個人資料委託處理契約

Data Processing Agreement (DPA)

好記 Hoki AI 輔助諮商紀錄系統

甲方（委託人）： _ _ _ _ _ _ _ _ _ _ _ _（以下簡稱「甲方」）

乙方（受託處理者）：張益善（好記 Hoki 系統開發營運者）（以下簡稱「乙方」）

甲方因使用乙方開發之「好記 Hoki」AI 輔助諮商紀錄系統（以下簡稱「本系統」），涉及個人資料之處理，雙方依據《個人資料保護法》第 4 條及相關規定，訂定本契約。

第一條　委託處理之目的與範圍

1. 甲方委託乙方透過本系統處理之個人資料，僅限於協助甲方產生諮商紀錄所必要之資料處理。
2. 委託處理範圍包括：
   - 諮商錄音之語音轉文字處理
   - 逐字稿之去識別化處理
   - 去識別化後之諮商紀錄生成
   - 去識別化後之諮商紀錄儲存與管理
3. 乙方不得將甲方委託處理之個人資料用於本條第一項所定目的以外之用途。

第二條　處理之個人資料類別

資料類別	處理方式	保存期間
諮商錄音（含案主聲紋）	經客戶端加密上傳後，於台灣專屬伺服器記憶體中解密處理，轉錄完成後立即銷毀	處理完成後即刪除（不保存）
諮商逐字稿	僅暫存於伺服器記憶體	當次操作結束後即消失（不保存）
去識別化諮商紀錄	經雙層去識別化後加密儲存	2 天（系統自動刪除，輔助筆記不長期保存）
使用者帳號資料	加密儲存（密碼 bcrypt 雜湊）	帳號存續期間
系統稽核紀錄	自動記錄，加密儲存	365 天

第三條　資料處理之技術架構

1. **客戶端加密**：音訊於使用者瀏覽器端以 AES-256-GCM 對稱加密，AES 金鑰再以 RSA-4096 公鑰包裝後上傳，傳輸中間節點無法解密。
2. **境內處理原則**：本系統所有 AI 模型（語音辨識、大型語言模型）皆自主部署於台灣境內之專屬伺服器，不呼叫任何外部 AI API（如 OpenAI、Google Gemini 等），諮商相關資料不離開台灣境內。
3. **去識別化機制**：系統採用 AI 語意辨識與正規表達式雙層去識別化處理，自動移除姓名、地點、電話、電子郵件等可辨識個人身分之資訊。
4. **記憶體處理原則**：原始錄音僅於伺服器記憶體中處理（tmpfs），不寫入永久儲存；逐字稿亦僅暫存於記憶體，處理完成後立即銷毀。

> 本系統架構使乙方在正常運作情況下，不會接觸或持有案主之可辨識個人資料。乙方僅負責系統之開發、部署與技術維護。

第四條　安全措施

乙方應就本系統採取以下安全措施：

1. **存取控制**：二層角色權限管理（系統管理員 / 心理師），所有 API 端點皆驗證使用者身分與權限。系統管理員僅具帳號管理、稽核紀錄查閱及資料庫備份等系統維護權限，不可存取個案之諮商紀錄內容或原始錄音。
2. **傳輸加密**：使用者與伺服器間之所有通訊採 HTTPS/TLS 加密。
3. **儲存加密**：資料庫採用 SQLCipher 256 位元 AES 加密，加密金鑰以雲端密鑰管理服務（Google Cloud Secret Manager）管理，不寫入程式碼或設定檔。
4. **密碼安全**：使用者密碼以 bcrypt 雜湊加密儲存，不保留明文。
5. **閒置登出**：使用者閒置超過 15 分鐘自動登出，防止未授權存取。
6. **稽核軌跡**：系統自動記錄所有重要操作事件，含事件類型、使用者、時間戳及 IP 位址。
7. **資料備份**：提供加密資料庫備份功能，備份自動排除諮商紀錄（系統自動移除諮商紀錄內容後方進行備份），僅保留系統管理資料，備份檔案保持 SQLCipher 加密狀態。
8. **客戶端加密**：音訊於瀏覽器端以 AES-256-GCM + RSA-4096 混合加密後上傳，傳輸中間節點無法解密。
9. **資料殘留防護**：記憶體暫存空間暫存、關閉 swap、停用 core dump、AI 模型處理完即釋放。
10. **數位浮水印**：匯出文件內嵌隱藏浮水印（使用者、時間戳），供事後追溯。

