PHOENIX DAO LLC

PRIVACY POLICY

[LAST UPDATED ON: 16th February, 2016]

This Privacy Policy ("**Policy**") describes how Phoenix DAO LLC, a limited liability company organized under the laws of the Republic of the Marshall Islands ("Company," "Umbra," "we," "us," or "our"), collects, uses, stores, discloses, and otherwise processes information in connection with access to and use of the Umbra protocol, dashboard related interfaces, documentation, and services (collectively, the "**Platform**").

This Policy is derived from, and implements, Umbra's internal privacy and data-handling standards, which are designed to reflect privacy-by-design, data minimisation, and security-by-default principles appropriate to a decentralised and non-custodial system. This Policy is intended to provide transparency into how those standards are applicable in practice and to accurately reflect the technical architecture and operational boundaries of the Protocol. It does not create any fiduciary, custodial, advisory, or monitoring obligations, nor does it imply that the Company possesses technical capabilities or access beyond what is expressly described in this Policy.

This Policy forms an integral part of the governance and disclosure documents governing the use of the Platform, including the Terms and Conditions (the "Terms") and applicable Risk Disclaimer. Each of these documents addresses different aspects of the Platform and should be read together with them. Capitalised terms not otherwise defined in this Policy have the meanings given to them in the Terms.

In the event of any inconsistency between this Policy and the Terms, the Terms shall prevail to the extent of such inconsistency.

1. PURPOSE AND SCOPE OF THIS POLICY

1.1. Umbra is designed and operated as a non-custodial, privacy-preserving software protocol deployed on the Solana blockchain. The Company develops and maintains reference implementations, interfaces, and tooling that allow users to interact directly with autonomous on-chain smart contracts.

Accordingly:

- Umbra does not operate or maintain user accounts;
- Umbra does not custody, control, or access user funds, private keys, viewing keys, encrypted balances, or cryptographic secrets;

- Umbra does not initiate transactions on behalf of users. Where users voluntarily enable features such as private mode, the Platform may facilitate transaction preparation or relayer routing; however, all transactions are authorised by the user through their self-custodied wallet and executed via independent third-party relayers; and
- Umbra does not maintain centralized records linking blockchain activity to real-world identities.

Any privacy properties associated with the Protocol arise from cryptographic design and user-controlled key management, not from trust placed in the Company.

For the avoidance of doubt, any execution coordination, routing logic, or cryptographic participation introduced at the interface or infrastructure layer (including through relayers or MPC or threshold mechanisms) does not grant the Company access to user assets, private keys, viewing keys, decrypted balances, transaction contents, or protocol state, and does not alter the non-custodial nature of the Platform.

1.2. This Policy applies solely to information processed by the Company in connection with inclusion but not limited to: (a) the Umbra website and web-based interfaces; (b) application programming interfaces (APIs); (c) software development kits (SDKs); (d) documentation and technical resources; (e) communications initiated by users with the Company; (f) application on iOS , Android and Seeker Systems and (g) any future products built by the Company

1.3. This Policy does not apply to public blockchain networks (including Solana); transactions broadcast or settled on-chain; third-party wallets, relayers, RPC providers, validators, or MPC node operators; decentralized applications or services not operated by the Company; or information processed entirely under a user’s sole control.

Users interact with such third parties at their own risk and subject to those parties’ respective privacy practices.

1.4. While Umbra is engineered to enhance transactional privacy through cryptographic techniques, the Company makes no representation or warranty that use of the Platform will:

- ensure anonymity, secrecy, or untraceability;
- prevent lawful access, analysis, or inference by third parties;
- exempt users from legal, regulatory, tax, or reporting obligations; or

- shield users from enforcement actions or compulsory disclosure orders.

Users remain solely responsible for understanding and complying with applicable data protection, financial, and other laws in their jurisdictions.

1.5. Umbra is developed in accordance with privacy-by-design and data-minimization principles, meaning the Platform is architected to avoid collecting personal data wherever technically feasible. However, nothing in this Policy shall be interpreted as an undertaking to eliminate all privacy risks; a commitment to maintain specific cryptographic standards indefinitely; or an assumption of obligations beyond those imposed by applicable law.

2. CORE PRIVACY POSITION AND REGULATORY BASELINE

2.1. Data Minimization and Architectural Constraints - Umbra is architected to minimise the collection, processing, and retention of information and to avoid processing information that could reasonably be used to identify users wherever technically feasible. The Protocol is designed such that the majority of user interactions occur on-chain or locally within the user's environment, without reliance on Company-operated accounts, centralised databases, or identity-linked records. As a result, the Company intentionally limits its information-handling activities to what is strictly necessary to operate, secure, and maintain the Platform interfaces and related off-chain infrastructure. The introduction of execution coordination, routing logic, relayer selection, or cryptographic participation mechanisms (including MPC or threshold-based mechanisms) does not expand the categories of information processed by the Company and does not alter the Company's limited role with respect to protocol-level data.

2.2. Absence of User Accounts and Identity Mapping - The Company does not create, maintain, or administer user accounts. Access to the Platform occurs through user-controlled blockchain wallets and does not require off - chain registration or Company - managed account creation. or the provision of usernames, passwords, email addresses, or other persistent identifiers to the Company.

