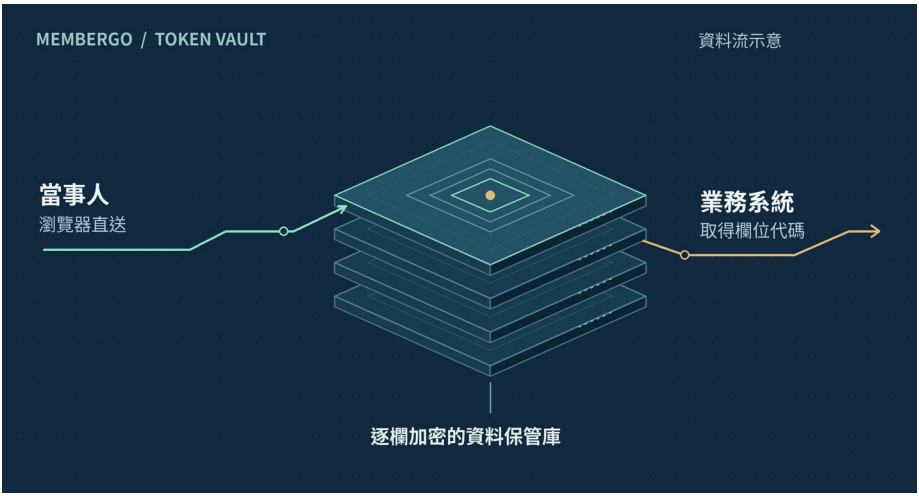
NSECURED

MemberGo

企業資料保護

產品與應用手冊



讓每一次查看敏感資料，都有明確的用途與負責人。

19 個應用情境 / 企業客戶與合作夥伴版

2026 年 11 月

產品摘要 / OVERVIEW

一筆薪轉帳號，誰需要看？

從新進員工報到來看，填寫、核對與匯款是三件不同的工作。每個角色只取得完成當下任務所需的資料。

角色	工作畫面與責任
新人	在 MemberGo 收集頁輸入帳號。原值由瀏覽器直送保管庫。報到系統只接收完成狀態與欄位代碼。
人資承辦	平常依狀態處理報到。需要核對時，說明用途、通過身分驗證，依欄位政策申請單欄揭露。
第二核准人	針對受限欄位，用自己的身分確認理由。核准後由授權人員限時查看一次。
薪資作業	產製銀行薪轉檔涉及批次交付，須另定收件銀行、必要欄位、交付方式與對帳責任。

