// 電商老闆必知的資安小講座 · 會後資料 · 題目整理自企業客戶實際寄給 SaaS 廠商的資安問卷

平台資安詢問表

給品牌方：簽約或續約前，把這份表寄給開店平台、金流、物流、寄信、客服與廣告代操廠商，請對方逐題書面回覆。回覆內容納入合約附件，就是你依個資法「監督受託者」的證據。

怎麼用這份表

STEP 1
列出所有拿著客人資料的廠商：平台、金流、物流、寄信、客服、代操。

STEP 2
每家寄一份，附上本表最後的詢問信，請對方填「平台回覆」欄。

STEP 3
對照「合格答案」欄與「判讀回覆」的紅旗，答不清楚的追問到具體為止。

STEP 4
回覆寫進合約附件；每年續約時再問一次，合約結束要求刪除資料。

受詢廠商

廠商名稱		**服務項目**	
回覆人／職稱		**回覆日期**	

詢問項目

#	問題	合格答案長這樣	平台回覆
一、出事時：通知與協助（必問）			
1	**個資外洩時，知悉後幾天內通知我們？**	一個具體天數，例如「24 小時內」。不是「第一時間」。品牌自己要在 72 小時內通報。	
2	**是否提供鑑識報告？**	外洩的欄位、筆數、時間區間，以及入侵途徑。	
3	**出事時怎麼分責、提供哪些協助？**	顧客通知範本、協助撰寫主管機關報告、窗口與時程、賠償上限。	
4	**過去 3 年發生過資安事件嗎？怎麼處理的？**	據實說明；有事件就附公告或處理摘要與改善措施。「從來沒有」也要書面寫下。	
二、資料在哪、誰碰得到（必問）			
5	**我們客人的資料放在哪？**	哪個雲端服務、哪個國家；備份放哪。最好附一張資料流向圖。	
6	**平台人員能看到我們客人的資料嗎？能替我們重設密碼、改權限嗎？** 含員工、外包、第三方工具	列出哪些角色可以看、看得到哪些範圍、能做哪些操作；需經授權才能存取，且每次存取都有紀錄。	

7	**我們的資料和其他店家分開存放嗎？**	每家店的資料有邏輯或實體隔離，查詢一律限定在自己的範圍。	
8	**我們可以稽核，或取得第三方驗證報告嗎？**	稽核權，或每年提供 ISO 27001 證書，且「適用範圍」涵蓋我們用的服務。	
三、AI 與遠端連線			
9	**我們的資料會被拿去訓練 AI 嗎？會送到第三方 AI 服務嗎？**	書面承諾不用於模型訓練；列出用到哪些 AI 服務、用途與處理地區。	
10	**用我們資料調整過的 AI 模型，會給其他公司用嗎？AI 產出內容歸誰？**	模型只用於服務我們；資料與 AI 產出內容的所有權、使用範圍寫進合約。	
11	**你們會遠端連進我們的電腦或系統嗎？**	標準服務不需要。若需要，說明連線方式、事先取得我方同意、可存取範圍與紀錄，用完即關閉。	
四、後台帳號與紀錄			
12	**後台能強制所有管理者開兩步驟驗證嗎？**	可以強制；支援驗證器 App、Passkey 或公司 SSO，不只簡訊。	
13	**密碼規則與登入防護是什麼？**	有最低長度與複雜度、連續輸錯會鎖定、可限制登入 IP 或地區。	
14	**能一人一帳號、依角色限權嗎？離職停用會立即生效嗎？**	可以；客服只能查單、不能匯出。停用後立即無法登入，並留下紀錄。	
15	**登入、匯出、帳號與權限異動的紀錄，我們查得到嗎？保存多久？**	含操作者、時間、IP；平台人員的操作也要記。至少保存 1 年，使用者無法竄改。	
16	**紀錄有人在監控嗎？大量匯出、異地登入會告警嗎？**	有 24 小時監控（自建或委外 SOC），異常會通知到我們指定的 Email 或手機。	
17	**API 金鑰能限權限、設期限、設呼叫頻率上限嗎？**	可以設唯讀、到期日與頻率上限，並能隨時撤銷。	
五、系統防護			
18	**資料傳輸與儲存有加密嗎？**	傳輸強制 HTTPS（TLS 1.2 以上）；資料庫與備份靜態加密；密碼與金鑰另外加密保存。	
19	**有哪些對外防護？**	網頁應用防火牆（WAF）、DDoS 防護、入侵偵測／防禦、暴力破解偵測與阻擋。	

