

WHITECHAIN PRIVACY POLICY

Last Updated and Effective Date: August 13, 2026

INTRODUCTION AND SCOPE OF THE POLICY

This Privacy Policy (hereinafter referred to as the “**Policy**”) governs the collection, processing, and protection of personal data performed by Clear White Solutions Limited, registration number 2043789, having its registered address at: Intershore Chambers, P.O.Box 4342, Road Town, Tortola, British Virgin Islands (hereinafter referred to as “**Company**”, “**Whitechain**”, “**we**”, “**us**”, or “**our**”) regarding all individuals accessing or using the Whitechain websites and services, including <https://whitechain.io/>, <https://legacy.whitechain.io/>.

This Policy has been developed and implemented in strict compliance with Regulation (EU) 2016/679 (General Data Protection Regulation or “**GDPR**”) as well as applicable data protection laws of the British Virgin Islands, including the Data Protection Act, 2021 (“**DPA**”).

This Privacy Policy operates as an independent statutory disclosure framework. In the event of any operational discrepancy, variance, or interpretive contradiction between the provisions of this Policy and any other Company document specifically regarding the legal bases, security, or regulatory compliance of personal data processing, the provisions of this Privacy Policy shall control and govern to ensure absolute alignment with applicable data protection laws.

By accessing or using our platform or services, you acknowledge that you have read, understood, and recognize the data processing operations described in this Privacy Policy.

SECTION 1: CATEGORIES OF PROCESSED DATA

1.1. In strict adherence to the principle of data minimization set forth in Article 5(1)(c) of the GDPR, the Company collects and processes only those categories of data that are strictly necessary to fulfill the specific operational, legal, and contractual purposes detailed in this Policy. Depending on the nature of your interaction with the platform, the Company processes the following categories of data:

- **Identification, Contact, and Customer Support Data:** Personal parameters directly provided by the user through website forms, input fields, or direct communication channels (including email, phone, or post), such as your name, email address, Telegram handle, social media profile links (e.g., X/Twitter), developer repository links (e.g., GitHub) and general contact details. This category also encompasses any additional information, diagnostic records, or attachments you voluntarily disclose to our customer support team during service inquiries.
- **Project, Grant Applications, and Ecosystem Submission Data:** Operational, team, technical, and financial parameters relating to projects submitted to us (including via the Whitechain Builders Program, Typeform-powered intake forms, direct links, or ecosystem partnership channels). This encompasses: project name, category, development stage, current blockchain infrastructure, pitch materials, one-pagers, presentation links (hosted via third-party services such as DocSend, Google Drive, or Notion), activity descriptions, team structure, key personnel blockchain experience, business model details, traction metrics (including TVL, user base, transaction volume, revenue), funding history (grant sizes, FDV, valuation terms), planned

milestones, proposed use of funds, referral attribution details, technical documentation, and contact channels (applicant name, email, Telegram handle, X/Twitter, website, GitHub).

Third-Party Data Warranty: Where application materials or pitch decks contain personal data of third parties (such as team members, advisors, or investors), you represent and warrant that you have provided all necessary privacy notices and obtained all required legal authorizations to disclose such data to us for evaluation purposes.

- **Events, Giveaways, and Community Engagement Data:** Data required to facilitate your registration and participation in events, hackathons, or giveaways organized by or through Whitechain. This includes your language preferences, company affiliation, corporate title, public wallet address pointers, and email address.
- **Direct Marketing and Operational Communications Data:** Your email address that is processed for direct marketing communications, strictly where you have provided explicit prior consent in accordance with Article 6(1)(a) of the GDPR.
- **Automatically Collected Technical, Log, and Usage Telemetry:** Machine logs and diagnostic parameters transmitted automatically by your browser, device, or network client upon accessing or interacting with the Website, including: IP addresses, unique device identifiers, hardware model, browser type and version, operating system, language settings, and referring URLs, pages visited, navigation paths, search queries, button interaction logs, access timestamps, and email engagement metrics (such as email delivery status, open rates, and link click telemetry).
- **Third-Party Single Sign-On (SSO) and Web3 Authentication Data:** Public identifiers received when you access or authenticate on our platforms (such as Testnet Faucet or Bridge services) via third-party providers or protocols.

1.2. For the purposes of applicable data protection laws, including GDPR and the BVI Data Protection Act, the Company acts as the Data Controller in respect of all data collected and processed through the website and associated services. As the Data Controller, the Company independently determines the specific legal bases, operational purposes, and technical means governing the processing of your personal data.

