產業個人資料保護快速自我檢視

序號	領域	評估內容	是否符合
1-1	配置管理之人員及相當資源	貴公司企業代表人是否指定管理階層為專人統籌、指揮企業內部個人資料保護事務事宜？	□是 □否
2-1	個人資料保護與管理制度-管理制度建置	貴公司是否以建置個人資料保護與管理制度？（亦即，貴公司是否有意識、有系統的管理個人資料，並設計相應的各種作業程序）	□是 □否
2-2	個人資料保護與管理制度-人員架構	貴公司是否配置有專責管理公司個人資料保護與管理之人員？或已就個人資料之保護與管理成立跨部門之常態任務編組？	□是 □否
2-3	個人資料保護與管理制度-權責分配	請問貴公司負責個人資料管理的人員是否為對全公司之重要事務具有決策權之人，或其就個人資料保護與管理事務可直接向公司決策階層負責？	□是 □否
2-4	個人資料保護與管理制度-資源	貴公司是否已提供必要資源（例如各項軟、硬體或經費），以進行貴公司之個人資料保護與管理？	□是 □否
3-1	界定個人資料之範圍-法規盤點	貴公司企業代表人是否指定採行任何程序或方式，以適時清查有哪些個人資料保護相關法令適用於貴公司？	□是 □否
3-2	界定個人資料之範圍-法規遵循	貴公司是否有任何程序，用以確保個人資料之蒐集、處理、利用有法律上依據？	□是 □否
3-3	界定個人資料之範圍-盤點個人資料及建立清冊	貴公司是否有任何機制用以清查、整理貴公司所持有之個人資料，並將相關資料做成清冊或資料庫？	□是 □否
3-4	界定個人資料之範圍-作業流程	貴公司是否已整理出各類個人資料檔案蒐集、處理、利用之作業流程？	□是 □否
3-5	界定個人資料之範圍-更新個資盤點清冊	貴公司是否定期或依公司營業項目、業務範圍有所變動不定期更新貴公司所持有之個人資料，並將相關資料做成清冊或資料庫？	□是 □否
4-1	個人資料之風險評估與管理機制-風險評估	貴公司是否有任何機制用以評估貴公司所持有之個人資料風險，並將相關資料做成清冊或資料庫？	□是 □否
4-2	個人資料之風險評估與管理機制-風險對策	貴公司是否有任何機制針對已評估貴公司所持有之個人資料風險作成對策，並彙整於清冊或資料庫中？	□是 □否
4-3	個人資料之風險評估與管理機制-風險管控與安全措施	貴公司是否已依據不同資料之敏感性、及各資料所面臨之風險情境與風險程度訂定不同的風險管控措施？	□是 □否

4-4	個人資料之風險評估與管理機制-風險管控方法	貴公司是否採行適當方式，以避免在資料蒐集、處理、利用、刪除之過程中被竄改、遺失或洩漏？	□是 □否
4-5	個人資料之風險評估與管理機制-更新風險評估	貴公司是否定期或與個資盤點清冊的更新連動不定期更新貴公司所持有之個人資料風險，並將相關資料做成清冊或資料庫？	□是 □否
5-1	事故之預防、通報及應變機制-事故應變	貴公司是否有任何程序，用以於事故發生時（例如裝有個資之筆電遺失，或資料庫系統遭駭客入侵）做適當、即時之緊急應變，以避免損害擴大？	□是 □否
5-2	事故之預防、通報及應變機制-事故處理	貴公司是否有任何程序，可在事故發生後做妥善之處理，避免類似事件再次發生？	□是 □否
6-1	個人資料蒐集、處理及利用之內部管理程序-特定情形	貴公司是否就各筆資料之蒐集、處理、利用符合法規依據之個別事實做成紀錄？（例如：於紀錄上載明係因買賣契約關係而蒐集、處理、利用）	□是 □否
6-2	個人資料蒐集、處理及利用之內部管理程序-特定目的	請問貴公司是否有任何用來確保所蒐集、處理之個人資料僅被用於蒐集之特定目的之程序或規則？	□是 □否
6-3	個人資料蒐集、處理及利用之內部管理程序-權限限制	貴公司是否訂有相關程序或規則，用以確保在個人資料被蒐集、處理、利用之過程中，僅有被授權之必要人員可以接觸個人資料？	□是 □否
6-4	個人資料蒐集、處理及利用之內部管理程序-特定目的外利用	貴公司是否有任何程序可用以確保當個人資料之利用係屬目的外利用時，此目的外利用符合法律規定？	□是 □否
6-5	個人資料蒐集、處理及利用之內部管理程序-告知義務	貴公司是否有任何程序，用以確保貴公司已依法令之規定踐行對個人資料之當事人的告知義務？（或用以確保貴公司依法無須告知）	□是 □否
6-6	個人資料蒐集、處理及利用之內部管理程序-告知義務之履行	貴公司是否有將已踐行告知義務之事實做成執行紀錄保存？（如為依法無須告知之情形，是否已將無須告知之法律依據做成紀錄？）	□是 □否
6-7	個人資料蒐集、處理及利用之內	貴公司是否有任何程序或規則，用以確保蒐集處理、利用、個人資料之方式符合法律之規定？（例如，有無要	□是 □否

