

個人資料保護之管理

1. 目的：為規範凱衛股份有限公司(以下簡稱「本公司」)因業務權責需要，對個人資料之蒐集、處理及利用，符合個人資料保護相關法令與本公司內部作業規定，以避免當事人之權利蒙受侵害，特制定本要點。

2. 範圍：

2.1. 本要點適用於以下範圍：

2.1.1. 適用之業務，涵蓋所有本公司之營運作業與本公司委外處理之業務中，直接或間接蒐集、處理、利用、傳輸、保存及銷毀本公司持有或遞交個人資料之業務流程。

2.1.2. 適用之資料種類，涵蓋所有因應本公司營運目的所需蒐集之個人資料，例如：員工資料、會員資料、消費者資料等。

2.1.3. 適用之資料形式，涵蓋所有本公司於營運作業中，蒐集、處理及利用含有個人資料之紙本文件、電子檔案、系統資料及電子媒體。

2.2. 本公司全體員工及與受本公司委託處理業務之第三人或事業體，例如：委外廠商、派遣人員及顧問等，均需遵守本要點及本公司個人資料保護相關規範。本作業適用於財物保險與員工團體壽險之契約簽訂及損害請求賠償等事項之辦理。

2.3. 名詞定義：

2.3.1. 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。

2.3.2. 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。

2.3.3. 蒐集

指以任何方式取得個人資料。

2.3.4. 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。

2.3.5. 利用

指將蒐集之個人資料為處理以外之使用。

2.3.6. 國際傳輸

指將個人資料作跨國（境）之處理或利用。

2.3.7. 公務機關：

指依法行使公權力之中央或地方機關或行政法人。

2.3.8. 非公務機關：

指前款以外之自然人、法人或其他團體。

2.3.9. 當事人

指個人資料之本人、與本公司有業務交易往來之廠商、財務金融機構等。

2.3.8. 個人資料處理生命週期

係指個人資料於本公司的處理過程，包含個人資料的蒐集、處理、利用、保存、傳輸及銷毀等階段。

2.3.9. 告知事項

係指本公司針對當事人所提供之個人資料，依本要點於蒐集時或首次處理利用時應向當事人告之事項。

3. 內容：

3.1. 流程圖號：無

3.2. 程序說明：

3.2.1. 個人資料保護認知與教育訓練

- (一) 管理處規劃全公司個人資料保護之法令宣導訓練事宜。
- (二) 各部門應要求所屬員工均須參與個人資料保護相關教育訓練，藉以提升個人資料保護之責任認知，並具備業務上執行個人資料保護事項與落實制度所需之能力。
- (三) 與外部相關機關、團體應維持適當之溝通管道，並得視需要派員參加外部教育訓練或研討會，以持續獲知與個人資料保護相關之議題資訊。

3.2.2. 個人資料隱私衝擊分析

- (一) 為確保個人資料相關蒐集、處理及利用之法令遵循性，應識別並評估個人資料所面臨之法令風險。
- (二) 本公司應於個資相關法令法規與主管機關規範之要求事項變動，或涉及個資相關之業務異動時，進行個人資料隱私衝擊分析，並檢視潛在法律風險事項。
- (三) 個人資料隱私衝擊分析之評估範圍應包含個人資料處理生命週期所面臨之法令風險。

3.2.3. 個人資料之蒐集

(一)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：

1. 法律明文規定。
2. 與當事人有契約或類似契約之關係。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 經當事人書面同意。
5. 與公共利益有關。
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。

(二)新增或修改個人資料蒐集之相關作業時，應進行隱私權衝擊分析並調整「個人資料檔案盤點表」。

(三)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：

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。
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。
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)。

(四)直接蒐集個人資料之告知事項內應包含下列事項：

1. 本公司名稱與聯絡方式。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人得行使之權利及方式。
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。