SECTION 2: PURPOSES AND LEGAL BASES OF DATA PROCESSING

2.1. In accordance with Article 5(1)(a) of the GDPR, the Company is committed to processing your Personal Information lawfully, fairly, and in a transparent manner. Pursuant to Article 6 of the GDPR, every processing operation executed by Us rests upon a valid statutory legal basis.

Depending on your specific interactions with the Platform, We process relevant categories of Personal Information under the following purposes:

- To render, deliver, and maintain access to the website, its user interfaces, and core platform capabilities, as well as to ensure the proper technical functioning, stability, and seamless operational performance of our web infrastructure. Legal basis: GDPR Art. 6(1)(b) (Performance of a Contract / Provision of requested service) and GDPR Art. 6(1)(f) (Legitimate Interests in maintaining technical infrastructure).
- To process, investigate, manage, and respond to user inquiries, technical support requests, platform feedback, or general correspondence submitted through website contact forms, input fields, or direct email communication channels. Legal basis: GDPR Art. 6(1)(b) (Performance of a

contract / Pre-contractual steps) and GDPR Art. 6(1)(f) (Legitimate Interests in effective customer support).

- To review, evaluate, and process project proposals, pitch materials, technical documentation, and ecosystem integration applications (including those submitted through the Whitechain Builders Program or strategic partnership channels), and to conduct related pre-contractual assessment and due diligence. Legal basis: GDPR Art. 6(1)(b) (Steps prior to entering into a contract) and GDPR Art. 6(1)(f) (Legitimate Interests in risk assessment, ecosystem growth, and anti-fraud verification).
- To manage user registrations, verify eligibility, coordinate participant communication, distribute promotional rewards or grants, and facilitate community engagement across hackathons, events, or giveaways organized by or through Whitechain. Legal basis: GDPR Art. 6(1)(b) (Performance of a contract / Event terms) and GDPR Art. 6(1)(f) (Legitimate Interests in community growth).
- To dispatch promotional newsletters, ecosystem announcements, product updates, and marketing communications regarding Whitechain features, community initiatives, and partner offerings. Legal basis: GDPR Art. 6(1)(a) (Explicit Consent).
- To conduct technical diagnostics, evaluate user interface performance, perform internal staff training, measure platform usage trends, and continuously optimize software usability, system content, and functional features. Legal basis: GDPR Art. 6(1)(f) (Legitimate Interests in service optimization and quality assurance).
- To monitor system activity, detect and mitigate malicious network behavior or cyberattacks, prevent systemic fraud, protect user assets, and preserve the ongoing security, resilience, and operational integrity of our software infrastructure. Legal basis: GDPR Art. 6(1)(f) (Legitimate Interests in network security and threat prevention).
- To comply with applicable statutory, regulatory, or court-ordered obligations, respond to lawful law enforcement mandates, enforce our Terms of Use, and establish, exercise, or defend the Company's legal rights and assets in administrative, judicial, or arbitral proceedings. Legal basis: GDPR Art. 6(1)(c) (Compliance with a legal obligation) and GDPR Art. 6(1)(f) (Legitimate Interests in legal defense).
- To authenticate user sessions, prevent Sybil attacks, and provide access to interactive infrastructure (such as Testnet Faucet or Bridge interfaces) via OAuth protocols (e.g., GitHub) or Web3 wallet connection protocols (e.g., WalletConnect). Legal basis: GDPR Art. 6(1)(b) (Performance of a Contract / Provision of requested service).
- To evaluate, conduct due diligence on, and administer project grant applications, Builders Program submissions, and ecosystem partnerships (including data collected via third-party form service providers like Typeform). Legal basis: GDPR Art. 6(1)(b) (Steps prior to entering into a contract) and GDPR Art. 6(1)(f) (Legitimate Interests in risk assessment, ecosystem growth, and anti-fraud verification).
- To facilitate, introduce, and execute third-party service connections, ecosystem integrations, or partnership opportunities upon the user's explicit request or initiative. Legal basis: GDPR Art. 6(1)(b) (Performance of a contract / Pre-contractual steps at the data subject's request) and GDPR Art. 6(1)(a) (Explicit Consent, where applicable).

2.2. Personal data may be processed for other purposes only when such objectives are transparently disclosed at the time of collection, authorized via explicit user consent, or executed under direct user instruction.

SECTION 3: DATA SHARING

3.1. Processed data is **never** sold, rented, leased, or traded to third-party marketing networks, advertising brokers, or analytical profiling agencies. This non-sale commitment does not restrict or limit necessary operational data transfers to authorized ecosystem partners, grant evaluators, or service providers executed under Section 3.2 upon user initiative or for program administration purposes.

