.5.1.6. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **個人資料保護法第 8 條第 1 項** 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項： 一、公務機關或非公務機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、	(3) 保存前二款相關紀錄。 **TPIPAS：2021 8.4.8. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。

		對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 **個人資料保護法第 9 條第 1 項** 公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。	
8. 是否於直接或間接蒐集個人資料時，告知蒐集個人資料之目的？	若申請組織回答為「**是**」，當責機構應查證申請組織已向資料當事人解釋蒐集個人資料之目的。解釋方式應以口頭或書面方式傳達。例如，透過網站，以網頁上的文字、附件、彈出視窗或其他方式。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織應符合本題之要求。若申請組織	同上。	**TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.4.8. 告知義務**

	說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。		**之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。
9. 是否於蒐集個人資料時，告知個人資料可能提供予第三方？	若申請組織回答為「**是**」，當責機構應查證申請組織已告知資料當事人其個人資料將會或可能提供予第三方共享以及其目的。 若申請組織回答為「**否**」且不適用「告知例外情形」，當責機構應通知申請組織必須告知個人資料將會提供予第三方。若申請組織說明其適用「告知例外情形」，當責機構應查證是否符合適用情形。	**TPIPAS：2016 4.5.1.1. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2016 4.5.1.6. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序	**TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.4.8.. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程

		暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **個人資料保護法第 8 條第 1 項** 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項： 一、公務機關或非公務機關名稱。 二、蒐集之目的。 三、個人資料之類別。 四、個人資料利用之期間、地區、對象及方式。 五、當事人依第三條規定得行使之權利及方式。 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。	序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。

		個人資料保護法第 9 條第 1 項 公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。	

告知例外情形

於蒐集個人資料時，符合以下情形之一者，無需遵守GLOBAL CBPR告知原則：

i. **符合明確性：**依資料當事人提供資料可推斷為已取得當事人同意，於蒐集、利用、第三方共享個人資料時，資料控管者無需進行告知（例如：於業務場合，資料當事人將他/她的名片主動提供另一位當事人，則無需針對該資料的蒐集與正常利用進行告知）。

ii. **公開資料之蒐集：**蒐集及利用公開可獲得之資料時，資料控管者無需進行告知。

iii. **技術上難以達成：**當個人資料是透過自動化蒐集時（例如：使用者登入網站，網站透過cookie自動蒐集資料），資料控管者無需於蒐集時或蒐集前進行告知。但是，資料控管者應於實際可執行之最短時間內進行告知。

iv. **因應政府機關依法要求揭露資料：**為調查目的而向執法機關揭露資料時，則個人資料控制者無需進行告知，否則將可能影響調查之公正性。

v. **依合法程序提供第三方：**根據合法程序的要求而向第三方揭露資料時（例如：民事訴訟過程中的蒐證（discovery）請求），資料控管者無需進行告知。

vi. **由第三方蒐集取得：**若個人資料是從第三方蒐集而來，資料控管者無需在蒐集時或蒐集前進行告知。

vii. **基於合法調查之目的：**若進行告知將可能損及資料的可用性或正確性，且個人資料之蒐集、利用與揭露行為基於調查目的被視為合理時，資料控管者無需進行告知。調查包含是否違反行為守則、違反契約或國內法之內部或外部調查。

緊急情況之措施：在危及資料當事人生命、健康或安全的緊急情況下，資料控管者無需進行告知。

限制蒐集（Q10~12）

評估目的—*確保個人資料僅限於特定目的內蒐集。個人資料之蒐集應與特定目的相關，而蒐集是否符合比例原則將影響與特定目的相關之判斷。在任何情況之下，蒐集個人資料之方式必須合法且正當。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
10. 如何取得個人資料： 10 (a) 從資料當事人直接蒐集？ 10 (b) 從第三方間接蒐集？ 10 (c) 其他方式。若「是」，請說明。	當責機構應查證申請組織取得個人資料之對象。 **若申請組織對 Q5(a)~(c) 任一題回答為「是」**，當責機構應查證申請組織取得個人資料之實務作法。 Q5(a)~(c) 必須至少一題回答為「是」。若並非如此，當責機構應通知申請組織並未正確完整回答。	**TPIPAS：2016 4.4.2. 納入管理之個人資料範圍** 組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。 **TPIPAS：2016 4.5.1. 基本原則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。	**TPIPAS：2021 8.2. 納入管理之個人資料範圍** 組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。。 **TPIPAS：2021 8.4.1. 總則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。
11. 個人資料之直接或間接蒐集是否僅限於特定目的或	若申請組織回答為**「是」**，並且表示僅於特定目的或與目的相關之其他目的範圍內蒐集個人資料，當	**TPIPAS：2016 4.5.1. 基本原則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用	**TPIPAS：2021 8.4.1. 總則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用

與目的相關之其他目的範圍內？	責機構應要求申請組織說明： ● 蒐集之資料類型； ● 蒐集之特定目的範圍；以及 ● 利用之方式； ● 與目的相關之其他目的範圍。 依據上述回答，當責機構應查證申請組織於特定目的或與目的相關之其他目的範圍內限制蒐集的個人資料數量及類型。 若申請組織回答為「**否**」，當責機構應通知申請組織必須限制限於特定目的之內利用所蒐集之個人資料。	方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 **TPIPAS：2016 4.5.1.1. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 **個人資料保護法第5條** 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。 **個人資料保護法第15條** 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：	方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 **TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。

		一、執行法定職務必要範圍內。 二、經當事人同意。 三、對當事人權益無侵害。 **個人資料保護法第 19 條第 1 項** 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。 三、當事人自行公開或其他已合法公開之個人資料。 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 五、經當事人同意。 六、為增進公共利益所必要。 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。	

		八、對當事人權益無侵害。	
12. 個人資料之直接或間接蒐集是否合法、正當，且符合國內個人資料保護法規相關要求？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應要求申請組織證明其已知曉並遵守國內規範個人資料蒐集之相關法規，且以正當、無欺騙的方式蒐集個人資料。 若申請組織回答為「**否**」，當責機構應通知申請組織必須以合法及正當方式蒐集個人資料以遵循限制蒐集原則。	**TPIPAS：2016 4.4.1. 識別法令及其他相關規範** 組織應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。 **TPIPAS：2016 4.5.1. 基本原則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 **TPIPAS：2016 4.5.1.1. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 8.1. 識別法令及其他相關規範** 組織應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。 **TPIPAS：2021 8.4.1. 總則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 **TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。

		個人資料保護法第5條 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。 **個人資料保護法第 15 條** 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、執行法定職務必要範圍內。 二、經當事人同意。 三、對當事人權益無侵害。 **個人資料保護法第 19 條第 1 項** 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。	

		三、當事人自行公開或其他已合法公開之個人資料。 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 五、經當事人同意。 六、為增進公共利益所必要。 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 八、對當事人權益無侵害。	

個人資料利用（Q13~18）

評估目的—*確保個人資料之利用限於蒐集之特定目的或與目的相關之其他目的範圍內。本節題目涵蓋個人資料的利用、傳輸與揭露。判斷是否符合此項原則應考量資料的性質、蒐集情境及預期用途。判斷利用目的是否與蒐集目的相關或相符之重點乃是基於或有利目的達成。而與目的相關之其他目的範圍內可擴張解釋，例如：設計並利用集中式資料庫使人力管理更有效率；由第三方處理員工薪資名冊業務；利用基於授信之目的所蒐集的資料作為後續收取欠款用途。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
13. 是否依據隱私聲明或蒐集時所告知之蒐集特定目的或與目的相關之其他目的範圍內，利用直接或間接蒐集之個人資料？請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織之政策及程序書，確保利用直接或間接蒐集之個人資料，限於蒐集時隱私聲明所告知之蒐集特定目的或與目的相關之其他目的範圍內。 若申請組織回答為「**否**」，當責機構應考量 Q9 回答。	**TPIPAS：2016 4.5.1. 基本原則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 **TPIPAS：2016 4.5.1.2. 處理** 組織為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。	**TPIPAS：2021 8.4.1. 總則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 **TPIPAS：2021 8.4.3. 處理** 組織為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。

		(2) 其他法令規定處理時應履行之義務。 (3) 組織應訂定適當且合法程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。	(2) 其他法令規定處理時應履行之義務。 (3) 組織應訂定適當且合法程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料。 (4) 保存前三款相關紀錄。 **TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。
14. 若 Q8 回答為「否」，於蒐集之特定目的範圍外利用所蒐集之個人資料，是否符合下列情形？請說明。 14(a) 取得資料當事人明確同意？	若申請組織 Q8 回答為「**否**」，申請組織應具體說明於蒐集之特定目的範圍外利用所蒐集之個人資料符合何種情形。 若申請組織選擇回答 Q9(a) ，當責機構應要求申請組織具體說明如何取得當事人之同意，且應查證申請組織利用個人資料是基於	**TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。