導入之後，管理者能問什麼？

哪些系統還保存完整帳號？誰有正當理由看過哪個欄位？若員工更正或離職，哪些舊代碼、授權及下游副本需要一起處理？

如何閱讀案例標示

「核心流程」可在架構所述測試版本演示。「串接設計」須接上企業端流程。「條件式應用」另有待開發功能、外部交付或保管資格等前提。

案例中的 DXI 為企業治理平台，VISCOR 為算力平台。

閱讀索引 / CONTENTS

從您的業務場景開始

每則情境占一頁。點選下列分類可前往該組首例。

讓資料從當事人直送保管庫 05–08
新人報到、供應商受款、股東名冊、外部人員

健康與高度敏感資料 09–10
病假與健檢、員工協助與申訴

代碼化與系統隔離 11–13
核心欄位、集團共用正本、測試環境

AI 助理與分析 14–15
AI 助理、分析資料集

當事人權利與法遵 16–18
權利請求、目的與同意、事件鑑識

高權限機密與交接 19–21
緊急存取、實體憑證、離職交接

會員與信任服務 22–23
會員客服、私密服務

產品架構與導入

四道資料關卡 04
選用邊界與作業備援 24
人員與 AI 的授權路徑 25
法遵與事件處理 26
概念驗證與正式上線 27

產品架構 / CONTROL POINTS

一筆資料經過的四道關卡

企業系統沿用自己的案件、訂單與人員流程，將需要保護的欄位交給 MemberGo 保管。

01

收集

企業建立一次性收集工作階段。當事人在保管庫頁面填值。業務端拿到欄位代碼（pii_…）及允許的遮罩摘要。

02

使用

業務系統用代碼關聯案件。人員查看明文時須有理由與多因素驗證（MFA）。受限欄位另由第二人核准。

03

稽核

用追蹤碼串起請求、動作與事件，紀錄人員、用途和欄位識別資訊。成功的 AI 工作負載用量按租戶連續編號。

04

控管

登錄用途、處理依據與保存期間。由型別決定可否交付 AI。刪除先登記獨立帳本，還原舊備份後據以重播。

代碼在業務系統的角色

pii_… 是欄位的參照。只憑代碼無法取得原值。若仍能與人員、訂單或其他線索連結，企業仍應按個資管理。

應用 01 / 收集與報到 • COLLECTION

新進員工報到

適用對象 人資與新進員工 / **串接設計**

新人報到前收到專屬填寫連結。人資需要知道哪些資料已交齊，財會則只在建立薪轉資料時需要帳號。

涉及資料	身分證字號、薪轉帳號、戶籍地址、緊急聯絡方式

實際如何運作

01 人資從報到流程發起一次性收集，新人在 MemberGo 頁面填寫，敏感欄位從瀏覽器直送保管庫。

02 DXI 報到清單保存代碼與完成狀態。只有業務確有核對需要的欄位才顯示末四碼。

03 遇到證號不符，人資以核對報到資料為由申請該欄。另一人完成核准後，授權人員限時查看一次。

業務效益

人資可催辦缺件與完成報到，承辦信箱和報到試算表省去一份明文。

驗收重點

驗收連結重用與逾期均失效。代填緊急聯絡人須確認告知方式。證件照及存摺影本另驗證文件保護。

示範時可以看什麼

一張遮罩報到清單、一筆單欄核准紀錄，以及同一收集連結再次開啟時的拒絕結果。

應用 02 / 收集與報到 • COLLECTION

供應商受款帳號變更

適用對象 採購、出納與財務主管 / **串接設計**

出納收到自稱供應商寄來的改帳通知。面對商業電郵詐騙（BEC），財務要先確認來信者及新受款人身分，再決定能否變更付款指示。

涉及資料	供應商受款帳號、戶名、銀行識別資訊

實際如何運作

01 採購使用主檔中既有的聯絡方式回撥確認，由已核實的供應商代表進入專屬收集頁更新資料。

02 ERP 暫存新代碼，維持舊的付款指示。另一名財務主管核對回撥紀錄、變更單與帳號摘要。

03 核准後，ERP 才切換生效的受款代碼，首筆付款再核對生效版本與核准紀錄。

業務效益

即使承辦人誤信改帳來信，尚有獨立確認與第二人放行兩個攔截點。