3.2. To ensure the continuous operation, delivery, and programmatic execution of the Services, the Company reserves the right to disclose or make accessible necessary technical data parameters and machine logs to third-party infrastructure providers, technical intermediaries, or operational partners. Such disclosures are executed strictly to the extent required to perform our contractual obligations, fulfill User-initiated protocol commands, or maintain overall network resilience under Article 6(1)(b) of the GDPR (*Performance of a Contract*) and Article 6(1)(f) of the GDPR (*Legitimate Interests*). These authorized functional operational categories include:

- Authorized operators and network validation software integrations, utilized strictly to transmit technical protocol parameters and facilitate automated programmatic routing across the Whitechain ecosystem;
- Infrastructure partners used to send essential transactional notifications, administrative alerts, account updates, or critical operational communications;
- Cloud service hosting, data storage, enterprise security, and monitoring providers leveraged to preserve system stability, DDoS protection, and operational integrity;
- Error-tracking, telemetry, and performance monitoring providers operating under strict data processing agreements to identify network bugs, system latency, and software faults;
- Third-party form management and data collection software providers (specifically Typeform SL), acting as Data Processors under data processing agreements to securely collect, structure, and route application forms and user responses;
- Identity authentication and connection protocol providers (such as GitHub, Inc. or WalletConnect, Inc.), strictly to the extent necessary to verify credentials, exchange OAuth tokens, or establish wallet session connections initiated directly by the user;
- Ecosystem partners, engaged in the review, scoring, due diligence, and administration of the Whitechain Builders Program or associated grant initiatives, strictly on a need-to-know basis;
- Third-party service providers, strategic partners, or independent operators, where the transfer of data is directly requested, initiated, or authorized by you (for example, when you request an introduction, opt into a partner integration, or apply for programs).

3.3. We may disclose processed data when required by applicable laws or regulations, or when such disclosure is strictly necessary to comply with an enforceable mandate from a competent court, regulatory authority, or law enforcement body having lawful jurisdiction over the Company. This framework includes:

- Responding to valid, legally binding judicial orders, subpoenas, search warrants, or official regulatory requests issued by authorized public bodies within a jurisdiction to which the Company is legally subject in accordance with Article 6(1)(c) GDPR;
- Executing mandatory operations required to investigate potential fraudulent or malicious network activities, protect the security of our software infrastructure, or establish, exercise, and defend the Company's legal rights and assets in legal proceedings in accordance with Article 6(1)(f) GDPR.

3.4. We may share limited Personal Information with third-party marketing and advertising networks, but only where you have given your explicit prior consent to such sharing for marketing purposes in accordance with Article 6(1)(a) of the GDPR. You maintain the unconditional right to withdraw your consent for marketing communications and associated data sharing at any time.

3.5. In the event that the Company is involved in a merger, acquisition, corporate reorganization, assignment, asset sale, or any structural transition of its operational business, the processed technical data arrays, log histories, and workspace metrics recorded within the platform may be transferred to the successor legal entity as an integrated component of the underlying technology transfer. Upon the execution of such a corporate transition, the successor entity shall assume the role of data controller, inheriting the operational management of the relevant processing activities. The continued interaction with the platform interface by the User following the effective date of such a transition shall serve as acknowledgment of the operational transfer. In any such scenario, the Company or its legal successor will ensure that your personal data continues to be protected under standards at least equivalent to those set forth in this Policy.

3.6. Where We anonymize Personal Information so that it can no longer be directly or indirectly linked to or identify you, the resulting information is no longer considered Personal Information under the GDPR. Consequently, the Company reserves the right to process, retain, and share such anonymized, de-identified, or aggregated datasets with third parties for research, statistical analysis, network metrics benchmarking, or system optimization purposes without further legal restriction.

SECTION 4: INTERNATIONAL DATA TRANSFER

4.1. Where personal data collected from individuals in the European Economic Area (EEA) is transferred to, stored, or processed in third countries outside the EEA — including the British Virgin Islands (where the Company is incorporated) or vendor, server, and operational partner locations globally — the Company ensures that all such cross-border transfers strictly comply with the requirements of Chapter V of the EU GDPR. To guarantee an equivalent level of protection, such transfers rely on the European Commission's approved Standard Contractual Clauses under Article 46(2)(c) of the GDPR with the data importer, supplemented by necessary technical and organizational measures.

SECTION 5: DATA RETENTION

5.1. The Company retains processed data strictly for the duration necessary to fulfill the purposes detailed in Section 2, preserve network security and system integrity, or comply with applicable mandatory statutory record-keeping requirements. Notwithstanding any automated deletion schedules, core security audit trails, internal system event logs, and IP metadata associated with infrastructure breaches or network anomalies shall be contractually exempted from immediate deletion and retained longer exclusively to the extent required to resolve active technical investigations, mitigate systemic fraud, or establish and defend legal positions within authorized arbitral venues.