(五)有下列情形之一者，得免為前項之告知：

1. 依法律規定得免告知。
2. 個人資料之蒐集係本公司履行法定義務所必要。
3. 告知將妨害第三人之重大利益。
4. 當事人明知應告知之內容。

(六)間接蒐集個人資料之告知事項，除6.5.4所定事項以外，尚應向當事人告知個人資料來源。

(七)間接蒐集個人資料有下列情形之一者，得免為告知：

1. 有3.2.4第5項以下所列各款情形之一。
2. 當事人自行公開或其他已合法公開之個人資料。
3. 不能向當事人或其法定代理人為告知。
4. 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。

(八)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。

3.2.4. 個人資料之處理與利用

(一)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。

(二)各部門如需新增或變更原個人資料之處理與利用，應進行隱私權衝擊分析並調整「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。

(三)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：

1. 法律明文規定。
2. 為增進公共利益。
3. 為免除當事人之生命、身體、自由或財產上之危險。

4. 為防止他人權益之重大危害。

5. 經當事人書面同意。

(四)個人資料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，且不逾越經告知之特定目的範圍。

(五)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。

(六)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。

(七)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。

(八)個人資料調閱之注意事項

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。

(九)個人資料如須提供予第三方時，須留存提供紀錄備查。

3.2.5. 個人資料之最小化原則

(一)蒐集、處理及利用之個人資料應符合最小化原則並與其蒐集目的相關，最小化原則如下：

1. 應確認僅蒐集聲明範圍內執行業務所需之個人資料。

2. 處理及利用時應僅使用所需之最少量個人資料。

3. 應確認不處理與特定目的範圍無關或不必要之個人資料。

(二)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。

3.2.6. 個人資料正確性之維護

(一)各部門於設計個人資料蒐集流程時，應建立檢核機制，以確認個人資料之正確性。

(二)接獲外部單位或個人通知個人資料有錯誤之虞時，應依檢核程序辦理。

- (三)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。
- (四)因可歸責於本公司之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。
- (五)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。

3.2.7. 個人資料之保存與銷毀

- (一)書面文件(含備份資料)保存應放置於上鎖櫃中，且相關鑰匙應妥善保管。書面文件之調借應留存相關紀錄。
- (二)個人資料之保存應制定保存期限，並傳達予所有相關人員知悉。如屆保存期限之個人資料，須進行銷毀，並確實執行安全控管措施。
- (三)各部門得考量實務狀況將個人資料永久保存。
- (四)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。
- (五)處理完畢後確認無需再使用之個人資料書面文件，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。
- (六)個人資料書面文件應使用碎紙機或其它無法還原之方式(如：溶為紙漿、焚化等)，電子媒體應使用實體毀損方式進行銷毀(如光碟片使用折毀方式、硬碟使用消磁或敲毀等無法還原資料的方式)。
- (七)涉及個資處理及利用的資訊資產之報廢，應循本公司『固定資產循環-報廢作業』相關規定辦理，以防止個人資料不當使用及洩漏。
- (八)各部門已達保存年限之個資書面文件，應定期銷毀並留存相關紀錄。

3.2.8 個人資料之傳輸

- (一)本公司對外進行數位或紙本之個人資料傳輸時，應確保傳輸過

程之安全。

(二)以電子方式傳輸涉及個人資料之檔案時，應事先取得所屬部門主管之核准，並應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。若採用加密技術，則解密方式應分開傳送。

(三)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。

3.2.9. 當事人權利行使

(一)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：

1. 查詢或請求閱覽。
2. 請求製給其複製本。
3. 請求補充或更正。
4. 請求停止蒐集、處理或利用。
5. 請求刪除。(針對離職員工，勞動基準法第7條規定雇主應置備勞工名卡，登記勞工之姓名、性別、出生年月日、本籍、教育程度、住址、身分證統一號碼、到職年月日、工資、勞工保險投保日期、獎懲、傷病及其他必要事項。前項勞工名卡，應保管至勞工離職後五年。)

