

法規名稱：(廢)當舖業個人資料檔案安全維護管理辦法

廢止日期：民國 111 年 04 月 06 日

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

本辦法所稱主管機關，在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第 3 條

- 1 當舖業應訂定個人資料檔案安全維護計畫（以下簡稱計畫），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 2 前項所稱當舖業，指依當舖業法規定許可，並經依法設立經營當舖業務之公司或商號。

第 4 條

- 1 當舖業依前條第一項規定訂定計畫時，得視其規模、特性、保有個人資料之性質及數量等事項，參酌第六條至第二十二條規定，訂定適當之安全維護管理措施。
- 2 前項計畫內容應包括下列事項，第二款相關事項必要時得整併之：
 - 一、當舖業之組織規模。
 - 二、個人資料檔案之安全管理措施：
 - （一）配置管理之人員及相當資源。
 - （二）界定蒐集、處理及利用個人資料之範圍。
 - （三）個人資料之風險評估及管理機制。
 - （四）事故之預防、通報及應變機制。
 - （五）個人資料蒐集、處理及利用之內部管理程序。
 - （六）設備安全管理、資料安全管理及人員管理措施。
 - （七）認知宣導及教育訓練。
 - （八）個人資料安全維護稽核機制。
 - （九）使用紀錄、軌跡資料及證據保存。
 - （十）個人資料安全維護之整體持續改善。
 - （十一）業務終止後之個人資料處理方法。

第 5 條

- 1 當舖業應於開業之日起七日內，將計畫報請當地直轄市或縣（市）主管機關備查。
- 2 當舖業於本辦法發布施行前已開業經營者，應於本辦法發布施行日起六個月內，將計畫報請當地直轄市或縣（市）主管機關備查。已經許可經營當舖業務而尚未完成公司設立登記或商業登記者，亦同。

第 6 條

- 1 當舖業應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。
- 2 當舖業應訂定個人資料保護管理政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於營業處所適當之處，如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉。

第 7 條

- 1 當舖業應確認蒐集個人資料之特定目的，於達成特定目的之必要範圍內，界定所蒐集、處理及利用個人資料之類別及範圍，並定期清查所保有個人資料檔案之現況。
- 2 當舖業依前項清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。

第 8 條

當舖業應依已界定蒐集、處理與利用個人資料之類別、範圍及流程，分析評估可能發生之風險，訂定適當之管控措施。

第 9 條

- 1 當舖業應訂定應變機制，於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，迅速處理以保護當事人之權益。
- 2 前項應變機制，應包括下列事項：
 - 一、採取適當之措施控制事故對當事人造成損害。
 - 二、查明事故發生原因及損害狀況，並以適當方式通知當事人事故事實、因應措施及諮詢服務專線等。
 - 三、研議改進措施，避免類似事故再度發生。
 - 四、發生重大個人資料事故者，應即以書面通報當地直轄市、縣（市）主管機關。
- 3 前項第四款所稱重大個人資料事故，指個人資料被竊取、洩漏、竄改或其他侵害事故，致危及大量當事人權益之情形。

第 10 條

當舖業所屬人員為執行業務蒐集個人資料時，應檢視符合蒐集要件及特定目的之必要範圍，並接受該當舖業監督。

第 11 條

當舖業蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第 12 條

中央主管機關依本法第二十一條規定，對當舖業為限制國際傳輸個人資料之命令或處分時，當舖業應通知所屬人員遵循辦理。

第 13 條

當舖業所蒐集之個人資料需作特定目的外利用者，應檢視有無本法第二十條第一項但書規定得為利用之情形。

第 14 條

當舖業於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

- 一、提供聯絡窗口及聯絡方式。
- 二、確認為個人資料當事人之本人，或經其委託者。
- 三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由，應附理由通知當事人。
- 四、收取必要成本費用者，應告知當事人收費基準。
- 五、遵守本法第十三條有關處理期限規定。

第 15 條

- 1 當舖業對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。
- 2 前項安全設備或防護措施，應包含下列事項：
 - 一、紙本資料檔案之安全保護設施。
 - 二、電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。
 - 三、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，當舖業對受託者之監督依第二十二條規定辦理。

第 16 條

- 1 當舖業為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。
- 2 前項管理措施，應包含下列事項：
 - 一、依據業務需求，適度設定所屬人員不同之權限控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。
 - 二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。
 - 三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。
 - 四、所屬人員離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

第 17 條

當舖業對於個人資料蒐集、處理及利用，應符合本法第十九條及第二十條相關規定，並定期或不

定期對於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規定、責任範圍及應遵守之相關管理措施。

第 18 條

- 1 當舖業應訂定個人資料檔案安全維護稽核機制，每半年定期或不定期檢查計畫執行情形，檢查結果並應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。
- 2 當舖業依前項檢查結果發現計畫不符法令或不符法令之虞者，應即改善。

第 19 條

當舖業應採行適當措施，留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，其保存期限至少五年。

第 20 條

當舖業應隨時參酌業務及計畫執行狀況，社會輿情、技術發展及相關法規訂修等因素，檢討所定計畫，必要時應予修正；修正後，應於十五日內將修正計畫報請當地直轄市或縣（市）主管機關備查。

第 21 條

當舖業業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年：

- 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
- 二、移轉：移轉之原因、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資料：刪除、停止處理或利用之方法、時間或地點。

第 22 條

- 1 當舖業委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定為適當監督。
- 2 當舖業為執行前項監督，應與受託者明確約定相關監督事項及方式。

第 23 條

本辦法自發布日施行。