第五條　乙方之義務

1. 乙方應依甲方之指示處理個人資料，不得逾越委託範圍。
2. 乙方應對所知悉之個人資料負保密義務，非經甲方書面同意或法令規定，不得向第三人揭露。
3. 乙方應確保其人員（包括員工、承攬人）亦受保密義務約束。
4. 乙方應定期檢視並更新系統安全措施，以因應資安威脅之變化。
5. 乙方應於知悉個人資料安全事故後，於 24 小時內通知甲方，並提供事故之初步評估及補救措施。
6. 乙方應配合甲方或主管機關進行個人資料保護之稽核或查核。
7. 非經甲方書面同意，乙方不得將委託處理之個人資料再委託第三方處理。如經甲方同意再委託，乙方應確保子處理者承擔與本契約同等之資料保護義務，並對子處理者之行為負連帶責任。

第六條　甲方之義務

1. 甲方應依《個人資料保護法》之規定，確保已合法蒐集案主之個人資料，並取得案主使用本系統之知情同意。
2. 甲方應妥善管理其使用者帳號，確保帳號密碼不被非授權人員使用。
3. 甲方應指定聯絡人（個人使用者即為甲方本人）負責與乙方聯繫個人資料保護相關事宜。
4. 甲方若為機構，應確保其所屬心理師知悉本系統之使用規範及個人資料保護義務。

第七條　當事人權利之處理

1. 案主依《個人資料保護法》第三條行使查詢、閱覽、複製、更正、停止處理或刪除等權利時，應透過甲方提出申請。
2. 甲方接獲案主之申請後，乙方應於合理期間內配合甲方完成相關處理。
3. 使用者（心理師）得透過系統功能自行行使其個人資料權利。

第八條　契約終止與資料處理

1. 本契約因下列事由之一終止：
   - 雙方合意終止
   - 任一方提前 30 日書面通知他方
   - 一方重大違約，經他方書面催告 15 日內未改善
2. 契約終止時，乙方應依甲方指示：
   - 將甲方之資料匯出交還甲方；或
   - 刪除甲方之所有資料，並提供刪除證明
3. 法令要求保存之資料，不在前項刪除範圍，但乙方仍應依本契約之安全措施保護之。

第九條　損害賠償

1. 因可歸責於乙方之事由，致甲方或案主之個人資料遭不法蒐集、處理、利用或其他侵害時，乙方應負損害賠償責任。
2. 乙方之賠償責任以甲方實際已支付之服務費用總額為上限，但因故意或重大過失所致者，不在此限。

第十條　契約期間與修訂

1. 本契約自雙方簽署之日起生效，有效期間為一年，屆滿前 30 日任一方未以書面通知終止者，自動續約一年。
2. 本契約之修訂應經雙方書面合意。
3. 本契約如有未盡事宜，依《個人資料保護法》及相關法規辦理。

第十一條　管轄法院

本契約之準據法為中華民國法律。因本契約所生之爭議，雙方同意以臺灣臺北地方法院為第一審管轄法院。

本契約一式二份，由甲乙雙方各執一份為憑。

甲方（委託人）	**乙方（受託處理者）**
姓名 / 機構名稱：	姓名：張益善（好記 Hoki 系統開發營運者）
負責人（機構適用）：	系統名稱：好記 Hoki
聯絡人：	電子郵件：hokinote.service@gmail.com
聯絡電話：	地址：
地址：	簽章：
簽章：	

簽約日期：中華民國　　年　　月　　日

本契約依《個人資料保護法》第 4 條、第 27 條及《個人資料保護法施行細則》第 8 條之規定訂定