

台灣東洋藥品工業股份有限公司
個人資料安全保護管理作業辦法

1 目的

本公司為依「個人資料保護法」(下簡稱「個資法」)及其相關規定落實執行個人資料之保護與管理，特訂定個人資料安全保護管理作業辦法(下簡稱「本辦法」)，以利各單位執行相關作業時有所遵循。

2 範圍

2.1 本辦法適用於本公司，並涵蓋客戶、供應商等所有與本公司有業務往來對象所涉及之個人資料。

2.2 本辦法適用於所有因執行業務而涉及個人資料之蒐集、處理、利用及存管、銷毀之作業等，包括紙本或電子資料檔案皆有適用。

3 定義

3.1 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

3.2 特種個人資料：有關醫療、病歷、基因、性生活、健康檢查及犯罪前科之個人資料。

3.3 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

3.4 蒐集：指以任何方式取得個人資料。

3.5 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

3.6 利用：指將蒐集之個人資料為處理以外之使用。

3.7 國際傳輸：指將個人資料作跨國(境)之處理或利用。

3.8 當事人：指個人資料之本人。

3.9 告知事項：係指本公司針對當事人所提供之個人資料，依本辦法於蒐集時或首次處理利用時應向當事人告知之事項。

4 權責

4.1 本辦法之制定、修訂、解釋之主責單位：法務暨法遵處。由法務暨法遵處指定一名「專責人員」，負責訂定、修訂本辦法，及於必要時指定一名「查核人員」負責稽核

本辦法的執行情況與成效。專責人員與查核人員不得為同一人。本辦法應根據執行狀況、技術發展、法令修改等因素，檢視並適時修正本辦法。

4.2 本辦法之核准：總經理。

4.3 本辦法相關部門：為所屬業務與因業務執行而進行資料蒐集、處理、利用個人資料之各業務執行單位。法務暨法遵處得視作業內容，必要時由人力資源處及資訊處協同辦理本辦法之相關程序。

