Privacy Policy

Updated August，2026 v2

1. Introduction

Thank you for choosing the ULinkOne Platform (the “Platform”) operated by Dena Investment Limited (operating as “Dena Trust”, hereinafter referred to as “we”, “us” or “our”).

The services made available through the Platform (the “Services”) may include technology services, payment-related services, credit facilities, card services, and other related services provided by us or our authorised financial partners.

By accessing or using the Services, you acknowledge that your Personal Data will be collected, used, stored and disclosed in accordance with this Privacy Policy. Where applicable, you represent and warrant that you have obtained the necessary consent and authority from any Relevant Person(s) for us to process their Personal Data as described herein.

This Privacy Policy describes how we collect, use, store, disclose and otherwise process your Personal Data when you access or use our Site, mobile applications, APIs, credit facilities, payment cards, banking services provided by our financial partners, and related services.

We may update this Privacy Policy from time to time by posting the amended version on the Site or notifying you by email or through other appropriate channels. Where required by applicable laws, we will provide prior notice of material changes. Your continued use of the Services after such notification constitutes acceptance of the amended Privacy Policy.

2. Our Role and Relationship with Financial Partners

2.1 Identity and Operating Model

Dena Trust operates as a technology provider, platform operator and, where applicable, program manager under agreements with regulated financial institutions and other Financial Partners.

Dena Trust does not operate as a bank, deposit-taking institution, payment institution, or other regulated financial institution unless expressly stated. We do not provide banking, deposit-taking or other regulated financial services directly.

Certain financial, banking, payment card, credit-related and other related services made available through the Platform may be provided by or through our authorized third-party financial institutions, sponsor banks, card issuers and other regulated service providers (collectively, the “Financial Partners”), including but not limited to FV Bank International Inc. and its affiliates.

Such services may be provided directly by the relevant Financial Partners or facilitated through the Platform operated by Dena Trust.

2.2 Data Controller and Processor Structure

Depending on the nature of the Services you use, Dena Trust and our Financial Partners may act as independent Data Controllers, Data Processors, or authorised service providers in relation to your Personal Data.

The allocation of responsibilities is generally as follows:

(1) Platform and Technology Services

For Personal Data collected and processed for the operation and management of the Platform, including account administration, user experience management, platform security, customer support, initial onboarding and platform risk management, Dena Trust acts as an independent Data Controller.

(2) Banking and Card Services

For banking accounts, payment cards, wire transfers, card transactions and other regulated financial services provided by Financial Partners, such Financial Partners (including FV Bank International Inc., where applicable) may act as independent Data Controllers.

Such Financial Partners are responsible for processing Personal Data in accordance with their own privacy policies and applicable regulatory obligations, including customer identification, AML/CTF compliance, transaction monitoring, fraud prevention and regulatory reporting requirements.

(3) Credit Services

For credit facilities or credit-related services provided through the Platform, Dena Trust may process Personal Data for purposes including credit assessment, credit limit determination, repayment monitoring, credit risk management and related compliance requirements.

(4) Third-Party Service Providers

Third-party service providers engaged by Dena Trust or our Financial Partners, including KYC/AML verification providers, credit risk analytics providers, cloud service providers and technical service providers, may process Personal Data as Data Processors or authorised service providers under applicable contractual arrangements and instructions.

3. What Personal Data We Collect

We may collect, process, and store Personal Data regarding you and, where applicable, your beneficial owners, directors, officers, authorized signatories, representatives, guarantors and other related individuals (collectively, the "**Relevant**

Persons”):

3.1 Identity Information

Full legal name, former names, gender, date and place of birth, nationality, residential address, passport/national ID details, tax identification numbers, contact information, email address, blockchain wallet addresses where applicable, and biometric identifiers used for identity verification.

3.2 Personal Financial Information

Total net wealth, purpose of account opening, source of wealth, source of funds, occupation/employment details, income information, tax residency information, bank account information, account statements and spending/transaction history.

3.3 Credit & Assessment Information

Credit history, credit scores, creditworthiness assessments, affordability metrics, debt obligations, repayment behavior, and internal/external credit risk assessment results.

3.4 Banking and Payment Information

Bank account details, account balance information, Virtual IBAN details where applicable, payment card details and related payment authentication information, transaction records, wire instructions, and merchant category codes.