Any on-chain registration, enrollment, or state recorded within Umbra's smart programs is publicly verifiable on-chain, pseudonymous in nature, and does not involve the creation or maintenance of user accounts or identity records by the Company.

Where the Umbra mobile application supports account-based or social login functionality through third-party wallet or key management infrastructure, such authentication credentials are processed exclusively by the relevant third-party provider and are not accessed, received, or stored by the Company.

2.3. The Company does not:

- request or collect government-issued identifiers;
- request or collect biometric information;
- require identity verification, onboarding procedures, or compliance screening;
- maintain records linking wallet addresses to real-world identities; or
- perform user identification, profiling, classification, or scoring.

Any association between a user and a blockchain address is established solely by the user through their chosen wallet software and exists independently of the Company's systems, records, or infrastructure.

2.4. Controller / Processor Positioning

To the extent that privacy or data protection principles may be deemed applicable, the Company determines the limited purposes and means of processing solely in relation to technical, operational, and administrative information processed in connection with the Website, Platform interfaces, documentation, and user-initiated communications. The Company does not act as a controller, processor, joint controller, fiduciary, custodian, or trusted intermediary in respect of:

- on-chain transaction data;
- encrypted balances, cryptographic commitments, or ciphertexts in their authoritative or protocol-governing form;
- nullifiers, Merkle tree data, or protocol state;
- private keys, plaintext viewing keys, or cryptographic secrets in a form accessible or controllable by the Company; or
- any data processed exclusively within user-controlled wallets, devices, or decentralised infrastructure.

The Company may operate non-authoritative off-chain infrastructure that mirrors or derives cryptographic commitments or UTXO-related data from publicly verifiable on-chain state solely to support Platform usability. Such infrastructure introduces no trust assumptions, does not alter protocol state, and can be independently replicated or verified using public blockchain data. The Protocol may also involve handling encrypted key material, including encrypted master viewing keys, which cannot be decrypted by the Company and may only be re-encrypted pursuant to explicit, user-authorised on-chain permissions. The Company has no unilateral ability to access, derive, or disclose private keys, viewing keys, balances, or other sensitive information.

2.5. **Public Blockchain Data Disclaimer -** Public blockchain networks, including Solana, are transparent, immutable, and globally accessible by design. The Company does not control, curate, modify, delete, or restrict access to blockchain data. For the avoidance of doubt:

- blockchain addresses, transaction hashes, timestamps, commitments, Merkle roots, and related metadata are not collected or processed by the Company as personal data;
- the Company does not determine the purposes or means of processing such data; and
- such data falls outside the Company's technical and operational control for the purposes of this Privacy Policy.

2.6. **No Custody, No Surveillance, No Profiling -** Umbra does not monitor user behaviour for the purpose of profiling, behavioural analysis, compliance surveillance, targeted advertising, or commercial exploitation. The Company does not:

- perform wallet clustering, transaction graph analysis, or linkage analysis;
- attempt to deanonymise users or infer identities; or
- sell, rent, license, or otherwise monetise user information.

Any privacy properties or risks associated with blockchain usage arise from the inherent transparency of public networks and the independent activities of third parties, not from Company-operated monitoring, analysis, or surveillance.

2.7. **Purposes and Justification for Processing**

Where the Company processes limited categories of information, such processing is undertaken solely for defined, proportionate, and legitimate purposes, including:

- operation, maintenance, and security of the Platform interfaces;
- prevention of abuse, misuse, or malicious activity targeting the Website or interfaces;
- response to user-initiated communications and support requests; and
- protection of the integrity, availability, and legitimate interests of the Company.

The Company does not process information for marketing, advertising, behavioural analysis, profiling, automated decision-making, or data monetisation purposes.

2.8. **No Expansion of Obligations -** Nothing in this Section shall be construed as an admission that the Company processes information beyond what is expressly described herein, nor as an agreement to assume obligations, roles, or technical capabilities beyond those expressly set out in this Privacy Policy. The Company may modify technical implementations over time to further reduce information processing where feasible, without expanding the scope of data processed or altering the non-custodial nature of the Platform.

3. INFORMATION PROCESSED

Guiding Principle: Minimal and Incidental Processing

The Company adheres to a principle of strict data minimisation. Information is processed only to the limited extent necessary to operate and maintain the Platform interfaces, ensure technical security and integrity, and respond to user-initiated communications. The Company does not process personal data as part of the core functioning of the Umbra Protocol itself. The Protocol operates autonomously on the Solana blockchain through decentralised smart contracts, without reliance on Company-controlled databases, identity systems, or custodial infrastructure.

For clarity and transparency, this Section distinguishes between:

- information processed by the Company in its capacity as an operator of off-chain interfaces and resources; and
- information that is neither processed nor controlled by the Company.

3.1. Information Processed by the Company

3.1.1. **Technical and Usage Information.** When users access the Website or Platform interfaces, the Company may incidentally process limited technical and usage-related information necessary to ensure functionality, security, and availability. Such information may include network metadata (such as IP addresses or truncated IP addresses), browser type, operating system, device characteristics, timestamps, referring URLs, session duration, and basic error or access logs. This information is processed solely for purposes such as maintaining platform stability, diagnosing technical issues, preventing abuse or malicious activity, and ensuring secure delivery of content. The Company does not use such information to identify users, create profiles, or associate technical data with wallet addresses, blockchain transactions, or protocol activity. Where feasible, technical and usage information is processed in an aggregated, transient, or anonymised form and is not retained as a persistent identifier.

