

## 綜合商品零售業個人資料檔案安全維護管理辦法修正草案總說明

綜合商品零售業個人資料檔案安全維護管理辦法（以下簡稱本辦法）於一百一十二年八月一日發布施行。考量除綜合商品零售業因經營關係而保有大量個人資料檔案外，專責特定商品之零售業亦有規範之必要，乃將本辦法名稱修正為「零售業個人資料檔案安全維護管理辦法」。又考量零售業之商業模式逐漸數位轉型，網路零售行為日益普及，其保有個人資料檔案數量亦有所增加，如發生個資外洩將造成廣泛的衝擊影響。為強化零售業落實個人資料保護安全維護措施，要求業者訂定個人資料檔案安全維護計畫，以加強管理、確保個人資料檔案之安全維護，爰擬具本辦法修正草案，其修正要點如下：

- 一、修正本辦法適用對象之名稱及定義。（修正條文第三條）
- 二、業者對於個人資料有加密、備份之必要者或傳輸個人資料時，及以資通系統直接或間接蒐集、處理或利用個人資料時，應實施之資料安全管理措施。（修正條文第九條及第十條）
- 三、本次修正納入零售業者應完成安全維護計畫訂定之期程。（修正條文第二十一條）

綜合商品零售業個人資料檔案安全維護管理辦法

修正草案條文對照表

修正名稱	現行名稱	說明
零售業個人資料檔案安全維護管理辦法	綜合商品零售業個人資料檔案安全維護管理辦法	考量除販售多種商品之綜合商品零售業外，專責特定商品之零售業亦有規範之必要，爰修正本辦法名稱。
修正條文	現行條文	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。	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。	本條未修正。
第二條 本辦法所稱主管機關：在中央為經濟部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。	第二條 本辦法所稱主管機關：在中央為經濟部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。	本條未修正。
第三條 本辦法所稱零售業（以下簡稱業者），指非其他中央目的事業主管機關主管之從事實體店面，或實體店面兼營網際網路方式銷售商品之零售，已辦理公司、有限合夥或商業設立登記，且資本額達新臺幣一千萬元以上，並有招募會員或可取得交易對象個人資料之業者，或受經濟部指定之公司、有限合夥或商業。但不包括應經特許、許可或受專門管理法令規範之行業。	第三條 本辦法適用之對象為綜合商品零售業位轉型，網路零售行為日者，指從事以非特定專益普及，所保有個人資料賣形式銷售多種系列商品之零售，已辦理公賣檔案數量增加，如發生資外洩將造成廣泛的衝擊司、有限合夥或商業設影響，且專責特定商品之立登記，且資本額達新零售業亦有納管之必要，臺幣一千萬元以上，並爰修正本辦法適用對象。有招募會員或可取得交又屬其他目的事業主管易對象個人資料之業關主管的零售業，如中藥者，或受經濟部指定之零售業、化妝品零售業、公司、有限合夥或商業西藥零售業、多層次傳銷業。但不包括應經特業、農業販賣業、醫療器材零售業等不屬本辦法法法令規範之行業。適用範圍，併予說明。	
第四條 業者應依其業務規模及特性，衡酌經營資源之合理分配，規	第四條 <u>綜合商品零售業</u> 者應依其業務規模及特性，衡酌經營資源之合	配合第三條之修正，將「綜合商品零售業者」修正為「業者」。

劃、訂定、檢討與修正安全維護措施，並納入個人資料檔案安全維護計畫（以下簡稱安全維護計畫），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。	理分配，規劃、訂定、檢討與修正安全維護措施，並納入個人資料檔案安全維護計畫（以下簡稱安全維護計畫），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。	
第五條 業者應指定安全維護計畫之專責人員，負責規劃、訂定、修正、執行安全維護計畫及其他相關事項，並定期向業者之代表人或經其授權之人員提出報告。	第五條 <u>綜合商品零售業者</u> 應指定安全維護計畫之專責人員，負責規劃、訂定、修正、執行安全維護計畫及其他相關事項，並定期向 <u>綜合商品零售業者</u> 之代表人或經其授權之人員提出報告。	酌作文字修正，理由同第四條修正說明。
第六條 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。 三、資料安全管理及人員管理。 四、認知宣導及教育訓練。 五、事故之預防、通報及應變機制。 六、設備安全管理。 七、資料安全稽核機制。 八、使用紀錄、軌跡資料及證據保存。 九、業務終止後，個人資料處理方法。 十、個人資料安全維護之整體持續改善方案。	第六條 <u>綜合商品零售業者</u> 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。 三、資料安全管理及人員管理。 四、認知宣導及教育訓練。 五、事故之預防、通報及應變機制。 六、設備安全管理。 七、資料安全稽核機制。 八、使用紀錄、軌跡資料及證據保存。 九、業務終止後，個人資料處理方法。 十、個人資料安全維護之整體持續改善方案。	酌作文字修正，理由同第四條修正說明。
第七條 業者訂定前條第一款及第二款所定事項	第七條 <u>綜合商品零售業者</u> 訂定前條第一款及第	第一項及第二項酌作文字修正，理由同第四條修正

