人力供應業者個人資料保護管理措施自評表

日期： 年 月 日

★主管機關行政檢查將依據本表及實地檢查結果綜合評估，請業者確實填寫。

檢查項目	自評內容				簡述執行情形
	符合	部分符合	不符合	不適用	
個人資料保護規劃					
1.個人資料保護規劃					
1.1是否指定專人或專責單位，負責辦理個人資料保護管理政策之研議、認知宣導與教育訓練、資料與設備安全管理、稽核等工作事項？					
1.2是否有個人資料管理人員組織配置？並依分工執行？					
1.3是否有個人資料保護管理政策？是否公告公司人員周知？					
1.4就個人資料之蒐集、處理及利用是否有相關程序規定？是否公告公司人員周知？					
1.5是否進行個人資料盤點並備有清冊？盤點之方式為何？結果之正確性？					
2.個人資料之風險評估及管理機制					
2.1是否進行個人資料風險評估並進行相應處理？風險評估之方式？結果之正確性？					
2.2是否訂定風險處理計畫，並根據該計畫導入控制措施，以降低風險？					
3.個人資料事故之預防、通報及應變機制					
3.1針對個人資料事故是否有可行之應變機制？					
3.2發生個人資料事故時，是否適時以適當方式通知當事人相關事故事實、因應措施及諮詢服務專線等？					
3.3是否訂有檢討預防機制，避免類似事故再次發生？					
3.4發現個人資料事故時，是否於72小時內填具通報紀錄表，通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關？					
4.個人資料蒐集、處理及利用之內部管理程序					

檢查項目	自評內容				簡述執行情形
	符合	部分符合	不符合	不適用	
4.1有無蒐集、處理或利用特種個人資料？如有，其蒐集、處理、利用及其他相關規定是否已遵守？					
4.2是否進行告知？如否，有無法定免告知事由？告知之時點與方式是否合法、適當?					
4.3蒐集、處理或利用個人資料是否具備並符合特定目的及特定情形？是否遵守其他依法令應遵守之事項？					
4.4是否有特定目的外利用？如有，是否有合法事由？					
4.5是否進行行銷？行銷是否符合特定目的？如進行行銷，是否提供當事人拒絕行銷之管道？是否於當事人拒絕行銷時，停止行銷？					
4.6如何決定是否委外？委外時如何選任受託人？與受託人間是否就個人資料保護法要求事項簽訂合約或設計監督規劃？					
4.7是否進行個人資料國際傳輸？是否於傳輸前檢視有無中央目的事業主管機關依個人資料保護法第21條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域？					
4.8對資料接收方預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式是否有監督機制？是否監督資料接收方有提供當事人行使個人資料保護法第3條所定權利等 相關事項之機制？					
4.9是否提供當事人權利行使管道？是否於法定期限內回復當事人？如展延回復，是否					

檢查項目	自評內容				簡述執行情形
	符合	部分符合	不符合	不適用	
依法定要式為之？拒絕當事人時是否有合法事由？					
4.10是否主動更正或補充當事人之個人資料？					
4.11是否曾（合法）提供資料予第三人？如提供內容有誤或不備之資料如何通知更正？					
4.12特定目的消失或期限屆至時，是否刪除、銷毀、停止蒐集、處理、利用個人資料？如否，有無法定事由？					
4.13業務終止時是否對個人資料進行妥善、合法之安排？					
4.14是否定期檢視個人資料管理之狀況並持續改善？					
5.個人資料保護管理措施					
5.1資料安全管理					
5.1.1是否訂定適用之資訊安全注意事項並公告周知？					
5.1.2運用電腦或自動化機器相關設備，是否訂定使用可攜式設備或儲存媒介物之規範?					
5.1.3保有之個人資料內容，有加密或遮蔽之必要時，是否採取適當之加密或遮蔽機制?					
5.1.4傳輸個人資料時，因應不同之傳輸方式，有加密必要時，是否採取適當加密機制?是否確認資料收受者之正確性?					
5.1.5依據保有資料之重要性，評估有備份必要時，予以備份，是否比照原件加密?儲存備份資料之媒介物，是否以適當方式保管?是否定期進行備份資					

