法規名稱：電業與公用天然氣事業及加油站業個人資料檔案安全維護管理辦法
修正日期：民國 112 年 11 月 03 日
生效狀態：※本法規部分或全部條文尚未生效
一百十二年十一月三日修正發布之第 2 條第 2 款，自發布後六個月施行。

## 第 1 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。

## 第 2 條

本辦法所稱非公務機關，定義如下：
一、用戶數在三千戶以上之電業及公用天然氣事業。
二、記名會員數達三千筆以上之加油站業。

## 第 3 條

1 非公務機關應依本辦法規定，按其業務規模及特性，衡酌經營資源之合理分配，建立個人資料檔案安全維護管理組織，配置相當人員及資源，負責規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）。
2 本計畫及處理方法之訂定或修正，應經非公務機關代表人或經其授權之人員核定。
3 個人資料檔案安全維護管理組織，應定期就執行任務情形向非公務機關代表人或經其授權之人員提出書面報告。
4 非公務機關應將本計畫及處理方法備置於總機構及營業處所。

## 第 4 條

非公務機關應依個人資料保護相關法令，定期查核確認所保有個人資料現況，界定其納入本計畫及處理方法之個人資料範圍。

## 第 5 條

非公務機關應依前條界定之個人資料範圍及其業務涉及個人資料蒐集、處理及利用之流程，評估可能產生之個人資料風險，並根據風險評估結果，訂定適當管理機制。

## 第 6 條

1 非公務機關為因應所保有之個人資料遭受竊取、竄改、毀損、滅失、洩漏或其他安全事故，應訂定下列應變、通報及預防機制：
一、採取之應變措施，包括下列事項：
（一）控制當事人損害方式。
（二）查明事故原因後通知當事人之方式。
（三）通知當事人事故之事實、所為之因應措施及諮詢服務專線等內容。
二、受通報之相關對象及通報方式。
三、事故發生後研議預防措施。
2 非公務機關因所保有之個人資料遭受竊取、竄改、毀損、滅失、洩漏或其他安全事故，致危及正常營運或大量當事人權益時，應於發現事故後七十二小時內依附表格式以書面通報經濟部。
3 經濟部接受前項通報後，得依本法第二十二條至第二十五條規定，為適當之監督管理措施。

## 第 7 條

非公務機關應就下列事項，訂定管理程序：

一、蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件；其經當事人書面同意者，並應符合本法第六條第二項準用第七條第一項、第二項及第四項規定。

二、檢視個人資料之蒐集、處理或利用，是否符合免爲告知之事由，及所告知之內容、方式是否合法妥適。

三、檢視一般個人資料之蒐集或處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應符合本法第七條規定。

四、檢視一般個人資料之利用，是否符合本法第二十條規定蒐集之特定目的必要範圍；爲特定目的外之利用者，檢視是否符合法定情形；其經當事人同意者，並應符合本法第七條規定。

五、利用個人資料爲行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定爲適當之監督，並於委託契約或相關文件中，明確約定其內容。

七、進行個人資料國際傳輸前，應檢視是否受經濟部限制，並且告知當事人其個人資料所欲國際傳輸之區域，同時對資料接收方爲下列事項之監督：

（一）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。

（二）當事人行使本法第三條所定權利之相關事項。

八、當事人行使本法第三條所定權利之事項：

（一）當事人身分之確認方式。

（二）提供當事人行使權利之方式。

（三）告知當事人需支付之費用。

（四）對當事人請求之審查方式，並遵守本法有關處理期限之規定。

（五）有本法所定得拒絕當事人行使權利之事由者，記載理由及通知當事人之方式。

九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。

十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定刪除、停止處理或利用。

## 第 8 條

非公務機關爲維護所保有個人資料之安全，應採取下列資料安全管理措施：

一、訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，採取適當防範措施。

二、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，採取適當加密機制。

三、作業過程有備份個人資料之需要，對備份資料，應比照原件，採取適當保護措施。

四、妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之需要，亦妥善爲之。

## 第 8-1 條

1 非公務機關以資通訊系統蒐集、處理或利用個人資料，且保有之用戶個人資料達一萬筆者，應採行下列資料安全管理措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、個人資料檔案及資料庫之存取控制與保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行爲之監控與因應機制。

2 前項第五款及第六款所定措施，應定期演練及檢討改善。

## 第 9 條

非公務機關爲維護所保有個人資料之安全，應對所屬人員採取下列管理措施：

一、依據業務特性、內容及需求，設定不同權限，以認證機制管理，定期檢視權限內容之適當性，並控管接觸個人資料之情形。

二、約定保密義務。

## 第 10 條

非公務機關保有之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、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施：

一、依據業務特性、內容及需求，實施適當進出管制。

二、訂定妥善保管個人資料儲存媒介物之方式。

三、依媒介物之特性、使用方式及其環境，建置適當保護設備或技術。

## 第 11 條

非公務機關於業務終止，依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應保存下列紀錄：

一、刪除、停止處理或利用所保有之個人資料之方法、時間、地點及證明方式。

二、將刪除、停止處理或利用所保有之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點及受移轉對象得蒐集、處理或利用該個人資料之合法依據。

## 第 12 條

非公務機關應定期對所屬人員進行個人資料保護認知宣導及教育訓練，使其明瞭相關法令之規定、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及管理措施。

## 第 13 條

非公務機關爲落實本計畫及處理方法之執行，應依其業務規模及特性，衡酌經營資源之合理分配，訂定適當之個人資料安全稽核機制。

## 第 14 條

非公務機關執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應保存下列紀錄：

一、提供當事人行使權利之紀錄。

二、備份及還原測試之紀錄。

三、所屬人員權限新增、變動及刪除之紀錄。

四、因應事故發生所採取行爲之紀錄。

五、其他必要之使用紀錄、軌跡資料及證據保存。

## 第 15 條

1 非公務機關爲持續改善個人資料安全維護，其個人資料檔案安全維護管理組織，應定期提出評估報告，並訂定下列機制：

一、檢視、修訂本計畫及處理方法與相關個人資料保護事項。

二、評估報告中有違反法令情形之虞者，規劃、改善及預防措施。

2 前項評估報告，應向非公務機關代表人或經其授權之人員提出。

## 第 16 條

本辦法自發布日施行。但中華民國一百十一年二月九日修正發布之第八條之一，自發布後三個月施行；一百十二年十一月三日修正發布之第二條第二款，自發布後六個月施行