

資安是智生活產品開發與治理的最高準則
守護用戶資料與隱私，是我們最重要、也最不可退讓的責任



針對近期媒體報導及消基會公布之資安檢測結果，智生活已啟動跨部門資安專案小組，依指稱項目進行逐條重現、盤點與風險評估，並同步加嚴高風險路徑控管與監測，對於外界疑慮，我們不找藉口——無論是版本不同或測試條件差異，保護資料安全就是我們的責任，為此提出具體修補與可驗證結果對外負責。

目前我們已啟動「雙重第三方驗證」機制，針對修補後版本進行獨立複測與交叉驗證；後續將依驗證進度分階段公布盤點進度、修補完成狀態與驗證摘要，讓外界以事實檢視我們的處置成效。以下為針對消基會指稱項目的最新處理進度報告：

最新處理進度報告(更新時間2026/02/14 12:00)

	消基會指稱不合格項目	目前狀態	資安強化行動(持續進行)	檢測項目編號
New!	行動應用程式應避免在 IPC 機制中洩漏敏感性資料	☑ 第三方驗證通過	【2026/02/14】通過第三方複驗，項目無資安疑慮 1.驗證結果：2026/02/13 18:44 已通過第三方驗證 2.智生活將在後續更新版本，持續強化資安防範	4.1.2.3.12.
New!	行動應用程式應於使用交易資源時進行使用者身分鑑別	☑ 第三方驗證通過		4.1.3.2.1.
New!	行動應用程式交談識別碼規則性	☑ 第三方驗證通過		4.1.4.2.1.
New!	敏感性資料應避免出現於行動應用程式之程式碼	● 已完成修正 待第三方驗證後上線	【2026/02/14】完成修正並送交平台上架審核 1.查證結果：報告提到的 API Key 為研發測試用參數 2.是否影響用戶？不會，報告提到的 API Key 為研發測試用參數僅存在公司內部封閉測試環境，未用於正式 App/正式系統 3.安全控管：權限嚴格限縮並留存稽核紀錄，避免誤用或外流 4.後續措施：已完成測試參數盤點與加嚴管理，管理制度會持續清理非必要測試設定	4.1.2.3.8.
New!	行動應用程式應於交易收款時主動通知使用者	● 已完成修正 待第三方檢驗	【2026/02/14】已完成版本更新，並部署至正式線上環境 1.已優化「付款成功即時提示」功能，付款完成當下即顯示成功提示 2.已強化「訂單明細查詢」功能，交易完成後可立即查看訂單資訊 3.目的：確保消費者即時掌握交易狀態與明細，提高資訊透明度與可追溯性	4.1.3.1.3.
New!	行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中	● 已完成修正 待第三方驗證後上線	1.盤點結果：經全面盤點，確認部分早期導入之輔助模組在「資料暫存管理」上仍有可再強化之處 2.已完成改善：相關套件已升級至新版，並同步調整裝置端資料儲存與清除邏輯，提升敏感資料保護強度、降低潛在風險 3.驗證現況：既既有資安監控與檢測紀錄，目前未發現敏感資訊外洩情形 4.後續驗證：已依複審建議完成優化，並啟動進一步驗證程序，包含委託第二家第三方機構進行交叉檢視 5.持續強化：未來將透過版本管理與定期檢測機制，持續強化行動應用程式在資料存取與暫存	4.1.2.3.4.
New!	行動應用程式冗餘檔案或日誌檔案敏感性資料儲存限制	● 已完成修正 待第三方驗證後上線		4.1.2.3.5.
New!	行動應用程式敏感性資料儲存保護	● 已完成修正 待第三方驗證後上線		4.1.2.3.6.
New!	行動應用程式敏感性資料分享權限控管	● 已完成修正 待第三方驗證後上線	4.1.2.5.3.	4.1.2.5.3.