3.5 App & Technical Telemetry Information

Device identifiers, device fingerprinting data, IP address, approximate geolocation data, mobile operating system information, push notification tokens, app crash logs, performance analytics, and browser/HTTP header data.

3.6 Sensitive Personal Information

Where required or permitted by applicable law, we may process certain categories of Sensitive Personal Data, including biometric data used for identity verification and fraud prevention, and other sensitive information required for regulatory compliance.

4. How We Use Personal Data

We process Personal Data based on applicable legal grounds, including the performance of contractual obligations, compliance with legal and regulatory requirements, protection of our legitimate interests, and consent where required by applicable law.

Category	Specific Operational Purposes
Account & Platform Services	• Verify your identity • Create and maintain your account

	• Provide customer support • Operate and improve the Platform、
Banking & Card Services	We use Personal Data to: • Facilitate account opening with Financial Partners • Support card issuance and payment transactions • Comply with banking, payment and regulatory requirements
Credit Facilities & Services	• Assess your eligibility for credit facilities • Determine credit limits • Evaluate repayment ability • Manage credit risk and collections
AML/CTF and Regulatory Compliance	• Perform customer due diligence • Conduct sanctions and PEP screening • Monitor transactions • Comply with applicable legal and regulatory requirements
Security and Fraud Prevention	• Detect and prevent fraud • Protect accounts and systems • Investigate suspicious activities • Maintain platform security

5. Sharing and Disclosure of Personal Data

We do not sell your Personal Data. However, in order to provide and maintain our integrated fintech, banking, payment and credit-related services, we may share your Personal Data with the following categories of recipients:

5.1 Financial Partners and Banking Institutions

We may share Personal Data with regulated financial institutions and service providers involved in providing financial services through the Platform, including sponsor banks, banking-as-a-service (BaaS) providers, account providers, card issuers, payment service providers, BIN sponsors and payment card networks.

Such sharing may be necessary for purposes including account opening, customer verification, card issuance, payment processing, transaction settlement, fraud prevention and regulatory compliance.

5.2 Credit Assessment and Risk Management Providers

We may share Personal Data with credit assessment providers, risk analytics providers, fraud prevention providers and other related service providers to assess creditworthiness, evaluate credit risks, determine eligibility for credit facilities, and support risk management activities.

5.3 Identity Verification and AML/Compliance Service Providers

We may share Personal Data with identity verification providers, sanctions screening providers, blockchain analytics providers and other AML/CTF compliance service providers to perform customer due diligence (CDD), enhanced due diligence (EDD), identity verification, transaction monitoring and regulatory compliance activities.

5.4 Technology, Cloud and Infrastructure Providers

We may share Personal Data with technology service providers, including cloud hosting providers, data storage providers, cybersecurity providers, analytics providers, mobile infrastructure providers and other technical service providers that support the operation, security and performance of the Platform.

Such providers process Personal Data under appropriate contractual arrangements and confidentiality obligations.

5.5 Professional Advisors, Regulatory Authorities and Law Enforcement

We may disclose Personal Data to professional advisors, including legal counsel, auditors, compliance consultants and other professional service providers.

We may also disclose Personal Data to regulatory authorities, government agencies or law enforcement bodies where required by applicable laws, regulations, court orders, legal processes, or regulatory obligations, including AML/CTF and tax reporting requirements.

5.6 Corporate Transactions and Business Transfers

We may disclose or transfer Personal Data in connection with a merger, acquisition, financing, restructuring, sale of assets, transfer of business operations or other corporate transactions, subject to applicable confidentiality and data protection requirements.

6. International Data Transfers

Your Personal Data may be transferred to, accessed from, processed, and stored in jurisdictions outside your country of residence where we, our Financial Partners, or our service providers operate. Data protection laws in such jurisdictions may differ from those in your jurisdiction of residence.

We take appropriate measures to ensure that cross-border transfers of Personal Data are conducted in accordance with applicable data protection laws and subject to appropriate safeguards, which may include:

- European Commission Standard Contractual Clauses (SCCs), UK International Data Transfer Agreements (IDTAs), or other equivalent lawful transfer mechanisms where applicable;
- Conducting Data Protection Impact Assessments (DPIAs) or similar risk assessments for high-risk cross-border processing activities where required or appropriate;
- Performing information security and privacy due diligence on Financial Partners, service providers, and sub-processors that receive or process Personal Data;

- Implementing contractual, technical, and organizational safeguards designed to protect the confidentiality, integrity, and security of Personal Data.

