個人資料管理<摘錄>及隱私權政策

一、目的

因應個人資料保護法規範，為防止個人資料外洩、造成資訊安全危機，同時釐清個人權責、義務，以作為公司所有人員在作業所需時存取、使用個人資料的依據，使個人資料之運用、外洩防範及風險發生時因應處理程序有所依循，特訂定此管理辦法。

二、適用範圍

凡公司各部門員工於日常工作運用公司內、外部(如客戶、企業夥伴、承包商)個人資料，皆應遵循本公司所訂定之個人資料管理辦法，包括使用紀錄、軌跡資料及證據保存等事宜，並落實於日常作業流程之中。

三、權責

1.全體同仁：應配合及遵守公司個資安全保護及管理事項。

2.個人資料管理委員會：公司根據法規需求事項，如個資風險因應、資料安全等規劃召集各單位合適人選組成個資管理委員會，負責各項因應事項。

3.部門主管：依業務需求瀏覽業務相關必要之資訊，並應符合 1、4 之權責。

4.個人資料處理人員：個人因業務需求進行個人資料蒐集、處理及運用等程序時，應克盡保密職責，並留存使用記錄以利日後舉證需求。

5.人力資源管理單位：負責檢核及修訂本作業要點、宣導與教育個資法相關事宜。

四、名詞定義：

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、聯絡方式、及其他得以直接或間接方式識別該個人之資料。

2.蒐集：指以任何方式取得個人資料，包含 e-mail、紙本、線上填寫等方式。

3.處理：指建立或使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、連結或內部傳送等。

4.利用：指將蒐集之個人資料於內、外部做各項使用。

5.當事人：指個人資料之本人。

6.舉證責任倒置：公司成員若違反個資法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，則部門及相關同仁需提出無故意或過失證明，稱舉證責任。

7.國際傳輸：指將個人資料作跨國(境)之處理或利用。

五、作業內容：

1.個人資料運用管理：

1.1 向當事人蒐集個人資料時，除法律明文規定外，需經當事人同意並明確告知蒐集目的、個人資料之類別、利用期間、地區、對象及方式，蒐集之個人資料不得任意揭露、販售或用於蒐集時的特定目的以外之用途。

1.2 蒐集個人資料時，需經適當之授權與監督並僅就所需之必要欄位進行蒐集。經授權同意交換個人資料時，電子類文件需對資料檔案加密或透過加密方式傳送、紙本類文件以彌封或其他安全方式進行傳遞。

1.3 個人資料若非經資料當事人之書面同意或經法令規定許可，不得任意揭露、販售或用於蒐集時的特定目的以外之用途。

1.4 告知義務：自當事人處直接取得資料時需於蒐集時一併告知，而從第三人處取得資料時於處理或利用前告知。

2.個人資料處理時保護作為：

2.1 涉及個人資料郵件，需透過加密方式傳送，並於系統設定傳送時出現個資警語。

2.2 涉及個人資料紙本文件，需要妥善封存歸檔，並設置個資放置區，以防外洩。

2.3 公文傳遞途中，若牽涉個人資料部份，需使用公文傳遞袋，減少個人資料洩露風險。

2.4 個人或公用電腦依資訊安全規定應設置密碼並定期更新密碼。

2.5 系統需設定使用/查詢個資權限，降低個人資料風險，並建立使用軌跡以利後續查詢。

2.6 系統在文件輸出時，請加註個人資料警示標語，提醒同仁切勿洩露個人資料。

2.7 所有公司同仁皆需簽署運用聲明，明瞭個人資料保護的重要性、個人資料所有人之權利義務並負保密責任。

3.個資處理人員管理：

3.1 處理接觸機密資料人員，應克盡保密之責，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且回收其識別證及相關證件。

3.2 禁止人員在報章雜誌、傳播媒體、社群網站、部落格、公開論壇或其他任何形式公開業務所知悉之個人資料。

4.個資危害事件(如竊取、洩露、竄改或其他侵害事件)處理：

4.1 通知個資管理委員會聯絡窗口

4.2 確認發生個資危害事件，即時成立應變小組並以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉的方式，通知個人資料受侵害項目、產生之影響及已採取之因應措施。

