

法規名稱：化粧品批發零售業個人資料檔案安全維護計畫實施辦法

發布日期：民國 111 年 01 月 27 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：在中央為衛生福利部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第 3 條

- 1 本辦法用詞，定義如下：
 - 一、化粧品批發零售業者：指從事化粧品之批發或零售，已辦理公司、商業或有限合夥設立登記，且資本額新臺幣三千萬元以上，並有招募會員或可取得交易對象個人資料之業者。
 - 二、專責人員：指由化粧品批發零售業者指定，負責個人資料檔案安全維護計畫（以下簡稱安全維護計畫）訂定及執行之人員。
 - 三、所屬人員：指化粧品批發零售業者，執行業務之過程中接觸個人資料之人員。
 - 四、查核人員：指由化粧品批發零售業者指定，負責稽核安全維護計畫執行情形及成效之人員。
- 2 前項第二款專責人員與第四款查核人員，不得為同一人。

第 4 條

化粧品批發零售業者，應依本辦法規定訂定安全維護計畫，載明下列事項：

- 一、個人資料蒐集、處理及利用之內部管理程序。
- 二、個人資料之範圍及項目。
- 三、資料安全管理及人員管理。
- 四、事故之預防、通報及應變機制。
- 五、設備安全管理。
- 六、資料安全稽核機制。
- 七、使用紀錄、軌跡資料及證據保存。
- 八、業務終止後，個人資料處理方法。
- 九、個人資料安全維護之整體持續改善方案。

第 5 條

化粧品批發零售業者，應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討及修正安全維護措施，並納入安全維護計畫，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。

第 6 條

- 1 化粧品批發零售業者，應於本辦法發布施行後六個月內，完成安全維護計畫之訂定。
- 2 化粧品批發零售業者應保存前項安全維護計畫；主管機關得定期派員檢查。

第 7 條

專責人員負責規劃、訂定、修正、執行安全維護計畫，及業務終止後個人資料處理方法與其他相關事項，並定期向化粧品批發零售業者提出報告。

第 8 條

- 1 化粧品批發零售業者，訂定第四條第一款個人資料蒐集、處理及利用之內部管理程序、第二款個人資料之範圍及項目時，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。
- 2 化粧品批發零售業者，經定期檢視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、期限屆至而無保存必要者，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。

第 9 條

- 1 化粧品批發零售業者蒐集個人資料時，應符合前條第一項所定之類別及範圍。
- 2 化粧品批發零售業者於傳輸個人資料時，應採取必要保護措施，避免洩漏。

第 10 條

化粧品批發零售業者蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並依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 11 條

化粧品批發零售業者將當事人個人資料為國際傳輸前，應檢視是否受中央主管機關限制，並告知當事人擬傳輸之國家或區域。

第 12 條

- 1 化粧品批發零售業者，依本法第二十條第一項規定利用個人資料為宣傳、推廣或行銷時，應明確告知當事人化粧品批發零售業者立案名稱及個人資料來源。
- 2 化粧品批發零售業者，首次利用個人資料為宣傳、推廣或行銷時，應提供當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷者，應立即停止利用，並周知所屬人員。

第 13 條

化粧品批發零售業者，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對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容。

第 14 條

化粧品批發零售業者，於當事人或其法定代理人行使本法第三條規定之權利時，得採取下列方式辦理：

- 一、提供聯絡窗口及聯絡方式。
- 二、確認為個人資料當事人本人、法定代理人，或經其委託之人。
- 三、有本法第十條但書、第十一條第二項但書或第三項但書，得拒絕當事人或其法定代理人行使權利之事由者，併附理由通知當事人或其法定代理人。
- 四、遵守本法第十三條處理期限規定。
- 五、告知依本法第十四條規定得酌收必要成本費用。

第 15 條

化粧品批發零售業者，訂定第四條第三款資料安全管理及人員管理之措施，應包括下列事項：

- 一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之必要性及適當性。

- 二、檢視各相關業務之性質，規範個人資料蒐集、處理、利用及其他相關流程之負責人員。
- 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、取消所屬人員離職時原在職之識別碼，並要求將執行業務所持有他人個人資料辦理交接，不得攜離使用。

第 16 條

- 1 化粧品批發零售業提供電子商務服務系統，應採取下列資訊安全措施：
 - 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、外部網路入侵防範對策。
 - 六、非法或異常使用系統之監控與因應機制。
- 2 前項所稱電子商務，指透過網際網路進行商品或服務之廣告、行銷、供應、訂購、遞送或其他商業交易活動。
- 3 第一項第五款對策及第六款機制，應定期演練及檢討改善。

第 17 條

- 1 化粧品批發零售業者，訂定第四條第四款事故之預防、通報及應變機制，應包括下列事項：
 - 一、採取適當措施，控制事故對當事人造成之損害，並於發現事故時起七十二小時內，通報直轄市、縣（市）主管機關及通知中央主管機關。
 - 二、查明事故發生原因及損害狀況，並通知當事人或其法定代理人。
 - 三、檢討缺失，並訂定預防及改進措施，避免事故再度發生。
- 2 化粧品批發零售業者，於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，應依前項事故之預防、通報及應變機制迅速處理，保護當事人之權益。
- 3 化粧品批發零售業者發生前項事故者，主管機關得依本法第二十二條第一項規定進入檢查、命相關人員為必要之說明、配合措施或提供相關證明資料，並視檢查結果為後續處置。
- 4 第一項第一款通報紀錄格式如附表。

第 18 條

- 化粧品批發零售業者，訂定第四條第五款設備安全管理措施，應包括下列事項：
- 一、紙本資料檔案之安全保護設施及管理程序。
 - 二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。
 - 三、紙本及電子資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。

第 19 條

查核人員應依第四條第六款規定，定期或不定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向化粧品批發零售業者提出報告。

第 20 條

- 化粧品批發零售業者，訂定第四條第七款使用紀錄、軌跡資料及證據保存之措施，應包括下列事項：
- 一、留存個人資料使用紀錄。
 - 二、留存自動化機器設備之軌跡資料或其他相關之證據資料。

第 21 條

- 1 化粧品批發零售業者，訂定第四條第八款業務終止後，個人資料處理方法之措施，應包括下列事項：
 - 一、銷毀：方法、時間、地點及證明銷毀之方式。
 - 二、移轉：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、刪除、停止處理或利用：方法、時間或地點。
- 2 前項措施應製作紀錄，並至少留存五年。

第 22 條

化粧品批發零售業者，訂定第四條第九款個人資料安全維護之整體持續改善方案，應參酌安全維護計畫執行狀況、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性；必要時應予修正。

第 23 條

本辦法自發布日施行。