7. Data Retention

7.1 General Retention

We retain Personal Data only for as long as necessary to provide and manage the Services, including platform services, banking-related services, payment services and credit facilities, or to satisfy legal, accounting, regulatory and compliance requirements.

The retention period may vary depending on the nature of the Personal Data, the purpose for which it was collected, applicable legal requirements, and our operational or risk management needs.

7.2 Deletion Requests and Legal Retention Requirements

You may request deletion of certain Personal Data relating to your Platform account or profile information, subject to the applicable rights and procedures described in this Privacy Policy.

However, certain categories of Personal Data cannot be deleted or erased where retention is required under applicable laws, regulations, contractual obligations, or legitimate business purposes, including financial transaction records, payment and transfer records, funding and withdrawal records, credit repayment records, and KYC/AML verification information.

Such information may be retained by us and/or our Financial Partners for the period required under applicable banking, tax, accounting, AML/CTF and regulatory requirements, which may typically range from five (5) to seven (7) years or longer where required by applicable law.

Any user interface features that allow users to hide, filter or organize transaction records do not remove the underlying records maintained for regulatory, audit or security purposes.

8. Device Telemetry, Mobile Identifiers, and Tracking Technologies

To operate, secure, and optimize our fintech infrastructure, we utilize cookies, mobile device telemetry, software development kits (SDKs), and automated tracking technologies across our Website and Mobile Application.

These technologies collect technical information necessary to deliver digital financial services, maintain system integrity, verify execution environments, enhance security controls, and support applicable risk management requirements established by us and our regulated Financial Partners.

8.1 Website Cookies and Local Storage

When you access our online interfaces, we may deploy session and persistent cookies, together with local browser storage technologies.

These mechanisms may be used to authenticate user sessions, maintain authorization status, preserve user preferences, improve interface functionality, and analyze website usage patterns.

Website cookies may also support security monitoring by helping detect anomalous activities, unauthorized access attempts and potential session hijacking risks.

You may adjust or restrict cookie permissions through your browser settings; however, restricting certain essential cookies may affect certain platform functions or user experience.

8.2 Mobile Device Telemetry and Security Metrics

When you access or interact with our Mobile Application, we may automatically collect device information and technical parameters, including device identifiers, mobile advertising identifiers where applicable, device model specifications, operating system information, network connection metadata, IP addresses, application version information, and device security-related information.

Where enabled by you, we may process operating-system-level biometric authentication confirmations (such as Face ID or Touch ID validation status) solely for the purpose of approving sensitive actions within the application. We do not access, collect, or store raw biometric samples.

Such information may be used to establish device risk profiles, perform device fingerprinting, detect unauthorized access, identify abnormal environments such as spoofed or emulated devices, and support fraud prevention and security controls.

8.3 Diagnostics, Application Analytics, and Infrastructure Logging

To maintain operational reliability and security, we may collect and analyze technical information, including application crash reports, system logs, API performance metrics, and aggregated usage statistics.

Such information may be processed by us and/or specialized third-party infrastructure, analytics and security providers to identify technical issues, improve application performance, monitor service reliability, and detect potential security incidents or malicious activities.

Third-party providers processing such technical information are subject to appropriate contractual confidentiality obligations, limited-use requirements, and security safeguards.

9. Data Security

We maintain administrative, technical and organizational safeguards designed to protect your Personal Data against unauthorized access, loss, destruction, alteration

or disclosure.
These measures may include encryption of data in transit and at rest, multi-factor authentication (MFA), role-based access controls (RBAC), access monitoring, vulnerability management and security incident response procedures.
While we implement commercially reasonable security measures, no electronic storage system or method of transmission over the Internet can be guaranteed to be completely secure. Accordingly, we cannot guarantee absolute security of your Personal Data.