14(b) 基於法律明文規定？	取得資料當事人明確同意之方式，包含但不限於： ● 蒐集時於線上取得； ● 透過電子郵件取得； ● 透過偏好設定或個人檔案取得； ● 透過電話取得； ● 透過郵寄信件取得；或 ● 其他（應具體說明）。 若申請組織選擇回答 Q9(a) ，當責機構應要求申請組織說明如何取得同意，且應符合 Q17~Q19 所規定之要求。 若申請組織選擇回答 Q9(b) ，當責機構應要求申請組織具體說明，所蒐集個人資料之共享、利用、揭露方式符合法律明文規定。 若申請組織未選擇回答 Q9(a) 或 Q9(b) ，當責機構應通知申請組織，除有符合本題所列之情形者外，必須於蒐集特定目的或與目的相關之其他目的範圍內，利用	**個人資料保護法第16條** 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。 **個人資料保護法第20條第1項** 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。	

	所蒐集之個人資料，以遵循個人資料利用原則。	但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。	
15. 是否將直接或間接蒐集之個人資料揭露予其他個人資料控管者？若「是」，請說明。	若申請組織 Q10、Q11 回答為**「是」**，當責機構應查證申請組織除有因資料當事人要求提供服務或產品所需而取得明確同意或基於法律明文規定之情形者外，必須於蒐集特定目的或與目的相關之其他目的範圍內，將個人資料揭露予其他資料控管者或傳輸予資料處理者。	**TPIPAS：2016 4.4.2. 納入管理之個人資料範圍** 組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。 **TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應	**TPIPAS：2021 8.2. 納入管理之個人資料範圍** 組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。 **TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應

	此外，當責機構應要求申請組織說明： 1） 揭露或傳輸之資料類型。 2） 揭露之資料其蒐集之特定目的範圍。 3） 為了實現明確目的（例如：履行訂單等）所為之揭露行為。 4）	符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。	符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。
16. 是否將個人資料傳輸予個人資料處理者？若「是」，請說明。	依據上述回答，當責機構應查證申請組織，係基於蒐集之特定目的或與目的相關之其他目的範圍內，揭露或傳輸個人資料。	**TPIPAS：2016 4.4.2. 納入管理之個人資料範圍** 組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。 **TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 8.2. 納入管理之個人資料範圍** 組織應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。 **TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督**

		TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。	組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。

		(9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	(9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。
17. 若 Q15 或 Q16回答為「是」，上述個人資料揭露、傳輸行為是否於蒐集特定目的或與目的相關之其他目的範圍內為之？若「是」，請說明。		同上。	**TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選

			任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。

			(10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。 組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。
18. 若 Q17 回答為「否」或者在其他適當情況下，上述個人資料揭露、傳輸行為是否符合下列情形？ 18(a) 取得資料當事人明確同意？ 18(b) 因資料當事人要求提供服務或產品所需？ 18(c) 基於法律明文規定？	若申請組織 Q18 回答為「否」，申請組織應具體說明於蒐集之特定目的範圍外揭露或傳輸個人資料符合何種情形。 若申請組織選擇回答 Q18(a) ，當責機構應要求申請組織具體說明如何取得資料當事人之同意，於特定目的範圍外進行資料揭露或傳輸行為，包含但不限於： ● 蒐3集時於線上取得； ● 透過電子郵件取得； ● 透過偏好設定或個人檔案取得； ● 透過電話取得； ● 透過郵寄信件取得；或 ● 其他（應具體說明）。	**TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。 **TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。	**TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安

	若申請組織選擇回答 Q13(b) ，當責機構應要求申請組織具體說明為何個人資料之揭露、傳輸是因提供服務或產品所需。當責機構應查證之。 若申請組織選擇回答 Q13(c) ，當責機構應要求申請組織具體說明個人資料之揭露、傳輸之具體法律明文規定為何。除非申請組織受到保密條款約束，申請組織應列出具體法律規定之要求。當責機構應查證是否適用該法律規定。 若申請組織 Q13(a)、(b)、(c) 回答為「**否**」，當責機構應通知申請組織，除有符合本題所列之情形者外，必須於蒐集特定目的或與目的相關之其他目的範圍內，揭露或傳輸所蒐集之個人資料，以遵循個人資料利用原則。	(2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。

		個人資料保護法第16條 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。 **個人資料保護法第20條第1項** 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。	組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。

		但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。	

當事人自主選擇（Q19~27）

評估目的－*確保資料當事人對於其個人資料之蒐集、利用及揭露擁有自主選擇權利。此項原則認為在某些情況下，若資料當事人同意已被明確推定或者無適用必要時，無需提供當事人自主選擇機制。參閱下方「當事人自主選擇機制例外情形」之說明。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則	
19. 是否提供資料當事人可就其個人資料之蒐集進行自主選擇的機制？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織對於當事人自主選擇機制提供具體說明，於蒐集個人資料時資料當事人得透過何種方式自主選擇，包含但不限於： ● 蒐集時於線上取得； ● 透過電子郵件取得； ● 透過偏好設定或個人檔案取得； ● 透過電話取得； ● 透過郵寄信件取得；或 ● 其他（應具體說明）。 當責機構應查證該機制已建立且運作，並清楚說明個人資料蒐集之目的。	**TPIPAS：2016 4.5.1.1. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2016 4.5.1.6. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。	**TPIPAS：2021 8.4.2. 蒐集** 組織針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.4.8. 告知義務之履行** 組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。

	若申請組織回答為「**否**」，申請組織應具體說明其適用「當事人自主選擇機制例外情形」，當責機構應查證是否符合適用情形。 若申請組織回答為「**否**」且不適用「當事人自主選擇機制例外情形」，當責機構應通知申請組織於蒐集個人資料時必須提供當事人自主選擇機制。	(2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。 **個人資料保護法第 15 條**	(2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。

		公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、執行法定職務必要範圍內。 二、經當事人同意。 三、對當事人權益無侵害。 **個人資料保護法第 19 條第 1 項** 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。 三、當事人自行公開或其他已合法公開之個人資料。 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 五、經當事人同意。 六、為增進公共利益所必要。	

		七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 八、對當事人權益無侵害。	
20. 是否資料當事人可就其個人資料之利用進行自主選擇的機制？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織對於當事人自主選擇機制提供具體說明，於利用個人資料時資料當事人得透過何種方式自主選擇，包含但不限於： ● 蒐集時於線上取得； ● 透過電子郵件取得； ● 透過偏好設定或個人檔案取得； ● 透過電話取得； ● 透過郵寄信件取得；或 ● 其他（應具體說明）。 當責機構應查證該機制已建立且運作，並清楚說明個人資料利用之目的。若適用「當事人自主選擇機制例外情形」且資料後續仍有利用之需要，必	**TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。 **TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理**	**TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理**

	須於蒐集時提供當事人自主選擇機制。若適用「當事人自主選擇機制例外情形」且於蒐集後但有下列利用情形之前，得提供當事人自主選擇機制： ● 於特定目的範圍外利用所蒐集之個人資料； ● 個人資料可能揭露或分享予非服務提供者之第三方。 若申請組織回答為「**否**」，申請組織應具體說明其適用「當事人自主選擇機制例外情形」，當責機構應查證是否符合適用情形。 若申請組織回答為「**否**」且不適用「當事人自主選擇機制例外情形」，當責機構應通知申請組織於利用個人資料時必須提供當事人自主選擇機制。	針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。 **個人資料保護法第16條** 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經	針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。

		蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。 **個人資料保護法第20條第1項** 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。	

21. 是否提供資料當事人可就其個人資料之揭露進行自主選擇的機制？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織對於當事人自主選擇機制提供具體說明，於揭露個人資料時資料當事人得透過何種方式自主選擇，包含但不限於： ● 蒐集時於線上取得； ● 透過電子郵件取得； ● 透過偏好設定或個人檔案取得； ● 透過電話取得； ● 透過郵寄信件取得；或 ● 其他（應具體說明）。 當責機構應查證該機制已建立且運作，並清楚說明個人資料揭露之目的。若適用「當事人自主選擇機制例外情形」且資料後續仍有揭露之需要，必須於蒐集時提供當事人自主選擇機制。若適用「當事人自主選擇機制例外情形」且於蒐集後但有下列揭露情形之前，得提供當事人自主選擇機制： ● 於特定目的範圍外揭露所蒐集之個人資料予非	**TPIPAS：2016 4.5.1.3. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。 **TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。	**TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.3 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。

	服務提供者之第三方；或當責機構發現申請機構之當事人自主選擇機制並未清楚明顯呈現或者未於蒐集之特定目的內。 若申請組織回答為「**否**」，申請組織應具體說明其適用「當事人自主選擇機制例外情形」，當責機構應查證是否符合適用情形。 若申請組織回答為「**否**」且不適用「當事人自主選擇機制例外情形」，當責機構應通知申請組織於揭露個人資料時必須提供當事人自主選擇機制。	(2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。 **個人資料保護法第16條** 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。	(2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。

		個人資料保護法第20條第1項 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。	
22. 是否允許資料當事人隨時對接收直接行銷做出選擇？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織之當事人自主選擇行銷機制確實清楚明顯。		**TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之

	● 讓資料當事人得在適用的情況下對接收直接行銷做出選擇。 ● 機制妥當且正常運作。 若申請組織回答為「**否**」，當責機構應通知申請組織於直接行銷時必須提供當事人自主選擇機制。		義務。 (3) 保存前二款相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 8.4.5. 行銷** 組織針對利用個人資料進行行銷，其程序應符合下列要求：

