工程技術顧問業個人資料檔案安全維護計畫及處理辦法草案總說明

個人資料保護法（以下簡稱本法）第二十七條規定，非公務機關應採行適當之安全措施，防止所保有之個人資料被竊取、竄改、毀損、滅失或洩漏，中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，並訂定相關計畫及處理方法之標準等相關事項之辦法。

為加強工程技術顧問業對於個人資料檔案安全之保護措施，爰依本法第二十七條第三項訂定本辦法，共計二十二條，其要點如下：

一、本辦法之訂定依據、適用對象、指定專人或建立專責組織及其任務。（第一條至第三條）

二、清查所保有個人資料之種類與數量並建立檔案、個人資料特定目的消失或期限屆滿之處理程序、個人資料之風險評估及管理機制、事故之預防、通報及應變機制。（第四條至第六條）

三、特種個人資料之界定及管理程序、告知義務之程序、利用個人資料行銷之程序、委託他人蒐集、處理或利用個人資料之監督及其程序、個人資料為國際傳輸前應遵循事項、當事人行使權利之程序、個人資料正確性有爭議之處理程序。（第七條至第十四條）

四、有關人員管理、資料安全管理、環境管理及業務終止後個人資料處理方法等事項。（第十五條至第十八條）

五、有關資料安全稽核機制、紀錄保存及整體持續改善等事項。（第十九條至第二十一條）

六、本辦法施行日期。（第二十二條）

工程技術顧問業個人資料檔案安全維護計畫及處理辦法草案

條　　文	說　　明
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	本辦法之訂定依據。
第二條　本辦法適用對象為工程技術顧問公司管理條例所稱工程技術顧問公司（以下簡稱顧問公司）。 顧問公司應訂定個人資料檔案安全維護計畫（以下簡稱維護計畫），並採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 維護計畫之內容應包括第三條至第二十一條規定之相關組織及程序，並應定期檢視及配合相關法令修正。 經營顧問公司，應於取得顧問公司登記證前完成第二項維護計畫之訂定；其於本辦法施行前已取得顧問公司登記證者，應於本辦法施行之日起六個月內完成。	一、依本法第二十七條第一項規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，爰於第一項規定依據工程技術顧問公司管理條例所稱工程技術顧問公司為適用對象。 二、本辦法規定之相關組織及程序要求，顧問公司應明定於維護計畫內，定期檢視及配合相關法令修正，並於規定之時間內完成所屬維護計畫。 三、第四項規定顧問公司訂定維護計畫之時限，俾期明確；另就本辦法施行前已取得顧問公司登記證者，給予六個月作業時間，以完成維護計畫之訂定。
第三條　顧問公司就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源。 前項專人或專責組織之任務如下： 一、規劃、訂定、修正與執行維護計畫及業務終止後個人資料處理方法等相關事項。 二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。 三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。	依本法施行細則第十二條第二項規定，為有效訂定與執行維護計畫，明定顧問公司就個人資料檔案安全維護管理得指定專人或建立專責組織，並配置相當資源，及專人或專責組織之任務。

第四條　顧問公司應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。 前項清查發現有下列情形者，顧問公司應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料： 一、非屬特定目的必要範圍內之個人資料。 二、特定目的消失或期限屆滿而無本法第十一條第三項但書之情形。	顧問公司應依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，定期清查所保有之個人資料現況，並於清查後適當處置。
第五條　顧問公司應依據前條所界定之個人資料範圍及其相關業務流程，分析可能產生之風險，並依據風險分析之結果，訂定適當之管控措施。	依本法施行細則第十二條第二項第三款之規定，維護計畫得就個人資料之風險評估及風險管理加以規定，爰明定顧問公司應依據其相關業務流程，分析於蒐集、處理及利用之過程中，個人資料安全可能發生之風險，並訂定適當之管控措施。
第六條　顧問公司為因應所保有之個人資料發生被竊取、竄改、損毀、滅失或洩漏等事故，應採取下列機制： 一、採取適當之應變措施，以控制並降低事故對當事人之損害，並通報行政院公共工程委員會。 二、查明事故之狀況並以適當方式通知當事人；其通知內容包含個人資料發生事故之事實、業者採取之因應措施及所提供之諮詢服務專線。 三、檢討缺失並研擬預防機制，避免類似事故再次發生。	依本法第二十七條第一項規定，顧問公司為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏，採取相關之因應機制，以降低或控制損害，顧問公司宜根據事故之類型，採取應變措施以控制對當事人之損害，並通報行政院公共工程委員會等機制。
第七條　顧問公司應檢視及確認所蒐集、處理及利用之個人資料是否包含本法第六條所定個人資料與其特定目的，及其是否符合相關法令之要件。	依本法第六條規定，非公務機關原則上不得蒐集、處理及利用病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，爰明定顧問公司應依個人資料之屬性分別建立程序，以檢視及確認是否有蒐集相關個人資料，如有蒐集時，並應確保蒐

