

味王股份有限公司

個人資料檔案安全維護計畫

壹、目的及依據

為防止爰依「個人資料保護管理辦法」、「食品業個人資料檔案安全維護計畫實施辦法」、「菸酒事業個人資料檔案安全維護管理辦法」及本公司訂定個人資料檔案安全維護計畫（以下簡稱計畫）。並以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

貳、依個人資料保護法之特定目的及個人資料之類別，據以界定本公司個人資料之範圍。

一、蒐集個人資料之特定目的與資料類別

1. 客戶：

- (1) 行銷。
- (2) 非公務機關依法定義務所進行個人資料之蒐集處理及利用。
- (3) 契約、類似契約或其他法律關係事務。
- (4) 食品、藥政管理。
- (5) 消費者、客戶管理與服務。
- (6) 消費者保護。
- (7) 其他經營合於營業登記項目或組織章程所定之業務。

2. 本公司員工或其他業務相關人員：

- (1) 人事管理。
- (2) 全民健康保險、勞工保險或其他社會保險。
- (3) 非公務機關依法定義務所進行個人資料之蒐集處理及利用。
- (4) 其他經營合於營業登記項目或組織章程所定之業務。
- (5) 契約、類似契約或其他法律關係事務。
- (6) 採購與供應管理。
- (7) 產學合作。

參、 個人資料之蒐集、處理與利用

依據本公司「個人資料保護法」及「個人資料保護管理辦法」等規定，進行資料蒐集、處理與利用，本公司應每年編列適當預算，建立適當安全措施。

肆、 個人資料檔案安全維護措施：

一、規劃

1. 依本計畫第二條之個人資料類別，客戶個人資料檔案，應由各單位指定專人定期清查檢視；持有之本公司員工或其他業務相關人員，應由人事單位指定專人定期清查檢視，如發現未經當事人同意之非屬必要性個人資料，或特定目的已經消失、期限屆滿而無保存必要者，應通報專責人員並主動或依當事

人請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

2. 指定專人負責依相關法令辦理個人資料檔案安全維護之規劃、執行事項，並作為本公司內部之個人資料管理代表，及對外個資保護聯絡窗口。被指定之專責人員，應定期(每年)向資安主管提出報告。
3. 定期(每年)對個人資料檔案保護風險進行評估並做成紀錄，如發現有影響個人資料安全之風險或漏洞，應立即採取改善及防備措施。
4. 當發生個人資料安全事件時，辦理個資保護之專人應立即報告資安主管；若事件發生導致個人資料被竊取、洩漏、竄改或其他侵害者，應立刻依下列步驟執行應變措施：
 - (1)採取適當之措施，控制事故擴大對當事人造成損害。
 - (2)立即查明事故發生原因及損害範圍與程度
 - (3)以言詞、書面、電子郵件、網路公告或等適當方式通知當事人，以免其權益受損。
 - (4)資料管理單位應填寫「個人資料通報單」(如表單 1)交由個資保護之專人備查。
 - (5)研議改進措施，避免事故再度發生。
5. 個人資料有錯誤或不足者，予以更正或補充後，應由該資料蒐集部門主動或經當事人請求，將正確、完整之個人資料，通知曾提供利用之對象。

二、執行

1. 各單位專人應對於執行業務所蒐集、持有的個人資料予以分類整理，將資料來源、資料類別、資料性質(數位或紙本)、業務利用目的、處理內容、內部傳送對象、利用方式等載明流程表，並依本計畫第二條之個人資料類別，客戶資料或其他業務資料送交資訊單位專人列管；本公司員工相關資料送交人事單位專人列管，彙整後應各別主動通報專責人員。
2. 各部門對於其所屬員工應製作業務職掌紀錄表，詳細記載執行業務是否蒐集、處理或利用個人資料及該個人資料之類別與範圍。
3. 辦理個資保護之專人應彙整各部門提交之個人資料蒐集、處理、傳送、利用之流程表與業務職掌紀錄表，分析評估可能發生之風險，對於有違法疑慮或保護不周之處，應立即查明並研提改進或控管措施。
4. 當事人行使個資法第 3 條之權利，請求查詢、閱覽、製給複製本或請求補充、更正、停止蒐集、處理或利用、請求刪除個人資料時，依下列方式辦理：
 - (1)設立申辦窗口及聯絡方式。
 - (2)確認申請人身分是否為本人，或經本人委託。
 - (3)依個資法第 10 條、第 11 條規定辦理，如有得拒絕之事由，應將理由告知申請人。
 - (4)告知是否酌收必要成本費用及其收費基準。
 - (5)辦理期限不得違反個資法第 13 條之規定。
5. 個人資料檔案安全管理