			(1) 提供當事人拒絕接受行銷之方式。 (2) 當事人可隨時拒絕接受行銷之管道，並於表示拒絕接受後，立即停止利用 其個人資料為行銷之用途。 (3) 保存前二款相關紀錄。
23. Q19、Q20、Q21提及有關資料當事人能夠限制蒐集、利用、揭露其個人資料之當事人自主選擇機制，是否清楚明顯？	若申請組織回答為「**是**」，當責機構應查證申請組織之當事人自主選擇機制確實清楚明顯。 若申請組織回答為「**否**」，或當責機構發現申請組織之當事人自主選擇機制並未清楚明顯，當責機構應通知申請組織提供當事人自主選擇機制必須清楚明顯，以遵循當事人自主選擇原則。	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.2. 當事人行使權利之程序事項** 組織為處理 4.5.2.1.之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。

		(4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	(4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。
23. Q19、Q20、Q21 提及有關資料當事人能夠限制蒐	若申請組織回答為「**是**」，當責機構應查證申請組織之當	**TPIPAS：2016 4.5.1.6. 告知義務之履行**	**TPIPAS：2021 8.4.8. 告知義務之履行**

集、利用、揭露其個人資料之當事人自主選擇機制，是否淺顯易懂？	事人自主選擇機制確實淺顯易懂。 若申請組織回答為「**否**」，或當責機構發現申請組織之當事人自主選擇機制並未淺顯易懂，當責機構應通知申請組織提供當事人自主選擇機制必須淺顯易懂，以遵循當事人自主選擇原則。	組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：20164.5.2.2. 當事人行使權利之程序事項** 組織為處理 4.5.2.1.之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。	組織針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3) 針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 **TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。

		(3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	(3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。

25. Q19、Q20、Q21 提及有關資料當事人能夠限制蒐集、利用、揭露其個人資料之當事人自主選擇機制，是否可近用且可負擔？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織之當事人自主選擇機制確實可近用且可負擔。 若申請組織回答為「**否**」，或當責機構發現申請組織之當事人自主選擇機制並未可近用且可負擔，當責機構應通知申請組織提供當事人自主選擇機制必須可近用且可負擔，以遵循當事人自主選擇原則。	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。
26. 是否以有效、迅速執行之方式提供當事人自主選擇機制？如有必要，請以附件說明。	若申請組織已建立當事人自主選擇機制，當責機構應要求申請組織提出相關政策或程序，以證明資料當事人如何落實 Q14~16 當事人自主選擇機制。	**TPIPAS：2016 4.5.1. 基本原則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。	**TPIPAS：2021 8.4.1. 總則** 組織應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。

	若申請組織未建立任何機制，申請組織應具體說明其適用「當事人自主選擇機制例外情形」，當責機構應查證是否符合適用情形。 若申請組織回答為「**否**」且不適用「當事人自主選擇機制例外情形」，當責機構應通知申請組織必須以有效、迅速執行之方式提供當事人自主選擇機制。	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。
27. 當蒐集目的已滅失，是否允許資料當事人撤回其同意？是否設有相應程序以回應	若申請組織已建立當事人自主選擇機制，當責機構必須確認申請組織已提供相關機制之說明，使個人得於其資訊不再為所述目的所需時，隨時撤		**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資

停止利用個資之請求？	回同意或請求停止使用及揭露其個人資訊，惟須受法律或契約義務保留該資訊之限制。當責機構必須確認該等機制已建置且可實際運作。 若申請組織回答「否」，當責機構必須告知該申請組織，實施此類程序為符合本隱私原則之必要條件。		料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利之方式。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 11.5. 當事人同意** 組織於取得當事人同意時，宜注意當事人同意給予之真摯性、自主性、

			任意性、具體特定且受充分告知。組織於當事人撤回同意時，其當事人撤回同意之方式宜與給予同意之方式等同便利。

當事人自主選擇機制例外情形

於蒐集個人資料時，符合以下情形之一者，無需遵守GLOBAL CBPR當事人自主選擇原則：

i. **符合明確性：**依資料當事人提供資料可推斷為已取得當事人同意，於蒐集、利用、第三方共享個人資料時，資料控管者無需提供當事人行使自主選擇機制。

ii. **公開資料之蒐集：**蒐集及利用公開可獲得之資料時，資料控管者無需提供當事人行使自主選擇機制。

iii. **技術上難以達成：**當個人資料是透過自動化蒐集時（例如：使用者登入網站，網站透過cookie自動蒐集資料），資料控管者無需於蒐集時或蒐集前提供當事人行使自主選擇機制。但是，資料控管者應於蒐集後提供當事人行使自主選擇機制。

iv. **由第三方蒐集取得：**若個人資料是從第三方蒐集而來，資料控管者無需提供當事人行使自主選擇機制。但是，若個人資料控管者委託第三方蒐集個人資料，資料控管者應指示第三方於蒐集資料時提供當事人行使自主選擇機制。

v. **應政府機關依法要求揭露資料：**為調查目的而向執法機關揭露資料時，則個人資料控制者無需提供當事人行使自主選擇機制，否則將可能影響調查之公正性。

vi. **依合法程序提供第三方：**根據合法程序的要求而向第三方揭露資料時（例如：民事訴訟過程中的蒐證（discovery）請求），資料控管者無需提供當事人行使自主選擇機制。

vii. **基於合法調查之目的：**若提供當事人行使自主選擇機制將可能損及資料的可用性或正確性，且個人資料之蒐集、利用與揭露行為基於調查目的被視為合理時，資料控管者無需提供當事人行使自主選擇機制。調查包含是否違反行為守則、違反契約或國內法之內部或外部調查。

緊急情況之措施：在危及資料當事人生命、健康或安全的緊急情況下，資料控管者無需提供當事人行使自主選擇機制。

個人資料完整性（Q28~32）

評估目的—*確保資料控管者維持資料之正確性與完整性並持續更新。此項原則認為資料控管者之義務僅限於利用目的之必要範圍內。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
28. 是否採取措施以查證所持有之個人資料，於利用目的之必要範圍內，保持最新、正確及完整？若「是」，請說明。	若申請組織回答為「**是**」，當責機構必須要求申請組織提供相關程序，以查證並確保個人資料於利用目的之必要範圍內為最新、正確及完整。 **<u>當責機構將查證申請組織是否建置合理程序，使個人資料於利用目的之必要範圍內，保持最新、正確及完整。</u>** 若申請組織回答為「**否**」，當責機構應通知申請組織必須建置相關程序以查證並確保個人資料於利用目的之必要範圍內為最新、正確及完整，以遵循個人資料完整性原則。	**TPIPAS：2016 4.5.3.1. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。	**TPIPAS：2021 8.6. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。

29. 是否設置機制，於利用目的之必要範圍內，更正或更新個人資料？請說明。如有必要，請以附件說明。	若申請組織回答為「**是**」，當責機構應要求申請組織提供個人資料更正之相關程序及措施，以更正不正確、不完整且未更新的個人資料，包括但不限於提供資料當事人質疑資料正確性之程序，**例如：以電子郵件、郵寄信件、電話或傳真、網站或其他方式，接受資料當事人更正個人資料之請求。當責機構應查證該機制已建立且運作。** 若申請組織回答為「**否**」，當責機構應通知申請組織必須建置相關程序或措施以查證並確保個人資料於利用目的之必要範圍內為最新、正確及完整，以遵循個人資料完整性原則。	**TPIPAS：2016 4.5.2.4. 當事人請求個人資料補充、更正、刪除、停止蒐集、處理及利用程序** 組織針對當事人請求補充、更正、刪除、停止蒐集、處理或利用個人資料，其程序應符合下列要求： (1) 確保於30日內為准駁之決定。 (2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (3) 決定延長 30 日作出准駁之決定時，應附理由以書面通知當事人。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.3.1. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.6. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。

		更正或補充後，通知曾提供利用對象。	
30. 當個人資料因其不正確、不完整、未更新將影響其利用目的，但於資料傳輸後已更正時，是否將更正內容通知個人資料所傳輸之處理者、代理人或其他服務提供者？若「是」，請說明。	若申請組織回答為「**是**」，當責機構必須要求申請組織提供相關程序以證明申請組織將更正內容通知個人資料所傳輸之處理者、代理人或其他服務提供者，並確保其代表申請組織更正資料當事人之個人資料。 當責機構應查證該程序已建立且運作，並確認資料處理者、代理人或其他服務提供者確實代表申請組織更正資料當事人之個人資料。 若申請組織回答為「**否**」，當責機構應通知申請組織必須建立溝通程序將更正內容通知個人資料所傳輸之處理者、代理人或其他服務提供者，以遵循個人資料完整性原則。	**TPIPAS：2016 4.5.3.1. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。	**TPIPAS：2021 8.6. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。
31. 當個人資料因其不正確、不完整、未更新將影響其利	若申請組織回答為「**是**」，當責機構必須要求申請組織提供相關程序以證明申請組織將更正內容通	**TPIPAS：2016 4.5.3.1. 維持個人資料之正確性**	**TPIPAS：2021 8.6. 維持個人資料之正確性**