10. Your Privacy Rights

Subject to applicable laws and statutory data retention requirements, including the AML/CTF and banking compliance retention requirements described in Section 7, you may have the right to request access to, correction of, deletion of, or restriction on the processing of your Personal Data, as well as the right to request a copy of your Personal Data in a structured, commonly used and machine-readable format.

Data Protection Contact

We have designated a person responsible for data protection matters to oversee questions, requests and concerns relating to this Privacy Policy and the processing of your Personal Data.

If you wish to exercise your applicable privacy rights, submit a data enquiry, or lodge a complaint regarding the processing of your Personal Data, please contact our designated privacy representative at:

Email: privacy@denatrust.com

Subject Line: DATA PROTECTION ENQUIRY

We are committed to reviewing and responding to verified data requests in a timely manner, generally within fifteen (15) business days after receipt and identity verification.

11. Changes to This Privacy Policy

We may update or modify this Privacy Policy from time to time to reflect changes in our Services, operational practices, legal or regulatory requirements, or data processing activities.

Any updated version of this Privacy Policy will be published on our Website, Mobile Application, or otherwise communicated to you through appropriate channels.

Where required by applicable laws, we will provide additional notice regarding material changes to this Privacy Policy.

Your continued access to or use of the Services after the updated Privacy Policy becomes effective constitutes your acknowledgement of such changes.

12. Governing Language

This Privacy Policy may be provided in multiple languages for your convenience.

The English version of this Privacy Policy shall prevail and govern in the event of any inconsistency, conflict, or discrepancy between the English version and any translated version, unless otherwise required by applicable laws.

- End of Document -

ULinkOne by *Dena Trust*

隱私政策

更新於 2026 年 8 月 v2

1. 引言

感謝您選擇由 Dena Investment Limited（以「Dena Trust」名義運營，以下簡稱「我們」）運營的 ULinkOne 平台（以下簡稱「本平台」）。

通過本平台提供的服務（以下簡稱「本服務」）可能包括由我們或我們授權的金融合作夥伴提供的技術服務、支付相關服務、信貸額度、卡片服務及其他相關服務。

訪問或使用本服務，即表示您知悉您的個人資料將按照本《隱私政策》進行收集、使用、存儲和披露。在適用情況下，您聲明並保證，您已從任何相關人士處獲得必要的同意和授權，允許我們按照本文所述處理其個人資料。

本《隱私政策》詳細說明了當您訪問或使用我們的網站、移動應用程序、API、信貸額度、支付卡、由我們的金融合作夥伴提供的銀行服務以及相關服務時，我們如何收集、使用、存儲、披露及以其他方式處理您的個人資料。

我們可能會不時在網站上發布修訂版本，或通過電子郵件或其他適當渠道通知您，以更新本《隱私政策》。在適用法律要求的情況下，我們將就重大變更發出事前通知。您在收到此類通知後繼續使用本服務，即視為您接受修訂後的《隱私政策》。

2. 我們的角色及與金融合作夥伴的關係

2.1 身份與運營模式

Dena Trust 根據與受監管金融機構及其他金融合作夥伴簽署的協議，作為技術提供商、平台運營商以及（在適用情況下）項目管理者進行運營。

除非明確說明，否則 Dena Trust 不作為銀行、接受存款機構、支付機構或其他受監管的金融機構運營。我們不直接提供銀行、接受存款或其他受監管的金融服務。

通過本平台提供的某些金融、銀行、支付卡、信貸相關及其他相關服務，可能由我們授權的第三方金融機構、贊助銀行、發卡機構及其他受監管的服務提供商（統稱「金融合作夥伴」，包括但不限於 FV Bank International Inc. 及其關聯公司）直接提供或通過其提供。

此類服務可由相關金融合作夥伴直接提供，或通過由 Dena Trust 運營的本平台予以協助提供。

2.2 資料控制者與處理者結構

根據您所使用本服務的性質，Dena Trust 及我們的金融合作夥伴就您的個人資料而言，可作為獨立的資料控制者（Data Controllers）、資料處理者（Data Processors）或授權服務提供商運營。

責任分配通常如下：

(1) 平台與技術服務

對於為本平台的運營和管理而收集和處理的個人資料（包括賬戶管理、用戶體驗管理、平台安全、客戶支援、初始客戶盡職審查及平台風險管理），Dena Trust 作為獨立的資料控制者。