3.1.2. **User-Initiated Communications.** Where users voluntarily contact the Company, including through email, support channels, vulnerability disclosure submissions, governance-related communications, or similar correspondence, the Company may process the information provided by the user. This may include names, usernames, or pseudonyms (if provided), contact details such as an email address, and the content of the communication and any attachments. The provision of such information is entirely voluntary, and users are encouraged not to include unnecessary or sensitive information in communications. Such information is processed solely for the purpose of responding to the inquiry, addressing technical or security matters, or engaging in protocol-related communications, and is not used for marketing, profiling, or unrelated purposes.

3.1.3. **Compliance and Security-Related Records.** The Company may process limited information relating to security incidents, abuse prevention, vulnerability disclosures, or misuse of the Platform interfaces, where reasonably necessary to protect the availability, integrity, and security of the Website and interfaces. Such information may also be processed in connection with internal investigations, dispute resolution, or response to legitimate requests directed to the Company. These records are handled proportionately, retained only as necessary, and are not used for surveillance, profiling, or commercial exploitation.

3.2. Information Not Collected or Controlled by the Company.

For the avoidance of doubt, the Company does not collect, store, process, or otherwise control the following categories of information in connection with the Platform or Protocol.

3.2.1. **Identity and KYC Information.** The Company does not collect or process identity verification or know-your-customer information, including government-issued identifiers, biometric identifiers, proof-of-address documentation, financial account numbers, or similar personal identification data.

3.2.2. **Wallet Credentials and Cryptographic Secrets.** The Company does not collect, store, access, or control any wallet credentials or cryptographic secrets, including private keys, seed phrases, signing keys, authentication material, master viewing keys, derived viewing keys, or encryption keys. All such credentials are generated, stored, and controlled exclusively by users within their self-custodied wallets or local environments.

3.2.3. **On-Chain Transaction Data.** The Company does not process blockchain transaction data as personal data. This includes transaction contents, commitments, nullifiers, Merkle tree positions, encrypted balances, ciphertexts, zero-knowledge proofs, and on-chain relayer routing metadata. The Company does not possess the technical capability to access, decrypt, modify, reverse, or associate such data with identified or identifiable individuals.

3.2.4. **Public Blockchain Data and Third-Party Indexing.** Use of the Protocol necessarily involves interaction with public blockchain infrastructure. Data associated with such interactions may be visible to independent third parties, including blockchain explorers, node operators, indexers, analytics providers, or other network participants. The Company does not operate blockchain indexers for surveillance or profiling purposes, does not enrich or correlate on-chain data with off-chain identifiers, and does not control or assume responsibility for any processing conducted by third parties that independently access public blockchain data. The Company may operate limited, non-authoritative indexing infrastructure solely to derive or mirror publicly available on-chain state (including commitment tree data) for ease of use and SDK functionality. Such indexing does not involve identity inference, profiling, or monitoring and does not alter the public or decentralised nature of the underlying blockchain data. Users are solely responsible for reviewing the privacy practices of any third-party services they elect to use.

3.2.5. **Cookies and Similar Technologies.** The Website may use limited cookies or similar technologies that are strictly necessary to support core functionality, security, and basic performance monitoring, such as error detection and service reliability. The Company does not deploy advertising cookies, behavioural tracking technologies, cross-site tracking mechanisms, fingerprinting techniques, or marketing analytics. Information derived from such technologies is not linked to wallet addresses, protocol activity, or on-chain data.

3.2.6. Sensitive Information and Children’s Data. The Company does not intentionally collect or process sensitive personal information or information relating to children. Users are instructed not to submit such information through the Platform or Company communication channels.

3.2.7. Data Accuracy and User Responsibility. To the extent users voluntarily provide information to the Company, users are responsible for ensuring that such information is accurate and appropriate. The Company does not independently verify user-provided information and does not rely on such information for automated decision-making, scoring, or profiling.

4. PURPOSE AND LEGAL BASIS FOR PROCESSING

The Company processes limited categories of information only where such processing is necessary, proportionate, and directly related to the operation, security, and integrity of the Platform interfaces, or to respond to user-initiated communications.

The Company does not process information for purposes unrelated to the functioning of the Platform interfaces, does not engage in surveillance or commercial data exploitation, and does not process information in a manner inconsistent with the non-custodial, decentralised design of the Umbra Protocol.

4.1. Permitted Purposes of Processing

The Company may process limited categories of personal data solely for the following purposes and on the corresponding legal bases:

4.1.1. **Operation and Security of the Platform Interfaces** - To operate, maintain, and secure the Website and Platform interfaces, including ensuring availability, performance, integrity, and protection against abuse, malicious activity, or technical failures. This includes processing limited technical or diagnostic information necessary to detect errors, mitigate attacks, ensure system stability, and safeguard the interfaces against misuse.

4.1.2. **User-Initiated Communications and Support** - To receive, review, and respond to communications voluntarily initiated by users, including support requests, technical inquiries, vulnerability disclosures, governance-related communications, or other protocol-related correspondence. Information provided in such communications is processed solely for the purpose of responding to the inquiry or taking appropriate follow-up action and is not used for marketing, profiling, or unrelated activities.

