天弘化學股份有限公司

個人資料保護管理作業

113/12/20

第一章 管理責任

壹、目的

本管理係天弘化學股份有限公司（以下稱「本公司」）為所蒐集、處理、利用及國際傳輸之個人資料，訂定適當保護之相關事項，以提升並維護本公司有關個人資料的管理作為為目的。

貳、適用範圍

所稱本公司個人資料保護管理制度保護管理對象之「個人資料」，係以本公司所蒐集、處理、利用及國際傳輸之所有個人資料，該個人資料包含自然人姓名、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。
適用範圍包含本公司之董事、定期、不定期職員，派遣職員，部分工時、全時職員均適用，並適用全公司之組織。

第二章 個人資料保護管理制度與政策

本公司為保護所持有之個人資料，依中國民國對個人資料保護相關法規及臺灣個人資料保護與管理制度規範，建置本公司之個人資料保護管理制度與個人資料保護管理政策。

壹、個人資料保護管理制度建置與運作

為有效運作個人資料保護管理制度，本公司制訂個人資料保護管理制度相關文件，並依以下工作排程協助各部門有效運作之；工作排程得視實際作業需要，於每年年底擬定下年專案年度計畫中異動預訂之執行時間。

貳、本公司個人資料保護管理政策

本公司除積極創造與提供超越顧客滿意之服務並善盡企業社會責任外，為確保顧客、員工及合作廠商個人資料之合理利用且避免人格權受侵害，將努力推動以下措施以落實個人資料之保護。

1. 法令遵循

本公司願恪遵中華民國保護個人資料安全之相關法規要求。

2. 個人資料管理制度

本公司依臺灣個人資料保護與管理制度規範，建立與公告全體事業人員周知本公司之個人資料管理制度，以明確訂定公司內個人資料保護管理相關之規範、作業準則，並跨部門成立資通安全暨個資管理小組(以下簡稱個資小組)，分配適當人員透過定期檢查、內評、檢視，以確保管理制度有效運作與持續改善，落實個人資料之保護與管理。

3. 個人資料之蒐集、處理與利用

本公司將依中華民國保護個人資料相關法規之要求，在特定目的範圍內蒐集、處理與利用個人資料，並為不逾越當事人提供個人資料達成之利用目的必要範圍所為之處理、利用採取之適切措施。

4. 提供於第三人之限制

本公司不會非法或隨意提供或公開個人資料予第三人。

5. 維持個人資料之正確性與保障當事人權利之行使

為維持個人資料之正確性與保障當事人權利之行使，本公司針對個人資料與清冊建立定期盤點機制，並訂定個人資料當事人申請、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除個人資料之規則與流程，以確實、迅速回應當事人之相關申請。

6. 安全適當管理措施

本公司將依據各部門所持有個人資料之風險分析，採取適當對策與安全管理措施，以防止個人資料不當存取、外洩、滅失、毀損等問題。

7. 緊急事故應變措施

本公司將訂定個人資料的不當存取、遺失、破壞、竄改及外洩事故應變措施，於確認發生個資外洩事故時，將迅速採取適切相關措施作為，並將事實通知當事人及提供相關查詢與處理管道，以避免個資外洩事故對當事人造成重大不利益及影響。

8. 教育訓練

本公司將對所屬員工實施必要教育訓練，使其了解本公司個人資料保護政策及相關管理措施。

9. 監督委託廠商

在委託廠商蒐集、處理或利用個人資料情形者，本公司將盡法定義務監督受委託廠商。

10. 政策之公告與維護

本公司將以適當之方式公告個人資料保護政策，並定期檢視政策進行必要之改善。

第三章 個人資料保護管理制度建置

壹、個人資料盤點程序

本公司為清查與識別所保有之個人資料檔案，及蒐集、處理或利用該等資料之現況，定期進行個人資料檔案與作業流程盤點，並將盤點結果彙整為「個資盤點表」。

一、個人資料盤點作業

各部門應指派個資管理人員，針對各該部門於營業項目或服務提供相關範圍內所持有或經手的個人資料進行盤點與鑑別，將盤點之資料依盤點表格式填寫。

二、個資盤點清冊建立

各部門指派之個資管理人員所盤點該部門應管理之個人資料，應經由該部門主管簽核確認，彙整成該部門之「個資盤點表」。

三、個資盤點清冊檢視修訂

各部門應定期於每年第一季進行並完成各部門內個人資料現況之盤點。

貳、風險管控程序

一、個人資料的風險分析程序

由各部門受指派之個資管理人員對該部門所盤點出的個人資料，是否有違反法令、不當存取、遺失、外洩、破壞、竄改、目的外利用等項目進行綜合考量，分析風險之程度，並於分析完成後呈由部門主管簽核作成「個資檔案風險評估彙整表」。