驗收重點

以未核准變更試做付款，應仍採舊指示。付款放行、銀行傳檔與回撥程序由財務端配合。

示範時可以看什麼

供應商既有窗口的回撥紀錄、變更單、生效版本，以及首筆付款的覆核結果。

應用 03 / 收集與報到 • COLLECTION

股東名冊與股利作業

適用對象 股務承辦與股東 / **條件式應用**

股東更改地址，股務同時準備通知股東會、發放股利及辦理扣繳。三項作業需要的欄位各不相同。

涉及資料	股東證號、通訊地址、股利受款帳號

實際如何運作

01 股務核實股東身分，發出收集頁，由股東自行更新。名冊平時保留股東編號、代碼與必要摘要。

02 股務按通知、匯款、扣繳分別列出必要欄位。例如寄發通知只需寄送資訊。

03 如需產製整份名冊，由股務系統另設限定收件人、申請理由、第二人核准，以及交付後的檔案管理。

業務效益

承辦人可沿用同一份股東資料準備不同作業，日常畫面減少暴露整份名冊。

驗收重點

現行揭露 API 限單欄。名冊批次輸出須另行設計並驗收，留下版本、範圍與收件紀錄。

示範時可以看什麼

將股東會通知與股利匯款的欄位清單並排，逐項確認收件人與交付後的保存期間。

應用 04 / 收集與報到 • COLLECTION

求職者與外部人員資料

適用對象 招募與外部人員 / **串接設計**

招募結案後，公司仍有顧問履約與實習生報到案件。資料應隨各自的用途與期限處理。

涉及資料	求職聯絡方式、顧問識別欄位、護照號碼、居留證號碼

實際如何運作

01 依作業階段蒐集必要欄位。例如確認聘任及辦理報到時，再請當事人填寫所需的證號。

02 招募系統記錄案件結案日與保存依據。若企業訂未錄取資料保存半年，即依核定起算日安排刪除。

03 承辦人核對到期案件、執行結果與刪除帳本，並另行清查人才庫及原始履歷檔。

業務效益

不同身分可分別設定保留期間，事後可說明哪項資料何時因何用途停止保留。

驗收重點

半年是政策範例。驗證結案日起算、例外保留及外部附件清除。文件內容保護另行評估。

示範時可以看什麼

用不同結案日的兩份虛構履歷，核對應刪、應留案件及原始附件的清除結果。

應用 05 / 健康與申訴 • SENSITIVE RECORDS

病假證明與健檢報告

適用對象 人資、排班與職護 / **條件式應用**

員工提出病假證明，排班主管只需掌握假期。承辦特定審查的人員，才需要接觸受限制的資料。

涉及資料	證明狀態、文件索引、必要醫療欄位，以及病假、健檢、職災或身心障礙證明

實際如何運作

01 先確認得以蒐集的依據及必要範圍，將證明狀態、受限欄位與原始附件分開。

02 假單顯示已附證明。承辦人為審核指定假單，提出單欄申請，由不同主管核准。

03 如需調閱整份報告，改走受限文件系統的權限與紀錄，將案件編號與調閱時間對應。

業務效益

主管可處理出勤，人資可追溯特定審查。兩者能接觸的醫療資訊範圍不同。

驗收重點

v3 所述 M3 文件與大型物件加密尚待實作。試辦先驗收欄位、文件索引及原有文件系統的存取管制。

示範時可以看什麼

分別以排班主管與醫療審查承辦人進入同一假單，核對兩個畫面可見的內容。

應用 06 / 健康與申訴 • SENSITIVE RECORDS

員工協助與申訴案件

適用對象 案件承辦與專業機構 / **條件式應用**

員工提出性騷擾或職場霸凌申訴，希望一般人資與直屬主管無法透過日常系統查到陳述。若涉及心理諮商，原始筆記的保管人也須事先界定。

涉及資料	當事人聯絡方式、案件編號、機密陳述索引、外部專業服務聯絡資訊

實際如何運作

01 案件系統建立代號與指定承辦名單，聯絡欄位分開收集。心理諮商原始筆記依職責由專業機構保管。

02 僅指定承辦人以案件理由調閱必要欄位。需要複核時，選擇與案件無利害關係的核准人。

03 案件移交時收回舊承辦權限，保留調閱者、理由與時間。證詞、調查附件另設閱覽紀錄。