New!	行動應用程式中的使用者介面應避免洩漏敏感性資料	● 已完成修正 待第三方檢驗	【2026/02/14】已完成版本更新，並部署至正式線上環境 1.關於訂單頁面顯示姓名與電話一事 (1)設計目的：讓用戶在付款前可核對配送與聯絡資訊，保障交易確認與消費者權益 (2)必要性考量：避免因資訊遮蔽導致聯絡資料錯誤、配送失敗或後續交易爭議 (3)揭露原則：僅在最小必要範圍內顯示本次訂單所需資訊，並搭配權限與存取控管，降低不當使用風險 (4)制度與告知：導入 ISO 27701 隱私資訊管理制度時，已同步修訂《隱私權政策》，並於相關條款說明交易/配送情境下的資料使用目的與範圍，確保透明與用戶知情 2.關於支付資訊顯示一事 (1)原因說明：信用卡資訊顯示疑慮，經查係第三方金流回傳資料的遮蔽格式未即時同步，導致前端顯示未達保護標準 (2)已完成修正：已於 2026/02/12 21:00 完成 WebView 前端遮蔽機制優化 (3)修正方式：前端介面改為獨立執行遮蔽 (masking)，確保敏感財務欄位於顯示層即受保護 (4)防護效果：任何敏感財務資訊不會在使用者介面上完整呈現，降低資訊暴露風險 即使資料來源為第三方回傳，我們仍以平台端顯示層保護為責任邊界，已加嚴防護以避免類似情況再次發生	4.1.2.3.13.
New!	行動應用程式應針對螢幕覆蓋攻擊進行防護 (只適用 Android)	● 已完成修正 待第三方檢驗	【2026/02/14】已完成版本更新，並部署至正式線上環境 1.背景考量：鑒於 Android 平台存在螢幕覆蓋 (Overlay) 攻擊風險，為保障資訊安全，同時兼顧配送聯繫之即時性，針對潛在風險進行強化，避免惡意程式影響敏感操作 2.治理依據：依循 ISO 27701 與行動應用程式資安要求，已啟動 Android 端風險盤點與修正規劃 3.評估原則：採「優先防護」原則，針對涉及登入、支付、個資查閱等敏感操作情境，實施嚴格防護 4.優化方向：盡可能不影響使用便利與服務效率前提下，強化 Android 端防覆蓋保護機制，包含 (1) 敏感頁面限制被覆蓋顯示之風險 (2) 畫面被覆蓋時限制互動/阻擋誤觸並提示 (3) 完成後，執行弱點掃描與情境測試驗證 5.目標：補齊 Android 特定攻擊面之防護要求，在資訊安全合規的同時，維持物流服務	4.1.5.1.3.
New!	行動應用程式應於發布時說明欲存取之敏感性資料、資源與用途	● 已完成修正 待第三方驗證後上線	【2026/02/14】完成《隱私權政策》指引更新，並部署至正式線上環境 待第三方驗證 1.未來將持續強化資安防範，包含 (1)敏感資料：儲存前取得同意、儲存內容加密保護。 (2)交易安全：執行交易時強制身分鑑別。 (3)防護機制：具備畫面擷取 (截圖) 警示功能。 (4)系統層級：確保 Session ID 亂數規則安全、第三方函式庫引用安全。	4.1.1.1.2.
New!	行動應用程式應於蒐集敏感性資料前取得使用者同意	● 已完成修正 待第三方驗證後上線		4.1.2.1.1.
New!	行動應用程式應於儲存敏感性資料前取得使用者同意	● 已完成修正 待第三方驗證後上線		4.1.2.3.1.
New!	行動應用程式畫面擷取警示	● 已完成修正 待第三方檢驗	【2026/02/14】完成截圖阻擋頁面，[個人頁、訂單詳情、服務聯絡資訊、服務常用收件人]更新	4.1.2.3.9.
	行動應用程式函式庫引用安全	● 自檢通過 待複測結果 依專業建議進行強化	2026/2/12 送交複測 原檢測單位，與增加新的檢測單位進行複查 待複測結果	4.1.5.3.1.

資安是一項持續精進的工程，後續我們將持續推進下列工作：

- 外部稽核 × 內部監控並行：啟動「雙重公正第三方驗證」，並委請第二家公正專業機構進行交叉檢視與比對。
 - 落實國際標準：依 ISO 27701 隱私資訊管理系統，持續強化個資治理、流程控管與透明揭露。
 - 零信任思維：以最小權限、分層防護與持續監測為原則，提升高風險路徑的控管強度。
- 我們將以可驗證的改善與定期檢測機制，持續提供用戶更安全、可信賴的數位服務環境。**

備註：

- ISO 27001 資訊安全管理制度 (ISMS)：通過國際標準認證，認證機構為台灣德國萊因技術監護顧問股份有限公司 (TÜV Rheinland)。
- ISO 27701 隱私資訊管理制度 (PIMS)：通過國際標準認證，認證機構為台灣德國萊因技術監護顧問股份有限公司 (TÜV Rheinland)。
- 支付安全合規：信用卡交易全程經由符合 PCI DSS 最高合規標準之第三方金流服務商 TapPay 進行技術串接，並由聯合信用卡處理中心 (NCCC) 執行收單作業，確保交易環境安全無虞。