二、檢討對策方案

由各部門受指派之個資管理人員就各該部門個人資料風險分析之結果進行檢討，及根據該部門風險分析得出的風險情狀與程度提出風險管控之對策方案。

三、風險分析清冊檢視修訂

各部門受指派之個資管理人員應定期於每年個資盤點完成後兩個月內完成「個資檔案風險評估彙整表」之修訂，並將其交由個資保護管理單位。

個資保護管理單位於收到完成之「個資檔案風險評估彙整表」後，依風險彙整情形擬定個資風險處理計畫，並定期將上述風險評估情形彙整成報告後呈個資小組主管，個資小組主管得視情形於董事會中報告。

於公司營業項目、範圍有新增變動時，或個人資料保護法及其他相關法令規範有修訂，或資訊安全技術、公司內部管理方法，或利害關係人有所請求時，作業流程相關之單位應於會議中提出及進行檢視，並修訂「個資檔案風險評估彙整表」，以維持風險分析清冊為最新之狀態。

參、事故之緊急應變

於本公司所持有之個人資料被竊取、洩漏、竄改、其他侵害，或其他違反個人資料保護相關法令或臺灣個人資料保護與管理制度規範之情事發生時，本公司依以下程

序進行事故之查明程序及其對應：

一、個資緊急事故應變組織、功能執掌與運作原則

1. 公司同仁應於發生事故時，立即通報個資小組，並由個資小組主管統籌掌握、指揮與協調相關單位對該個資緊急事故之處理。
2. 發生事故時，由個資管理單位做為緊急事故應變單位，負責個資事故發生時之事故分析、跨單位聯繫、通知當事人知悉事故發生並提供後續查詢與處理管道，並於查明後告知當事人等事宜。
3. 若相關事件須通報主管機關或發布重大訊息時，由個資小組主管負責將事故通報相關機關，並由個資管理單位記錄個資事故發生期間各項處理狀況，以做成日後內部檢討學習之教案，納入個資管理人員進階課程教材。

二、事故預防

由個資管理單位監督各部門依各項標準作業程序控管各該部門內個人資料使用狀況，並定期蒐集與發布近日國內外發生之個資事故案例，做為內部個資內控作業流程、規範之檢視參考，以減少個資事故發生可能之頻率。

三、事故處理

1. 如公司同仁發現疑似與個資外洩有關的異常徵兆時，發現人員應立即通知個資小組，視需要邀請相關人員共同進行調查，以了解該異常發生之原因，並分析判斷是否為個資事故。
2. 如判斷非為個資事故，個資小組應安排相關權責單位負責持續監控，直到該異常解除或排除；如判斷為個資事故，則應進行以下評估:

(1)影響範圍，有那些系統、應用程式或個人資料檔案受影響。
(2)事故發生來源與原因。
(3)事故對公司營運損失及對財務報表影響情形。
(4)可採取應變措施。
(5)所需協助應變之支援。

3. 個資小組主管應於了解個資事故影響範圍後，協助相關單位就現行補救措施及未來可能處理方式，並研擬相關通知及標準應對話術，及安排適當方式通知當事人，通知內容至少應包含:

(1)事故發生之方式。
(2)已採取之因應措施。
(3)後續查詢與處理管道。

4. 個資小組主管應對主管機關之窗口進行事故通報；並通知個資管理單位將事故應變處置與復原之過程加以記錄。
5. 個資小組主管於通知時，應邀集相關維運管理及業務承辦單位並指定負責人員，共同研判事故發生之原因與嚴重性，就以下事項評估現況與尋求解決方案:

(1)作業影響情況。
(2)事故損害情況。
(3)作業延誤情況。
(4)可能個資外洩管道。

(5)估算回復正常作業所需時間。

6. 如發現事故為重大個資事件或認有必要時，應由個資小組主管向最高管理階層呈報並請核示處理方式。
7. 如發現個資事故有危及人員人身安全或設備遭破壞等涉及民、刑事案件時，應由個資小組主管確認並報請最高管理階層或其授權人之同意後，通知檢警調單位協助處理。