檢查項目	自評內容				簡述執行情形
	符合	部分符合	不符合	不適用	
料之還原測試，以確保有效性?					
5.1.5儲存個人資料之媒介物於報廢或轉作其他用途時，以物理或其他方式是否確實破壞或刪除媒介物中所儲存之資料?					
5.1.6是否妥善保存管理機制及加密機制中所運用之密碼?					
5.2.人員管理					
5.2.1是否確認蒐集、處理及利用個人資料之各相關業務流程之負責人員？					
5.2.2對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工，是否有妥適分工與分散權責？是否定期確認權限內容之適當性及必要性？					
5.2.3被賦予敏感資訊存取權之所有員工，是否在被允許存取資訊處理設施之前，簽署適當之機密性或保密協議？					
5.2.4員工離職時，是否取消其識別碼?是否依規定繳回其通行證（卡）及相關證件？					
5.2.5員工離職時，是否依規定繳回其使用或保管之個人資料？					
5.3設備安全管理					
5.3.1依據作業內容不同、作業環境及個人資料之種類與數量，實施必要之門禁管理？					
5.3.2是否以適當方式或場所保管個人資料之儲存媒介物？					

檢查項目	自評內容				簡述執行情形
	符合	部分符合	不符合	不適用	
5.3.3針對不同作業環境，是否加強天然災害及其他意外災害之防護，並建置必要之防災設備？					
5.4.技術管理措施					
5.4.1是否於電腦、自動化處理設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別及控管?					
5.4.2認證機制使用之帳號及密碼，是否具備一定之複雜度，並定期更換密碼？					
5.4.3是否於電腦、自動化處理設備或系統上設定警示與相關反應機制，以對不正常之存取進行適當之反應及處理？					
5.4.4個人資料存取權限之數量及範圍，是否依作業必要予以設定?是否禁止共用帳戶和密碼？					
5.4.5是否採用防火牆或入侵偵測等設備，避免儲存個人資料之系統遭受無權限之存取?					
5.4.6使用能存取個人資料之應用程式時，是否確認使用者具備使用權限?					
5.4.7是否定期測試權限認證機制之有效性？					
5.4.8是否定期檢視個人資料之存取權限設定？					
5.4.9是否於處理個人資料之電腦系統中安裝防毒、防駭軟體?是否定期更新病毒碼？					
5.4.10對於電腦作業系統及相關應用程式之漏洞，是否定期安裝修補程式？					
5.4.11對於具備存取權限之電					

檢查項目	自評內容				簡述執行情形
	符合	部分符合	不符合	不適用	
腦或自動化處理設備，是否禁止安裝檔案分享軟體？					
5.4.12測試處理個人資料之資訊系統時，是否不使用真實個人資料？有使用真實個人資料之情形時，是否明確規定使用程序？					
5.4.13處理個人資料之資訊系統有變更時，是否確認其安全性並未降低？					
5.4.14是否定期檢查處理個人資料資訊系統之使用狀況，及個人資料存取情形？					
6.認知宣導及教育訓練					
6.1管理階層是否有要求員工，依照公司訂定之政策及程序施行安全事宜？					
6.2是否對所有員工提供個人資料保護認知宣導及教育訓練？					
7.紀錄機制					
7.1是否保存「因應事故發生所採取之行為、受託者執行委託人要求之事項、提供當事人行使之權利、個人資料之維護及修正、所屬人員權限之異動、所屬人員違反權限之行為、備份及還原之測試、個人資料之交付及傳輸、個人資料之刪除、銷毀或移轉、存取個人資料者之資訊、定期檢查處理個人資料之資訊、教育訓練、計畫稽核及改善措施之執行紀錄」5年？					