(2) 銀行與卡片服務

對於由金融合作夥伴提供的銀行賬戶、支付卡、電匯、卡交易及其他受監管金融服務，該等金融合作夥伴（在適用情況下包括 FV Bank International Inc.）可作為獨立的資料控制者。

該等金融合作夥伴有責任根據其自身的隱私政策及適用的監管義務處理個人資料，包括客戶身份識別、反洗錢/反恐怖融資（AML/CTF）合規、交易監控、欺詐預防及監管報告要求。

(3) 信貸服務

對於通過本平台提供的信貸額度或信貸相關服務，Dena Trust 可出於包括信貸評估、信貸額度確定、還款監控、信貸風險管理及相關合規要求等目的處理個人資料。

(4) 第三方服務提供商

由 Dena Trust 或我們的金融合作夥伴聘用的第三方服務提供商（包括 KYC/AML 身份驗證提供商、信貸風險分析提供商、雲端服務提供商及技術服務提供商），可在適用的合同安排和指令下，作為資料處理者或授權服務提供商處理個人資料。

3. 我們收集哪些個人資料

我們可能會收集、處理和存儲有關您以及（在適用情況下）您的最終受益所有人、董事、高級職員、授權簽署人、代表、擔保人及其他相關個人（統稱「相關人士」）的個人資料：

3.1 身份信息

法定全名、原名、性別、出生日期及地點、國籍、居住地址、護照/身份證件詳情、稅務編號、聯繫方式、電子郵件地址、區塊鏈錢包地址（如適用），以及用於身份驗證的生物識別特徵。

3.2 個人財務信息

淨資產總額、開戶目的、財富來源、資金來源、職業/僱傭詳情、收入信息、稅務居民身份信息、銀行賬戶信息、賬戶結單以及支出/交易歷史。

3.3 信貸與評估信息

信貸歷史、信用評分、信貸能力評估、可負擔性指標、債務負擔、還款行為以及內部/外部信貸風險評估結果。

3.4 銀行與支付信息

銀行賬戶詳情、賬戶餘額信息、虛擬 IBAN 詳情（如適用）、支付卡詳情及相關支付驗證信息、交易記錄、電匯指令及商戶類別代碼。

3.5 應用程序與技術測報信息

設備識別碼、設備指紋數據、IP 地址、粗略地理位置數據、移動操作系統信息、推送通知令牌、App 崩潰日誌、性能分析數據以及瀏覽器/HTTP 標頭數據。

3.6 敏感個人資料

在適用法律要求或允許的情況下，我們可能會處理某些類別的敏感個人資料，包括用於身份驗證和欺詐預防的生物識別數據，以及監管合規所需的其他敏感信息。

4. 我們如何使用個人資料

我們基於適用的法定依據處理個人資料，包括履行合同義務、遵守法律和監管要求、維護我們的合法利益，以及在適用法律要求時取得您的同意。

類別	具體運營目的
賬戶與平台服務	• 核實您的身份 • 創建並維護您的賬戶 • 提供客戶支援 • 運營並改進本平台
銀行與卡片服務	• 協助在金融合作夥伴處開立賬戶 • 支援發卡及支付交易 • 遵守銀行、支付及監管要求
信貸額度與服務	• 評估您獲得信貸額度的資格 • 確定信貸額度 • 評估還款能力 • 管理信貸風險及催收
反洗錢/反恐怖融資及監管合規	• 執行客戶盡職審查 (CDD) • 進行制裁及政治敏感人物 (PEP) 篩查 • 監控交易 • 遵守適用的法律和監管要求
安全與欺詐預防	• 檢測和預防欺詐 • 保護賬戶及系統 • 調查可疑活動 • 維護平台安全

5. 個人資料的共享與披露

我们不會出售您的個人資料。但是，為了提供和維護我們集成的金融科技、銀行、支付及信貸相關服務，我們可能會與以下類別的接收方共享您的個人資料：

5.1 金融合作夥伴及銀行機構

我們可能會與參與通過本平台提供金融服務的受監管金融機構及服務提供商共享個人資料，包括贊助銀行、銀行即服務（BaaS）提供商、賬戶提供商、發卡機構、支付服務提供商、BIN 贊助商及支付卡網絡。