5 內容

5.1 個人資料盤點

5.1.1 本公司各部門應進行個人資料盤點，並維護【個人資料檔案盤點表】，盤點表內容應符合以下原則：

5.1.1.1 應包含紙本或電子資料檔案。

5.1.1.2 應說明使用該檔案項目之流程或目的。

5.1.1.3 應記載個人資料之蒐集方式、告知事項，以及保存方式及年限。

5.1.1.4 其他法定應記載之事項及必要之事項。

5.2 個人資料之蒐集

5.2.1 各部門於蒐集個人資料時，應與業務內容具有正當合理之關聯，不得逾越特定目的之必要範圍，並符合下列情形之一：

5.2.1.1 法律明文規定。

5.2.1.2 與當事人有契約或類似契約之關係。

5.2.1.3 當事人自行公開或其他已合法公開之個人資料。

5.2.1.4 經當事人書面同意。

5.2.1.5 與公共利益有關。

5.2.1.6 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

5.2.2 如有新增或修改個人資料蒐集之相關作業時，應評估確認是否符合個資法規範並調整【個人資料檔案盤點表】。

5.2.3 除法定免告知或受他人委託處理業務之情形，蒐集當事人個人資料時，本公司應制定並提供告知事項，並應注意以下事項：

- 5.2.3.1 應於直接蒐集個人資料時，即主動提供告知事項予當事人，並經當事人確認後方得蒐集其個人資料。請參見【個人資料告知聲明暨同意書】。
- 5.2.3.2 告知事項應有版本控管機制，取用時應注意版本之最新，相關文件內容及版本控管紀錄保存期限，應至少等同於當事人之個人資料保存期間。
- 5.2.3.3 蒐集之個人資料若使用於行銷目的，應明確告知當事人拒絕接受行銷之方式（如：提供免付費電話或免費回郵信封等）。
- 5.2.4 直接蒐集個人資料之告知事項內應包含下列事項：
 - 5.2.4.1 本公司名稱與聯絡方式。
 - 5.2.4.2 蒐集之目的。
 - 5.2.4.3 個人資料之類別。
 - 5.2.4.4 個人資料利用之期間、地區、對象及方式。
 - 5.2.4.5 當事人得行使之權利及方式。
 - 5.2.4.6 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
- 5.2.5 有下列情形之一者，得免為第 5.2.4 條之告知：
 - 5.2.5.1 依法律規定得免告知。
 - 5.2.5.2 個人資料之蒐集係本公司履行法定義務所必要。
 - 5.2.5.3 告知將妨害公共利益。
 - 5.2.5.4 當事人明知應告知之內容。
- 5.2.6 間接蒐集個人資料之告知事項，除第 5.2.4 條所定事項以外，還應向當事人告知個人資料來源。
- 5.2.7 間接蒐集個人資料有下列情形之一者，得免為告知：
 - 5.2.7.1 有以下所列情形之一者：
 - A.符合第 5.2.5 條所定之情形。
 - B.當事人自行公開或其他已合法公開之個人資料。
 - C.不能向當事人或其法定代理人為告知。
 - D.基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

5.2.8 非由當事人提供之個人資料，應要求提供者確認第三人已於事前同意，且該第三人提供之個人資料均為真實且正確。

5.2.9 各部門於業務新增或變更時，應檢視所蒐集之個人資料符合特定目的。

5.3 個人資料之處理與利用

5.3.1 除法令或主管機關有其他特殊規定外，各部門應要求所管轄範圍內之個人資料處理與利用，不逾越原蒐集當事人個人資料之特定目的範圍。各部門所蒐集之個人資料皆屬於【文件管理辦法】中所定義之機密等級之文件，並應依照【文件管理辦法】相關規定處理與利用。

5.3.2 各部門如需新增或變更原個人資料之處理與利用，應確認符合法令規定並調整【個人資料檔案盤點表】；除法定得行使特定目的外之利用情形，不得為特定目的外之處理或利用其個人資料。

5.3.3 各部門僅得於下列情形之一，對當事人個人資料為特定目的外利用：

5.3.3.1 法律明文規定。

5.3.3.2 為增進公共利益。

5.3.3.3 為免除當事人之生命、身體、自由或財產上之危險。

5.3.3.4 為防止他人權益之重大危害。

5.3.3.5 經當事人書面同意。

5.3.4 個人資料如需交予第三方單位做為行銷用途時，應確認符合法令及主管機關之要求；與第三方單位簽署之契約應載明雙方權利義務，並採取適當程序要求個人資料之使用有適當保護，且不逾越已經告知個資當事人之特定目的範圍。

5.3.5 使用個人資料進行業務行銷時，應先確認於當事人同意範圍內為之；當事人表示拒絕接受行銷時，應即停止利用其個人資料進行行銷。

5.3.6 使用不同蒐集來源之個人資料進行綜合分析時，應確認符合法令要求。

5.3.7 個人資料做跨國（境）之處理或利用時，應確認該行為符合個人資料保護法令或主管機關之相關規定辦理。

5.3.8 個人資料調閱之注意事項

5.3.8.1 個人資料如遇第三方進行查調時，應確認相關提出公文或文件是否符合法令、主管機關規定及本公司規定，始得提供資料。

5.3.8.2 相關之調閱，應依照【文件管理辦法】填具【機密文件調閱申請單】，留存紀錄備查。

5.3.9 個人資料如須提供予第三方時，須留存提供紀錄備查。

5.4 個人資料正確性之維護

5.4.1 各部門於個人資料之蒐集、處理、利用個人資料時，應先確認個人資料之正確性。

5.4.2 接獲外部單位或個人通知個人資料有錯誤之虞時，應立即進行資料檢核確認。一經檢核後確認資料有誤應及時更正；如當事人個人資料發生錯誤且無法被更正時（例如歷史資料等），應註明於相關文件或資訊系統，並視情況記錄其正確之個人資料。