<p>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。</p> <p>業者經定期檢視發現有非屬特定目的必要範圍內或特定目的消失、期限屆至而無保存必要之個人資料，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。</p>	<p>二款所定事項時，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。</p> <p><u>綜合商品零售業</u>業者經定期檢視發現有非屬特定目的必要範圍內或特定目的消失、期限屆至而無保存必要之個人資料，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。</p>	<p>說明。</p>
<p>第八條 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，及符合前條第一項所定之類別及範圍。</p> <p>業者於傳輸個人資料時，應採取避免洩漏之必要保護措施。</p> <p>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。</p>	<p>第八條 <u>綜合商品零售業</u>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，及符合前條第一項所定之類別及範圍。</p> <p><u>綜合商品零售業</u>業者於傳輸個人資料時，應採取避免洩漏之必要保護措施。</p> <p><u>綜合商品零售業</u>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。</p>	<p>第一項至第三項酌作文字修正，理由同第四條修正說明。</p>
<p>第九條 業者訂定第六條第三款所定資料安全管理及人員管理之措施，應包括下列事項：</p> <p>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</p>	<p>第九條 <u>綜合商品零售業</u>業者訂定第六條第三款所定資料安全管理及人員管理之措施，應包括下列事項：</p> <p>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</p>	<p>一、序文酌作文字修正，理由同第四條修正說明。</p> <p>二、參考本法施行細則第十二條第二項第六款及中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項第四點第一款，規定</p>

<p>性及適當性。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p><u>五、傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。</u></p> <p><u>六、個人資料有加密之必要者，應於蒐集、處理或利用時，採取適當之加密措施。</u></p> <p><u>七、個人資料有備份之必要者，應對備份資料採取適當之保護措施。</u></p>	<p>認權限內容之必要性及適當性。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>業者蒐集、處理或利用個人資料檔案者，應依據個人資料風險評估之結果，於安全維護計畫中訂定相關資料安全管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰增訂第五款至第七款。</p>
<p><u>第十條 業者以資通安全管理法所稱資通系統直接或間接蒐集、處理或利用個人資料，應採取下列安全措施：</u></p> <p>一、<u>資通訊系統存有個人資料者，應設定認證機制，其帳號及密碼須符合一定之複雜度。</u></p> <p>二、<u>評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。</u></p>	<p><u>第十條 綜合商品零售業者應採取下列安全措施：</u></p> <p>一、使用者身分確認及保護機制。</p> <p>二、個人資料顯示之隱碼機制。</p> <p>三、網際網路傳輸之安全加密機制。</p> <p>四、個人資料檔案與資料庫之存取控制及保護監控措施。</p> <p>五、防止外部網路入侵對策。</p> <p>六、非法或異常使用行</p>	<p>一、業者透過資通系統蒐集、處理或利用個人資料時，若個人資料不慎外洩，將對當事人造成較大損害。為維護上開資通系統所蒐集、處理或利用個人資料之安全，並配合行政院及所屬各機關落實個人資料保護聯繫作業要點第五點第一項第二款，及參考數位經濟相關產業個人資料檔案安全維護管理辦法第十一條</p>

<p>三、<u>確認蒐集、處理或利用個人資料之電腦、相關設備或系統具備必要之安全性，採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅。</u></p> <p>四、<u>與網路相聯之資通訊系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。</u></p> <p>五、<u>建置防火牆、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。</u></p> <p>六、<u>資通訊系統存有個人資料者，應設定異常存取資料行為之監控及定期演練因應機制。</u></p> <p>七、<u>處理個人資料之資通訊系統進行測試時，應避免使用真實個人資料；使用真實個人資料者，應訂定使用規範。</u></p> <p>八、<u>處理個人資料之資通訊系統有變更時，應確保其安全性未降低。</u></p> <p>九、<u>定期檢視處理個人資料之資通訊系統，檢查其使用狀況及存取個人資料之情形。</u></p> <p>前項各款機制，應定期演練及檢討改善。</p>	<p>為之監控及因應機制。</p> <p>前項第五款對策及第六款機制，應定期演練及檢討改善。</p>	<p>第二項，修正第一項序文、第一款至第六款，並增訂第七款至第九款。</p> <p>二、第二項酌作文字修正。</p>
第十一條 業者訂定第六條第四款所定認知宣導	第十一條 綜合商品零售業訂定第六條第四款所	酌作文字修正，理由同第四條修正說明。