4.1.3. **Abuse Prevention and Platform Integrity** - To implement proportionate measures to protect the Website and Platform interfaces from abuse, misuse, denial-of-service attacks, automated scraping, or other activities that could compromise availability, security, or user experience. Such measures are applied at the interface or infrastructure level only and do not involve monitoring, analysing, or restricting protocol-level transactions or on-chain activity.

4.1.4. **Protection of Rights and Legitimate Interests** - To the extent reasonably necessary, to establish, exercise, or defend the Company's rights and interests, including in connection with dispute resolution, investigations, enforcement of the Terms, or response to credible claims or requests directed at the Company. Any processing for such purposes is limited in scope, handled proportionately, and confined to off-chain information within the Company's possession or control.

4.2. **No Secondary or Incompatible Use** - Information processed by the Company is not used for secondary purposes that are incompatible with the purposes described in this Section. In particular, the Company does not process information for:

- marketing, advertising, or promotional activities;
- behavioural analysis or user profiling;
- targeted communications or segmentation;
- automated decision-making producing legal or similarly significant effects; or
- sale, rental, licensing, or monetisation of information.

4.3. **No Automated Decision-Making or Profiling** - The Company does not engage in automated decision-making, profiling, scoring, or classification of users that produces legal or similarly significant effects. Any automated processes associated with the Umbra Protocol, including cryptographic verification, transaction validation, or smart contract execution, are performed autonomously by decentralised systems and do not constitute decisions made by the Company.

4.4. **Public Blockchain Processing Disclaimer** - To the extent that information recorded on public blockchains could be interpreted as personal data under certain frameworks, such information is not processed by the Company. Such data is generated, propagated, and made publicly available by decentralised blockchain infrastructure operating independently of the Company. The Company does not determine the purposes or means of such processing and does not have the technical ability to modify, delete, or restrict access to on-chain data.

4.5. **Purpose Limitation and Proportionality** - The Company applies strict purpose limitation and proportionality principles and ensures that only the minimum amount of information necessary is processed for each permitted purpose. Information is not retained or repurposed beyond what is reasonably required to achieve the specific purpose for which it was processed, and processing activities are periodically reviewed to ensure continued alignment with the non-custodial and privacy-preserving design of the Platform.

5. DATA SHARING AND DISCLOSURE

5.1. **No Sale or Commercial Disclosure** - The Company does not sell, rent, license, trade, monetise, or otherwise commercially disclose information processed in connection with the Platform. Information is disclosed to third parties only where such disclosure is strictly necessary to operate and secure the Platform interfaces, to respond to user-initiated requests, or to protect the integrity and legitimate interests of the Company, and only to the minimum extent required for the relevant purpose.

5.2. **Disclosure to Service Providers Acting as Data Processors** - The Company may disclose limited categories of information to carefully selected third-party service providers that support operation of the Website and Platform interfaces. Such service providers may include providers of hosting, infrastructure, security monitoring, communications tooling, incident response, and professional advisory services. All such service providers are engaged under contractual arrangements that require them to:

- process information solely on the Company's instructions and only for the specified purpose;
- maintain appropriate confidentiality and security safeguards;
- refrain from using information for independent or commercial purposes; and
- delete or return information once the relevant services are complete, where feasible.

Disclosure to service providers does not include access to private keys, cryptographic secrets, decrypted balances, transaction contents, or protocol-level state.

5.3. **Disclosure for Security, Abuse Prevention, and Platform Integrity** - The Company may disclose limited information where reasonably necessary to investigate, prevent, or respond to security incidents, abuse, misuse of the Platform interfaces, or violations of the Terms. Such disclosures are limited to off-chain information within the Company's possession or control and do not involve monitoring or disclosure of on-chain activity, transaction data, or cryptographic material.

5.4. **Disclosure to Protect Rights and Interests** - The Company may disclose limited information where reasonably necessary to establish, exercise, or defend its rights or interests, including in connection with disputes, claims, investigations, or enforcement of the Terms. Any such disclosure is proportionate, limited in scope, and confined to information relevant to the specific matter.

5.5. **No Disclosure of Wallet or Cryptographic Data -** The Company does not disclose, and does not possess the technical capability to unilaterally access or disclose, private keys, seed phrases, viewing keys, master viewing keys, derived keys, encryption keys, cryptographic secrets, decrypted balances, zero-knowledge proofs, nullifiers, or any data enabling unilateral tracing or deanonymisation of protocol activity. Accordingly, the Company cannot and does not disclose such information to any third party under any circumstances, except through an expressly defined, governance-authorised mechanism.

5.6. **Decentralised Infrastructure and Independent Third Parties -** The Umbra Protocol operates on decentralised blockchain infrastructure and relies on independent third parties, including blockchain validators, relayer operators, MPC node operators, RPC providers, wallet providers, and other network participants. These parties operate autonomously, are not controlled or directed by the Company, and independently determine the purposes and means of any information processing they perform. The Company does not act as a joint controller or intermediary with respect to such parties and does not assume responsibility for their data handling practices. Users interact with such third parties at their own discretion and are responsible for reviewing their respective privacy practices.