5.4.3 如有發現因本公司內處理個人資料之資訊系統或流程導致個人資料錯誤，應及時修正錯誤。

5.5 個人資料之保存與銷毀

5.5.1 紙本個人資料檔案（含備份資料）保存應放置於有門禁管制的檔案室或上鎖櫃中，且相關鑰匙應妥善保管。紙本之個人資料之調借應留存相關紀錄。

5.5.2 電子個人資料檔案應儲存於具有存取控制及加密機制之公司資訊系統或設備中，不得儲存於個人使用之隨身碟、行動硬碟，或私人電腦等個人裝置或外接儲存設備。

5.5.3 各部門應考量實務狀況於法令許可範圍內，訂定個人資料之保存期限，並傳達予所有相關人員知悉。

5.5.4 處理完畢後確認無需再使用之紙本個人資料檔案，應歸檔保存或銷毀，不得作為回收紙使用，以防止個人資料不當使用及洩漏。

5.5.5 紙本個人資料檔案應使用碎紙機或其它無法還原之方式（如：溶為紙漿、焚化等）進行銷毀。電子檔案應使用不可還原之方式進行銷毀。

5.5.6 涉及個資處理及利用的資訊資產之報廢，應循本公司【資訊安全政策】相關規定辦理，以防止個人資料不當使用及洩漏。

5.5.7 各部門已達保存年限之個人資料檔案，應定期銷毀並確實執行安全控管措施，且須留存相關紀錄，銷毀紀錄應包含方法、時間、地點及證明銷毀之方式，銷毀紀錄應至少留存五年。

5.6 個人資料之傳輸

5.6.1 本公司對外進行紙本或電子個人資料檔案傳輸時，應確保傳輸過程之安全。若涉及國際傳輸，應檢視是否受中央主管機關限制，並告知個資當事人擬傳輸之國家或區域。

- 5.6.2 使用影印機、印表機及傳真機等輸出入設備列（影）印或收受含有個人資料之文件時，應避免將文（證）件留置於多功能事務機上。留置於影印機、印表機、傳真機及多功能事務機之文件，經發現含有個人資料且確認無人認領時，應立即銷毀。
- 5.6.3 個人資料以傳真方式傳輸時，應於傳真前通知接收對象，並於傳真後與接收對象進行確認。
- 5.6.4 以電子方式傳輸涉及個人資料之檔案時，應按【文件管理辦法】中機密性文件所規範之方式採用適當之加密技術（如：加密連線、專線等）或其他足以確保傳輸安全性之方式進行傳輸。

5.7 當事人權利行使

- 5.7.1 本公司直接或間接蒐集持有之各項個人資料，均應提供當事人得行使以下權利，且不得要求當事人預先拋棄或以特約限制之：
 - 5.7.1.1. 查詢或請求閱覽。
 - 5.7.1.2. 請求製給其複製本。
 - 5.7.1.3. 請求補充或更正。
 - 5.7.1.4. 請求停止蒐集、處理或利用。
 - 5.7.1.5. 請求刪除。
- 5.7.2 當事人請求行使前條之權利時，應確認請求人為當事人本人、法定代理人或經其委託之人後，依以下程序辦理：
 - 5.7.2.1 受理當事人依第 5.7.1.1 條與第 5.7.1.2 條事項之申請時，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。
 - 5.7.2.2 受理當事人依第 5.7.1.3 條至第 5.7.1.5 條事項之申請時，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。
- 5.7.3 受理當事人查詢或請求閱覽個人資料或製給複製本者，得視必要成本費用訂定手續費之收取標準，並應告知當事人收取之費用。
- 5.7.4 有關當事人權利行使之處理，需以【當事人權利行使申請書】留存紀錄。