20	**多久做一次弱點掃描與滲透測試？由誰做？**	至少每季弱點掃描、每年第三方滲透測試，可提供結果摘要。	
21	**發現重大漏洞，多久內修補？**	具體天數，例如高風險 30 天內；持續追蹤公開的「已遭利用漏洞」清單。	
22	**維運人員的電腦怎麼管？外包維運有簽保密協議嗎？**	公司配發、裝防毒與裝置管理（MDM），遺失可遠端清除、不在本機存客戶資料；外包須簽保密協議並遵守同樣規範。	
六、備份與持續營運			
23	**多久備份一次？有異地備份嗎？保留多久？**	每日備份、異地加密保存（3-2-1 原則），可還原到指定時間點；只有特定人員能存取備份。	
24	**系統掛掉多久能恢復？最多會遺失多少資料？有演練嗎？**	具體小時數（RTO／RPO），每年實際演練一次並有結果紀錄。	
25	**服務可用率保證多少？沒達到怎麼補償？**	SLA 寫明可用率、事故回應時限與補償方式。	
七、寄信、資料保存與退場			
26	**代寄的通知信能用我們的網域，並通過 SPF／DKIM／DMARC 嗎？**	可以，並提供 DNS 設定說明。	
27	**訂單與會員資料保存多久？能設定到期自動刪除嗎？**	有明確保存期限，品牌可設定或要求刪除。	
28	**我們能自己匯出全部資料嗎？要額外收費嗎？**	隨時可自行匯出，標準格式（如 CSV、Excel），不額外收費、不限量。	
29	**合約結束後，資料怎麼刪除？**	說明刪除範圍（含備份）與時程，並提供刪除證明。	

判讀回覆

紅旗：要追問或考慮換廠商

- 「第一時間通知」「盡快處理」：沒有天數
- 「我們很安全」「符合業界標準」：沒有具體做法
- 「機密，無法提供」：連證書與適用範圍都不給
- ISO 證書的適用範圍不包含你用的服務
- 平台人員不需授權就能看全部資料，也沒有紀錄
- 後台沒有紀錄可查，或只能請客服代查
- AI 用途說不清楚，不肯書面承諾不拿資料訓練
- 有備份但從沒做過還原演練

合格：可以寫進合約

- 每一題都有數字、名單或文件
- 願意把回覆列為合約附件
- 提供事件聯絡窗口與 24 小時聯絡方式
- 每年主動更新證書與子處理者清單
- 弱點掃描、演練有日期和結果，不只是「有在做」

詢問信範本（把【】換成你的資料）

主旨：【品牌名稱】資安與個資保護事項詢問（簽約／續約前確認）

【廠商名稱】您好：

我們是【品牌名稱】，目前使用貴公司的【服務名稱】。依個人資料保護法，我們須監督受託處理個人資料的廠商，因此附上「平台資安詢問表」，請貴公司逐題以書面回覆。回覆內容將列為合約附件，並於每年續約時更新。

其中第 1 至 8 題為必答項目；若有無法提供的項目，也請說明原因與替代做法。如貴公司已有資安白皮書、架構圖、ISO 證書或弱點掃描摘要，也歡迎一併提供。

煩請於【日期】前回覆，謝謝。

【姓名／職稱／公司／聯絡方式】