用目的，但於資料揭露後已更正時，是否將更正內容通知個人資料所揭露之第三方？若「是」，請說明。	知個人資料所揭露之第三方。當責機構應查證該程序已建立且運作。 若申請組織回答為**「否」**，當責機構應通知申請組織必須建立溝通程序將更正內容通知個人資料所揭露之第三方，以遵循個人資料完整性原則。	組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。	組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。
32. 是否要求受託處理資料之處理者、代理人或其他服務提供者，發現不正確、不完整、未更新之個人資料時向組織通報？	若申請組織回答為「是」，當責機構必須要求申請組織提供相關程序，以接收資料處理者、代理人或其他服務提供者通報之更正內容，確保其通報申請組織任何不正確、不完整、未更新之當事人個人資料。 當責機構應查證機制已建立且維運且個人資料已更正。 若申請組織回答為「否」，當責機構應通知申請組織必須建立接收資料處理者、代理人或其他服務提	**TPIPAS：2016 4.5.3.1. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。	**TPIPAS：2021 8.6. 維持個人資料之正確性** 組織為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於組織之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。

	供者之通報程序，以遵循個人資料完整性原則。	**TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。	**TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。

		(9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	(8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。

安全維護（Q33~42）

評估目的－*確保資料當事人將其個人資料委託申請組織時，申請組織將採取合理安全維護措施以避免資料遺失或防止他人未經授權不當存取、利用、修改、揭露或其他濫用個人資料之行為。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
33. 是否已施行資料安全政策？	若申請組織回答為「**是**」，當責機構應查證相關政策之書面文件。 若申請組織回答為「**否**」，當責機構應通知申請組織必須施行資料安全政策並以書面文件呈現，以遵循安全維護原則。	**TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。 (3) 技術性安全管理措施（如資訊傳輸、系統監看等）。	**TPIPAS：2021 8.7. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。 **TPIPAS：2021 7.3.1.1. 文件** 組織應製作及保存下列文件： (1) 個人資料保護管理政策。

		TPIPAS：2016 7.1.1. 文件 組織應製作及保存下列文件： (1) 個人資料保護管理政策。 (2) 個人資料保護管理手冊，及其相關具體規則。 (3) 個人資料內部管理程序相關表單。	(2) 個人資料保護管理手冊，及其相關具體規則。 (3) 個人資料內部管理程序相關表單。
34. 為避免資料遺失或防止他人未經授權不當存取、利用、修改、揭露或其他濫用個人資料之行為所產生之風險，請說明在物理面、技術面、行政管理面已採取哪些安全維護措施？	若申請組織提出說明，針對物理面、技術面、行政管理面之安全維護措施以保護個人資料，當責機構應查證安全保護措施確實具備，可包括： ● **驗證與存取控制（例如：密碼保護）；** ● **資料加密；** ● **邊界防護（例如：防火牆、侵入檢測）；** ● **審計軌跡；** ● **監控（例如：外部及內部稽核、弱點掃描）；** ● **其他（應具體說明）。** 申請組織應參酌組織規模及複雜度、活動性質及範圍、以及所蒐集	**TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。 (3) 技術性安全管理措施（如資訊傳輸、系統監看等）。	**TPIPAS：2021 8.7. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。

	個人資料之敏感度，於物理面、技術面、行政管理面採取合理之安全維護措施，以避免資料遭到外洩、遺失或防止他人未經授權不當存取、利用、修改、揭露或其他濫用個人資料之行為。 申請組織所採取之安全維護措施應與濫用行為之發生機率及可能造成的損害、個人資料之敏感度與內容成正比。 申請組織必須採取合理措施，要求個人資料傳輸之處理者、代理人、承包商或其他服務提供者保護個人資料免於遭到外洩、遺失或防止他人未經授權不當存取、利用、修改、揭露或其他濫用個人資料之行為。申請組織必須定期審查並重新評估其安全維護措施以判斷關聯性與有效性。 若申請組織表示**未採取**物理面、技術面、行政管理面之安全維護措施以保護個人資料，當責機構應通知		

	申請組織必須施行相關安全維護措施以遵循安全維護原則。		
35. 請說明 Q34 所採取之安全維護措施，如何與濫用行為之發生機率及可能造成的損害、個人資料之敏感度與內容成正比。	若申請組織提供說明於物理面、技術面、行政管理面採取之安全維護措施，當責機構應查證申請組織所採取之安全保護措施與其所識別的風險成正比。 申請組織基於組織規模及複雜度、活動性質及範圍、以及直接或間接蒐集個人資料之敏感度，應於物理面、技術面、行政管理面採取合理之安全維護措施，以避免資料遭到外洩、遺失或防止他人未經授權不當存取、利用、修改、揭露或其他濫用個人資料之行為。 為防止申請組織所蒐集的個人資料遭到未授權洩漏、遺失、利用、修改、揭露、提供、或存取，申請組織應實施合理的物理、技術、管理保護措施，保護措施應與申請組織之規模與複雜度、其活動的性質	**TPIPAS：2016 4.4.3. 風險管控措施** 組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨的風險，視需求訂定管控措施。 **TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。	**TPIPAS：2021 6.3.2. 風險管控措施** 組織應考量個人資料隱私衝擊風險評鑑結果，決定適當之個人資料風險管控措施，並確保符合附表 A 所列必要管理措施。 **TPIPAS：2021 8.7. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。

	與範圍、個人資料（包含直接和間接蒐集）的機敏性相稱。	(3) 技術性安全管理措施（如資訊傳輸、系統監看等）。	
36. 請說明如何使員工認知維護個人資料安全的重要性（例如：定期訓練或監督）？	當責機構應查證申請組織的員工透過定期訓練與監督，已瞭解維護個人資料安全的重要性與**相關義務**，方式包含： ● 員工訓練計畫。 ● 定期的員工會議或其他溝通形式。 ● 員工簽署的安全管理政策。 ● 其他（應具體說明）。 若申請組織未透過定期訓練與監督使員工瞭解維護個人資料安全的重要性與相關義務，當責機構必須通知申請組織必須執行相關程序，以遵循安全維護原則。	**TPIPAS：2016 4.2. 個人資料保護管理政策** 組織應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。 **TPIPAS：2016 4.5.3.3. 組織人員之監督** 組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 **TPIPAS：2016 4.6.1一般要求** 組織應以適當方式確保組織人員對個人資料管理具有正確的認知及能力。 **TPIPAS：2016 4.6.2基本教育訓練** 組織針對組織人員應提供必要的個人資料管理教育訓練。	**TPIPAS：2021 5.2. 個人資料保護管理政策** 最高管理階層應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。個人資料保護管理政策應包含以下事項： (1) 個人資料管理制度之目標。 (2) 承諾落實本制度規範要求事項與法令。 (3) 承諾定期檢視與持續改善。 **TPIPAS：2021 8.8. 組織人員之監督** 組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 **TPIPAS：2021 7.2.1. 總則**

		TPIPAS：2016 4.6.3. 權責人員教育訓練 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。 **TPIPAS：2016 4.6.4. 成果維持及改善措施** 組織應針對組織人員教育訓練成果建立紀錄與改善機制。	組織應以適當方式確保組織人員對個人資料管理、管理與獎懲制度具有正確的認知及能力。 **TPIPAS：2021 7.2.2.基本教育訓練** 組織針對組織人員應提供必要的個人資料管理教育訓練。 **TPIPAS：2021 7.2.3. 權責人員教育訓練** 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。 **TPIPAS：2021 7.2.4. 成果維持及改善措施** 組織應針對組織人員教育訓練成果建立紀錄與改善機制。
37. 是否採取與濫用行為之發生機率及可能造成的損害、個人資料之敏感度與內容成正比之安全保護措施：	若申請組織針對 Q37(a)~(d) 回答為「**是**」，當責機構應查證相關安全保護措施確實具備。 申請組織所採取之安全保護措施必須與濫用行為之發生機率及可能造成的損害、個人資料之敏感度	**TPIPAS：2016 4.4.3. 風險管控措施** 組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨的風險，視需求訂定管控措施。	**TPIPAS：2021 8.3. 風險管控措施** 組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨的風險，考

37(a) 實施教育訓練、員工管理或採取其他措施？ 37(b) 採用資訊管理系統，包含網路與軟體設計，以及資料處理、儲存、傳輸和銷毀措施？ 37(c) 對於攻擊、入侵或其他安全機制失效之偵測、預防及應變措施？ 37(d) 物理上之安全保護措施？	與內容成正比。申請組織必須採取適當且合理方式，例如：以資料加密保護個人資料。 若申請組織針對 Q37(a)~(d) 回答為「**否**」，當責機構應通知申請組織必須採取相關安全維護措施以遵循安全維護原則。	**TPIPAS：2016 4.4.4. 資源管理** 組織應提供並維持個人資料管理制度所需之人力及軟硬體資源，確保相關資源管理之實施、維持及改善方式之有效性，並就資源管理事項留存相關紀錄。 **TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。 (3) 技術性安全管理措施（如資訊傳輸、系統監看等）。	量個人資料隱私衝擊風險評鑑結果，落實適當風險管控措施。 **TPIPAS：2021 7.1. 資源** 組織應提供並維持個人資料管理制度所需之人力及軟硬體資源，確保相關資源管理之實施、維持及改善方式之有效性，並就資源管理事項留存相關紀錄。 **TPIPAS：2021 8.7. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。 **TPIPAS：2021 8.8. 組織人員之監督**