	部管理程序-蒐集、處理、利用之方式	求員工於蒐集個人資料時不得有誤導當事人的言論或暗示？）	
6-8	個人資料蒐集、處理及利用之內部管理程序-拒絕行銷之方式	貴公司是否有任何程序，用以確保當個人資料被用於行銷目的時，已依法律規定，提供當事人拒絕行銷之合理方式？	□是 □否
6-9	個人資料蒐集、處理及利用之內部管理程序-當事人權利行使	貴公司是否有任何程序，用以確保當事人之權利行使（例如當事人要求閱覽、複製、更正、補充、刪除其個人資料之權利等）？	□是 □否
6-10	個人資料蒐集、處理及利用之內部管理程序-資料正確性之維持	貴公司是否有任何程序用以確保當事人之資料有錯誤、變動等情形時，貴公司可盡快掌握並主動加以更正之程序？	□是 □否
6-11	個人資料蒐集、處理及利用之內部管理程序-資料之停止蒐集、停止處理、停止利用、刪除	貴公司是否有任何程序或方法，用以確保在特定目的消失、時限屆滿時，個人資料將被停止蒐集、處理、利用或將被刪除？	□是 □否
6-12	個人資料蒐集、處理及利用之內部管理程序-申訴、諮詢	貴公司是否有任何程序，以使當事人對個人資料相關之事宜有疑問或不滿時，可獲得適當之諮詢與處理？	□是 □否
6-13	個人資料蒐集、處理及利用之內部管理程序-個案改善	貴公司是否有任何程序，用以避免此一令當事人不滿之狀況再次發生？	□是 □否
7-1	資料安全管理及人員管理-權限限制	貴公司是否訂有相關程序或規則，用以確保個人資料僅有被授權之必要人員可以接觸個人資料？	□是 □否
7-2	資料安全管理及人員管理-處理紀錄	貴公司是否訂有相關程序或規則，用以確保個人資料僅有被授權之必要人員接觸個人資料之紀錄？	□是 □否
7-3	資料安全管理及人員管理-保密契約	貴公司是否訂有相關規則，用以確保個人資料有被授權之必要人員必須於任職期間或離後之一定期間內應保守可接觸個人資料之秘密？	□是 □否

7-4	資料安全管理及人員管理-委外監督	如貴公司有委外蒐集處理利用個人資料之情形，請問是否訂定有任何機制，以確保受託單位已遵循個人資料保護相關法令及貴公司與個人資料保護與管理相關之要求？	□是 □否
8-1	認知宣導及教育訓練-認知宣導	請問貴公司是否提供員工關於個人資料保護法令的教育訓練，或提供個人資料保護法令的相關資訊並要求員工瞭解？	□是 □否
8-2	認知宣導及教育訓練-教育訓練	請問貴公司是否提供員工關於個人資料保護與管理的教育訓練，或提供相關資訊並要求員工瞭解？	□是 □否
9-1	設備安全管理-進出限制	貴公司否訂定或使用任何機制，以確保確實為公司職員進出辦公區域？	□是 □否
9-2	設備安全管理-防止盜竊	貴公司否訂定或使用任何機制，以確保公司財產避免遭竊？	□是 □否
9-3	設備安全管理-防災	貴公司否訂定或使用任何機制，以確保公司財產避免遭到火災、水災、地震或停電而受損？	□是 □否
10-1	資料安全稽核機制-稽核之組織	貴公司是否有獨立、公正並可直接向企業代表人報告之稽核機制？	□是 □否
10-2	資料安全稽核機制-稽核執行	貴公司之稽核機制是否按擬定之稽核計畫進行稽核？	□是 □否
10-3	資料安全稽核機制-稽核結果	貴公司之稽核機制是否於稽核執行過後將稽核結果直接向企業代表人報告？	□是 □否
10-4	資料安全稽核機制-稽核結果之查核	貴公司是否按稽核結果訂定期限進行改善，並由稽核機制再次查核之辦法？	□是 □否
11-1	使用紀錄、軌跡資料及證據保存-紀錄保存	貴公司是否有機制或程序留存所有有關蒐集、處理及利用個人資料之紀錄？	□是 □否
11-2	個人資料安全維護之整體持續改善-制度改善	貴公司是否有任何程序，用以定期檢視貴公司個人資料保護與管理制度之成效，並進行制度的持續改善？	□是 □否