4.3 事件發生後復原或完成損害管制，並留存處理記錄。

4.4 危害事件如歸責為員工個人蓄意、失職導致，應遵循工作規則及懲戒管理辦法，依其事件危害程度判定懲戒並同時負擔個人資料保護法法令內既定之罰責。

六、隱私權保護政策

公司網站隱私權保護政策請參網址：https://esg.darfon.com.tw/privacy

七、當年度實施情形

2025 年為協助新進同仁理解企業文化，自報到日起即安排新進訓練課程，課程內容包含資訊安全宣導、誠信守則與保密規範、個資運用管理等課程，2025 年合計 231 人次完成相關訓練課程。

2024 年個人資料保護相關教育訓練及相關執行情形如下：

▶資安管理教育訓練

為持續強化全體員工的資訊安全意識與防護能力，本公司透過內部網站不定期更新資訊安全知識，並以電子郵件推播資安公告，提升同仁對潛在資安風險的敏感度與應變能力。對於新進員工，公司在入職時即安排基礎資安宣導，使其能迅速掌握公司資安政策。

此外，達方電子每年兩次為全體同仁規劃資安主題線上教育訓練，並列為必修課程。2024 年執行課程內容涵蓋資安政策、社交工程防範、個資保護、常見資安威脅等，藉此提升員工實務操作中的資安警覺與應對能力。資通安全相關人員除已接受 ISO 27001:2022 內部稽核員培訓，並積極參與外部研討會，如：CYBERSEC 台灣資安大會、資安 365 年會、落實個資安全維護辦法之營運實務研討會、產業雲端資安 AI 研討會、軟體安全開發及資安佈署研討會、台灣金融研訓院資安課程、資安保險應對與策略研討會及 TWCERT 台灣資安通報年會等，參與時數超過 80 小時，以確保專業技能持續精進。

2024 年，達方電子針對員工進行社交工程模擬演練，整體點擊率為 8.4%，符合公司所訂低於 10% 的管控目標。對於點擊模擬釣魚郵件的員工，已安排進行加強式再訓練，藉此強化資安意識，進一步降低潛在資訊安全風險。

訓練對象	訓練主題	訓練人次	訓練人時數
新進同仁	資安政策宣達、郵件安全、軟體合法化	230	230
一般同仁	資訊安全教育訓練 1. 資安政策宣達 2. 基礎通識 3. 資安威脅防範 (釣魚郵件、公共 WIFI) 4. 新興資安威脅 (供應鏈攻擊、深度偽造) 5. 個人資安意識 (密碼安全、個人資料保護法)	1,620	4,860
資通安全人員	ISO 27001:2022 內部稽核員培訓	47	1,504

▶近四年資安與個資保護違反情形

達方電子重視資訊安全與客戶資料隱私，建立完善的資安管理制度與事故應變流程，過去四年並無發生任何重大資訊安全事件。

近四年資安違反情況說明				
項目	2021 年	2022 年	2023 年	2024 年
重大資訊安全事件數	0	0	0	0
涉及客戶隱私之違規事件數	0	0	0	0
因資訊洩漏致受影響的客戶數量	0	0	0	0
因資訊安全事件而支付的罰款 / 罰金總額	0	0	0	0

此外，我們依循隱私保護相關法規，近四年並未接獲任何經證實成立之隱私或個資相關投訴事件。

經證實侵犯客戶隱私或遺失客戶資料的投訴				
項目名稱	2021 年	2022 年	2023 年	2024 年
外部組織投訴件數	0	0	0	0
監管機關投訴件數	0	0	0	0
經證實之資訊洩露、 失竊或遺失客戶資料事件的總數	0	0	0	0

2024 年資安事件

過去四年並無發生任何重大資訊安全事件 0 件