(二)當事人請求行使前條之權利時，應依以下程序辦理：

1. 受理當事人依6.10.1.1與6.10.1.2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。
2. 受理當事人依6.10.1.3至6.10.1.5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。
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。

3.2.10. 個人資料安全控管措施

(一)個人資料之儲存與處理應注意以下安全控制措施：

1. 機密性與敏感性之個人資料具有相當之預防措施，以確保個人資料受到安全之儲存和處理。
2. 資訊處應針對端末處理個人資料之資訊設備(包含備份磁帶、可移除式USB 設備、可移除式硬碟、筆記型電腦及手持式設備等)訂定適當之管理方式。

(二)個人資料之存取控制措施應注意以下事項：

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。
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。
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及內部控制管理程序等相關規定遵循辦理。
4. 宣導使人員清楚瞭解其經合法授予之個人資料存取權僅得使用於工作目的，且個人資料應只能在合法目的下被存取。
5. 處理大量或特種個人資料時，應加強審視其存取權限。

(三)可攜式儲存媒體與資訊設備管理

1. 各部門員工因業務需要需使用可攜式儲存媒體或資訊設備，應向資訊部門登記申請方可使用。
2. 可攜式儲存媒體或資訊設備之持有員工異動時，需辦理移交動作，並登載於移交清冊。
3. 可攜式儲存媒體或資訊設備移交前，應由資訊部門人員進行資料抹除(Erase)作業，並記錄執行人員、執行日期及執行項目，以防止資料不當使用及洩漏。
4. 各部門員工若因業務需要，需攜出本公司之可攜式儲存媒體或資訊設備，應採取適當之安全防護措施，以降低可攜式儲存媒體或資訊設備因遺失或不當使用造成之個人資料外洩風險。

(四)事故之預防、通報及應變機制

1. 預防：
 - a. 本公司員工如因工作執掌而須輸出、輸入個人資料時，

均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

- b. 非承辦之人員參閱契約書類時應得公司權責主管或經指定之管理人員之同意。
- c. 個人資料於本公司與各營業處所間或受委託之公司或商業間互為傳輸時，加強管控避免外洩。
- d. 加強員工教育宣導，並嚴加管制。

2. 通報及應變：

- a. 發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向本公司權責主管或經指定之管理人員通報，並立即查明發生原因及責任歸屬，依實際狀況採取必要措施。
- b. 對於個人資料遭竊取之客戶，應儘速以適當方式通知使其知悉，並告知本公司已採取之處理措施及聯絡電話窗口等資訊。
- c. 針對事故發生原因研議改進措施。

3.2.11. 作業委外處理

- (一) 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，是否符合個人資料保護管理制度之要求。
- (二) 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。
- (三) 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。
- (四) 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包含下列事項：
 - 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。
 - 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。
 - 3. 有複委託者，其約定之受託人。

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. 本公司對委外廠商保留指示之事項。
 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。
- (五)非屬執行該委外作業所必須之個資當事人個人資料，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。
- (六)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。

3.2.12. 監控與審查個人資料管理制度

- (一)為確保本公司個人資料管理制度與規範之被有效執行，本公司應定期辦理內部稽核作業。
- (二)發現個人資料處理有任何重大偏離本公司程序的情況，應立即進行改善，並將結果提供給管理階層審視。

3.2.13. 個人資料管理制度之維護時機

- (一)為確保個人資料管理相關制度文件之落實符合相關法令，本公司應定期或不定期確認個人資料保護相關制度文件及措施之執行及落實狀況。
- (二)作業環境、程序或科技技術發生重大變動時，應重新審視個人資料管理制度或措施之適切性並予以因應調整。

3.2.14. 本公司得依以下方式持續改善並維持本公司個人資料管理制度運作之有效性：

- (一)稽核過程中個人資料相關查核結果。
- (二)當事人申訴(抱怨)、個人資料安全事故、個人資料權利請求及其他等有可能改善個人資料管理制度之相關議題。