PRIVACY POLICY

LAST REVISED ON: [22ND APRIL 2026]

Please read this Privacy Policy ("**Policy**") carefully. This Policy describes how Asula Research Holdings Ltd. ("**Asula**", "**us**", "**our**", and "**we**") collects, uses, discloses, and otherwise processes personal information in connection with any mobile application made available by us that links to this Policy (each, an "**Application**") and the information and services made available thereby (each a "**Service**" and collectively, the "**Services**"). Capitalized terms used but not defined in this Policy have the meanings given to them in our Terms of Use.

THIS POLICY APPLIES TO ALL USERS VISITING, ACCESSING, OR USING THE SERVICES, WHETHER THROUGH THE APPLICATION OR OTHERWISE. BY ACCESSING OR USING THE SERVICES, CONNECTING A WALLET THROUGH THE APPLICATION, AND/OR DOWNLOADING THE APPLICATION, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THIS POLICY. IF YOU DO NOT AGREE WITH THE PRACTICES DESCRIBED IN THIS POLICY, DO NOT ACCESS AND/OR USE THE SERVICES.

THE SERVICES ARE A SELF-CUSTODIAL INTERFACE TO COMPATIBLE BLOCKCHAIN NETWORKS. ASULA DOES NOT HOLD, CONTROL, OR HAVE ACCESS TO YOUR PRIVATE KEY OR USER ASSETS AT ANY TIME. WE CANNOT RECOVER YOUR PRIVATE KEY OR REVERSE ANY ON-CHAIN TRANSACTION YOU INITIATE. BLOCKCHAIN TRANSACTIONS ARE PUBLIC AND, BY THEIR NATURE, IMMUTABLE; ONCE WRITTEN TO A SUPPORTED BLOCKCHAIN, THEY CANNOT BE MODIFIED OR DELETED BY ASULA, BY YOU, OR BY ANY OTHER PARTY.

PLEASE NOTE THAT THIS POLICY IS SUBJECT TO CHANGE BY ASULA IN ITS SOLE DISCRETION AT ANY TIME. When changes are made, Asula will make a new copy of this Policy available within the Services. We will also update the "Last Revised" date at the top of this Policy. Your continued use of the Services following the posting of any changes constitutes your acceptance of such changes. PLEASE REGULARLY CHECK THE SERVICES TO VIEW THE THEN-CURRENT POLICY.

---

1. **SCOPE AND APPLICATION.** This Policy applies to personal information that Asula processes in its capacity as a controller (or the equivalent concept under applicable data-protection law) in connection with the Services. This Policy does not apply to:

1.1 **Third-Party Services.** The Services integrate with third-party infrastructure, protocols, and service providers, including without limitation authentication providers, wallet providers, analytics providers, custodial hardware wallet manufacturers, blockchain validators, decentralized exchanges, liquidity routing protocols, issuers of tokenized securities, and cross-chain execution venues (each, a "**Third-Party Service**"). Third-Party Services are controlled by parties other than Asula. Your interactions with any Third-Party Service, including the personal information you provide to such Third-Party Service, are governed solely by that Third-Party Service's own privacy policy and terms, and Asula disclaims any liability for the processing of personal information by any Third-Party Service. We encourage you to review the privacy policies of each Third-Party Service before using it.

1.2 **Blockchain Data.** Information that you or any Third-Party Service broadcasts to a Supported Blockchain (including your Wallet address, transaction amount, counterparty address, and transaction metadata) becomes part of a public, decentralized ledger operated by validators and node operators over which Asula has no control. Asula is not a controller, processor, or custodian of blockchain data. YOU ACKNOWLEDGE THAT ANY PERSONAL INFORMATION ASSOCIATED WITH AN ON-CHAIN TRANSACTION IS PUBLIC BY DESIGN AND, BECAUSE OF THE IMMUTABLE NATURE OF SUPPORTED BLOCKCHAINS, CANNOT BE ERASED, RECTIFIED, OR OTHERWISE MODIFIED ON THE BLOCKCHAIN BY ASULA IN RESPONSE TO ANY REQUEST.

1.3 **Aggregated and De-Identified Data.** This Policy does not restrict our collection, use, or disclosure of information that has been aggregated or de-identified such that it cannot reasonably be used to identify you.