5.7. **Corporate Transactions** - In the event of a merger, acquisition, restructuring, financing, insolvency, or similar corporate transaction, limited information may be disclosed to professional advisers, counterparties, or potential acquirers solely to the extent reasonably necessary to evaluate or complete the transaction. Any such disclosure is subject to appropriate confidentiality obligations and does not expand the purposes for which information is processed.

5.8. **Cross-Border Data Handling** The Platform is globally accessible, and limited categories of information processed by the Company may be accessed or handled across jurisdictions as part of normal operation of the Website and interfaces.

Where information is handled across borders, the Company applies reasonable contractual, technical, and organisational safeguards proportionate to the limited nature of the information involved.

5.9. **No Public Disclosure by the Company** - The Company does not publicly disclose information processed in connection with the Platform, including through public reports, transparency dashboards, or analytics outputs. Any information visible on public blockchains exists independently of the Company's actions and is not disclosed, published, or controlled by the Company.

6. COOKIES AND SIMILAR TECHNOLOGIES

6.1. The Website may use cookies or similar technical mechanisms that are strictly necessary to support core functionality, security, and basic performance of the Website and Platform interfaces. Such technologies are used solely to enable essential services, maintain session integrity, prevent abuse, and ensure the secure and reliable delivery of content.

6.2. The Company limits its use of cookies and similar technologies to the following categories only:

- **Strictly Necessary Cookies**, which are required for the operation, security, and basic functionality of the Website and interfaces; and
- **Performance and Error-Monitoring Technologies**, used solely to detect technical issues, diagnose errors, and maintain operational stability.

6.3. The Company does not deploy cookies or similar technologies for advertising, behavioural tracking, cross-site tracking, fingerprinting, profiling, or marketing purposes.

6.4. Information derived from cookies or similar technologies is not linked, correlated, or associated with:

- wallet addresses or wallet connection metadata;
- blockchain transactions or protocol activity;
- cryptographic commitments, balances, or proofs; or
- any on-chain or protocol-level state.

6.5. Cookie-derived information is processed independently of the Umbra Protocol and is limited to off-chain Website functionality. Users may configure their browser settings to refuse or limit cookies. However, disabling strictly necessary cookies may affect the functionality, security, or availability of certain Website features.

6.6. The Company does not permit third-party advertising networks, data brokers, or marketing analytics providers to place cookies or similar tracking technologies on the Website.

6.7. The Company limits its use of cookies to the following categories only:

- Strictly necessary cookies, required to enable core Website functionality and security features; and

- Performance and error-monitoring cookies, used exclusively to detect technical issues, diagnose system errors, and maintain operational stability.

6.8. Users may configure their browser settings to refuse or limit cookies. However, disabling strictly necessary cookies may affect the functionality, security, or availability of certain Website features.

6.9. The Company does not permit third-party advertising networks, data brokers, or marketing analytics providers to place cookies or similar tracking technologies on the Website.

7. FRONTEND DIAGNOSTICS AND PLATFORM PERFORMANCE DATA

7.1. To ensure the availability, stability, and security of the Website and Platform interfaces, the Company may process limited technical and diagnostic information generated through user interactions with the frontend. Such information is processed solely to identify and resolve technical malfunctions, improve reliability, prevent abuse or malicious activity targeting the interfaces, and maintain the integrity and availability of the Platform.

7.2. Frontend diagnostic and performance information may include:

- error logs and crash reports;
- failed or incomplete interface loads;
- transaction broadcast or submission failures at the interface level;
- connectivity or latency issues related to RPC or network access;
- basic performance metrics relating to interface responsiveness or availability.

7.3. Frontend diagnostic information is:

- processed only at the interface or infrastructure level;
- not used to identify individual users;
- not correlated with wallet addresses, blockchain transactions, or protocol activity; and
- not used for profiling, behavioural analysis, analytics, or tracking.

Where feasible, such information is processed in an aggregated, transient, or anonymised form.

7.4. Frontend diagnostic information is retained only for the period reasonably necessary to investigate and resolve the relevant technical issue, after which it is deleted or irreversibly anonymised. The Company does not retain frontend diagnostic data as a persistent identifier or for long-term analytical purposes.

7.5. Processing of frontend diagnostic and performance information does not involve monitoring, analysing, or restricting protocol-level transactions or on-chain activity. The Company does not observe, record, or infer user behaviour within the Umbra Protocol as part of frontend diagnostics.

8. WALLET CONNECTION METADATA

8.1. When a user connects a self-custodied blockchain wallet to the Platform interface, the Company may incidentally process limited connection-related metadata strictly necessary to enable the connection and facilitate interface functionality. Such metadata may include the wallet software type, network selection, connection status, and basic success or failure indicators.

8.2. The Company does not collect, store, access, or process:

- private keys, seed phrases, signing material, or authentication credentials;
- wallet addresses as persistent personal identifiers;
- transaction payloads, message contents, or execution parameters;
- balances, encrypted balances, commitments, nullifiers, or cryptographic proofs; or
- protocol-level state or on-chain activity.

8.3. Wallet connection metadata is:

- processed on an ephemeral basis;
- not retained as a persistent identifier;
- not used to track users across sessions or visits;
- not correlated with protocol activity, transaction outcomes, or blockchain data; and
- not used for profiling, behavioural analysis, analytics, or marketing.

