SAMSUNG

築起隱私安全堡壘：一窺安全、個人化 Galaxy AI 體驗背後隱藏的科技

結合 Personal Data Intelligence 和 Knox Enhanced Encrypted Protection 雙重安全機制

縝密分析並保護用戶數據 重新定義AI 安全真諦

AI 擁有無限潛力，但唯有結合使用者的投入，方能充分釋放潛力。當 AI 能理解使用者偏好與日常作息，其所打造的行動體驗，便能宛如日常生活的自然延伸。

Galaxy AI 擁有直覺且能感知情境脈絡的特性，實現更貼近人心的個人化體驗，他讓人們手中的智慧型手機不再只是工具，而是能預測需求並提出完善建議的智慧夥伴，讓生活事半功倍、創意無限且緊密互聯。

為成就極致的個人化體驗，存取特定數據是不可或缺的一環。唯有如此，AI 才能真切理解用戶，做出真正貼近生活且有實質幫助的回應。置身 AI 新紀元，三星秉持對用戶資料隱私的高度重視，持續創新強化保護機制，避免個資落入不肖人士手中。

Personal Data Intelligence 實現個人化體驗

三星精心打造的 Personal Data Intelligence（PDE）[註一]，是實現安全且高度個人化體驗的關鍵。隨著 Galaxy S25 系列登場而首次亮相的 PDE，為生活帶來翻天覆地的改變，實現 Galaxy 迄今最卓越的 AI 體驗。它隱身於後台靜默地運作，學習用戶的習慣與偏好，帶來真正個人化且獨特的體驗。

無論是 Now Brief[註二] 透過貼心的個人動態助力使用者掌握一天行程，或藉由自然的口語指令，從媒體瀏覽器的大量檔案中，找到心心念念的照片，在 Galaxy AI 的強力應援下，由 AI 驅動的每一個動作，皆猶如

行雲流水般流暢。加上 PDE 在裝置端安全的處理數據，用戶得以在隱私安全一點也不打折的情況下，盡享深度客製 AI 帶來的種種好處。

Knox Enhanced Encrypted Protection 帶來強大升級

為強化 Galaxy AI 體驗的安全性，三星精心開發 **Knox Enhanced Encrypted Protection (KEEP)**[註三]，其為裝置端的一道強大保護屏障，能在不阻礙使用體驗的情況下，守護最敏感的資料。KEEP 最初專為 PDE 而設計，而今將其他 Galaxy AI 功能納入保護傘，例如智慧回覆、Now Brief、Samsung Moments 等，它於後台安靜的運作，確保其支援的應用程式，時時刻刻安全無虞。

想像手機是一棟房子。每一個應用程式如同各有專屬的空間，彼此獨立，但共處一個屋簷下。而「**安全資料夾**」[註四]像是獨棟式客房，與主居所分處二地，有專用的通行鑰匙。此空間是保存高度隱私內容的絕佳場所，尤其當用戶欲將資料與裝置的其他部分完全隔離時。隨著諸如 PDE 等 AI 功能，開始即時處理更敏感的任務，人們對於保護力道足以因應現狀，並與日常體驗無縫接軌的資安需求亦日益強烈。

在此背景下，KEEP 應運而生。想像將房子隔出一間私人套房，雖然與主屋共處一個屋簷下，卻擁有獨立的安全出入口，唯有用戶本人能夠進出。其隱私性優於一般房間，但又不像獨棟式客房那般完全獨立。KEEP 以相同的原理運作：它為諸如 PDE 等各別的應用程式，建立各自專屬的空間，確保敏感資料受到妥善保護，同時也不影響使用者原有的操作習慣與體驗。

隨著行動體驗日益智慧化，KEEP 將嚴密守護用戶最私密的資料作為安全架構的設計核心。結合「安全資料夾」等其它工具相輔相成，為三星的多層級資料防護，築起另一道防線，針對不同的隱私需求，為用戶和服務提供合宜的安全保障。

因應 Galaxy AI 朝個人化發展，諸如 Personal Data Intelligence 和 Knox Enhanced Encrypted Protection 等機制，正為行動智慧樹立新標竿，個人化與隱私防護的關係，不再二元對立、而是相輔相成。隨著該等體驗日益智慧且更貼近需求，最敏感的資訊將原封不動地留在裝置端，有其專屬的安全歸宿，令用戶備感安心。

註一：Personal Data Engine 僅可於開啟 Personal Data Intelligence 選單時使用。Personal Data Intelligence 關閉後，先前分析的資料將立即刪除。

註二：Now Brief 功能需登入三星帳號方可使用。服務的可用性，可能因市場、語言、裝置型號、應用程式而異。部分功能需連接網路。

註三：適用於搭載 One UI 8 或更新版本的 Galaxy 智慧型手機與平板。

註四：「安全資料夾」為手機或平板用戶提供一個安全的獨立空間，用以儲存敏感的應用程式和數據。用戶可在當中建立新資料夾，將應用程式複製至此處。用戶可自訂資料夾內的應用程式，並設定鎖定類型，包括 PIN 碼、圖形、密碼和指紋。為提升安全性，用戶另可選擇隱藏和加密安全資料夾，為資料提供進階防護，遠離網路安全威脅。處於隱藏狀態時，應用程式將停止運作，以確保資料安全性。一旦重啟，加密機制隨之解除，應用程式恢復正常運作。