2. **INFORMATION WE COLLECT.** As set forth in Section 5 of the Terms of Use, by accessing or using the Services you acknowledge and agree that Asula has the right to collect, use, and disclose the information described in this Section 2 (including any personal data you provide to us and your Wallet address and IP address) in accordance with this Policy. We collect information about you in three categories: information that you provide directly to us, information that is collected automatically when you use the Services, and information that we receive from Third-Party Services.

2.1 **Information You Provide to Us.**

(a) *Registration Data.* When you register an Account on the Services, we collect Registration Data (as defined in the Terms of Use). Registration Data may include your email address, phone number, and any other information you are prompted to provide by the registration form. Additional information may be required to access certain features of the Services.

(b) *Communications.* If you contact us directly (for example, by emailing us at the address in Section 14 or using any in-Application support feature), we will receive any information you choose to provide, including your name, email address, the contents of your message, and any attachments.

(c) *Surveys, Beta Programs, and Feedback.* From time to time, we may invite you to participate in surveys, beta tests of pre-release functionality, or user-research sessions, or you may otherwise submit Feedback (as defined in Section 3.7 of the Terms of Use) to us. Participation is voluntary, and we will collect only the information you choose to provide. Personal information that you submit through such participation is processed in accordance with this Policy; Asula's rights in the content of any Feedback are governed by Section 3.7 of the Terms of Use and are not limited by this Policy.

2.2 **Information Collected Automatically.** When you access or use the Services, we and our service providers may automatically collect the following categories of information:

(a) *Device and Application Information.* Information about the device you use to access the Services, including device model, operating system and version, application version, device identifiers (such as IDFV on iOS or Android ID), language and locale settings, time zone, and device capabilities.

(b) *Log and Usage Data.* Information about your interaction with the Services, including the screens and features you access, the actions you take, the date and time of your access, crashes and other diagnostic events, performance metrics, and any error messages generated.

(c) *Network Information.* Your internet protocol (IP) address, internet service provider, and approximate location inferred from your IP address (generally no more precise than the country or region level). We do not collect precise geolocation data from your device.

(d) *Wallet Address and On-Chain Activity.* In order to display balances, transaction history, and other User Asset Information, the Services query Supported Blockchains and blockchain indexers for activity associated with the Wallet address you have connected to the Services. We associate this Wallet address with your Account.

2.3 **Information Received from Third-Party Services.** Where you link a Third-Party Account (as defined in Section 1.6 of the Terms of Use) to the Services, we may receive Linked Account Content (as defined in Section 1.6 of the Terms of Use) and other information from such Third-Party Service as permitted by the applicable terms, your authorization, and the privacy settings you have configured for such Third-Party Account.

(a) *Authentication Providers.* If you sign in to the Services using a Third-Party Service that provides authentication, we receive the information that such Third-Party Service has been authorized to share with us, which may include your email address, phone number, and a unique user identifier.

(b) *Wallet Providers.* Dawn uses Privy as its default wallet provider, as referenced in Section 3.6 of the Terms of Use. When you create or connect a Wallet through Privy or another Third-Party Service, we receive your public Wallet address. WE DO NOT RECEIVE, STORE, OR HAVE ACCESS TO YOUR PRIVATE KEY OR ANY OTHER CREDENTIAL USED TO SIGN TRANSACTIONS ON YOUR WALLET. Your Private Key is generated, stored, and controlled exclusively by you through the applicable Third-Party Service. Your relationship with Privy is governed by the Privy privacy policy (currently available at https://www.privy.io/privacy-policy) and by the Privy terms of service referenced in Section 3.6 of the Terms of Use.

(c) *Blockchain Data Providers and Indexers.* We receive publicly available on-chain information associated with your Wallet address from blockchain indexers, data providers, and infrastructure operators we use to query Supported Blockchains.

(d) *Analytics and Error-Reporting Providers.* We receive aggregated and event-level usage and diagnostic information from our analytics and error-reporting providers.

(e) *Payment Service Providers and Onramp/Offramp Partners.* If you use a feature of the Services that is enabled by a Payment Service Provider (as defined in the Terms of Use), we may receive limited information from such Payment Service Provider about the status of your transaction. We do not receive your full payment instrument (for example, credit-card number).