業務效益

調查可持續交接。一般主管只會取得工作安排所需資訊，敏感陳述接觸面較小。

驗收重點

以非承辦人測試跨案讀取及搜尋。釐清各資料的法律性質、文件保護與外部機構保管責任。

示範時可以看什麼

同部門的非承辦人嘗試開啟指定案件時的拒絕結果，以及移交後權限變更的時間。

應用 07 / 代碼化與隔離 • TOKENIZATION

核心識別欄位代碼化

適用對象 資訊、財會與資料管理 / **核心流程**

企業準備縮減 ERP 備份中的完整證號與帳號，同時保留重複資料核對與主檔關聯。

涉及資料	身分證號、護照號碼、銀行帳號、欄位代碼與必要摘要

實際如何運作

01 新值由收集頁直送，ERP 以代碼參照，依需要顯示遮罩。既有明文遷移應另外清查副本。

02 需精準比對的型別，可在保管庫側啟用帶金鑰的 HMAC 索引。機密型別關閉索引。

03 財會要產製薪轉檔時，另設僅限薪轉用途的交付機制，約定接收端、保存期與交付紀錄。

業務效益

業務備份可保留關聯性，受保護欄位的完整值留在保管庫。其他識別線索仍需盤點。

驗收重點

核驗 ERP、匯出與日誌。一般服務帳號無人員揭露權，薪轉批次交付須獨立設計與驗收。

示範時可以看什麼

用同一筆虛構證號檢查業務資料庫備份、錯誤日誌及匯出檔，看哪些位置仍出現原值。

應用 08 / 代碼化與隔離 • TOKENIZATION

集團多系統共用資料正本

適用對象 集團資訊與資料治理 / **串接設計**

同一名員工在 DXI 與其他獲授權系統更新聯絡地址，企業希望更正一次即可更新相關作業。

涉及資料	租戶內主體參照、地址欄位代碼、欄位版本

實際如何運作

01 先確認資料控制權及租戶邊界。在同一租戶內，透過受控的對照將各系統員工編號連回同一主體。

02 員工於收集頁更正，主檔系統更新有效參照。各系統依核定用途重新取得必要摘要。

03 逐一驗證舊代碼失效、快取更新與更正紀錄。不同法人或租戶另訂合法交換流程。

業務效益

地址維護集中，承辦人可追出哪個系統仍使用舊參照，減少各自留存與人工同步。

驗收重點

共用主機不會自動合併身分。驗收同租戶同步，並測試另一租戶無法查到同一代碼。

示範時可以看什麼

一份地址更正紀錄，加上各訂閱系統更新時間與失敗後重新處理的結果。

應用 09 / 代碼化與隔離 • TOKENIZATION

測試與正式環境隔離

適用對象 研發、測試與維運 / **串接設計**

工程團隊需要重現報到或客服流程，希望在測試環境（staging）看到遮罩與核准結果，並避免複製正式個資。

涉及資料	合成資料、測試租戶代碼、遮罩值、案例狀態

實際如何運作

01 建立獨立測試租戶、服務帳號與憑證，以虛構值跑完整收集流程，產生測試專用代碼。

02 測試環境限制對正式保管庫的連線與授權，開發者以合成案例驗證成功、拒絕與逾期。

03 帶入非本租戶的代碼驗證無法讀取，同時抽查測試附件、錯誤報告及日誌沒有正式資料。

業務效益

測試可涵蓋真實的權限分支，減少靠人工遮蔽正式資料來準備測試的工時。

驗收重點

測試租戶、憑證、資料來源與網路出口都要驗收。自由文字或舊資料匯入仍可能夾帶明文。

示範時可以看什麼

同一測試代碼在本租戶與他租戶的不同結果，並核對測試出口無法連線到正式保管庫。

應用 10 / AI 與分析 • AI & ANALYTICS

AI 助理的欄位存取

適用對象 AI 產品與資料負責人 / **核心流程**

DXI 助理要摘要憑證作業進度。它需要單據類別與處理狀態，無須讀取證號、受款帳號或密碼。

涉及資料	憑證作業狀態、個資代碼、模型版本、允許工作負載使用的自訂欄位

實際如何運作

01 DXI 將必要狀態與代碼交給助理。機密與雙人核准型別禁止機器取值，內建個資也不向工作負載釋出。