Personal data and evaluation records submitted as part of the Builders Program or grant application process shall be retained for the duration of the evaluation period and, for successful applicants, throughout the term of the grant agreement plus applicable statutory limitation periods. Unsuccessful application records shall be purged or anonymized within twelve (12) months following the completion of the review cycle, unless further retention is requested by the applicant for future cohort consideration.

5.2. Data retention management is systematically governed by the structural principles of data minimization and automated platform optimization. If a user interaction completely ceases active operations on the Company's infrastructure for a continuous duration exceeding ninety (90) consecutive calendar days, all coincident technical telemetry records, web session history logs, and temporary operational caches shall be automatically and permanently purged from active operational databases. While such technical logs are promptly erased from live operational environments, residual data nodes may temporarily persist within encrypted, isolated recovery backups and system archives until such storage mediums are overwritten in accordance with the Company's automated server backup rotation cycles, which shall not exceed an additional sixty (60) calendar days.

5.3. To ensure strict alignment with data protection principles, the Company systematically conducts periodic reviews of all retained data against our operational objectives, legal basis, and statutory storage requirements. If, upon such review, it is determined that specific data is no longer necessary for the purposes for which it was originally collected or legally mandated to be retained, the Company shall ensure that such data is promptly deleted, permanently purged, or fully anonymized without unreasonable delay.

SECTION 6: DATA SECURITY

6.1. We implement appropriate technical and organisational measures to protect collected data against unauthorised or unlawful processing and against accidental loss, destruction or damage, in accordance with Art. 32 GDPR, taking into account the state of the art, the costs of implementation, and the risk to individuals.

6.2. While the Company implements robust technical and organizational security measures designed to safeguard data against unauthorized access, alteration, disclosure, or destruction, no method of electronic transmission over the Internet or method of digital storage can be guaranteed as completely secure. Consequently, while the Company endeavors to protect your data using industry-standard security protocols, the Company cannot warrant or guarantee its absolute security. You acknowledge and agree that you are also responsible for taking reasonable and appropriate precautions to protect your own information.

6.3. To mitigate internal vulnerabilities and enforce operational privacy boundaries, personnel workflows are governed by the following strict administrative protocols:

- Access Control: Internal administrative access to databases is strictly restricted on a *need-to-know* basis.
- Confidentiality: All system operators and engineers are bound by legally enforceable non-disclosure agreements.
- Security Audits: Infrastructure patches and system configurations are regularly reviewed to counter emerging threats.

SECTION 7: PRIVACY RIGHTS

7.1. Depending on your location (e.g., if you are in the EEA/UK), you may have the following rights regarding your data:

- Right of Access — You may request confirmation whether we process your personal data and, if so, obtain a copy of that data.
- Right to Rectification — You may request the correction of inaccurate or incomplete active configuration parameters within your workspace settings. This right applies strictly to User-configurable variables (such as your designated email pointer or destination wallet layout) and programmatically excludes any retrospective modification of automatically recorded historical machine telemetry, share logs, or network validation metrics, except where mandatory statutory obligations apply or where processing takes place outside non-amendable public ledger structures.
- Right to Erasure — You may request the deletion of your personal data, subject to legal obligations that may require us to retain certain information.
- Right to Restriction of Processing — You may request that we restrict the processing of your personal data in certain circumstances.
- Right to Data Portability — You may request to receive the specific technical variables you have directly provided to the Platform under contract in a structured, commonly used, and machine-readable format. In strict accordance with applicable regulations, this right shall not adversely affect the rights, freedoms, or trade secrets of others, and explicitly excludes any extraction rights over the Company's proprietary hash-balancing algorithms or aggregate internal ledger infrastructure systems, save for user-provided data required to be portable pursuant to Article 20 GDPR.
- Right to Object — You have the right to object to the processing if it is carried out on a legal basis other than consent.
- Right to Lodge a Complaint: You have the right to lodge a complaint with a competent supervisory authority if you believe We have infringed your rights.

7.2. To exercise any valid privacy rights outlined in Section 7.1, requests must be transmitted directly to support@whitechain.io.

7.3. Pursuant to Article 11(2) and Article 12(6) of the GDPR, the execution of any data subject request under Section 7.1 is strictly conditional upon the User providing additional information necessary to verify their identity and confirm technical control over the requested dataset. To preserve infrastructure security and prevent unauthorized data extraction, the Company reserves the right to require Users to authenticate their authorization through platform-designated validation procedures. Failure to satisfy these technical authentication thresholds shall result in the rejection of the request due to the objective impossibility of verifying the identity of the data subject.

