Lark 隱私白皮書

目錄

前言 3

1. 個人資料處理的基本原則 4

2. Lark 的隱私保護管理系統 5

2.1 隱私保護組織與人員 5

合規團隊 5

合規宣導與培訓計畫 5

2.2 個人資料處理的生命週期管理 5

資料收集 5

資料使用 6

資料共享 6

資料保存與銷毀 6

2.3 資料主體權利的保護 6

2.4 資料駐留與跨境傳輸管理 6

2.5 隱私風險管理 7

隱私影響評估 (PIA) 7

安全合規風險掃描 7

2.6 資料外洩事件的應對 8

2.7 資料安全 8

3. Lark 的安全與隱私合規認證 9

結語 13

版本變更紀錄 14

前言

Lark Technologies Pte. Ltd（以下稱為「Lark」）提供新一代企業辦公服務：Lark 辦公平台，「行動友好、即時協作與統一存取」，幫助企業提升工作效率並降低生產及管理成本。

Lark 辦公平台提供強大的辦公協作服務，包括但不限於即時通訊、雲端文件、雲端儲存、智慧行事曆、音視頻會議、開放平台、信箱、OKR、審批等，均具有高度的擴展性與可用性。

Lark 非常重視客戶資料安全及保護客戶用戶的隱私。在產品設計和開發過程中，Lark 堅持「以隱私為設計核心」和「預設隱私」的理念，致力於為客戶提供透明、可信賴、安全、可靠、高效且協作的辦公體驗。

注意：為方便起見，本文件中所指的「客戶」係指經由授權之自然人註冊帳戶於 Lark，並建立組織架構及享有管理權利的法人或其他組織；「使用者」則指經客戶授權或邀請加入客戶於 Lark 建立之組織架構並使用服務的自然人，包括團隊建立者及管理者。

我們希望藉由這份白皮書，與您分享 Lark 在此領域的基本原則及隱私管理實踐。

1. 個人資料處理的基本原則

Lark 已根據適用的法律法規確定其個人資料處理的基本原則，並透過適當的管理與技術措施確保在處理個人資料時遵循以下基本原則：

· 合法性、正當性與透明性：個人資料應以合法、公平及透明的方式進行處理。

· 目的限制：個人資料應僅為特定、明確的目的進行處理，且不得以與該目的不相符的方式進行進一步處理。

· 資料最小化：個人資料應適足、相關且限於為達處理目的所必要的範圍。

· 準確性：個人資料應保持準確並在必要時進行更新。將採取合理措施，根據資料處理目的及時刪除或更正不準確的個人資料。

· 儲存限制：個人資料不應儲存超過為達成資料處理目的所必要的期限。

· 完整性與機密性：個人資料的處理應以確保個人資料適當安全為前提，防止未經授權的存取或修改個人資料，並避免個人資料的損壞或遺失，採用適當的技術及組織措施。

· 問責制：必須維護與數據處理和隱私控制相關的記錄，以便在必要時證明符合上述原則。

2. Lark 的隱私保護管理系統

2.1 隱私保護組織與人員

合規團隊

Lark設有專門的合規團隊，該團隊與在其業務所在國家和地區的多個法律、安全及其他團隊協同合作，為包括隱私保護在內的各種合規實踐提供專業支持。其職責包括但不限於建立、運行和優化數據合規管理系統，以及開發基於產品的數據合規能力和解決方案等。Lark將確保我們的產品本身符合全球有關數據合規的法律法規要求，並為客戶提供更完善的合規功能和服務。

合規宣傳與培訓計劃

Lark 透過各種形式，為所有人員定期進行合規培訓與宣導，包括根據全球法律法規對數據合規的要求所設計的一般知識培訓課程，以及針對關鍵崗位員工的專項培訓課程，以提升全體人員對數據保護的意識並降低合規風險。

2.2 個人資料處理的生命週期管理

資料收集

Lark 嚴格遵守合法性、正當性、透明性及資料最小化原則，以適當的方式和頻率蒐集提供服務所必要的個人資料。在蒐集個人資料前，我們會在《隱私權政策》中揭露所蒐集的個人資料類型、蒐集目的及方法，並依照適用法律法規取得用戶同意。同時，Lark 也提供多項隱私設定功能，使用者可隨時透過隱私設定或聯繫 Lark 團隊撤回先前授予的同意。