<p>及教育訓練計畫，應包括定期對所屬人員進行個人資料保護認知宣導與教育訓練，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。</p>	<p>定認知宣導及教育訓練計畫，應包括定期對所屬人員進行個人資料保護認知宣導與教育訓練，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。</p>	
<p>第十二條 業者訂定第六條第五款所定事故之預防、通報及應變機制，應包括下列事項：</p> <p>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，通報主管機關。如向地方主管機關通報者，並應副知中央主管機關。</p> <p>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，其內容應包括個人資料被侵害之事實及已採取之因應措施。</p> <p>三、檢討缺失，並訂定預防及改進措施，避免事故再度發生。</p> <p>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。</p> <p>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為行政調查、命相</p>	<p>第十二條 <u>綜合商品零售</u>業者訂定第六條第五款所定事故之預防、通報及應變機制，應包括下列事項：</p> <p>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，通報主管機關。如向地方主管機關通報者，並應副知中央主管機關。</p> <p>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，其內容應包括個人資料被侵害之事實及已採取之因應措施。</p> <p>三、檢討缺失，並訂定預防及改進措施，避免事故再度發生。</p> <p><u>綜合商品零售</u>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。</p> <p><u>綜合商品零售</u>業者發生前項事故者，主管機關得依本法第二十二</p>	<p>第一項序文、第二項及第三項酌作文字修正，理由同第四條修正說明。</p>

<p>關人員為必要之說明、配合措施或提供相關證明資料，並視調查結果為後續處置。</p> <p>第一項第一款通報紀錄格式如附表。</p>	<p>條第一項規定進入為行政調查、命相關人員為必要之說明、配合措施或提供相關證明資料，並視調查結果為後續處置。</p> <p>第一項第一款通報紀錄格式如附表。</p>	
<p>第十三條 業者訂定第六條第六款所定設備安全管理措施，應包括下列事項：</p> <p>一、紙本資料檔案之安全保護設施及管理程序。</p> <p>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。</p> <p>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。</p>	<p>第十三條 <u>綜合商品零售</u>業者訂定第六條第六款所定設備安全管理措施，應包括下列事項：</p> <p>一、紙本資料檔案之安全保護設施及管理程序。</p> <p>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。</p> <p>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。</p>	<p>序文酌作文字修正，理由同第四條修正說明。</p>
<p>第十四條 業者訂定第六條第七款所定資料安全稽核機制，應指定資料安全稽核之查核人員，定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向業者之代表人或經其授權之人員提出報告。</p> <p>業者依前項稽核結果發現計畫不符法令或不符法令之虞者，應即改善。</p> <p>業者依第五條規定指定之專責人員與第一項規定之查核人員，不</p>	<p>第十四條 <u>綜合商品零售</u>業者訂定第六條第七款所定資料安全稽核機制，應指定資料安全稽核之查核人員，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<u>綜合商品零售</u>業者之代表人或經其授權之人員提出報告。</p> <p><u>綜合商品零售</u>業者依前項稽核結果發現計畫不符法令或不符法令之虞者，應即改善。</p> <p><u>綜合商品零售</u>業者依第五條規定指定之專</p>	<p>第一項至第三項酌作文字修正，理由同第四條修正說明。</p>



得為同一人。	責人員與第一項規定之查核人員，不得為同一人。	
第十五條 業者訂定第六條第八款所定使用紀錄、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。 業者依前項規定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。	第十五條 <u>綜合商品零售</u> 業者訂定第六條第八款所定使用紀錄、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。 <u>綜合商品零售</u> 業者，依前項規定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。	第一項序文及第二項酌作文字修正，理由同第四條修正說明。
第十六條 業者訂定第六條第九款所定業務終止後，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。 前項措施應製作紀錄，其保存期限至少五年。	第十六條 <u>綜合商品零售</u> 業者訂定第六條第九款所定業務終止後，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。 前項措施應製作紀錄，其保存期限至少五年。	一、第一項序文酌作文字修正，理由同第四條修正說明。 二、第二項未修正。
第十七條 業者訂定第六條第十款所定個人資料安全維護之整體持續改善方案，每年應參酌安	第十七條 <u>綜合商品零售</u> 業者訂定第六條第十款所定個人資料安全維護之整體持續改善方案，	酌作文字修正，理由同第四條修正說明。