8.4. Wallet connection functionality does not grant the Company custody, control, or access to user assets or cryptographic material. The Company does not monitor, analyse, or infer user activity within connected wallets or within the Umbra Protocol.

8.5. Wallet software and wallet providers are independent third parties. The Company does not control their operations, security practices, or data handling and is not responsible for information processed by such providers.

Users are responsible for reviewing and understanding the privacy practices of their chosen wallet providers.

9. ABUSE PREVENTION AND PLATFORM INTEGRITY

9.1. The Company may implement proportionate technical measures at the Website or interface level to protect the Platform from abuse, misuse, or malicious activity, including rate limiting, automated traffic controls, denial-of-service mitigation, and similar safeguards. Such measures are designed solely to protect the availability, stability, and security of the Platform interfaces and do not involve monitoring, analysing, or restricting protocol-level transactions or on-chain activity.

9.2. Abuse-prevention measures:

- operate at the interface or infrastructure access layer only;
- rely on limited technical indicators necessary to detect abnormal or malicious traffic patterns;
- do not involve persistent tracking of users or devices; and
- are not used for profiling, behavioural analysis, surveillance, or compliance monitoring.

The Company does not use abuse-prevention mechanisms to identify users, infer identities, or associate activity across sessions or platforms.

9.3. Any measures implemented under this Section affect only access to Company-operated interfaces and do not alter, restrict, or interfere with the autonomous operation of decentralised smart contracts or on-chain protocol functionality.

9.4. Users may continue to interact directly with the Umbra Protocol through other means independent of the Company's interfaces.

10. SDKs, DEVELOPER TOOLS, AND THIRD-PARTY IMPLEMENTATIONS

10.1. The Umbra Protocol may be accessed or integrated through software development kits (SDKs), reference implementations, or tooling made available by the Company. Third-party developers who integrate the Protocol or SDK into their own applications operate independently and are solely responsible for any information processing conducted within their applications or services.

10.2. The SDKs and reference implementations provided by the Company do not transmit personal information, telemetry, analytics, or usage data to the Company by default. The Company does not receive information regarding how third-party applications use the Protocol, including information relating to transaction execution, relayer usage, MPC participation, or routing outcomes, unless such transmission is explicitly implemented by the third-party developer.

10.3. The Company does not control, audit, or monitor third-party applications built using the Umbra Protocol or SDKs and does not act as an intermediary, controller, or processor with respect to information processed by such applications. Users interact with third-party applications at their own discretion and are responsible for reviewing the privacy practices and terms of such applications.

10.4. The decentralised and open nature of the Umbra Protocol permits independent implementations and integrations beyond the Company's control. The Company does not assume responsibility for the data handling practices, security measures, or compliance obligations of independent developers or third-party services.

11. BROWSER BASED PREFERENCE

11.1. Certain user interface preferences, such as language selection, display settings, or interface configuration options, may be stored locally within the user's browser or device environment to improve usability and functionality.

11.2. Such preferences:

- are stored locally and remain under the user's control;
- are not transmitted to the Company unless technically necessary for Website functionality;
- are not linked to wallet addresses, protocol activity, or on-chain data; and
- are not used to identify users, track behaviour, or infer identities.

11.3. The Company does not use browser-based preferences to create user profiles or persistent identifiers. Certain user interface preferences, such as language selection, display settings, or interface configuration options, may be stored locally within the user's browser or device environment to improve usability and functionality.

11.4. Such preferences:

- are stored locally and remain under the user's control;
- are not transmitted to the Company unless technically necessary for Website functionality;
- are not linked to wallet addresses, protocol activity, or on-chain data; and

- are not used to identify users, track behaviour, or infer identities.

The Company does not use browser-based preferences to create user profiles or persistent identifiers.

12. DATA RETENTION AND STORAGE LIMITATION

12.1. **Principles of Data Minimisation and Storage Limitation -** The Company adheres to strict data minimisation and storage limitation principles. Information is retained only for as long as is reasonably necessary to fulfil the specific, explicit, and legitimate purposes for which it is processed, as described in this Privacy Policy. The Company does not retain information on a continuous, indefinite, or speculative basis, and does not retain information for profiling, behavioural analysis, surveillance, or any purpose inconsistent with the non-custodial, decentralised, and permissionless nature of the Umbra Protocol.

12.2. **Categories of Information Subject to Retention -** To the limited extent that information is processed, retention applies only to the following categories:

- **Technical and Security Information**, including limited network or device metadata, truncated IP address fragments, timestamps, and error or access logs, processed solely for security, integrity, and operational purposes;
- **User-Initiated Communications**, including correspondence voluntarily submitted by users through support, disclosure, governance, or contact channels; and
- **Security, Abuse, or Integrity Records**, where retention is reasonably necessary to investigate incidents, prevent misuse of the Platform interfaces, or protect the Company's legitimate interests.

For the avoidance of doubt, the Company does not retain private keys, seed phrases, viewing keys, master viewing keys, cryptographic secrets, decrypted balances, transaction contents, protocol state, or persistent identifiers intended to track or correlate user activity over time.