請貴公司針對自我檢視問題如有回答否或不確定的項目，對照以下管理作法建議之各項步驟，建置作業流程管理或於資訊系統上增加控制點，以保存相關紀錄，作為遵循個資法要求之相關證據。

個人資料管理機制作法建議

步驟一：訂定個人資料保護與管理政策

企業制定個資保護與管理政策時，應包含以下兩項重點。首先，建議包含企業為什麼推動個人資料保護管理制度之理由，除此之外，建議於政策內說明個人資料保護與管理制度將採取之作法。

步驟二：成立個人資料保護管理執行小組

管理小組織分工以及職責規劃可依據公司之實際狀況組成之。基本上，建議各部門主管及業務人員進行任務編組，以成立個人資料保護管理執行小組。個人資料管理組織當中，以功能而言，必須具備至少三種角色：

第一、「管理代表」：管理組織的總負責人，扮演的角色為統合整個管理組織，並分配相關工作。同時為使企業之負責人能盡其督導及監督之責，以使其遵守個資法對於負責人之防止義務要求，管理代表定期向事業之負責人報告個人資料管理組織運作之相關事項。

第二、「監督人員」：為有效督導並評核個資保護管理程序運作及安全措施執行之成效，除個人資料管理代表外，管理組織亦應有監督或評核計畫是否落實執行之監督人員，或可稱為個人資料內部評量人員。

第三、「管理人員」：如果將管理代表比擬為組織之大腦，也必須有手足才有辦法執行所有的工作，並且落實在企業各個部門。所以，因應企業的規模及組織架構，在各個部門亦有其部門的個資管理負責人員，或可稱為個人資料管理人員。其作用在傳達管理組織所吩咐的工作，讓各部門可以落實個資管理安全措施的要求。執行小組須根據個人資料保護管理政策之內容，建置個人資料保護管理制度，由企業負責人指定召集人領導執行小組，並且指示業務部門協助執行管理制度。

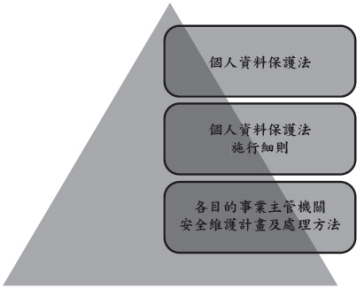
步驟三：製作個人資料管理作業時程表

執行小組完成任務編組後，執行小組便應著手進行個人資料管理作法的詳細時程規劃，並應於規劃時程表後，通知相關業務人員協助。

步驟四：公告個人資料保護管理政策

於個人資料保護管理政策制定完成後，建議執行小組將管理政策向外公告。公告之方法很多，透過公司之官方網頁建立隱私專區是一個常見、普遍而且有效率之方式。

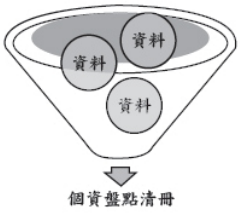
步驟五：盤點法規命令以及相關主管機關之規範



公司必須確認本身有無蒐集、處理以及利用個人資料之相關法令與中央目的事業主管機關所訂定之行政規範可依循。盤點法令之目的在於，一方面可以藉此確立公司在法規上應遵循之事項，另一方面也可藉由法規的盤點進而調整公司對於蒐集、處理或利用個人資料之作法。

步驟六：盤點個人資料

盤點個人資料為建置個人資料管理制度之重要步驟。由公司所蒐集、處理以及利用之資料中盤點出應受保護之個人資料，進行個資盤點之目的在於清查公司所擁有之個人資料類別，並可從個人資料作業流程中識別各種情境並評估風險，以訂定風險對策。



個資盤點之作法不只一種，也沒有絕對精準無疏漏之方法，但建議可使用分析個資流程之方法，盤點出公司所蒐集、處理以及利用之個人資料。個資盤點不僅在一開始建置個人資料管理制度時須進行，於公司新增業務以及業務變更終止時亦須進行，以更新公司之前所建立之個資盤點清冊。

步驟七：進行個人資料風險評估並擬定風險對策

做完個資盤點的工作之後，掌握了資料的現況以及在作業流程當中資料的生命週期，就可以進行關於個人資料之風險評估以及相關的風險管理機制。由於在前一個階段已經大致瞭解資料是從哪裡來又到哪裡去，以及相關的儲存與管理狀況，因此可以評估在這樣的過程與情況當中，可能產生的風險。