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。	每年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。	
<p>第十八條 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，應採取下列方式辦理：</p> <p>一、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。</p> <p>二、遵守本法第十三條處理期限之規定。</p> <p>三、告知依本法第十四條規定得酌收必要成本費用。</p> <p>業者得提供聯絡窗口及聯絡方式，以供當事人或其法定代理人行使前項權利。</p>	<p>第十八條 <u>綜合商品零售</u>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，應採取下列方式辦理：</p> <p>一、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。</p> <p>二、遵守本法第十三條處理期限之規定。</p> <p>三、告知依本法第十四條規定得酌收必要成本費用。</p> <p><u>綜合商品零售</u>業者得提供聯絡窗口及聯絡方式，以供當事人或其法定代理人行使前項權利。</p>	第一項序文及第二項酌作文字修正，理由同第四條修正說明。
<p>第十九條 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。</p>	<p>第十九條 <u>綜合商品零售</u>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。</p>	酌作文字修正，理由同第四條修正說明。
<p>第二十條 業者依本法第二十條第一項規定利用個人資料為行銷時，應明確告知當事人<u>公司</u>登記名稱及個人資料來源。</p>	<p>第二十條 <u>綜合商品零售</u>業者依本法第二十條第一項規定利用個人資料為行銷時，應明確告知當事人<u>綜合商品零售</u>業者登記名稱及個人資料</p>	第一項及第二項酌作文字修正，理由同第四條修正說明。

<p>業者首次利用個人資料為行銷時，應提供當事人或其法定代理人表示拒絕接受行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受行銷者，應立即停止利用，並周知所屬人員。</p>	<p>來源。</p> <p><u>綜合商品零售業</u>者首次利用個人資料為行銷時，應提供當事人或其法定代理人表示拒絕接受行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受行銷者，應立即停止利用，並周知所屬人員。</p>	
<p>第二十一條 業者應於本辦法發布施行之日起六個月內完成安全維護計畫之訂定。</p> <p>業者應保存前項安全維護計畫；主管機關得派員檢查。</p>	<p>第二十一條 <u>綜合商品零售業</u>者應於本辦法發布施行之日起六個月內完成安全維護計畫之訂定。</p> <p><u>綜合商品零售業</u>者應保存前項安全維護計畫；主管機關得派員檢查。</p>	<p>一、第一項及第二項酌作文字修正，理由同第四條修正說明。</p> <p>二、此次修正納入非綜合商品零售業之零售業為適用對象，爰予上開業者於本辦法發布施行之日起六個月內期限完成安全維護計畫之訂定。另綜合商品零售業已於本辦法訂定發布施行之日起六個月內即一百一十三年一月三十一日完成安全維護計畫之訂定，併予說明。</p>
<p>第二十二條 本辦法自發布日施行。</p>	<p>第二十二條 本辦法自發布日施行。</p>	<p>本條未修正。</p>

第十二條附表修正對照表

修正規定		現行規定		說明 本附表未修正。
個人資料侵害事故通報與紀錄表				
事業名稱   通報機關  	通報時間： 年 月 日 時 分	個人資料侵害事故通報與紀錄表		
	通報人： 簽名(蓋章)	通報時間： 年 月 日 時 分		
	職 稱：	通報人： 簽名(蓋章)		
	電 話：	職 稱：		
	Email：	電 話：		
地 址：		Email：		
地 址：		地 址：		
事件發生時間				
事件發生種類		事件發生種類	<input type="checkbox"/> 竊取	個資侵害之總筆數(大約) _____
			<input type="checkbox"/> 洩漏	
			<input type="checkbox"/> 竄改	
			<input type="checkbox"/> 毀損	
			<input type="checkbox"/> 滅失	
<input type="checkbox"/> 其他侵害事故		<input type="checkbox"/> 一般個資_____筆 <input type="checkbox"/> 特種個資_____筆		
發生原因及事件摘要	發生原因及事件摘要			
損害狀況	損害狀況			
個資侵害可能結果	個資侵害可能結果			
擬採取之因應措施	擬採取之因應措施			