此類共享對於開戶、客戶驗證、發卡、支付處理、交易清算、欺詐預防及監管合規等目的是必要的。

5.2 信貸評估及風險管理提供商

我們可能會與信貸評估提供商、風險分析提供商、欺詐預防提供商及其他相關服務提供商共享個人資料，以評估信貸能力、評估信貸風險、確定信貸額度資格，並支援風險管理活動。

5.3 身份驗證及反洗錢/合規服務提供商

我們可能會與身份驗證提供商、制裁篩查提供商、區塊鏈分析提供商及其他反洗錢/反恐怖融資合規服務提供商共享個人資料，以執行客戶盡職審查（CDD）、加強型盡職審查（EDD）、身份驗證、交易監控及監管合規活動。

5.4 技術、雲端及基礎設施提供商

我們可能會與技術服務提供商共享個人資料，包括雲端託管提供商、數據存儲提供商、網絡安全提供商、分析提供商、移動基礎設施提供商以及支援本平台運營、安全和性能的其他技術服務提供商。

此類提供商在適當的合同安排和保密義務下處理個人資料。

5.5 專業顧問、監管機構及執法部門

我們可能會向專業顧問披露個人資料，包括法律顧問、審計師、合規顧問及其他專業服務提供商。

在適用法律、法規、法院命令、法律程序或監管義務（包括反洗錢/反恐怖融資及稅務申報要求）要求時，我們亦可能會向監管機構、政府機關或執法部門披露個人資料。

5.6 公司交易及業務轉讓

在合併、收購、融資、重組、資產出售、業務運營轉讓或其他公司交易中，我們可能會根據適用的保密和數據保護要求披露或轉讓個人資料。

6. 國際數據傳輸

您的個人資料可能會被傳輸至、調閱自、處理及存儲在您居住國以外的司法管轄區，即我們、我們的金融合作夥伴或我們的服務提供商運營所在的地點。該等司法管轄區的數據保護法律可能與您居住地司法管轄區的法律有所不同。

我們採取適當措施，確保個人資料的跨境傳輸符合適用的數據保護法律，並受到適當保障措施的約束，其中可能包括：

歐盟委員會標準合同條款（SCCs）、英國國際數據傳輸協議（IDTAs）或在適用情況下的其他同等合法傳輸機制；

在要求或適當情況下，針對高風險跨境處理活動開展數據保護影響評估（DPIA）或類似的風險評估；

對接收或處理個人資料的金融合作夥伴、服務提供商和子處理者進行信息安全和隱私盡職審查；

實施旨在保護個人資料保密性、完整性和安全性的合同、技術和組織保障措施。

7. 資料保留

7.1 一般保留原則

我們僅在提供和管理本服務（包括平台服務、銀行相關服務、支付服務及信貸額度）所需的時間內，或在滿足法律、會計、監管及合規要求的期限內保留個人資料。

保留期限可能因個人資料的性質、收集目的、適用的法律要求以及我們的運營或風險管理需要而異。

7.2 刪除請求與法定保留要求

在受本《隱私政策》所述適用權利和程序的約束下，您可要求刪除與您的平台賬戶或個人資料信息相關的某些個人資料。

但是，若根據適用法律、法規、合同義務或合法商業目的要求必須保留某些類別的個人資料，則該等資料不得被刪除或擦除，包括金融交易記錄、支付和轉賬記錄、資金充值及提現記錄、信貸還款記錄以及 KYC/AML 身份驗證信息。

我們和/或我們的金融合作夥伴可在適用的銀行、稅務、會計、反洗錢/反恐怖融資及監管要求規定的期限內保留此類信息，該期限通常為五（5）至七（7）年，或在適用法律要求時保留更長時間。