02 若 VISCOR 推論確需其他資料，另建可供機器取用的型別，以啟用的服務帳號逐次提出用途與模型版本。

03 MemberGo 先核對政策並記錄，再由 Key Broker 逐欄解開授權值。拒絕時不釋出資料。

業務效益

企業可說明某次模型呼叫取得了哪些欄位、依據何在，並保留模型與執行參照。

驗收重點

提示詞、OCR 原圖、自由文字與上傳檔須各自過濾。v3 的硬體遠端驗證尚待完成。

示範時可以看什麼

一筆允許、一筆拒絕的模型請求。對照模型版本、用途、欄位清單與推論端實際收到的內容。

應用 11 / AI 與分析 • AI & ANALYTICS

人資分析與統計資料集

適用對象 人資分析與資料治理 / **串接設計**

人資分析師想比較不同職系的流動率與薪資區間，報告讀者只需要趨勢，無須辨認員工。

涉及資料	專案代碼、職系、薪資區間、到離職月份、群組人數

實際如何運作

01 資料負責人先核定分析用途與期間，以分析專用代碼連結紀錄，移除姓名、證號與明細備註。

02 分析師只取得經核准的欄位。依情境將精確金額與日期轉為區間，合併人數過少的分組。

03 發出報表前，檢視可否從部門、職稱與期間推回特定員工，並依期限清除分析副本。

業務效益

團隊仍能比較群體差異，資料交付範圍與讀者權限也有明確紀錄。

驗收重點

代碼化的資料仍可能被重新識別。分析用代碼產生、小群組門檻與輸出檢查須由分析流程實作。

示範時可以看什麼

一份以小型部門為例的報表。當部門只剩一人時，檢查能否由報表推知該員工薪資。

應用 12 / 權利與法遵 • DATA RIGHTS

當事人查閱、更正與刪除

適用對象 客服、法遵與資料管理 / **串接設計**

離職員工請求查閱、更正聯絡方式，並詢問哪些資料可以刪除。承辦人需要能說明處理範圍與結果。

涉及資料	租戶內主體參照、資料型別、用途依據、刪除工作與復原紀錄

實際如何運作

01 受理單位驗證身分與租戶範圍，彙整用途、資料類型及外部副本，依請求提供查閱或複本。

02 更正時更新有效參照。如請求停止蒐集、處理、利用或刪除，由權責人員確認法定保存與例外。

03 核定刪除後先記入刪除帳本再清除。還原演練中重播帳本並覆核結果，據以製作處理回覆。

業務效益

客服能分項答覆已處理、依法保留及需由其他系統跟進的資料。

驗收重點

刪除紀錄涵蓋已納管資料。還原後要完成帳本重播。驗收時核對下游副本，約定處理回覆與刪除證明的格式。

示範時可以看什麼

一份逐項處理回覆，附上保管庫刪除工作編號、備份復原演練及下游追蹤結果。

應用 13 / 權利與法遵 • DATA RIGHTS

用途限制與同意撤回

適用對象 人資、行銷與網站維運 / **串接設計**

員工同意在公司官網刊登活動照片，之後提出撤回。人資仍須依法辦理日常人事管理。

涉及資料	主體參照、官網刊登用途、同意版本與時間、撤回紀錄

實際如何運作

01 分別登錄官網刊登與人事管理用途，記錄各自的法律依據。告知與同意流程保存對應版本。

02 發布流程先核對該用途及版本有效。收到撤回後終止此用途的後續取用，由網站承辦人下架已發布照片。

03 檢查網站、快取及受委託通路的處理結果，另有合法依據的人事作業依原範圍繼續。

業務效益

員工可撤回一項具體授權，承辦人亦可交代停用的範圍與網站下架進度。

驗收重點

用途檢查與下游撤回同步均須驗收。原始照片的保存、媒體副本及下架交由相應系統處理。

示範時可以看什麼

一筆撤回前後的官網發布測試，分別記錄政策拒絕時間、實際下架時間與快取清除狀態。

應用 14 / 權利與法遵 • DATA RIGHTS

事件鑑識與通知範圍

適用對象 資安應變與法遵 / **串接設計**

客服帳號疑似遭冒用。資安人員需要釐清哪些請求被拒、哪些欄位確曾揭露，以及哪些當事人可能受影響。

涉及資料	人員或服務帳號、欄位參照、申請理由、時間、請求追蹤碼

實際如何運作