2.4 **Sensitive Information.** We do not intentionally collect any special category of personal data (as that term is defined under the EU General Data Protection Regulation) or sensitive personal information (as that term is defined under applicable U.S. state law), and we ask that you not submit any such information to us through the Services.

3. **HOW WE USE INFORMATION.** We use the information described in Section 2 for the following purposes:

3.1 **To Provide the Services.** To operate, maintain, and deliver the Services, including to: create and manage your Account; connect your Wallet to the Services; query Supported Blockchains for balances and transaction history; display User Asset Information; draft transaction messages; enable integrations with Third-Party Services you elect to use; and communicate with you about the Services (including service announcements, security alerts, and support messages).

3.2 **To Secure the Services.** To protect the security, integrity, and availability of the Services, including to: detect, prevent, and respond to fraud, abuse, and unauthorized use; enforce our Terms of Use and other policies; verify Account ownership; rate-limit requests; and comply with legal and regulatory obligations.

3.3 **To Improve the Services.** To analyze how users interact with the Services and to improve existing features and develop new ones, including through the use of analytics and product-research tools. Where required by applicable law, we will use only de-identified or aggregated information for these purposes, or will do so on the basis of your consent.

3.4 **To Communicate with You.** To respond to your inquiries, provide customer support, administer surveys and user-research programs, and (where you have provided your email address and in accordance with applicable law) send you product announcements. You may opt out of non-transactional email communications at any time by following the unsubscribe link in any such email.

3.5 **To Comply with Legal Obligations.** To comply with applicable laws, regulations, and legal process; to respond to lawful requests from governmental authorities; and to establish, exercise, or defend legal claims.

3.6 **With Your Consent.** For any other purpose disclosed to you at the time we collect the information, or otherwise with your consent.

3.7 **Legal Bases (EEA, UK, and Similar Jurisdictions).** Where the EU General Data Protection Regulation, the UK General Data Protection Regulation, or a substantially similar law applies, we rely on one or more of the following legal bases for the processing described above: (a) performance of a contract with you (Section 3.1 and Section 3.4, to the extent related to service messages); (b) our legitimate interests in operating, securing, and improving the Services (Sections 3.2 and 3.3), balanced against your rights and interests; (c) compliance with a legal obligation (Section 3.5); and (d) your consent (Section 3.6, and Section 3.3 where required). You have the right to object to, or withdraw consent for, processing based on consent or our legitimate interests, as described in Section 9.

4. **HOW WE SHARE INFORMATION.** Except as described in this Section 4, we do not sell your personal information to third parties. We share personal information only in the following circumstances:

4.1 **Service Providers and Subprocessors.** We share personal information with third parties that process it on our behalf under written agreements that restrict their use of the information to the purposes we specify. These include providers of authentication, wallet infrastructure, blockchain-data indexing, cloud hosting, analytics, error reporting, customer support, and payment processing. You may request an up-to-date list of our subprocessors by contacting us as described in Section 14.

4.2 **Third-Party Services You Elect to Use.** When you elect to interact with a Third-Party Service through the Services (including any feature that routes a transaction, swap, deposit, or order through a third-party protocol, liquidity venue, lending program, equity-token issuer, cross-chain bridge, or hardware wallet manufacturer), we will share the information reasonably necessary to effect your requested interaction. Such Third-Party Services process your personal information as independent controllers and their processing is governed by their own privacy policies.

4.3 **Legal Process and Protection.** We may disclose personal information where we have a good-faith belief that such disclosure is necessary to: (a) comply with applicable law, regulation, subpoena, court order, or other legal process; (b) respond to a lawful request from a governmental authority; (c) protect the rights, property, or safety of Asula, our users, or any third party; or (d) investigate, prevent, or take action against suspected violations of the Terms of Use, fraud, or security incidents.

4.4 **Corporate Transactions.** In the event of a merger, acquisition, financing, reorganization, bankruptcy, receivership, sale of company assets, or transition of the Services to another provider, we may transfer the information described in Section 2 to the successor or acquirer, subject to customary confidentiality protections.

4.5 **Aggregated or De-Identified Data.** We may share aggregated or de-identified information with third parties for any purpose.

4.6 **With Your Consent.** We may share personal information with your consent or at your direction.