資料使用

Lark 嚴格遵守目的限制原則，並且僅會將所蒐集的個人資料用於客戶及用戶授權的使用目的。預設情況下，Lark 員工無法存取上述個人資料，且所有員工的操作均受到嚴格限制和審核。

資料分享

Lark 處理的個人資料僅依據我們的 PrivacyPolicy 進行公開。在 Lark 需要與第三方分享個人資料的情況下，Lark 嚴格審核第三方在資料安全合規方面的能力與資格，並盡合理努力要求第三方依照其高標準來保護資料。

資料保存與銷毀

我們將保留您的個人資料達到隱私政策中所述的用途所需時間，除非法律要求更長的保留期限，例如為了遵守法律義務或請求，或為了建立、行使或辯護法律索賠，或出於合法商業目的，或依法規定。

2.3 個人資料主體權利的保護

Lark 允許用戶向客戶提交數據主體權利請求。若情況需要 Lark 協調，客戶可透過相應的客戶成功經理聯繫 Lark 尋求協助。

Lark設有專門的合規團隊，負責上述渠道的管理和運營，以回應資料主體權利的請求，並確保回應符合相關的合規要求。

2.4 數據駐留與跨境傳輸管理

Lark 已建立多個數據中心節點以支援與客戶自身數據駐留相關的合規要求。以下表格提供有關數據中心位置及供應商的資訊。

國家	供應商
新加坡	Amazon Web Services
日本	Amazon Web Services
美利堅合眾國	Amazon Web Services

涉及 Lark 本身跨境傳輸個人資料的情況，將接受嚴格的法律與安全合規評估。我們依據允許的法律依據和例外情況，並將遵守適用法律中關於此類傳輸的相關要求。同時，Lark 也會採取適當的管理和技術措施，以確保資料傳輸的安全。

2.5 隱私風險管理

隱私影響評估 (PIA)

Lark 一直廣泛落實「以隱私為設計基礎」和「以隱私為預設」的理念，將隱私保護的基本原則貫穿於產品需求的設計、開發與運營過程中。對於涉及個人資料處理的業務功能或場景，應進行隱私影響評估，以評估所涉及的個人資料類型、處理的目的與方式，以及可能對資料主體權益造成的影響。對於識別出的中高風險項目，應依照既定的風險緩解措施進行相應的風險整改，以降低隱私風險。

應依據既定的風險緩解措施進行相應的風險整改，以降低隱私風險。

風險掃描以符合安全規範

在每個 Lark 應用版本發佈前後，將進行嚴格的風險掃描以符合安全合規性，及時識別並處理相關風險項目，確保客戶資料與隱私的安全。

在應用程式版本發布之前，將對應用程式進行靜態程式碼掃描。版本發布後，將定期對每個產品模組進行安全合規風險測試。針對各類識別出的中高風險安全漏洞、隱私合規問題等，將在限定時間內進行修復和整改。

2.6 對資料外洩事件的回應

Lark 已建立完善的信息安全管理及內部控制相關系統與流程，並採用身份識別與存取管理、資料加密、去識別化、安全合規掃描、滲透測試、安全資訊與事件管理平台（SIEM）等技術手段與工具，以防範潛在的安全事件。

如發生資料外洩事件，資訊安全與合規團隊將立即並妥善依相關事件管理流程及應變計畫處理該事件，並依適用法律法規及時向監管機構報告，通知可能受影響的客戶、使用者或相關方。此外，事件處理完畢後，將進行審查與總結，並採取相關改進措施以防止類似事件再次發生。

2.7 資料安全

Lark 非常重視客戶的數據安全，並始終秉持「您的數據由您掌控」的合規理念，通過多種管理和技術手段確保數據安全。

在控制流程方面，已建立高標準的分層分類與加密系統，並進行大規模數據標記，以確保上述系統的有效實施。在技術手段方面，採用了先進的加密技術，可用於伺服器端加密及端對端加密。在金鑰管理方面，獨立的 Bring Your Own Key (BYOK) 服務隨時可用。

如需更多有關資料安全措施的資訊，請參考 Lark Trust Center。

3. Lark 的安全與隱私合規認證

Lark 已獲得多項國際認可的安全與隱私合規證書，這充分證明了我們對安全合規與隱私保護的長期承諾。

ISO 27001 資訊安全管理系統

ISO 27001在資訊安全管理領域被業界廣泛認可為國際權威認證。此認證表示Lark已經與該領域的國際標準接軌，並符合此認證所要求的安全標準。

ISO 27701 隱私資訊管理系統

ISO 27701 是隱私保護領域的國際權威認證。它是在資訊安全管理系統的基礎上，將隱私保護實踐納入考量。此認證表明 Lark 已符合本認證所要求的隱私保護標準。