01 先保存相關時段的 Vault 紀錄，再對照登入紀錄、DXI 工單、核准與接收端事件。

02 用主體與欄位參照建立受影響清單，標示已證實及待釐清的範圍，避免在調查表重抄明文。

03 由權責人員依適用法規評估通知、通報對象及時點，保留調查依據與後續補正紀錄。

業務效益

調查人員能重建已納管的資料存取順序，提供通知決策所需的案件證據。

驗收重點

v3 明載無缺號的是各租戶成功工作負載用量事件。其他稽核應分別對帳。DXI 租戶稽核匯出在該版列為待開發。

示範時可以看什麼

一條可回溯至登入與工單的調查時間線，明列已證實欄位、待釐清範圍與通知決定。

應用 15 / 高權限機密 • PRIVILEGED ACCESS

緊急存取與事後輪替

適用對象 資訊值班與資產負責人 / **條件式應用**

主要管理員無法登入網域註冊商，值班主管需要啟用緊急存取（break-glass），動用備援管理帳號。這次救援也要能追溯決定與責任人。

涉及資料	組織持有的雲端與網域備援帳號密碼、資料庫緊急帳號、核准保管的復原份額

實際如何運作

01 將機密設為無索引、禁止 AI 與連接器發送。DXI 記錄保管人、資產編號與代碼。

02 值班人員以事件單申請單欄揭露，另一人經近期 MFA 核准，授權者在有效期限內只看一次。

03 事件流程通知權責人員，結案後在來源服務換密碼或輪替份額，更新保管紀錄並覆核。

業務效益

臨時救援有明確的核准、使用與善後責任，例外存取也能納入事後檢討。

驗收重點

DXI 揭露頁、通知與輪替流程須驗收。保管庫自身失效時，另備獨立復原通道。

示範時可以看什麼

一張緊急事件單，串起申請、核准、通知、來源密碼輪替及用舊密碼登入失敗的結果。

應用 16 / 高權限機密 • PRIVILEGED ACCESS

實體載具與密碼分管

適用對象 憑證保管與授權使用者 / **條件式應用**

辦理企業憑證簽章時，保管硬體載具的人與核准動用 PIN 的人各負一項職責。

涉及資料	經授權可由組織保管的工商憑證 PIN、機房密碼、載具或保險箱識別碼

實際如何運作

01 先確認發行機構與持有人允許的保管方式，登錄載具編號，把可代管的 PIN 設為受限制機密。

02 載具由指定保管人簽領。核准人核對作業單後，由授權使用者限時查看 PIN 並完成作業。

03 返還載具時對照領用、揭露與簽章時間。掛失、交接時依發行機構流程辦理停用或重設。

業務效益

實體領用與數位揭露各有責任紀錄，可重建哪一次授權對應哪一次簽章。

驗收重點

自然人憑證與 PIN 由本人掌管。企業網銀啟用碼依銀行授權規則辦理，並驗證實體、數位分管。

示範時可以看什麼

同一次簽章的載具簽領單、PIN 核准紀錄及歸還紀錄，分別標示責任人。

應用 17 / 高權限機密 • PRIVILEGED ACCESS

離職清查與帳號交接

適用對象 人資、資訊與系統管理 / **條件式應用**

資訊主管接獲離職通知。停用員工登入後，還要找出他曾看過哪些共享密碼、掌管過哪些外部服務。

涉及資料	員工身分、帳號清冊、歷次揭露事件、資產負責人、輪替狀態

實際如何運作

01 人資觸發離職清查，身分管理人員停用身分、撤銷現有工作階段，確認生效時間。

02 DXI 離職清查流程（A3-2）按揭露歷史、帳號所有權及實體領用紀錄列出交接與輪替清單。

03 資產負責人在各來源服務更換憑證、更新保管值，複核人查驗舊憑證失效後結案。

業務效益

交接單可逐項對應誰完成換密與驗證，降低因共用帳號而遺漏的風險。

驗收重點

以測試帳號驗證停權與舊憑證失效。租戶級稽核匯出、離職清單及來源系統輪替須串接。

示範時可以看什麼

一張已結案的離職清單，每項共享帳號都附負責人、輪替時間與失效驗證。

應用 18 / 會員與信任 • CUSTOMER PRIVACY

會員客服與行銷授權