12.3. **Determination of Retention Periods -** Retention periods are determined on a category-specific basis and are proportionate to the purpose for which the information is processed:

- Technical and security logs are retained only for a short, rolling period necessary to maintain platform security, diagnose issues, and prevent abuse, after which they are deleted or irreversibly anonymised;

- User-initiated communications are retained for the duration necessary to respond to the inquiry and for a reasonable follow-up period, unless longer retention is justified by security, operational, or integrity considerations; and
- Security or abuse-related records may be retained for longer periods where reasonably necessary to investigate incidents, resolve disputes, or protect the Platform and the Company.

Where feasible, information is anonymised or aggregated prior to extended retention.

12.4. **On-Chain and Decentralised Data -** Blockchain data, including transaction records, commitments, nullifiers, Merkle tree updates, encrypted balances, and other protocol-level state, is recorded on public or permissionless blockchain infrastructure outside the Company's control. Such data is not stored by the Company in off-chain databases, cannot be modified, deleted, or selectively retained by the Company, and is governed exclusively by the rules of the underlying blockchain networks. Accordingly, on-chain data does not constitute Company-retained information for the purposes of this Privacy Policy.

12.5. **Storage Location and Access Controls -** Where information is retained, it is stored on systems subject to access controls proportionate to the sensitivity and nature of the information. Access is restricted to authorised personnel on a need-to-know basis, and reasonable technical and organisational safeguards are implemented to prevent unauthorised access, loss, alteration, or misuse. The Company does not operate centralized databases mapping protocol activity to identifiable users.

12.6. **Deletion and Anonymisation -** The Company implements procedures designed to ensure that information is deleted without undue delay once it is no longer necessary for the purposes for which it was processed, or irreversibly anonymised so that it can no longer be associated with an identifiable individual.

Deletion may occur automatically through system processes or manually following periodic review.

12.7. **Retention Exceptions -** Where information is reasonably required to address security incidents, misuse of the Platform interfaces, disputes, or other integrity-related matters, the Company may retain such information for the duration necessary to resolve the relevant issue.

12.8. No Custodial, Monitoring, or Recordkeeping Obligations - Nothing in this Section shall be interpreted as creating any obligation on the Company to monitor user activity, retain transaction-level data, act as a recordkeeper, or assume custodial, fiduciary, or surveillance responsibilities in respect of user assets or protocol interactions.

12.9. Explicit Exclusions - For the avoidance of doubt, the Company does not:

- conduct behavioural analytics or user profiling;
- perform wallet clustering, transaction surveillance, or deanonymisation;
- deploy fingerprinting or cross-device tracking technologies;
- monitor protocol activity for compliance or enforcement purposes;
- sell, rent, monetise, or commercially exploit information;
- enrich blockchain data with off-chain identifiers; or
- use automated tools to score, classify, or rank users.

13. DATA SECURITY AND SAFEGUARDS

13.1. Security-by-Design and Proportionality - The Company implements security measures designed to protect information processed in connection with the Platform against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. Such measures are implemented on a proportionate basis, taking into account the limited nature of the information processed by the Company, the decentralised and non-custodial architecture of the Umbra Protocol, the role of the Company as an interface and tooling provider, and the technical feasibility of safeguards. The Company does not maintain centralized repositories of protocol transaction data, decrypted cryptographic material, or user identity records.

13.2. Technical Safeguards - The Company employs technical safeguards appropriate to the nature and scope of its operations, which may include:

- secure hosting and infrastructure environments;
- encryption of data in transit where appropriate;
- access controls, authentication mechanisms, and role-based permissions;
- system hardening, patch management, and environment segregation;
- logging and monitoring for security and integrity purposes; and
- reasonable measures to prevent unauthorised access or misuse of systems.

The Company does not have access to private keys, seed phrases, viewing keys, encryption keys, or decrypted protocol data and therefore cannot secure, recover, or restore such information.

13.3. **Organisational Measures** - The Company implements organisational safeguards proportionate to its operational scope, which may include internal access restrictions, confidentiality obligations for personnel and contractors, and internal procedures governing handling of information processed in connection with the Platform. Access to information is limited to authorised individuals on a need-to-know basis and is restricted to the minimum extent necessary to perform operational, security, or support functions.

13.4. **Decentralised and Cryptographic Security Boundary** - The Umbra Protocol relies on cryptographic primitives, decentralised blockchain infrastructure, independent validator networks, relayer operators, MPC node operators, and other third-party systems. The security of on-chain transactions, encrypted balances, and protocol-level state depends in part on factors outside the Company's control, including the security of user-managed wallets, private keys, devices, and third-party infrastructure. The Company does not control and cannot guarantee the security, availability, or correctness of decentralised networks or third-party systems.

13.5. **No Absolute Security Guarantee -** No system is completely secure. The Company does not warrant or guarantee that information, cryptographic mechanisms, decentralised infrastructure, or third-party services will be immune from unauthorised access, compromise, failure, or attack. Users acknowledge and accept that residual risks are inherent in the use of decentralised and cryptographic systems.

13.6. **User Security Responsibilities** - Users are solely responsible for safeguarding their private keys, seed phrases, viewing keys, credentials, devices, wallet software, and any other tools used to access the Platform. The Company cannot recover lost credentials, restore access, or reverse transactions resulting from user error, compromise, loss of keys, or misuse of third-party services.

