February, 2024

THY
Taiwan International
Law Offices

NEWSLETTER

綜合商品零售業個人資料檔案安全維護管理辦法增訂

經濟部依據個人資料保護法第 27 條[1]之規定，公布〈綜合商品零售業個人資料檔案安全維護管理辦法〉(下稱本辦法)，以促使因經營關係而保有大量個資之綜合商品零售業投入人力、技術及成本，落實保護民眾個人資料之責任。該辦法於 112 年 8 月 1 日發布施行，業者應於本辦法發布施行之日起 6 個月內完成個人資料檔案安全維護計畫之訂定。按個人資料保護法第 48 條[2]之規定，未按同法第 27 條與管理辦法之規定訂定「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」者，將面臨最高一千五百萬元之罰鍰。

一、規範對象

(一) 依公司法、有限合夥法或商業登記法登記者

凡是依公司法登記之股份有限公司、有限公司、兩合公司、無限公司；依有限合夥法登記之有限合夥；或依商業登記法登記之合夥或獨資，均可能係本辦法得適用之對象。

(二) 綜合商品零售業

本辦法所稱綜合商品零售業，係指從事以非特定專賣形式銷售多種系列商品之零售店，如連鎖便利商店、百貨公司及超級市場等。至於銷售單一系列商品之零售店及汽車百貨之零售店，不在前開適用之範圍。

(三) 資本額達新台幣一千萬元以上

所稱資本額，在有限公司、無限公司或兩合公司係指資本總額；在股份有限公司係指實收資本額；在有限合夥係指實收出資額；在商業係指資本額。符合此要件之事業，其個人資料管理之風險將因其規模而升高，有特別予以強化規範之必要。

[1] 個人資料保護法第 27 條：
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。
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。
前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

[2] 個人資料保護法第 48 條第 2 項與第 3 項：
非公務機關違反第二十七條第一項或未依第二項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者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。
非公務機關違反第二十七條第一項或未依第二項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，其情節重大者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。

（四）有招募會員或可取得交易對象個人資料者（或受經濟部指定者）

二、個人資料檔案安全維護機制重點簡介

綜合商品零售業者應按本辦法之規定，按其規模大小採取技術上及組織上之措施，制定安全維護計畫以防止個資被竊取、竄改、毀損、滅失或洩漏。按本管理辦法第 6 條之規定，安全維護計畫中應載明以下事項：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。以下就本法之安全維護機制重點予以簡介：

（一）業者應配置人員專責負責該計畫之規劃與執行，訂定相關之人員管理措施，以及認知宣導及教育訓練計畫[3]。

（二）業者蒐集個資時，應向當事人履行其依個資法所負擔之告知義務；業者利用個人資料為行銷時，應明確告知當事人綜合商品零售業者之登記名稱及個人資料來源[4]。

（三）業者初次利用個資為行銷時，提供當事人或法定代理人拒絕行銷之方式，並支付所需費用；若當事人或其法定代理人拒絕接受行銷，即應立即停止利用[5]。

（四）蒐集個資應有其特定之目的，業者應確認之並定期清查所蒐集之個資是否合於該特定目的之必要性，就非屬該特定目的或特定目的消失、期限屆至而無保存必要之個人資料予以刪除、銷毀、停止利用等其他適當之處置[6]。

（五）為因應資料外洩事故，應完善處理個資之設備安全管理，並訂定相關事故之預防、通報及處理機制、個人資料檔案安全維護稽核機制與訂定使用紀錄、軌跡資料及證據保存之措施[7]。

（六）關於事故預防、通報及處理之機制，其中應包含業主應於發現事故起 72 小時內通報主管機關；查明事故發生原因與損害狀況，並通知當事人或其法定代理人；檢討缺失，並訂定預防及改進措施[8]。

（七）綜合商品零售業者之業務終止後，對其保有之個人資料應視情況採取銷毀、移轉、刪除、停止處理獲利用等妥善處置，並就此些行為留存紀錄保存五年[9]。

[3] 參照綜合商品零售業個人資料檔案安全維護管理辦法第 5 條、第 9 條與第 11 條。
[4] 參照同前註管理辦法第 20 條第 1 項。
[5] 參照同註 3 管理辦法第 20 條第 2 項。
[6] 參照同註 3 管理辦法第 7 條。
[7] 參照同註 3 管理辦法第 12 條、第 13 條、第 14 條與第 15 條。
[8] 參照同註 3 管理辦法第 12 條。
[9] 參照綜合商品零售業個人資料檔案安全維護管理辦法第 16 條。