		TPIPAS：2016 4.5.3.3. 組織人員之監督 組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 **TPIPAS：2016 4.6.1. 一般要求** 組織應以適當方式確保組織人員對個人資料管理具有正確的認知及能力。 **TPIPAS：2016 4.6.2. 基本教育訓練** 組織針對組織人員應提供必要的個人資料管理教育訓練。 **TPIPAS：2016 4.6.3. 權責人員教育訓練** 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。 **TPIPAS：2016 4.6.4. 成果維持及改善措施**	組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 **TPIPAS：2021 7.2.1. 總則** 組織應以適當方式確保組織人員對個人資料管理、管理與獎懲制度具有正確的認知及能力。 **TPIPAS：2021 7.2.2. 基本教育訓練** 組織針對組織人員應提供必要的個人資料管理教育訓練。 **TPIPAS：2021 7.2.3. 權責人員教育訓練** 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。 **TPIPAS：2021 7.2.4.成果維持及改善措施** 組織應針對組織人員教育訓練成果建立紀錄與改善機制。

		組織應針對組織人員教育訓練成果建立紀錄與改善機制。	
38. 是否施行個人資料銷毀安全政策？	若申請組織回答為「**是**」，當責機構應查證個人資料銷毀安全政策確實施行。 若申請組織回答為「**否**」，當責機構應通知申請組織必須施行個人資料銷毀安全政策，以遵循安全維護原則。	**TPIPAS：2016 4.5.1.2. 處理** 組織為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。 (2) 其他法令規定處理時應履行之義務。 (3) 組織應訂定適當且合法程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。	**TPIPAS：2021 8.4.3. 處理** 組織為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。 (2) 其他法令規定處理時應履行之義務。 (3) 組織應訂定適當且合法程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料。 (4) 保存前三款相關紀錄。 **TPIPAS：2021 8.7. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。

		必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。 (3) 技術性安全管理措施（如資訊傳輸、系統監看等）。	如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。
39. 是否施行偵測、預防及應變措施，以預防攻擊、入侵或其他安全機制失效之情況？	若申請組織回答為「**是**」，當責機構應查證申請組織施行偵測、預防及應變措施，以預防攻擊、入侵或其他安全機制失效之情況。 若申請組織回答為「**否**」，當責機構應通知申請組織必須施行偵測、預防及應變措施，以預防攻擊、入侵或其他安全機制失效之情況，以遵循安全維護原則。	**TPIPAS：2016 4.4.6. 事故之緊急應變** 為避免事故可能產生之不利益及影響，組織應訂定事故緊急應變措施。相關措施應至少包括： (1) 查明後以適當方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 防止組織所受損害擴大之方法。 (3) 避免類似事件再次發生之方法。 (4) 將事故通報授證機關。 **TPIPAS：2016 4.5.3.2. 安全管理**	**TPIPAS：2021 8.10. 事故之緊急應變** 為避免事故可能產生之不利益及影響，組織應訂定事故緊急應變措施。相關措施應至少包括： (1) 查明後以適當方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 防止組織所受損害擴大之方法。 (3) 避免類似事件再次發生之方法。 (4) 將事故通報授證機關。 **TPIPAS：2021 8.7. 安全管理措**

		措施 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。 (3) 技術性安全管理措施（如資訊傳輸、系統監看等）。	**施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。
40. 是否制定流程以測試 Q39 所採取安全措施之有效性？請說明。	當責機構應查證申請組織於適當合理期間進行有效性測試，且依測試結果確實調整相關安全措施。	**TPIPAS：2016 6. 有效性量測** 組織應針對個人資料管理制度之實施，建立分析量測機制，藉由使用各項方式，使管理代表能判定個人資料管理制度內所建立之程序與機制是否有效，將所進行之分析量測作成紀錄，以確保制度之持續有效運作。	**TPIPAS：2021 9.1. 有效性量測** 組織應針對個人資料管理制度之實施，建立分析量測機制，藉由使用各項方式，使管理代表能判定個人資料管理制度內所建立之程序與機制是否有效，將所進行之分析量測作成紀錄，以確保制度之持續有效運作與改善。

		TPIPAS：2016 9.1. 定期檢視 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事項，並據以調整與修正個人資料管理制度： (1) 檢視報告。 (2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 組織業務領域之變化。 (4) 組織內外部之改善建議。	**TPIPAS：2021 9.3. 定期檢視** 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事項，並據以調整與修正個人資料管理制度： (1) 檢視報告。 (2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 組織業務領域之變化。 (4) 組織內外部之改善建議。

		(5) 其他可能影響個人資料管理制度的任何變更。	(5) 其他可能影響個人資料管理制度的任何變更。
41. 是否進行**風險評鑑或第三方驗證**？請說明。	當責機構應查證申請組織於適當合理期間進行**風險評鑑或第三方驗證**，並依據評鑑或驗證結果調整安全維護措施。例如：若申請組織施行隱私法遵內部稽核，當責機構應查證內部稽核提出之建議事項已確實執行。	**TPIPAS：2016 4.4.3. 風險管控措施** 組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨的風險，視需求訂定管控措施。 **TPIPAS：2016 8. 內部評量** 組織每年應依其特性規劃執行內部評量，以瞭解個人資料管理制度是否符合下列要求： (1) 符合法規及本制度之要求。 (2) 符合個人資料保護管理政策、手冊及相關具體規則之要求。 組織應規劃內部評量方式及流程，以決定內部評量之準則、範圍、頻率及方法。 組織應將內部評量之規劃、執行、報告、改善、追蹤等事項製作書面之內部評量報告。	**TPIPAS：2021 6.3.2. 風險管控措施** 組織應考量個人資料隱私衝擊風險評鑑結果，決定適當之個人資料風險管控措施，並確保符合附表 A 所列必要管理措施。 **TPIPAS：2021 9.2. 內部評量** 組織每年應依其特性規劃執行內部評量，以瞭解個人資料管理制度是否符合下列要求： (1) 符合法規及本制度之要求。 (2) 符合個人資料保護管理政策、手冊及相關具體規則之要求。 組織應規劃內部評量方式及流程，以決定內部評量之準則、範圍、頻率及方法。 組織應將內部評量之規劃、執行、報告、改善、追蹤等事項製作書面之內部評量報告。

		內部評量計畫應由具備個人資料內評師或個人資料驗證師資格者規劃，並由其確保內部評量執行之有效性與出具內部評量報告。 **TPIPAS：2016 9.1. 定期檢視** 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事項，	內部評量計畫應由具備個人資料內評師或個人資料驗證師資格者規劃，並由其確保內部評量執行之有效性與出具內部評量報告。 **TPIPAS：2021 9.3. 定期檢視** 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事項，

		並據以調整與修正個人資料管理制度： (1) 檢視報告。 (2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 組織業務領域之變化。 (4) 組織內外部之改善建議。 (5) 其他可能影響個人資料管理制度的任何變更。 **TPIPAS：2016 9.2. 矯正及預防措施** 組織針對內部評量及本管理制度實施之結果，應規劃矯正措施及預防措施，並確保相關措施之執行。 **TPIPAS：2016 9.2.1. 矯正措施** 組織針對不符合事項，應規劃及完成執行矯正措施，並完成以下事項： (1) 確認不符合事項之內容並判定其發生原因。 (2) 評估需求並提出矯正方案，以確保不符合事項不再發生。	並據以調整與修正個人資料管理制度： (1) 檢視報告。 (2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 組織業務領域之變化。 (4) 組織內外部之改善建議。 (5) 其他可能影響個人資料管理制度的任何變更。 **TPIPAS：2021 10.1. 總則** 組織針對內部評量及本管理制度實施之結果，應規劃矯正措施及預防措施，並確保相關措施之執行。 **TPIPAS：2021 10.2. 矯正措施** 組織針對不符合事項，應規劃及完成執行矯正措施，並完成以下事項： (1) 確認不符合事項之內容並判定其發生原因。 (2) 評估需求並提出矯正方案，以確保不符合事項不再發生。 (3) 訂定合理之執行期限。