	集、處理及利用個人資料，符合相關法令之要求。
第八條　顧問公司為遵守本法第八條及第九條關於告知義務之規定，應採取下列方式： 一、檢視蒐集、處理個人資料之特定目的。 二、檢視蒐集、處理之個人資料，是否符合免告知之事由；其不符者，依據資料蒐集之情形，採取適當之告知方式。	依本法第八條及第九條規定，顧問公司應適時履行告知義務，爰明定顧問公司應檢視蒐集、處理個人資料之特定目的，是否符合免告知當事人之事由及依據資料蒐集之情況，採取適當之告知方式，以有效履行告知義務。
第九條　顧問公司應檢視蒐集、處理個人資料是否符合本法第十九條規定，具有特定目的及法定要件，並檢視利用個人資料是否符合本法第二十條第一項特定目的必要範圍內利用之規定；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外利用要件。	參酌本法第十九條及第二十條第一項規定，明定顧問公司應檢視蒐集、處理、利用個人資料，是否符合本法第十九條及第二十條第一項規定。
第十條　顧問公司於首次利用個人資料行銷時，應提供當事人免費表示拒絕接受行銷之方式。當事人表示拒絕接受行銷時，應立即停止利用其個人資料行銷，並週知所屬人員。	為維護資料當事人之權益，明定顧問公司於首次利用個人資料行銷時，應提供當事人拒絕接受行銷之方式，且當事人表示拒絕接受行銷時，應立即停止利用其個人資料行銷，並週知所屬人員。
第十一條　顧問公司委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。	依本法施行細則第八條規定，委託他人蒐集處理或利用個人資料時，委託機關應對受託者為適當之監督，爰明定顧問公司委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。
第十二條　顧問公司進行個人資料國際傳輸前，應檢視有無行政院公共工程委員會依本法第二十一條規定為限制國際傳輸之命令或處分，並應遵循之。	依本法第二十一條規定，中央目的事業主管機關於一定之法定情形，得限制非公務機關對於個人資料進行國際傳輸，爰明定顧問公司應於國際傳輸前確認行政院公共工程委員會是否有所限制，並加以遵守之。
第十三條　顧問公司為提供資料當事人行使本法第三條所規定之權利，應採	依本法第三條規定，當事人就其個人資料得行使查詢、閱覽、製給複製本、補充或

取下列方式為之： 一、確認是否為個人資料之本人，或經其委託授權。 二、提供當事人行使權利之方式，並遵守本法第十三條有關處理期限之規定。 三、告知是否酌收必要成本費用。 四、有本法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人行使權利之事由，應附理由通知當事人。	更正、停止蒐集、處理或利用及刪除之權利，爰明定顧問公司應採取之方式。
第十四條　顧問公司為維護其所保有個人資料之正確性，應採取下列方式為之： 一、檢視個人資料於蒐集、處理或利用過程，是否正確。 二、發現個人資料不正確時，適時更正或補充。 三、個人資料正確性有爭議者，應依本法第十一條第二項規定處理。 因可歸責於顧問公司之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。	為避免當事人發生因資料不正確所產生之損失，爰明定顧問公司為確保所有個人資料之正確性，應採取之方式。
第十五條　顧問公司得採取下列人員管理措施： 一、依據蒐集、處理及利用個人資料個別作業之需要，適度設定所屬人員不同之權限並控管其接觸個人資料。 二、檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員。 三、要求所屬人員負有保密義務。 四、所屬人員離職或完成受指派工作後，應將其執行業務所持有之個人資料辦理交接，亦不得私自持有複製物而繼續使用該個人資料。	顧問公司得採取之人員管理措施。

第十六條　顧問公司應採取下列資料安全管理措施： 一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，應訂定使用可攜式設備或儲存媒體之規範。 二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，應採取適當之加密機制。 三、作業過程有備份個人資料之需要時，應比照原件，依本法規定予以保護。 四、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物於報廢或轉作其他用途時，應採適當防範措施以避免洩漏個人資料；其委託他人執行者，準用第十一條規定辦理。	顧問公司應採取之資料安全管理措施。
第十七條　顧問公司針對保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物之環境，應採取下列環境管理措施： 一、依據作業內容之不同，實施適宜之進出管制方式。 二、所屬人員妥善保管個人資料之儲存媒介物。 三、針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。	顧問公司應採取之環境管理措施。
第十八條　顧問公司業務終止後，其保有之個人資料應依下列方式處理及記錄；其紀錄並應至少保存五年： 一、銷毀者，記錄其方法、時間、地點及證明銷毀之方式。 二、移轉者，記錄其原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。 三、其他刪除、停止處理或利用個人	有關顧問公司業務終止，包括依工程技術顧問公司管理條例第十八條規定自行停業，或受行政院公共工程委員會撤銷、廢止或註銷登記，針對個人資料應為之處理方式及紀錄。

資料者，記錄其方法、時間或地點。	
第十九條　顧問公司應訂定個人資料安全稽核機制，定期或不定期查察是否落實執行所訂之維護計畫或業務終止後個人資料處理方法等相關事項。	顧問公司應訂定個人資料安全稽核機制。
第二十條　顧問公司應採行適當措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所訂之維護計畫之執行情況。	顧問公司應就個人資料保存機制，採行適當措施，以供必要時說明其所訂之維護計畫之執行情況。
第二十一條　顧問公司宜參酌執行業務現況、社會輿情、技術發展、法令變化等因素，檢視所訂之維護計畫是否合宜，必要時予以修正。	顧問公司宜參酌相關因素檢視所訂之維護計畫是否合宜，必要時予以修正。
第二十二條　本辦法施行日期，由行政院公共工程委員會定之。	本辦法施行日期。