使用者界面中允許使用者隱藏、過濾或整理交易記錄的任何功能，均不會刪除為監管、審計或安全目的而維護的底層記錄。

8. 設備測報、移動標識符與追蹤技術

為了運營、保障和優化我們的金融科技基礎設施，我們在網站和移動應用程序中使用了 Cookie、移動設備測報、軟件開發工具包（SDK）以及自動追蹤技術。

這些技術收集交付數字金融服務、維護系統完整性、核實執行環境、增強安全控制以及支援我們及受監管金融合作夥伴所確立的適用風險管理要求所需的技術信息。

8.1 網站 Cookie 及本地存儲

當您訪問我們的線上界面時，我們可能會部署會話 Cookie 和持久 Cookie，以及瀏覽器本地存儲技術。

這些機制可用於驗證用戶會話、維護授權狀態、保留用戶偏好、改進界面功能以及分析網站使用模式。

網站 Cookie 還可通過協助檢測異常活動、未授權訪問嘗試及潛在的會話劫持風險來支援安全監控。

您可通過瀏覽器設置調整或限制 Cookie 權限；但是，限制某些必要的 Cookie 可能會影響某些平台功能或用戶體驗。

8.2 移動設備測報與安全指標

當您訪問或使用我們的移動應用程序時，我們可能會自動收集設備信息和技術參數，包括設備識別碼、適用的移動廣告標識符、設備型號規格、操作系統信息、網絡連接元數據、IP 地址、應用程序版本信息以及設備安全相關信息。

在您啟用的情況下，我們可能會處理操作系統層面的生物識別驗證確認（例如 Face ID 或 Touch ID 驗證狀態），且僅用於在應用程序內核准敏感操作。我們不會調閱、收集或存儲原始生物識別特徵樣本。

此類信息可用於建立設備風險檔案、執行設備指紋識別、檢測未授權訪問、識別異常環境（如偽造或模擬設備），以及支援欺詐預防和安全控制。

8.3 診斷、應用程序分析及基礎設施日誌

為了維護運營可靠性和安全性，我們可能會收集並分析技術信息，包括應用程序崩潰報告、系統日誌、API 性能指標以及匯總的使用統計數據。

此類信息可由我們和/或專業的第三方基礎設施、分析和安全提供商進行處理，以識別技術問題、提高應用程序性能、監控服務可靠性，並檢測潛在的安全事件或惡意活動。

處理此類技術信息的第三方提供商須遵守適當的合同保密義務、限制使用要求及安全保障措施。

9. 資料安全

我們維護行政、技術和組織保障措施，旨在保護您的個人資料免受未授權訪問、丟失、毀損、篡改或披露。

這些措施可能包括傳輸中及靜止數據的加密、雙重身份驗證（MFA）、基於角色的訪問控制（RBAC）、訪問監控、漏洞管理及安全事件應對程序。

儘管我們實施了商業上合理的安全措施，但沒有任何電子存儲系統或通過互聯網傳輸的方法可以保證絕對安全。因此，我们無法保證您個人資料的絕對安全。

10. 您的隱私權利

在受適用法律及法定數據保留要求（包括第 7 條所述的反洗錢/反恐怖融資和銀行合規保留要求）約束前提下，您可能有權要求查閱、更正、刪除或限制處理您的個人資料，並有權要求以結構化、通用且機器可讀的格式索取您的個人資料副本。

11. 資料保護聯繫方式

我們已指定一名負責資料保護事務的人員，監督與本《隱私政策》及您的個人資料處理相關的問詢、請求和關注事項。

如果您希望行使適用的隱私權利、提交資料查詢或就個人資料的處理提出投訴，請通過以下方式聯繫我們的指定隱私代表：

電子郵件 (Email): privacy@denatrust.com

郵件主題 (Subject Line): DATA PROTECTION ENQUIRY

我們致力於及時審查並回復經驗證的資料請求，通常會在收到請求並完成身份核驗後的十五（15）個工作天內给予答覆。

12. 本隱私政策的變更

我們可能會不時更新或修改本《隱私政策》，以反映我們服務、運營實踐、法律或監管要求或數據處理活動的變更。

本《隱私政策》的任何更新版本都將發布在我們的網站、移動應用程序上，或通過適當渠道另行通知您。

在適用法律要求的情況下，我們將就本《隱私政策》的重大變更提供額外通知。

在更新後的《隱私政策》生效後，您繼續訪問或使用本服務即構成您對此類變更的知悉。

13. 管轄語言

為方便起見，本《隱私政策》可能提供多種語言版本。

如果英文版本與任何翻譯版本之間存在任何不一致、衝突或差異，概以本《隱私

政策》的英文版本為準並具管轄力，除非適用法律另有規定。

- 文件結束 -

ULinkOne by *Dena Trust*