4.7 **No Sale of Personal Information; Targeted Advertising.** We do not sell your personal information for monetary consideration, and we do not use your personal information for cross-context behavioral advertising or targeted advertising.

5. **COOKIES AND SIMILAR TECHNOLOGIES.** The Application is a native mobile application and does not use browser cookies. The Application and its service providers may use mobile-application analytics software-development kits ("**SDKs**") that generate device-local identifiers and collect the information described in Section 2.2. Where required by applicable law, we will obtain your consent before activating non-essential SDKs, and you may manage such consent through the in-Application privacy controls.

6. **DATA RETENTION.** We retain personal information for as long as is necessary to provide the Services to you, comply with our legal obligations, resolve disputes, and enforce our agreements, after which it will be deleted or de-identified. The specific retention period depends on the type of information and the purpose for which it is processed. You may request deletion of your Account and associated personal information by contacting us as described in Section 14, subject to the limitations described in Section 9.6.

7. **SECURITY.** We maintain administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, disclosure, alteration, and destruction. HOWEVER, NO METHOD OF ELECTRONIC TRANSMISSION OR STORAGE IS 100% SECURE, AND WE CANNOT GUARANTEE THE ABSOLUTE SECURITY OF ANY INFORMATION YOU PROVIDE TO US. You are responsible for protecting access to your device, Account, Wallet, and Private Key. ASULA HAS NO ABILITY TO RECOVER A LOST OR COMPROMISED PRIVATE KEY AND IS NOT RESPONSIBLE FOR ANY LOSS OF USER ASSETS RESULTING FROM A COMPROMISE OF YOUR DEVICE, ACCOUNT, WALLET, OR PRIVATE KEY.

8. **INTERNATIONAL DATA TRANSFERS.** Asula is established in the Cayman Islands. Our service providers are located in a number of jurisdictions, including the United States. When you use the Services, personal information that we or our service providers collect will be transferred to, stored in, and processed in jurisdictions that may have data-protection laws different from those of your country of residence. Where we transfer personal information from the European Economic Area, the United Kingdom, or Switzerland to a jurisdiction that has not been recognized as providing an adequate level of protection, we rely on appropriate safeguards, including the European Commission's Standard Contractual Clauses and, where applicable, the UK International Data Transfer Addendum. You may contact us as described in Section 14 to request a copy of the relevant safeguards.

9. **YOUR PRIVACY RIGHTS.** Depending on your jurisdiction, you may have certain rights with respect to the personal information we hold about you, as described in this Section 9. These rights are not absolute and are subject to the exceptions and limitations set forth in applicable law and in this Policy, including the blockchain-immutability limitation described in Sections 1.2 and 9.6.

9.1 **Access and Portability.** You may request confirmation as to whether we process personal information about you, a copy of that information, and, where applicable, a copy in a structured, commonly used, machine-readable format.

9.2 **Correction.** You may request that we correct personal information that is inaccurate or incomplete.

9.3 **Deletion.** You may request that we delete personal information that we hold about you, subject to the limitations in applicable law and in Section 9.6.

9.4 **Objection and Restriction (EEA, UK, and Similar Jurisdictions).** Where our processing is based on our legitimate interests, you may object to such processing on grounds relating to your particular situation. You may also request restriction of processing in certain circumstances.

9.5 **Withdrawal of Consent.** Where our processing is based on your consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

9.6 **Limitations for On-Chain Data.** INFORMATION THAT HAS BEEN BROADCAST TO A SUPPORTED BLOCKCHAIN CANNOT BE CORRECTED OR DELETED BY ASULA BECAUSE SUPPORTED BLOCKCHAINS ARE DECENTRALIZED AND IMMUTABLE. Requests under Sections 9.1 through 9.5 will apply only to personal information held by Asula in its own systems (or in systems operated by its subprocessors on Asula's behalf), and not to personal information recorded on any blockchain, held by any independent Third-Party Service, or held by any other independent controller.