		(3) 訂定合理之執行期限。 (4) 紀錄執行結果。 (5) 檢視所採取的矯正方案成果。 **TPIPAS：2016 9.2.2. 預防措施** 組織針對潛在不符合事項之風險，應規劃及執行預防措施時，並完成以下事項： (1) 依據組織因持有個人資料可能面臨的風險，確認各項潛在不符合事項之內容及其原因。 (2) 評估需求並提出預防方案，以確保不符合事項不再發生。 (3) 訂定合理之執行期限。 (4) 紀錄執行結果。 (5) 檢視所採取的預防方案成果。	(4) 紀錄執行結果。 (5) 檢視所採取的矯正方案成果。 **TPIPAS：2021 10.3. 預防措施** 組織針對潛在不符合事項之風險，應規劃及執行預防措施時，並完成以下事項： (1) 依據組織因持有個人資料可能面臨的風險，確認各項潛在不符合事項之內容及其原因。 (2) 評估需求並提出預防方案，以確保不符合事項不再發生。 (3) 訂定合理之執行期限。 (4) 紀錄執行結果。 (5) 檢視所採取的預防方案成果。 (6) 持續改善個人資料管理制度。
42. 為避免資料遺失或防止他人未經授權不當存取、利用、修改、揭露個人資料或其他濫用個	當責機構應查證申請組織已採取合理措施（例如：使用適當的契約條款），要求個人資料傳輸之處理者、代理人、承包商或其他服務提供者，保護個人資料避免資料遺失	**TPIPAS：2016 4.4.6. 事故之緊急應變** 為避免事故可能產生之不利益及影響，組織應訂定事故緊急應變措施。相關措施應至少包括：	**TPIPAS：2021 8.10. 事故之緊急應變** 為避免事故可能產生之不利益及影響，組織應訂定事故緊急應變措施。相關措施應至少包括：

人資料之行為所產生之風險，是否要求資料處理者、代理人、承包商或其他服務提供者： 42(a) 採取與資料敏感度及所提供服務成正比之資料安全計畫？ 42(b) 發現個資事故時，立即通知組織？ 42(c) 立即處理解決造成個資事故之缺失？	或防止他人未經授權不當存取、利用、修改、揭露個人資料或其他濫用個人資料之行為。申請組織必須定期審查並重新評估其安全維護措施以判斷關聯性與有效性。	(1) 查明後以適當方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 防止組織所受損害擴大之方法。 (3) 避免類似事件再次發生之方法。 (4) 將事故通報授證機關。 **TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。	(1) 查明後以適當方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 防止組織所受損害擴大之方法。 (3) 避免類似事件再次發生之方法。 (4) 將事故通報授證機關。 **TPIPAS：20218.7. 安全管理措施** 組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。 **TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方

		(3) 技術性安全管理措施（如資訊傳輸、系統監看等）。 **TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事	式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受

		項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。 組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。

近用及更正（Q43~45）

評估目的－*確保資料當事人能夠近用及更正其個人資料。本節涵蓋可視為合理近用之特定要件。資料近用亦受到各項安全措施要求所限制，防止資料直接近用並且在提供近用前進行充分的身份驗證。而近用及更正資料之程序，可能根據資料性質及其他利害事項而有所差異。因此，在某些情況下，請求更改、隱藏或刪除紀錄是不可能、不可行或不必要的。*
能夠近用及更正個人資料一般被視為是隱私保護重要一環，但並非是一種絕對權利。儘管組織應秉持誠信原則竭力提供資料近用，但是符合特定情形時，可能有必要拒絕資料當事人近用及更正的請求。「近用及更正機制例外情形」列出可拒絕資料近用及更正請求之情形。組織在拒絕資料近用請求時，應向資料當事人提出解釋及說明，並提供其可尋求之申訴管道。然而，若前述揭露將會違反法律或司法命令則無需解釋及說明。參閱下方「近用及更正機制例外情形」之說明。

自我評量問卷題目	**當責機構評估標準**	**其他相關驗證規則** TPIPAS 規範及《個人資料保護法》	
43. 當資料當事人提出請求時，是否向資料當事人確認所持有其個人資料？請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織制定相關程序以回應當事人請求。 取得充分資訊足以驗證資料當事人身份後，申請組織必須授予近用權限。 申請組織必須依據當事人請求提出方式及個人資料的性質，以合理程序或機制提供當事人近用個人資料。個人資料必須以簡單易懂的方式提供予資料當事人。申請組織	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.2. 當事人行使權利之程序事項** 組織為處理 4.5.2.1 之當事人請求之程序，內容至少符合下列要求：	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請

	必須提供資料當事人請求之回應期間。 若申請組織回答為「**否**」且不適用「近用及更正機制例外情形」，當責機構應通知申請組織必須具備當事人請求回應程序並以書面文件呈現，以遵循近用及更正原則。若申請組織說明其適用「近用及更正機制例外情形」，當責機構應查證是否符合適用情形。	(1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。	求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。
44. 當資料當事人提出請求時，是否向資料當事人就其個人資料提供近用？若	若申請組織回答為「**是**」，當責機構應查證申請組織所提供每個回答。	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製

「是」，請回答 Q44(a)~(e) 並說明接受及處理近用請求之相關政策或制度。若「否」，請回答 Q45。 44(a) 是否採取措施驗證資料當事人身分？若「是」，請說明。 44(b) 是否依據資料當事人請求，於合理期間內提供資料當事人近用？若「是」，請說明。 44(c) 是否以普遍可理解且清楚的方式傳達資料？請說明。 44(d) 是否以資料當事人互動的普遍形式提供資料（例如：透過電子郵件或相同語言等）？ 44(e) 是否收費？若「是」，請說明定價標準及其合理性。	申請組織必須落實合理且適當流程或機制（例如：透過用戶帳號或聯絡資訊）提供資料當事人近用其個人資料。 若申請組織駁回當事人近用其個人資料之請求，必須向資料當事人說明駁回原因，並提供聯絡資料以便資料當事人進行申訴。 若申請組織回答為**「否」**且不適用「近用及更正機制例外情形」，當責機構應通知申請組織可能需要允許資料當事人近用其個人資料。若申請組織說明其適用「近用及更正機制例外情形」，當責機構應查證是否符合適用情形。	止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.2. 當事人行使權利之程序事項** 組織為處理 4.5.2.1 之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 **TPIPAS：2016 4.5.2.3. 提供查詢、閱覽、複製本之方式** 組織針對當事人請求查詢、閱覽個人資料或製給個人資料複製本，其程序應符合下列要求： (1) 確保於 15 日內為准駁之決定。 (2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (3) 決定延長 15 日作出准駁之決	本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間

		定時，應附理由以書面通知當事人。 (4) 保存前三款相關紀錄。	作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。
45. 是否允許資料當事人質疑其個人資料的正確性，並請求更正、補充、刪除其個人資料？請說明相關政策或程序並回答Q45(a)~(e)。 45(a) 近用及更正機制是否清楚明顯？請說明。若有必要，請以附件說明。	若申請組織 **Q38(a) 回答為「是」**，當責機構應查證該機制對於全球CBPR各會員體是否可用且可理解。 若申請組織駁回當事人更正個人資料之請求，應說明原因，並適時提供申請組織的聯絡資料供當事人進行申訴。 所有近用與更正機制皆應簡單且容易使用、以明確易讀的方式呈	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.2. 當事人行使權利之程序事項** 組織為處理 4.5.2.1 之當事人請求之程序，內容至少符合下列要求：	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請

45(b) 資料當事人表示其個人資料不完整或不正確時，是否已請求進行更正、補充，或於必要時刪除其個人資料？ 45(c) 資料當事人提出更正或刪除請求後，是否於合理時間內更正或刪除其個人資料？ 45(d) 是否於更正後提供資料當事人其個人資料複製本，或向資料當事人確認其個人資料已修正或刪除？ 45(e) 若駁回資料當事人近用或更正之請求，是否通知資料當事人並附上理由及聯繫資訊，以供資料當事人進行後續聯繫？	現、於合理時間內回應請求，且向資料當事人確認已更正、修改或刪除不正確的資料。相關機制施行方式包括但不限於：接受資料當事人以書面或電子郵件提出請求、由員工複製相關資料並發送提出要求之當事人。 若申請組織 Q38(a)~(e) 回答為「**否**」且不適用「近用及更正機制例外情形」，當責機構應通知申請組織必須具備當事人請求回應程序並以書面文件呈現，以遵循近用及更正原則。若申請組織提出適用「近用及更正機制例外情形」，當責機構應確認是否適用。	(1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 **TPIPAS：2016 4.5.2.4. 當事人請求個人資料補充、更正、刪除、停止蒐集、處理及利用程序** 組織針對當事人請求補充、更正、刪除、停止蒐集、處理或利用個人資料，其程序應符合下列要求： (1) 確保於 30 日內為准駁之決定。 (2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (3) 決定延長 30 日作出准駁之決定時，應附理由以書面通知當事人。 (4) 保存前三款相關紀錄。 **TPIPAS：2016 4.5.2.5 申訴及諮詢之處理**	求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製

		針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。

近用及更正機制例外情形

雖然申請組織應秉持誠信原則竭力提供資料近用，但是符合特定情形時，可能有必要拒絕資料當事人近用及更正請求。若有適用以下例外情形，請在空白處說明並扣合 Q43~45 回答。

i. **成本或負擔顯不合理：**若提供近用及更正的負擔或費用明顯不合理，或與資料當事人所承擔的隱私風險不成比例時，資料控管者無需提供資料近用及更正。例如：不斷重複或毫無根據的請求近用。

ii. **保護機密資訊：**基於法律或安全理由，或是為了保護商業秘密（例如：已採取措施防止揭露之資料，且一旦資料被揭露，將被其他市場競爭者利用以傷害商業利益，造成申請組織重大財務損失）而無法揭露個人資料時，資料控管者無需提供資料近用及更正。然而，若該個人資料可輕易將商業秘密與被請求近用的資料分離，資料控管者應對商業秘密進行遮蔽後將非涉及商業祕密之個人資料提供資料當事人近用。