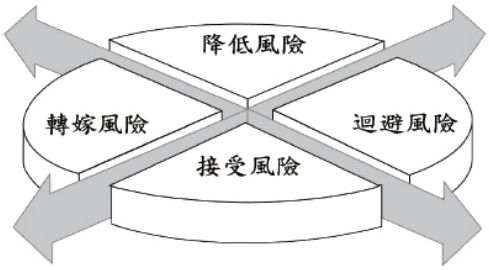
評估個人資料所可能發生的風險之後，就要依據所評估出的結果，採取適當的因應對策。從因應對策的大方向來看，大致上可以分為降低、迴避、接受與轉嫁四大類型，簡單說明如下：

降低-設計控管程序降低風險發生之可能性。

迴避-放棄可能會產生風險的業務流程。

接受-訂定該風險之衝擊屬於可接受之範圍，不進行任何處理。

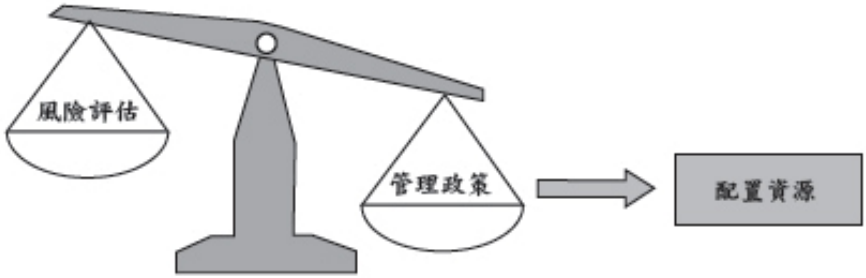
轉嫁-將風險結果請求他人協助分擔，例如保險或賠償基金。



公司可以依據本身對於風險的承受程度以及可以負擔的處理風險成本，來決定應該採取何種類型的因應對策。而選定了因應對策的類型之後，再進一步依據風險的不同，細部化決定採取何種因應手段，而該等因應手段之彙整，將會成為後續所述之各項管理程序。

步驟八：配置相當資源

配置相當資源為個資法施行細則草案安全維護事項之內容，公司內部之個人資料管理執行小組在進行風險評估並制定因應對策後，須依照風險對策之結論，確立公司所必要投入之資源。



步驟九：訂定個人資料保護管理作業手冊

建議公司應將步驟一至步驟八經決定執行之事項歸納為內部規範。該手冊應規定各部門以及各層級負責人之責任、權限。

手冊內容除了公司對於個人資料保護管理制度之作法以及內部個人資料蒐集、處理以及利用之標準流程外，個資盤點清冊、法規盤點結果、資訊安全管理措施、監督受委託處理個資者等亦應包含在作業手冊內。

例如，公司應將內部個資保護事件緊急應變程序作法清楚訂於個人資料保護管理制度之作業手冊內，以供同仁參考。又例如當事人權利行使程序也應該訂於作業手冊內，以因應個人資料當事人提出查閱、刪除、更正等相關權利之要求。

步驟十：實施個人資料保護管理教育訓練

教育訓練與個資法認知宣導其實為個資法針對個人資料安全維護事項之規定,公司應指派教育訓練負責人實施教育訓練，同時，也應留下教育訓練之記錄，以供日後參考，並且作為公司已符合個資法規範要求之證明。

步驟十一：運作個人資料保護與管理

組織依步驟一至步驟十之內容所建立之計畫及所配置之相當資源後,則可以開始執行其公司之個人資料保護管理程序，使其管理作業正式運作。

步驟十二：檢視

建議公司定期檢視個人資料保護管理制度之運作情形，並且進行改善。例如檢視各業務部門是否依據內部管理程序以及個人資料保護法之規定蒐集、處理或利用個人資料。

在檢視過程當中，可以考量下列相關事項，以決定如何調整安全管理制度：

1.安全措施之執行狀況

2.內部評量所得結果與應改善之部分

3.個人資料保護相關法令之修訂狀況

4.社會情勢、國民認知、技術發展等各種環境之變遷

5.機關業務領域之變化

6.機關內外部之改善建議

7.其他可能影響管理制度的任何變更

步驟十三：持續改善

持續改善為個人資料保護管理作法中非常重要的一環，由於個資保護管理機制係依循 PDCA（Plan，Do，Check，Act）之作法為之，因此檢視個資保護管理制度後，應列出應改善措施，並透過持續改善之作法，補充並且修正個人資料保護管理制度不足之處。