四、存證與避免類似事件再次發生

1. 個資小組之資安管理單位應負責將個資事故處置復原過程中之事故發生原因分析及檢討改善方案、防止類似事件再次發生之具體方案以及事故稽查軌跡、分析相關證據加以記錄建檔，協助做成日後內部檢討學習之教案。
2. 發生之事故為重大個資事件或認有必要時，相關處理人員應保留事件發生之線索，經個資小組主管呈請最高管理階層或其授權人同意後，向檢警調單位或民間專業鑑識單位申請追縱鑑識與偵查支援，藉由稽查記錄資料，釐清事故發生原因與責任，並找出防護漏洞以進一步尋求補強保護方法，以避免事故再次發生。

第四章 個人資料保護管理制度實施

壹、實施程序之訂定

本公司為有效運作個資保護管理制度，將實施程序明確訂定於本管理手冊及相關通報中，並公告全體事業人員周知。

貳、個人資料之蒐集、處理、利用及國際傳輸之基本原則

本公司將以誠實信用方式，在未逾越特定目的之必要範圍及與蒐集之目的有正當合理關聯下，並符合以下各項要求進行個人資料之蒐集、處理、利用及國際傳輸:

一、個人資料之蒐集

應合於個人資料保護法規之要求。

二、個人資料之處理

為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送等行為，應符合個人資料保護法規之要求及確立各部門得接觸資料之人員、個人資料處理專責人員之範圍與權限。

三、個人資料之利用

1. 本公司將藉由公告周知個人資料保護管理及明確記載利用目的之「個資盤點表」，使全公司員工於達成特定目的之必要範圍及職務權限內利用所蒐集、處理之個人資料。
2. 如利用個人資料有逾越特定目的之必要範圍有疑義時，由該部門主管向個資推動單位確認利用目的，並核決告知事項內容及告知義務履行方法。
3. 於有資料共同利用時，則應確認是否有進行共同利用之告知。

四、個人資料之商業行銷

1.本公司利用個人資料進行商業行銷行為，依個人資料保護法，提供當事人首次行銷得表示拒絕接受該行銷之方式；

2.如當事人未於首次行銷時即提出拒絕表示，當事人嗣後仍得依本公司提供之管道及方式表示拒絕，本公司於接受當事人之拒絕表示後，將即停止利用其個人資料。

五、特種個人資料之蒐集、處理及利用限制

非有個資法第六條但書規定之情形，本公司不蒐集有關醫療、病歷、基因、性生活、健康檢查、犯罪前科等特種個人資料。

六、告知義務之履行

1.直接蒐集個人資料時於確認無下列任一得免告知情形者:

(1)依法律規定得免告知。

(2)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(3)告知將妨害公務機關執行法定職務。

(4)告知將妨害第三人之重大利益。

(5)當事人明知應告知之內容。應依個人資料保護法規所訂法定告知時點以適當之方式，就以下事項進行告知:

A.公司名稱

B.蒐集目的。

C.個人資料類別。

D.個人資料利用之期間、地區、對象及方式。

E.如有委託給第三人，受委託單位名稱、委託的個資種類、方式。

F.當事人權利行使方式。

G.不提供時對當事人權益的影響。

2.間接蒐集個人資料時，於確認無下列任一得免告知情形者:

(1)依法律規定得免告知。

(2)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(3)告知將妨害公務機關執行法定職務。

(4)告知將妨害第三人之重大利益。

(5)當事人明知應告知之內容。

(6)當事人自行公開或其他已合法公開之個人資料。

(7)不能向當事人或其法定代理人為告知。

(8)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。

(9)大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

應依個人資料保護法規所訂法定告知時點以適當之方式，就以下事項進行告知:

(1)公司名稱。

(2)蒐集目的。
(3)個人資料類別。
(4)個人資料利用之期間、地區、對象及方式。
(5)如有委託給第三人，受委託單位名稱、委託的個資種類、方式。
(6)當事人權利行使方式。
(7)個人資料之來源。