其他情況包含資料揭露將會有利於其他市場競爭者，例如：特定的電腦或模組程式。

此外，若提供資料近用將構成違法行為或有損安全性，資料控管者亦得拒絕近用請求。

第三方風險：若提供資料近用及更正將可能侵害第三方資料隱私時，個人資料控管者無需提供資料近用及更正。若第三方的個人資料可與被請求近用或更正的資料分離，資料控管者應對第三方之個人資料進行遮罩後提供資料當事人近用。

責任（Q46~57）

評估目的－*確保組織確實負責遵守前述各項原則之實踐。此外，當資料傳輸並非取得資料當事人同意作為合法處理要件，組織有責任確保資料接收者持續遵守前述各項原則保護個人資料，且組織應採取合理措施以確保個人資料隱私安全。然而，在盡職調查（due diligence）執行困難的情況下（例如：組織與第三方無任何關係），組織可選擇其他方式（例如：取得資料當事人同意），以確保個人資料依照前述各項原則受到保護。但是，若依據國內法律要求揭露資料，則無需遵守盡職調查或取得同意之義務。*

自我評量問卷題目	當責機構評估標準	其他相關驗證規則 TPIPAS 規範及《個人資料保護法》	
46. 組織採取何種措施確保符合全球CBPR資料隱私原則？請選擇並說明所採取之措施（可複選）。 ● 組織內部準則或政策（請說明如何實施） ● 契約 ● 與其所屬產業相關之法律或規則 ● 行為自律守則或規範 ● 維護資料處理活動	當責機構應查證申請組織採取措施以確保遵循全球CBPR資料隱私原則。包括維護用以證明合法資料處理活動之相關紀錄，且得於受請求時得提供。 若申請組織回答為「**否**」，當責機構應通知申請組織，必須建立維護資料處理活動紀錄之相關程序。	**TPIPAS：2016 4.2. 個人資料保護管理政策** 組織應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。 **TPIPAS：2016 4.3. 個人資料保護管理手冊** 組織為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供組織依循使用。	**TPIPAS：2021 5.2. 個人資料保護管理政策** 最高管理階層應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。個人資料保護管理政策應包含以下事項： (1) 個人資料管理制度之目標。 (2) 承諾落實本制度規範要求事項與法令。

之紀錄 ● 其他（請說明）		具體規則內容至少包括： (1) 識別法令與其他相關規範。 (2) 識別組織所保有之個人資料。 (3) 組織蒐集、處理或利用個人資料之事宜。 (4) 個人資料相關之風險分析及管控措施。 (5) 事故緊急應變。 (6) 組織各部門以及層級所擁有個人資料管理權限與責任。 (7) 當事人權利之行使。 (8) 維持個人資料正確性。 (9) 安全管理措施。 (10) 組織人員之監督與獎懲。 (11) 委託蒐集、處理或利用個人資料之監督。 (12) 教育訓練。 (13) 個人資料管理制度之文件與紀錄管理。 (14) 當事人申訴及諮詢。 (15) 內部評量。 (16) 矯正及預防措施。 (17) 最高管理階層定期檢視。	(3) 承諾定期檢視與持續改善。 **TPIPAS：2021 6.2. 個人資料保護管理手冊** 組織為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供組織依循使用。 具體規則內容至少包括： (1) 識別法令與其他相關規範。 (2) 識別組織所保有之個人資料。 (3) 組織蒐集、處理或利用個人資料之事宜。 (4) 個人資料相關之風險分析及管控措施。 (5) 事故緊急應變。 (6) 組織各部門以及層級所擁有個人資料管理權限與責任。 (7) 當事人權利之行使。 (8) 維持個人資料正確性。

		TPIPAS：2016 4.4.1. 識別法令及其他相關規範 組織應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。 **TPIPAS：2016 9.1. 定期檢視** 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事	(9) 安全管理措施。 (10) 組織人員之監督與獎懲。 (11) 委託蒐集、處理或利用個人資料之監督。 (12) 教育訓練。 (13) 個人資料管理制度之文件與紀錄管理。 (14) 當事人申訴及諮詢。 (15) 內部評量。 (16) 矯正及預防措施。 (17) 最高管理階層定期檢視。 (18) 個人資料或資通安全維護計畫。 **TPIPAS：2021 8.1. 識別法令及其他相關規範** 組織應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。

		項，並據以調整與修正個人資料管理制度： (1) 檢視報告。 (2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 組織業務領域之變化。 (4) 組織內外部之改善建議。 (5) 其他可能影響個人資料管理制度的任何變更。	**TPIPAS：2021 9.3. 定期檢視** 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事項，並據以調整與修正個人資料管理制度： (1) 檢視報告。

			(2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 組織業務領域之變化。 (4) 組織內外部之改善建議。 (5) 其他可能影響個人資料管理制度的任何變更。
47. 是否於組織內指定專責人員負責執行APEC資料隱私原則？ 是否於組織內指定適合的專責人員，負責貴組織整體遵循個人資料保護計畫及全球CBPR隱私原則的相關事宜？	若申請組織回答為「**是**」，當責機構應查證申請組織已指派專責人員負責執行APEC資料保護與隱私原則。 申請組織應就該專責人員之資格符合個資保護特性進行說明。 申請組織必須指派一名或多名員工負責確保遵守隱私權聲明中所述的資料保護與隱私保護原則、且針對接受、調查及回應與隱私相關之申訴必須採取適當程序並適時說明救濟程序。 若申請組織回答為「**否**」，當責機構應通知申請組織必須指派專責人員以遵循責任原則。	**TPIPAS：2016 5.1. 最高管理階層** 最高管理階層之責任應包括： (1) 決定個資保護管理政策 (2) 決定資源管理 (3) 決定個資保護管理組織架構及權責劃分 (4) 定期檢視管理制度 (5) 建立有效的溝通機制 **TPIPAS：2016 5.2. 管理代表** 最高管理階層應指派管理階層成員之一，擔任個人資料保護制度管理代表，其應有之責任與職權包括：	**TPIPAS：2021 5.1. 最高管理階層** 最高管理階層之責任應包括： (1) 決定個人資料管理制度目標，確保符合組織需求與發展策略。 (2) 決定個人資料保護管理政策。 (3) 決定資源管理。 (4) 決定個人資料保護管理組織架構及權責劃分。 (5) 定期檢視管理制度，確保管理制度達成預期效果。 (6) 建立有效的溝通機制，適時指導與支援組織人員。

		(1) 負責維持個人資料管理制度運作之有效性，並建立必要內部人員結構。 (2) 確保職務執行過程之公正性與客觀性。 (3) 確保個人資料管理制度所需的各項程序被建立、實施與維持。 (4) 向最高管理階層報告個人資料管理制度之實施成效與改善措施。 **TPIPAS：2016 5.3. 個資管理人員** 組織應由取得下列資格之一者，擔任個資管理人員，以實際推動並確保個人資料管理制度之有效運作： (1) 個人資料管理師。 (2) 個人資料內評師。 (3) 個人資料驗證師。 個資管理人員得由個資管理代表兼任。	(7) 傳達落實個人資料管理制度之重要性。 **TPIPAS：2021 5.4. 管理代表** 最高管理階層應指派管理階層成員之一，擔任個人資料保護制度管理代表，其應有之責任與職權包括： (1) 負責維持個人資料管理制度運作之有效性，並建立必要內部人員結構。 (2) 確保職務執行過程之公正性與客觀性。 (3) 確保個人資料管理制度所需的各項程序被建立、實施與維持。 (4) 向最高管理階層報告個人資料管理制度之實施成效與改善措施。 **TPIPAS：2021 5.5. 個人資料管理人員** 組織應由取得下列資格之一者，擔任個資管理人員，

			以實際推動並確保個人資料管理制度之有效運作： (1) 個人資料管理師。 (2) 個人資料內評師。 (3) 個人資料驗證師。 個資管理人員得由個資管理代表兼任。
48. 是否設置申訴處理程序以處理申訴案件，包含接受、調查、結果回覆？請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織制定相關申訴程序，包括接受、調查、結果回覆，例如： (1) 說明資料當事人向申請組織提出申訴的方式（例如：透過電子郵件/電話/傳真/郵寄信件/線上表單）；以及/或 (2) 指派專人處理有關申請組織遵守「全球CBPR隱私綱領」及/或當事人要求近用個人資料之申訴；以及/或 (3) 正式的申訴解決流程；以及/或 (4) 其他（必須具體說明）。 若申請組織回答為「**否**」，當責機構應通知申請組織必須設置申訴處理程序以遵循責任原則。	**TPIPAS：2016 4.5.2.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2016 4.5.2.2. 當事人行使權利之程序事項** 組織為處理4.5.2.1之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。	**TPIPAS：2021 8.5.1. 個人資料之相關權利** 組織應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 **TPIPAS：2021 8.5.2. 當事人行使權利之程序事項** 組織為處理前條之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。

		(2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 **TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	(2) 具備確認當事人身分之方式。 (3) 具備確認組織是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 (5) 確保當事人行使權利於法令規定期間內為准駁之決定。 (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。 (8) 保存相關紀錄。 **TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求：