ISO 27018 公有雲個人資訊保護管理系統

ISO 27018 是一項專注於雲端個人資訊保護的國際認證。此認證表示 Lark 已達到國際標準， 在雲端資料安全與個人資訊保護方面具備相應水準。

ISO 27017 雲端安全管理系統

ISO 27017 是一項國際認證，專注於雲端服務資訊安全管理領域。此認證表示 Lark 在雲端安全控管的機制與實施方面已達到國際標準。

ISO 42001 人工智慧管理系統

一項國際標準，提供建立、實施及持續改進人工智慧管理系統（AIMS）的要求，確保組織內人工智慧的負責任、透明及良好治理的發展與使用。

SOC 2（類型II）及 SOC 3

SOC（系統與組織控制）報告是一份關於組織內部控制的保證報告，由獨立第三方在根據美國註冊會計師協會（AICPA）建立的保證標準進行評估後發布。SOC 2（Type II）和SOC3報告表明Lark在系統和內部控制方面符合SOC標準要求的安全性、可用性、機密性和隱私原則。

資料保障信任標章 (DPTM)

DPTM 是一項由新加坡資訊通信媒體發展管理局（IMDA）頒發的數據保護信任標章，用以認證具備數據保護措施的公司，展示其數據合規做法符合新加坡個人資料保護法（PDPA）。此認證表明 Lark 已達到該認證所要求的個人資料保護標準。

全球 CBPR

全球 CBPR 系統的開發旨在提供一個簡單且透明的系統，供組織用於保護跨司法管轄區流動的個人資訊。全球 CBPR 系統連結全球 CBPR 論壇成員之間不同的國家隱私法，降低全球貿易資訊流通的障礙。

全球CBPR系統為組織提供了一種轉移的方式

跨司法管轄區以一種讓消費者信任其個人資訊受到保護的方式處理個人資訊。全球 CBPR 系統允許企業透過展示企業對國際認可的資料保護和隱私標準的遵守情況，來彰顯其對消費者隱私的承諾。此認證表明 Lark 已符合此認證要求的個人資料保護標準。

全球 PRP

全球PRP系統是專為設計的
協助資料處理者證明
資料處理者的能力
個人資訊的處理與
確保處理維持在最低限度
與控制器適用的一致
處理的要求
全球CBPR系統。

此認證表示 Lark 已符合此認證所要求的隱私保護標準。

EU-U.S. DPF、美國英國延展及瑞士美國DPF

EU-美國資料保護框架（DPF）、英國對EU-美國資料保護框架的延伸以及瑞士-美國資料保護框架分別由美國商務部與歐洲委員會、英國政府及瑞士聯邦行政機構共同制定，旨在為美國組織提供可靠的個人資料從歐盟、英國及瑞士轉移至美國的機制，同時確保符合歐盟、英國及瑞士法律的一致資料保護。

TrustArc GDPR 驗證

TrustArc GDPR 驗證是由 TrustArc 針對 44 項 GDPR 隱私計劃管理驗證要求（「驗證要求」）所進行的評估，這些要求包含 TrustArc GDPR 隱私計劃管理合規性驗證。這些驗證要求著重於計劃層級的措施，用以證明 Lark 所進行的個人資料處理符合歐盟一般資料保護條例（GDPR）。

結論

Lark 尊重其客戶的全球 IT 策略和國際發展需求，願意進行長期投資，並基於充分理解客戶對數據安全和隱私保護的需求，通過各種安全合規解決方案為客戶提供相關能力，幫助他們應對開放且複雜的網絡環境所帶來的安全挑戰，以及日益嚴格的全球數據合規和隱私保護要求，並且願意在安全合規領域展開更深入的合作。

版本變更記錄

日期	版本	備註
2023年1月1日	V1.0	初始版本
2024年6月11日	V2.0	新增歐盟-美國 DPF、英國延期及瑞士-美國雙重納稅協定(DFP)
2025年6月18日	V3.0	新增 TrustArc GDPR 驗證 取代APEC CBPR與PRP與 Global CBPR & PRP
2026年3月24日	V3.1	新增 ISO 42001