3.如資料有與其他公司共同利用時，需告知共同利用單位名稱、共同利用個資種類、方式。

七、特定目的範圍變更

針對原已告知當事人之利用目的範圍之變更，本公司將依下列要求作業：

1.於個資盤點時確認原始蒐集個人資料目的外利用是否具合法要件，如無，應準用告知義務履行之方式，主動再行通知當事人，並重新取得當事人書面同意。

2. 將利用目的範圍變更之控制予以紀錄。

參、當事人之相關權利

個人資料當事人得依個人資料保護法向本公司行使請求查詢或閱覽、請求製給複製、請求補充或更正、請求停止蒐集、處理、利用以及請求刪除個人資料等權利，亦可向本公司提出前揭事項之相關申訴與諮詢；本公司將以誠實迅速之態度對應當事人之請求與作成紀錄。

肆、管理監督

一、為確保個人資料檔案之合法且正當蒐集、處理或利用，以及防止個人資料被竊取、竄改、毀損、滅失或洩露，本公司將在所須支出之費用與所欲達到之個人資料保護目的符合適當比例下，於技術上及組織上建置必要、適當之安全措施。

二、前項必要措施，應包括以下事項:

1.成立個人資料安全管理組織，配置相當資源。

2.界定個人資料之範圍。

3.個人資料之風險評估及管理機制。

4.事故之預防、通報及應變機制。

5.個人資料之蒐集、處理及利用之內部管理程序。

(1) 個人資料之蒐集、處理或利用，應尊重當事人之權益，讓當事人有決定被蒐集、處理或利用之權利，並依規定填具「個資使用同意書」。

(2) 公司對個人資料之蒐集、處理或利用不得逾越特定目的之必要範圍。

6.資訊安全管理及人員管理。

7.認知宣導及教育訓練。

8.設備安全之管理。

(1)建置個人資料之有關電腦、自動化機器相關設備、可攜式設備，資料保有單位應定期保養維護，於保養維護或更新設備時並應注意資料之備份及相關安全措施。

(2)客戶個人資料檔案應定期備份，並應進行異地存放。

(3)對於有儲存數位內容之媒體，應實施必要之門禁管理；媒體之儲存空間需要有防災設備。

(4)所有儲存媒體在報廢或另作他用時，必須徹底清除所含資料 ，或以物理方式破壞之，以避免資料不當外洩。

(5)附加必要之封裝措施，如需透過郵遞傳輸時，應以掛號方式寄出，並以膠帶密封保護，記錄資料收取者。

9. 資料安全稽核機制。

(1)稽核單位應至少每年需辦理一次個資安全維護稽核作業，檢視相關單位是否符合規範事項，並針對結果不符合及潛在之風險應劃改善與預防措施並確保相關措施之執行。

10. 必要之使用紀錄、軌跡資料及證據之保存。

(1)應保留與個人資料有關之紀錄、軌跡資料及證據。

(2)因應法規規定，保存個人資料檔案至法定期限五年為止。

11. 個人資料安全維護之整體持續改善。

伍、教育訓練及基礎設施

一、個資保護與管理教育訓練

1. 本公司之員工於任職期間，至少接受一次有關個人資料保護法規或管理制度之基礎訓練。
2. 個資小組成員除前項訓練外，應另參與資訊安全、隱私保護、安全維護措施有關之進階課程，並於課後向所屬部門單位進行宣導。
3. 前述教育訓練課程需保存相關紀錄，以便日後查核所用。

三、成果維持與改善措施

1. 教育訓練課程後以測驗方式進行適當之檢測，如未達標準將補行訓練，並保存相關訓練紀錄。
2. 資安/個資管理單位應彙整教育訓練記錄，向個資推動單位提交訓練紀錄與報告教育訓練結果之有效性。
3. 如有違反個人資料保護相關規定，將通知業務所屬主管，並列入個人考績評分與記錄事項。如違反情節重大者，將依公司內部獎懲辦法進行懲戒。

陸、業務終止個人資料處理

一、本公司因業務考量欲結束相關業務時，須在結束業務結束日起算 3 個月內以碎紙、委外焚化或水銷等方式銷毀紙本；個人資料儲存於伺服器、磁碟陣列、

磁帶等媒介物者，應以格式化方式進行資料刪除，如設備不再使用該媒介物於報廢時應採取消磁、剪斷、敲擊等破壞措施，以免由該媒介物洩漏個人資料。

二、本公司進行前項個人資料銷毀處理時，應記載處理之時間、地點，並以螢幕畫面擷取、照相或錄影等方式留存紀錄。

柒、實施修改

本作業經董事會通過後實施，修正時亦同。

捌、修訂日期

本辦法訂於：中華民國一一三年十二月二十日。