9.7 **California Residents (CCPA / CPRA).** If you are a California resident, you have the rights described in Sections 9.1, 9.2, 9.3, and 9.5, as well as the right to request information about (a) the categories of personal information we have collected, used, disclosed, and (if applicable) sold or shared in the preceding twelve (12) months, (b) the categories of sources from which we collected such information, (c) our business or commercial purposes for collecting or disclosing such information, and (d) the categories of third parties with whom we disclosed such information. As stated in Section 4.7, we do not sell your personal information and do not share it for cross-context behavioral advertising. You have the right not to receive discriminatory treatment for exercising your rights under California law. You may designate an authorized agent to submit a request on your behalf, subject to verification.

9.8 **Other U.S. State Residents.** If you are a resident of a state that has enacted a comprehensive consumer privacy law (including Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Delaware, Montana, Iowa, Tennessee, New Jersey, Indiana, or any other such state), you have the rights described in Sections 9.1, 9.2, 9.3, and 9.5, to the extent provided by applicable law, as well as the right to appeal our refusal to act on any such request.

9.9 **Global Privacy Control.** Where required by applicable law, we treat Global Privacy Control ("**GPC**") signals as a valid opt-out of the sale or sharing of personal information. As stated in Section 4.7, we do not currently sell or share personal information for cross-context behavioral advertising.

9.10 **How to Exercise Your Rights.** To exercise any right under this Section 9, please contact us as described in Section 14. We may ask you to verify your identity before acting on your request. We will respond within the timeframe required by applicable law. If you are not satisfied with our response, you may have the right to lodge a complaint with your local data-protection authority.

10. **CHILDREN.** THE SERVICES ARE NOT INTENDED FOR, AND WE DO NOT KNOWINGLY COLLECT PERSONAL INFORMATION FROM, ANYONE UNDER EIGHTEEN (18) YEARS OF AGE. If you are under 18, do not access or use the Services. If we learn that we have collected personal information from a person under 18, we will delete that information. If you believe that we may have collected personal information from a person under 18, please contact us as described in Section 14.

11. **CHANGES TO THIS POLICY.** We may revise this Policy from time to time. When we make a material change, we will notify you by updating the "Last Revised" date at the top of this Policy and, where required by applicable law, by providing additional notice (for example, by email or by a prominent notice within the Services). Any change will be effective immediately for new users and, for existing users, on the effective date indicated in the notice. Your continued use of the Services following the effective date constitutes your acceptance of the revised Policy. PLEASE REGULARLY CHECK THE SERVICES TO VIEW THE THEN-CURRENT POLICY.

12. **MOBILE APPLICATION STORES.** The Application is made available through third-party mobile-application stores. As provided in Section 3.9 of the Terms of Use, with respect to any Application accessed through or downloaded from the Apple App Store, you acknowledge that Apple Inc. and its subsidiaries are third-party beneficiaries of the Terms of Use, and upon your acceptance of the Terms of Use, Apple will have the right (and will be deemed to have accepted the right) to enforce the Terms of Use as they relate to your license of such Application against you as a third-party beneficiary thereof. Your use of any mobile-application store is also governed by that store's own terms and privacy policy, and Asula disclaims any liability for the processing of your personal information by the operator of any such store.

13. **GOVERNING LAW AND DISPUTE RESOLUTION.** THIS POLICY AND ANY ACTION RELATED TO IT WILL BE GOVERNED AND INTERPRETED BY AND UNDER THE LAWS OF THE STATE OF DELAWARE, CONSISTENT WITH THE FEDERAL ARBITRATION ACT, WITHOUT GIVING EFFECT TO ANY PRINCIPLES THAT PROVIDE FOR THE APPLICATION OF THE LAW OF ANOTHER JURISDICTION. Any dispute, claim, or controversy arising out of or relating to this Policy, including the processing of your personal information by Asula, is subject to the dispute-resolution provisions set forth in Section 12 (Arbitration Agreement) of the Terms of Use, including the mandatory binding arbitration, class-action waiver, and thirty (30) day opt-out right described therein. Nothing in this Section 13 limits any non-waivable right you may have under applicable data-protection law to lodge a complaint with a supervisory authority, as described in Section 9.10.

14. **CONTACT INFORMATION.** If you have any questions about this Policy or our privacy practices, or if you wish to exercise a right described in Section 9, please contact us at:

ATTN: Asula Research Holdings Ltd. Address: 190 Elgin Avenue, George Town, Grand Cayman KY1-9001, Cayman Islands Email: krane@asula.xyz