5.8 個人資料安全控管措施

- 5.8.1 個人資料之儲存與處理應注意以下安全控制措施：

5.8.1.1 個人資料之儲存、調閱、傳遞、銷毀等，應按【文件管理辦法】中機密性文件所規範之方式及本辦法進行，以確保個人資料受到安全之儲存和處理。

5.8.2 個人資料之存取控制措施應注意以下事項：

5.8.2.1 授權部門(人員)應僅授予工作人員職務上需求之個人資料存取權限；各部門使用之資訊系統權限授予，應僅限於業務執掌範圍內之人員。

5.8.2.2 針對重要之個人資料應定期執行備份作業，以確保資料之可用性。個人資料電子檔備份之存取權限應與正式資料相同。

5.8.2.3 有關資訊系統之密碼維護以及個人電腦使用管理，應依本公司【資訊安全政策】、【資訊設備安全管理辦法】、【資訊系統管理辦法】等相關規定遵循辦理。

5.8.3 若有發生個人資料被竊取、竄改、毀損、滅失或洩漏，本公司應：

5.8.3.1 迅速採取適當措施，控制事故對當事人造成之損害，並於發現事故起七十二小時內，通報台北市政府及衛生福利部等主管機關。

5.8.3.2 於查明後依法令以適當方式通知當事人或其法定代理人。

5.8.3.3 將事故處理過程紀錄於【個人資料侵害事故通報與處理紀錄表】，並應檢討缺失，訂定預防及改進措施。

5.9 作業委外處理

5.9.1 包含個人資料之業務如須委外處理，須評估委外廠商執行委託業務之資訊安全技術與控制措施，是否符合本公司個人資料保護管理之要求。

5.9.2 委外處理包含個人資料之業務時，所簽訂之契約應載明雙方權利義務，包含委外廠商之安控層級要求及進行實質審查之權利，或至少須要求委外廠商簽訂保密切結書。

5.9.3 非經本公司書面同意，委外廠商不得將作業複委託他人處理。

5.9.4 涉及個人資料業務若有委託第三人處理，本公司至少應視委外業務性質，確認下列事項：

5.9.4.1 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

5.9.4.2 應定期確認委外廠商為防止個人資料被竊取、竄改、毀損、滅失或洩漏採取技術上及組織上之必要措施，並將確認結果記錄之。

5.9.4.3 有複委託者，其約定之受託人。

5.9.4.4 委外廠商或其受僱人違反個人資料保護法規或委託契約條款時，應向本公司通知之事項及採行之補救措施。

5.9.4.5 本公司對委外廠商保留指示之事項。

5.9.4.6 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。

5.9.5 非屬執行該委外作業所必須之當事人個人資料，不得提供予廠商；如另有其他法令限制該個人資料之處理或利用，本公司亦不得予以提供。

5.9.6 廠商或其聘僱人員於執行委外作業時，因故意或過失致使個資當事人權益受損時，若由本公司對個資當事人負責，嗣後應依委外契約約定向廠商請求賠償。

5.10 教育訓練

5.10.1 為提升本公司全體人員對個人資料保護及個資法相關法規之認識，並落實本辦法，本公司將視情況不定期辦理個人資料保護之教育訓練。

5.11 資料安全稽核

5.11.1 查核人員將不定期進行本辦法執行情形之查核，且就查核結果向總經理提出報告，並留存相關紀錄，其保存期限至少五年。

5.11.2 前項檢查結果發現有不符法令或有不符法令之虞者，本公司相關單位應研提改善措施並確保相關措施之執行。

5.12 個人資料業務之規範適用

5.12.1 關於個人資料業務之規範，應以本辦法優先適用，惟本辦法如有未盡之處，應依【文件管理辦法】及其他相關辦法補充辦理之，若有衝突時，應遵守較嚴格之規定。

6 相關/參考文件

【資訊安全政策】

【文件管理辦法】

【資訊設備安全管理辦法】

【資訊系統管理辦法】

【機密文件調閱申請單】

7 表單及/或附件

【個人資料檔案盤點表】

【個人資料告知聲明暨同意書】

【當事人權利行使申請書】

【個人資料侵害事故通報與處理紀錄表】