			(1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。
49. 是否設置回覆程序以確保於合理時間內回覆資料當事人申訴結果？	若申請組織回答為「**是**」，當責機構應查證申請組織制定相關回覆程序，以確保資料當事人的申訴獲得及時回應。 若申請組織回答為「**否**」，當責機構應通知申請組織必須設置回覆程序以遵循責任原則。	**TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	**TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。
50. 若Q49回答為「是」，該回覆是否包含救濟程序之說明？請說明。	當責機構應查證申請組織提供救濟程序說明。	**TPIPAS：2016 4.5.2.5. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求：	**TPIPAS：2021 8.5.3. 申訴及諮詢之處理** 針對申訴與諮詢事項，組織應確保迅速有效之處理，其程序應符合下列要求：

		(1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。	(1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。
51. 是否制定相關程序進行員工教育訓練，以了解組織所定個人資料保護政策及制度，內容包含如何應對申訴案件？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織制定相關員工訓練，教育員工瞭解其隱私政策與程序，包含如何回應與隱私相關的申訴。 若申請組織回答未制定相關員工訓練，教育員工瞭解其隱私政策與程序，包含如何回應與隱私相關的申訴，當責機構應通知申請組織必須制定教育訓練相關程序以遵循責任原則。	**TPIPAS：2016 4.6.1. 一般要求** 組織應以適當方式確保組織人員對個人資料管理具有正確的認知及能力。 **TPIPAS：2016 4.6.2. 基本教育訓練** 組織針對組織人員應提供必要的個人資料管理教育訓練。 **TPIPAS：2016 4.6.3. 權責人員教育訓練** 組織應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。	**TPIPAS：2021 7.2.1. 總則** 組織應以適當方式確保組織人員對個人資料管理、管理與獎懲制度具有正確的認知及能力。 **TPIPAS：2021 7.2.2. 基本教育訓練** 組織針對組織人員應提供必要的個人資料管理教育訓練。 **TPIPAS：2021 7.2.3. 權責人員教育訓練** 組織應決定個人資料管理制度相關權責人員之必要

		TPIPAS：2016 4.6.4. 成果維持及改善措施 組織應針對組織人員教育訓練成果建立紀錄與改善機制。	能力與教育訓練需求，並規劃與執行。 **TPIPAS：2021 7.2.4. 成果維持及改善措施** 組織應針對組織人員教育訓練成果建立紀錄與改善機制。
52. 是否制定相關處理程序以因應法院或其他政府機關要求提供個人資料之傳票或法院命令？	若申請組織回答為「**是**」，當責機構應查證申請組織已針對傳票及法院命令之回覆制定相關程序，尤其傳票及法院命令之回覆涉及個人資料之揭露，並為員工提供相關教育訓練。 若申請組織回答為「**否**」，當責機構應通知申請組織必須制定處理程序以遵循責任原則。	**TPIPAS：2016 4.3. 個人資料保護管理手冊** 組織為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供組織依循使用。 具體規則內容至少包括： (1) 識別法令與其他相關規範。 (2) 識別組織所保有之個人資料。 (3) 組織蒐集、處理或利用個人資料之事宜。 (4) 個人資料相關之風險分析及管控措施。 (5) 事故緊急應變。	**TPIPAS：2021 6.2. 個人資料保護管理手冊** 組織為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供組織依循使用。 具體規則內容至少包括： (1) 識別法令與其他相關規範。 (2) 識別組織所保有之個人資料。 (3) 組織蒐集、處理或利用個人資料之事宜。 (4) 個人資料相關之風險分析及管控措施。

		(6) 組織各部門以及層級所擁有個人資料管理權限與責任。 (7) 當事人權利之行使。 (8) 維持個人資料正確性。 (9) 安全管理措施。 (10) 組織人員之監督與獎懲。 (11) 委託蒐集、處理或利用個人資料之監督。 (12) 教育訓練。 (13) 個人資料管理制度之文件與紀錄管理。 (14) 當事人申訴及諮詢。 (15) 內部評量。 (16) 矯正及預防措施。 (17) 最高管理階層定期檢視。 **TPIPAS：2016 4.4.1. 識別法令及其他相關規範** 組織應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。	(5) 事故緊急應變。 (6) 組織各部門以及層級所擁有個人資料管理權限與責任。 (7) 當事人權利之行使。 (8) 維持個人資料正確性。 (9) 安全管理措施。 (10) 組織人員之監督與獎懲。 (11) 委託蒐集、處理或利用個人資料之監督。 (12) 教育訓練。 (13) 個人資料管理制度之文件與紀錄管理。 (14) 當事人申訴及諮詢。 (15) 內部評量。 (16) 矯正及預防措施。 (17) 最高管理階層定期檢視。 (18) 個人資料或資通安全維護計畫。 **TPIPAS：2021 8.1. 識別法令及其他相關規範**

		TPIPAS ： 2016 4.5.1.3. 利用 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。 **個人資料保護法第16條** 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。	組織應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。 **TPIPAS：2021 8.4.4. 利用** 組織對於個人資料之利用程序應符合下列要求： (1) 於蒐集之特定目的必要範圍之內利用個人資料。 (2) 其他法令規定利用時應履行之義務。 (3) 保存前二款相關紀錄。

		五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。 **個人資料保護法第20條第1項** 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。	

		六、經當事人同意。 七、有利於當事人權益。	
53. 對於受託處理個人資料之處理者、代理人、承包商或其他服務提供者，是否建立機制以確保履行對資料當事人的義務？請選擇所採取之機制（可複選） ● 組織內部準則或政策（請說明如何實施） ● 契約 ● 與其所屬產業相關之法律或規則 ● 行為自律守則或規範 ● 其他（請說明）	若申請組織回答為「**是**」，當責機構應查證確實執行各項監督機制。 若申請組織回答為「**否**」，當責機構應通知申請組織必須執行監督機制以遵循責任原則。	**TPIPAS：2016 4.5.3.3. 組織人員之監督** 組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 **TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。	**TPIPAS：2021 8.8. 組織人員之監督** 組織應對組織人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 **TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特

		(5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令

			規定之情事，應立即通知委託人。 組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。
54. Q53 所列機制是否要求受託處理個人資料之處理者、代理人、承包商或其他服務提供者： ● 遵循申請組織經全球CBPR認可且已於隱私聲明中表述的隱私政策及規定？ ● 實施與申請組織大致相同的隱私政策及規定？ ● 遵循申請組織指示處理個人資料？ ● 非經申請組織同意，限制複委託行為？ ● 通過全球CBPR驗證？	當責機構應查證申請組織採用適當方法確保受託處理個人資料之處理者、代理人、承包商或其他服務提供者履行其義務。	**TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之	**TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。

● 發生個資事故時，通報申請組織？ ● 其他（請說明）		事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	(5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。 組織應定期確認與審查受

			託人執行之狀況，並將確認結果紀錄之。
55. 是否要求受託處理個人資料之處理者、代理人、承包商或其他服務提供者，提供隱私保護自我評估，以確保遵守指示或契約？若「是」，請說明。	當責機構應查證自我評估機制確實具備。	**TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事	**TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同

		項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。 組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。

56. 是否定期實地審查或監督受託處理個人資料之處理者、代理人、承包商或其他服務提供者，以確保遵守指示或契約？若「是」，請說明。	若申請組織回答為「**是**」，當責機構應查證申請組織所採取抽查或監督機制確實具備。 若申請組織回答為「**否**」，當責機構應要求申請組織說明未使用抽查或監督機制之原因。	**TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受	**TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。 (3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個

		託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。 組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。
57.在無法以盡職調查或合理方式確保他方遵守全球CBPR規定之情	若「**是**」，當責機構應要求申請組織提出解釋： 1） 為何無法以盡職調查或合理方	**TPIPAS：2016 4.5.3.2. 安全管理措施** 組織應針對因蒐集、處理及利用	**TPIPAS：2021 8.7. 安全管理措施** 組織應針對因蒐集、處理及

形下，是否向**其他自然人或組織**揭露所持有之個人資料？	式確保他方遵守全球CBPR規定；以及 2） 確保資料保護符合全球CBPR隱私保護原則之其他方式。若申請組織是依據資料當事人同意，申請組織必須向當責機構提出可接受的解釋，說明該同意的性質以及取得方式。	個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施（如存取控制、技術檢視、識別鑑別、媒體安全等）。 (2) 物理性安全管理措施（如實體與環境安全等）。 (3) 技術性安全管理措施（如資訊傳輸、系統監看等）。 **TPIPAS：2016 4.5.3.4. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。	利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施： (1) 管理面安全管理措施。 (2) 技術面安全管理措施。 **TPIPAS：2021 8.9. 委託蒐集、處理或利用個人資料之監督** 組織委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。

		(3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。	(3) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (4) 受託人對個人資料之安全管理措施。 (5) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意且應具備完善之安全管理措施。 (6) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (7) 委託人對受託人保留指示之事項。 (8) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (9) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (10) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認

			委託人之指示有違反法律或基於法律所發布之命令規定之情事，應立即通知委託人。 組織應定期確認與審查受託人執行之狀況，並將確認結果紀錄之。