SECTION 8: CHILDREN'S PRIVACY

8.1. The website and services offered by Whitechain are strictly intended for adult users and are not directed to, marketed to, or designed for children. The Company does not knowingly solicit, collect, store, or process data from individuals under the age of eighteen (18) years (or the applicable statutory age of majority / digital consent in your jurisdiction). If you are under the required age threshold, you are expressly prohibited from accessing the platform or submitting any data through our interfaces.

8.2. If the Company discovers or is formally notified that it has inadvertently collected or processed personal data from a child under the applicable age limit without verified parental or legal guardian consent, the Company shall initiate immediate internal verification procedures. Upon confirmation, the Company will take all necessary technical and organizational measures to permanently delete such data from our active databases, system logs, and operational caches without undue delay.

8.3. If you are a parent or legal guardian and have reason to believe that your child has provided personal data to us without appropriate consent, please contact our Data Protection Team immediately at support@whitechain.io.

SECTION 9: AUTOMATED DECISION-MAKING PROHIBITION

9.1. The Company does not utilize Personal Information collected through the website or services for automated decision-making, including profiling, that produces legal effects concerning you or similarly significantly affects you within the meaning of Article 22 of the GDPR.

9.2. While technical features, decentralized node interactions, or smart contract interfaces may execute automated programmatic logic initiated directly by the User, such automated routing does not constitute automated individual decision-making, behavioral scoring, or profiling under applicable data protection legislation. All administrative, compliance, and account-level determinations remain subject to human review and oversight.

SECTION 10: CHANGES TO THIS POLICY

10.1. The Company retains the unilateral right to amend, update, modify, or overhaul any portion of this Privacy Policy at any time to reflect shifting regulatory mandates, technical infrastructure optimizations, or operational data-routing modifications. Any updated version of this Policy will be deployed directly on the Platform, with the dynamic "Last Updated and Effective Date" modified at the very top of the document. For material modifications that substantially alter the scope, categories, or legal bases of data processing, the Company shall provide a general conspicuous programmatic announcement within the Platform's graphical workspace dashboard interface prior to or concurrent with the implementation of such updates to satisfy corporate transparency benchmarks.

SECTION 11: DISPUTE RESOLUTION

11.1. This Privacy Policy, alongside any non-contractual obligations or infrastructural data disputes arising out of or in connection with it, shall be governed by, and construed exclusively in accordance with, the laws of England and Wales, without reference to its choice of law or conflict of laws principles. Subject to the regulatory carve-out specified in Section 11.2, any controversy, claim, technical divergence, or dispute arising out of or relating to this Policy, including its formation, interpretation, breach, or validity, shall be referred to and finally and exclusively resolved by binding, confidential, individual arbitration under the Arbitration Rules of the London Court of International Arbitration (LCIA) in force at the time of commencement. The seat, or legal place, of the arbitral proceedings shall be London, United Kingdom. The tribunal shall consist of one single independent arbitrator selected in strict accordance with the LCIA Rules, and the language to be utilized throughout the entire proceedings shall be English.

11.2. In strict conformity with mandatory international data protection frameworks, nothing in this Section shall impair, block, or prejudice the User's statutory right to lodge an administrative complaint or technical reporting alert with a competent supervisory data protection authority.

In strict accordance with Article 79 of the GDPR, nothing in this Section shall prejudice or impair the statutory right of users residing within the EEA or the United Kingdom to bring data protection claims before the competent judicial authorities of the EU Member State or UK jurisdiction where they have their habitual residence. For all other jurisdictions, or where such statutory consumers carves-out do not apply by law, any civil causes of action, contractual disputes, or claims for material or non-material compensation arising directly out of the technical data processing operations of this Policy shall be exclusively and finally resolved via the individual, confidential LCIA arbitral framework detailed in Section 11.1. Class-wide actions and collective multi-party damages claims are irrevocably waived to the maximum extent permitted by applicable law.

11.3. This Privacy Policy is executed in the English language. In the event of any operational discrepancy, translation variance, or interpretive contradiction between the English version and any translated version deployed on the Platform, the English language text shall control, govern, and prevail in all circumstances.

SECTION 12: CONTACT US

If you have any questions regarding this Policy, please do not hesitate to contact us using the contact details below:

Contact details:

Clear White Solutions Limited

Registration Number: 2043789

Registered Address: Intershore Chambers, P.O.Box 4342, Road Town, Tortola, British Virgin Islands

General Privacy Email: support@whitechain.io