適用對象 會員客服與行銷營運 / **核心流程**

會員來電修改配送地址，並要求停止促銷通知。客服需要分別處理這兩項目的與授權。

涉及資料	手機、地址、生日、會員參照。特定業務確有必要時使用的證號

實際如何運作

01 會員自行填寫必要資料，按訂單通知、物流、行銷記錄用途依據。客服先完成身分驗證，再以遮罩值核對會員欲更改的項目。

02 需檢視受限單欄時，客服填寫理由並依政策核准。配送僅依有效訂單授權交付必要姓名、電話及地址。

03 撤回行銷同意後停止後續取用，並由行銷系統同步排除該會員，記錄生效時間。

業務效益

同一位會員可繼續完成獲授權的訂單服務，客服也能交代促銷聯繫何時停止。

驗收重點

測試跨會員、跨店與到期配送授權均被拒。行銷另行告知並記錄同意。既有名單與排程發送也須驗收撤回效果。

示範時可以看什麼

一筆成功配送的必要欄位收據，以及同一會員撤回後被行銷排程排除的紀錄。

應用 19 / 會員與信任 • CUSTOMER PRIVACY

高隱私服務與客戶信任

適用對象 服務營運與委外夥伴 / **串接設計**

智慧祈福服務受託辦理家庭祈願。承辦人需要完成指定服務，會員則想知道家人資料會由誰看見、保留多久。

涉及資料	祈福對象、生辰、家庭成員關係。如另涉健康資料，另審必要性與依據

實際如何運作

01 於收集前逐項說明用途、必要性及保存期間，確認代家人提供資料的適當依據，並提供可選欄位。

02 會員透過獨立收集頁提交，訂單介面顯示服務項目與代碼。只在履約確有需要時授權指定人員查看。

03 履約後依保存政策結案，清查紙本名單、現場作業單與委外副本，提供當事人權利申請窗口。

業務效益

企業能向會員具體交代哪些資訊由誰保管、何種情況有人查看，以及如何辦理更正或刪除。

驗收重點

以一筆模擬訂單檢查門市、列印、通知與合作方資料流。對外說明應與實際可見範圍一致。

示範時可以看什麼

從會員填單、現場列印到委外交付的一筆服務紀錄，每個接觸點都對應保管人與保存期限。

選用指引 / SCOPE

哪些欄位適合進保管庫？

先看業務如何使用一個欄位，再決定原值、代碼與衍生統計各由誰保存。

需求	建議資料配置
少數人偶爾核對	證號、帳號、護照號碼可優先評估。ERP 保留參照或遮罩，原值進保管庫，另定揭露條件。
頻繁搜尋與排序	部門、到職日等業務欄位可留在業務端。姓名同樣屬個資，宜依查找需求與風險決定是否拆欄保護。
大量計算或整批交付	薪資計算、整批匯款與名冊輸出各自規劃。只將所需欄位送到核准接收端，記錄產檔、取用與銷毀。
不能中斷的作業	先定可等待時間、重試和復原順序。可先受理案件並標示待核對，恢復後再完成授權與交付。

備援演練的觀察點

模擬保管庫暫停服務。觀察是否仍可建立不含敏感值的案件，待恢復後是否能對帳。另確認承辦人沒有改由通訊軟體或電子郵件補收原值。

試辦起點

選擇原值容易流入信箱或試算表、人工查看次數低、負責人清楚的欄位。新進員工的證號核對是可獨立驗收的起點。

架構詳解 / ACCESS PATHS

誰能取得哪些欄位？

租戶界定資料邊界。人員、配送連接器與 AI 工作負載各有自己的用途、身分與授權條件。

取用路徑	允許的範圍與條件
人員揭露	以理由與 MFA 申請單欄。受限欄位要求不同人核准。核准人的 MFA 須在 5 分鐘內，核准後 15 分鐘內只可查看一次。
配送連接器	訂單放行並具有有效授權時，送出必要的姓名、電話與地址並留存使用收據。證號與自訂型別不在配送範圍。
AI 工作負載	僅限明確開放的自訂型別。啟用的服務帳號要符合用途、依據、模型、時段及配額。先寫存取紀錄，再由獨立金鑰服務 Key Broker 逐欄解開。

資料庫與金鑰如何分工

各欄位獨立以 AES-256-GCM 信封加密。密文綁定租戶與欄位，資料金鑰由 OpenBao 包裝。需要精準比對時可按型別開啟 HMAC 查詢索引。密碼等機密不建索引。