- (1)對於廢棄之紙本個人資料，應以碎紙機粉碎之，不得回收再利用。數量過鉅之紙本個人資料，應以其他方式徹底銷毀，銷毀過程應派員監督。
- (2)紙本個人資料有保存必要者，應選擇適當之保管場所並予上鎖責由專人保管，未符合相關程序或許可者，不得調閱或使用。
- (3)個人資料檔案應定期備份，並防止備份檔案被竊取、洩漏、竄改、毀損、滅失、或洩漏。
- (4)含有個人資料之紙本報表之申請、讀取、列印、使用、存檔、轉交等處理或利用行為，應有相關之管理機制。
- (5)個人資料輸入、輸出、存取、更新、更正或註銷等處理行為，應依據確定使用範圍及權限為之。
- (6)個人資料檔案之處理行為應設置使用者帳號及密碼，使用者帳號不得與他人共用，密碼須定期更新。
- (7)電子個人資料檔案禁止存放於未控管內部網路目錄。
- (8)電子個人資料檔案存放之電腦或自動化機器相關設備，應配置安全防護系統(防火牆)或加密機制，並隨時更新。
- (9)未具存取、查閱利用個人資料權限者，對個人資料檔案之處理、利用應留存使用者身分、識別帳號與其行為紀錄以供事後稽查。
- (10)電腦應使用螢幕保護程式，設定螢幕保護密碼，離開座位時應予開啟。
- (11)儲存個人資料之資訊設備應安裝防毒軟體，除至少每日更新病毒碼外，並應每週執行排程掃描。

(12)儲存個人資料之資訊設備應定期檢視、更新作業系統、應用程式漏洞。

(13)內部傳遞或與其他單位交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向備查。

(14)原則上不得允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行。

6. 人員安全管理

(1)依據業務作業需要，設定員工接觸、使用個人資料檔案之權限，以建立管理機制。權限設定內容及其適當性，應隨時檢討並做必要之修正。

(2)處理、持有或保管個人資料檔案之人員，如離職或職務異動，應將所保管之儲存媒體及有關資料列冊移交。如有設置使用者帳號，接辦人員應於相關系統重置密碼外，並視需要更換使用帳號。

(3)處理、持有或保管個人資料之人員，應簽訂保密切結書，並確認於離職時或合約終止時，取消或停用其使用者帳號，且註銷和收繳其員工證件。

7. 設備安全管理

(1)儲存個人資料之資訊設備應注意場所之安全性，並做必要之管制措施，避免無關人員任意出入或接觸。

(2)儲存個人資料檔案之磁碟、磁帶等相關儲存媒體，應指定專人管理，並置於上鎖之實體保護環境，必要時應建立備援機制，以防止資料損壞、遺失

或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

(3)儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

(4)更新或維修電腦設備時，應派員在場監督，確保個人資料之安全及防止個人資料外洩。

三、 認知宣導與教育訓練

1. 新進員工應由教育訓練負責單位，施予有關個人資料保護法之宣導或教育訓練，提高個資保護之意識。

2. 定期或不定期在機構內辦理，或指派所屬員工參加其他機構辦理之相關個人資料保護教育訓練或講習，並作成學習紀錄。

四、 稽核、檢查與紀錄保存

1. 資料安全之稽核檢查

(1)應定期或不定期執行稽核作業，檢查安全維護措施有無疏漏之處，以確保相關措施之有效性。

(2)稽核人員由資安主管指派，且不得與辦理個資保護之專責人員相同。檢查結果稽核人員須向資安主管提出報告。

2. 下列個人資料檔案之使用紀錄、軌跡資料及其他相關證據資料應予保存或記錄於業務職掌紀錄表中，以便日後釐清責任或作為證據。

(1)個人資料蒐集、存取、交付、傳輸等紀錄。

- (2)個人資料利用之紀錄。
- (3)權限新增、變動及刪除之紀錄。
- (4)當事人行使權利之紀錄。
- (5)當事人拒絕接受行銷及相關處理紀錄。
- (6)個人資料變動、更正、補充等紀錄。
- (7)個人資料刪除、廢棄、銷毀紀錄。
- (8)風險評估紀錄。
- (9)業務委外辦理時，依個資法施行細則第 8 條規定之監督紀錄。
- (10)因應事故發生所採取行為之紀錄。
- (11)稽核作業檢查與改善程序執行紀錄。
- (12)專責人員定期向資安主管提出報告之紀錄。
- (13)執行宣導、教育訓練或員工學習紀錄。
- (14)其他與個人資料檔案有關之紀錄。

五、業務終止之資料處理

1. 業務終止後，所保存之個人資料原則應予銷毀，並應記錄銷毀之方法、時間、地點、執行人等資訊。
2. 業務終止後，如保存之個人資料得移轉者，應記錄移轉原因、對象、方法、時間、地點、執行人及受移轉對象得保有該個人資料之合法依據等資訊。
3. 業務終止後，須刪除、停止處理或利用個人資料時，應記錄其時間、地點、方法與執行人等資訊。

六、 改善行動

1. 稽核發現缺失時，應立刻進行風險評估與改進措施，以確保安全維護計畫之有效性。
2. 若發生個資安全事件或其他違法情事，應立即進行檢討改進，修正執行程序或行為，並採取預防措施，以避免再度發生。
3. 隨時注意社會輿情報導、技術發展及法令修正等事項，檢討本安全維護計畫之合宜性，必要時應立即予以修正，確保個人資料檔案之安全維護。

伍、 修定日期：

本計畫經總經理核定公布後生效，其後經變更或修改者，亦同。

中華民國 111 年 4 月 14 日訂定。