

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2026/02/13)			
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
敏感性資料應避免出現於行動應用程式之程式碼	改版上線 待第三方驗證	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;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.
行動應用程式應於交易收款時主動通知使用者	改版上線 待第三方驗證	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.
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:依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管理上的安全性	4.1.2.3.4.
行動應用程式冗餘檔案或日誌檔案敏感性資料儲存限制			4.1.2.3.5.
行動應用程式敏感性資料分享權限控管			4.1.2.5.3.
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 待第三方驗證後上線	1.關於訂單頁面之姓名與電話顯示 (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.關於支付資訊顯示之優化 (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, 導致前端顯示未達我們的保護標準 (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.
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 待第三方驗證後上線	1.背景考量:物流配送需即時聯繫, 避免因資訊不足影響配送與服務流程 2.治理依據:依循 ISO 27701 個資保護管理架構, 已 啟動全面盤點與風險評估 3.評估原則:針對涉及個人資料顯示之情境, 採「最小必要揭露」原則進行審慎檢視與優化 4.優化方向:在不影響使用便利與服務效率前提下, 強化以下功能 (1)部分遮蔽(降低直接暴露) (2)必要時點擊顯示(控制可見範圍) (3)告知機制(提升透明度與用 戶知情) 5.目標:在服務效率與資訊安全之間取得合理平衡。	4.1.5.1.3.
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	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	4.1.1.1.2.
行動應用程式應於蒐集敏感性資料前取得使用者同意			4.1.2.1.1.
行動應用程式應於儲存敏感性資料前取得使用者同意			4.1.2.3.1.
行動應用程式敏感性資料儲存保護			4.1.2.3.6.
行動應用程式畫面擷取警示			4.1.2.3.9.
行動應用程式應避免在 IPC 機制中洩漏敏感性資料			4.1.2.3.12.
行動應用程式應於使用交易資源時進行使用者身分鑑別			4.1.3.2.1.
行動應用程式交談識別碼規則性			4.1.4.2.1.
行動應用程式函式庫引用安全			4.1.5.3.1.