卡片與企業機密有不同規則

完整卡號由卡片執行器在授權時交給銀行，業務端只持卡片代碼與摘要。卡號沒有取回 API。企業帳號密碼則可另設受限的人員揭露流程。

法遵與證據 / TAIWAN

把法遵問題放回作業流程

以下對照臺灣個人資料保護法。企業應為每項用途指定負責人，判斷適用依據，並保存可查驗的決定與執行結果。

主題	企業應做的判斷與留存
用途與同意 **§ 5、7、19、20**	訂出特定目的與必要欄位。以同意為依據時，保存告知版本、意思表示與時間。目的外利用依適用條件另行處理。
特種個資 **§ 6**	病歷、醫療、基因、性生活、健康檢查及犯罪前科原則上不得蒐集、處理或利用。先確認法定例外，再設計權限。申訴卷宗依內容判斷。
行使權利 **§ 3、11**	受理查詢、閱覽、製給複製本、補充或更正、停止蒐集處理利用及刪除。核實身分與範圍，記錄保留事由並回覆當事人。
事件通知 **§ 12**	對照保管庫、身分與業務端紀錄，研判影響範圍。依事件當時有效條文與業別要求辦理通知或通報，說明侵害事實與已採措施。

查核法源

個人資料保護法｜條文與施行註記

https://law.pdpc.gov.tw/LawContent.aspx?id=FL010627

個人資料保護法施行細則｜全國法規資料庫

https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050022

第 12 條曾於 2025 年 11 月修正公布。適用版本應連同法規沿革及施行日期查核。

導入與驗收 / PILOT

用一筆測試資料完成驗收

以虛構身分證號演練報到。讓人資、資訊與資安各持一份結果，共同核對這筆資料何時可見、何時應被拒絕。

驗收動作	應看見的結果
當事人提交	收集頁成功一次，重用連結失敗。ERP、日誌與通知均查無測試原值。
承辦人核對	沒有理由或第二人核准時拒絕受限欄位。合法核准後限時單次可見，稽核可回查。
AI 助理請求	內建證號不能傳給工作負載。檢查提示詞、原始附件與外送請求的實際內容。
刪除並還原	先留下刪除帳本紀錄。將較舊資料備份還原並重播後，再查測試值應已清除。

從試辦到正式使用

架構文件記載，租戶、用途、自訂型別、AI 政策、獨立 Key Broker 與用量匯出已部署到測試環境。正式導入仍須完成企業身分整合、金鑰服務高可用、資料庫傳輸加密、告警、災備演練與獨立安全測試。

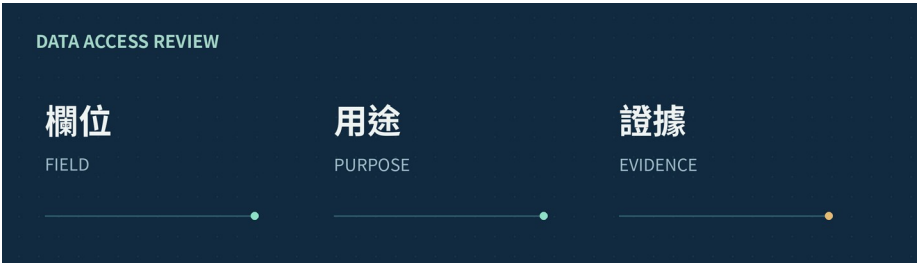
需明列於專案範圍

架構 v3 將文件與大型物件保護、DXI 揭露頁、驗證碼代產生與租戶稽核匯出列為待開發。硬體遠端驗證尚待落地，要求真實驗證的型別在正式設定下會拒絕釋出。

導入討論 / FIRST WORKSHOP

下一次討論，帶一張表單。

選一張員工、供應商或會員實際填寫的表單。用以下三個問題，決定第一個試辦欄位與驗收方式。



01 欄位

哪一欄最容易被抄進信箱、聊天訊息或試算表？原值目前出現在哪幾個位置？

02 用途

哪些人只需知道資料已交齊？哪些人在什麼條件下才應看見原值？由誰核准？

03 證據

用哪一張遮罩畫面、一筆拒絕紀錄及一次還原演練，證明流程符合預期？

NSECURED / MemberGo

企業客戶與合作夥伴版 • 2026 年 11 月 22 日

架構依據：《MemberGo 資料保護架構 v3》（2026 年 11 月 19 日更新，測試部署紀錄截至 11 月 15 日）。實際交付項目以導入版本與雙方驗收範圍為準。