13.7. **Incident Response** - The Company maintains internal procedures designed to identify, assess, and respond to security incidents affecting information processed in connection with the Platform interfaces. Where a security incident materially affects the integrity or availability of the Website or interfaces, the Company may take reasonable steps to mitigate impact, investigate the issue, and restore functionality. The Company does not monitor protocol-level activity as part of incident response.

13.8. **No Monitoring or Surveillance Obligation** - Nothing in this Section shall be construed as imposing any obligation on the Company to monitor user activity, conduct proactive surveillance, analyse protocol transactions, or assume custodial, fiduciary, compliance, or enforcement responsibilities.

14. USER RIGHTS

14.1. To the extent the Company processes limited categories of information in connection with the Platform, users may request reasonable access to, correction of, or deletion of such information, subject to the technical and operational constraints described in this Privacy Policy. For the avoidance of doubt, this Section applies only to information processed by the Company in its capacity as an operator of off-chain interfaces and resources. It does not apply to:
data recorded on public or permissionless blockchain networks;
cryptographic commitments, encrypted balances, nullifiers, Merkle tree data, or protocol-level state;
information processed exclusively within user-controlled wallets or devices; or
information processed independently by third parties outside the Company's control.

Nothing in this Section requires the Company to collect additional information, re-identify users, or compromise the privacy-preserving design of the Umbra Protocol in order to respond to a request.

14.2. **Access to Information** - Users may request confirmation as to whether the Company processes information relating to them and, where applicable, request access to such information. Due to the non-custodial, pseudonymous, and decentralised nature of the Platform, the Company may be unable to associate information with a specific individual without additional information provided by the user. Access requests are therefore limited to information the Company can reasonably identify and retrieve without disproportionate effort.

14.3. **Correction of Information -** Where information processed by the Company is demonstrably inaccurate or incomplete, users may request correction. This right does not apply to immutable blockchain data, cryptographic protocol state, or information generated or controlled by decentralised infrastructure or independent third parties.

14.4. **Deletion of Information** - Users may request deletion of information processed by the Company where such information is no longer necessary for the purpose for which it was processed. Users acknowledge that the

Company cannot delete, modify, or reverse on-chain data or protocol-level state, and that anonymised or aggregated information may no longer be attributable to an identifiable individual. Deletion requests may be declined where retention is reasonably necessary to address security incidents, prevent misuse, or protect the Company's legitimate interests.

14.5. **Limitation of Processing -** Where appropriate, users may request that processing of certain information be limited. Any such limitation applies solely to off-chain information processed by the Company and does not affect autonomous protocol execution or decentralised infrastructure.

14.6. Exercising Requests - Requests relating to this Section may be submitted to: Privacy Contact Email: legal@umbraprivacy.com

14.7. To protect security and integrity, the Company may request reasonable information to verify the request and may decline requests that are manifestly unfounded, excessive, technically infeasible, or incompatible with the decentralised design of the Platform.

15. CHILDREN'S DATA

15.1. The Platform and Umbra Protocol are not intended for use by children. The Company does not knowingly collect or process information relating to individuals below the age at which they may lawfully provide information without parental consent.

15.2. The Company does not implement age-verification mechanisms or identity checks, as the Platform operates on a permissionless, non-custodial, and pseudonymous basis. Compliance with age-related requirements remains the responsibility of users.

15.3. If the Company becomes aware that it has inadvertently processed information relating to a child, it will take reasonable steps to delete such information where technically feasible and appropriate.

16. CROSS BORDER DATA HANDLING

16.1. The Platform is globally accessible, and limited categories of information processed by the Company may be handled across jurisdictions as part of operating the Website and interfaces. Such handling is limited in scope and confined to information necessary for the purposes described in this Privacy Policy.

16.2. Where information is handled across borders, the Company applies reasonable technical, organisational, and contractual safeguards proportionate to the limited nature of the information involved.

16.3. Decentralised infrastructure participants, including validators, relayer operators, MPC node operators, RPC providers, and wallet providers, operate independently and may process information in jurisdictions of their choosing. The Company does not control the location, governance, or data handling practices of such participants and does not act as an intermediary or joint operator in respect of their activities.

17. POLICY UPDATES, CONTACT DETAILS, AND GOVERNANCE

17.1. Updates to This Privacy Policy

The Company may amend or update this Privacy Policy from time to time to reflect changes in Platform functionality, technical architecture, operational practices, or organisational structure. Updates will be effective as of the date indicated at the top of the Policy. Continued use of the Platform following an update constitutes acknowledgement of the revised Policy.

17.2. Relationship to Terms and Protocol Architecture

This Privacy Policy must be read together with the Terms and Conditions governing access to and use of the Platform. Nothing in this Policy modifies the non-custodial or decentralised nature of the Umbra Protocol, creates custodial or monitoring obligations, or expands the Company's role beyond that of an off-chain interface and tooling provider. In the event of any inconsistency, the Terms shall prevail.

17.3. Contact Information

For questions, requests, or concerns relating to this Privacy Policy, users may contact:
Privacy Contact Email: legal@umbraprivacy.com

The Company does not maintain user accounts or identity databases. Accordingly, responses may be limited by technical feasibility and privacy-preserving constraints. Nothing in this Privacy Policy shall be construed as a waiver of any rights or defences available to the Company, or as a representation that the Company processes information beyond what is expressly described herein.