

PRIVACY POLICY

Effective Date: August 8th, 2026

This Privacy Policy ("**Policy**") describes how Ridgeline Mining, along with its affiliates ("**Ridgeline**," "**we**," "**us**," or "**our**") collects, uses, discloses, and protects personal information in connection with our blockchain Hashrate Contract services, web dashboard, mining operations, and related products and services (collectively, the "**Services**"). This Policy applies to information collected through our website, customer portal, mobile applications, and other platforms where this Policy is posted or referenced.

Ridgeline is based in the United States and provides Services to customers worldwide. Depending on your location, different privacy laws and regulations may apply to our processing of your personal information. This Policy identifies applicable legal frameworks and your rights under those laws.

ARTICLE 1 – SCOPE AND APPLICATION

- I. Geographic Scope.** This Policy applies to all users and customers of Ridgeline Services, regardless of geographic location. We process personal information in accordance with applicable privacy laws in the jurisdictions where our customers reside, including but not limited to:
 - A. United States Federal Law:** Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA) where applicable, CAN-SPAM Act, and sector-specific regulations.
 - B. U.S. State Privacy Laws:** California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA), Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA), and other applicable state privacy statutes.
 - C. European Economic Area and United Kingdom:** General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and UK GDPR as retained under the Data Protection Act 2018.
 - D. Other Jurisdictions:** Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial privacy laws,

Brazil's Lei Geral de Proteção de Dados (LGPD), Australia's Privacy Act 1988, and other applicable data protection and privacy laws.

II. Services Covered. This Policy covers all Ridgeline Services, including:

- A.** Blockchain Hashrate Contracts and the underlying Bitcoin and Bitcoin Cash mining operations we perform pursuant to those contracts.
- B.** Our web-based customer dashboard that allows customers to observe detailed contract information and adjust mining parameters.
- C.** Bitcoin and Lightning Network payout processing and wallet integration.
- D.** Commercial Forge and Frontier deployment services, including facility assessments and equipment monitoring.
- E.** Customer support, promotional communications, and account services.

III. Updates to this Policy. We may update this Policy periodically to reflect changes in our practices, Services, or applicable law. We will post the revised Policy with a new Effective Date and, where required by law, provide advance notice or obtain consent before material changes take effect. Your continued use of the Services after the Effective Date constitutes acceptance of the updated Policy.

ARTICLE 2 – PERSONAL INFORMATION WE COLLECT

We collect the following categories of personal information in connection with providing our Services:

I. Identifiers and Contact Information.

- A.** Name, email address, telephone number, mailing address, date of birth, and billing address.
- B.** Account credentials, including username and password.
- C.** Authentication information, including email authentication tokens.

II. Financial and Payment Information.

- A.** Bitcoin wallet addresses and Lightning Network addresses for payout processing.

- B. Transaction identifiers, payout records, account balances, and accrual histories.
- C. Payment confirmation data received from third-party payment processors. We do not directly collect or store payment card information when customers select credit card payment methods; such information is processed by third-party payment processors.

III. Identity Verification and Compliance Data.

- A. Know Your Customer (KYC) verification results and identity documentation required to comply with anti-money laundering (AML), sanctions screening, fraud prevention, and other legal requirements.

IV. Hashrate Contract and Account Information.

- A. Hashrate Contract details, purchase history, contract assignments, mining earnings and accruals, payout history, and portfolio values.
- B. Customer selections regarding mining parameters, including allocation between Bitcoin and Bitcoin Cash mining.

V. Device and Technical Information.

- A. IP addresses, device identifiers, browser type and version, operating system, and device settings.
- B. Login history, session data, activity logs, and usage patterns within the customer dashboard.
- C. Precise or approximate geolocation information derived from IP addresses or provided by the user.

VI. Communications and Support Records.

- A. Communications with customer support, including email correspondence, recorded phone calls, chat transcripts, and support ticket histories.
- B. Feedback, inquiries, survey responses, and other voluntary communications.

VII. Commercial and Deployment Information.

- A. Information submitted by commercial customers through proposals, site assessments, contracts, and deployment agreements.

- B. Facility information, energy usage data, equipment specifications, utility account details, and operational performance data related to Forge and Frontier deployments.

VIII. Marketing and Promotional Content.

- A. Photos, videos, audio recordings, quotes, testimonials, case study materials, and other content provided by customers for marketing purposes.

IX. Employment Application Information.

- A. Information provided by employment applicants, including resumes, cover letters, application forms, and interview notes.

X. Third-Party Service Integration Data.

- A. Information obtained through OAuth authentication and wallet linking with third-party services, including Pura Vida Bitcoin (our current default Lightning wallet provider) for optional authentication and Bitcoin/Lightning payment processing.

ARTICLE 3 – SOURCES OF PERSONAL INFORMATION

We collect personal information from the following sources:

- I. **Directly from You.** Most personal information is provided directly by customers and users when creating accounts, purchasing Hashrate Contracts, configuring dashboard settings, submitting support requests, engaging in commercial transactions, applying for employment, or otherwise interacting with our Services.
- II. **Automatically Through Technology.** We automatically collect device and technical information, IP addresses, activity logs, and usage data through cookies, web beacons, log files, and similar tracking technologies when you access or use our Services.
- III. **Third-Party Service Providers.** We receive information from:
 - A. Payment processors that confirm order payments when customers select credit card or other third-party payment methods.
 - B. Identity verification and KYC service providers that perform compliance screening.

C. Pura Vida Bitcoin and other wallet providers when customers authenticate or link external wallets.

D. Analytics providers, fraud prevention services, and security vendors.

IV. Blockchain Networks. We collect and observe transaction identifiers, wallet addresses, and payment records from public blockchain networks (Bitcoin and Lightning Network) in connection with mining payouts.

V. Public and Commercial Sources. We may collect information from publicly available sources, commercial data providers, and business contact databases for commercial customer outreach and verification purposes.

ARTICLE 4 – PURPOSES AND LEGAL BASES FOR PROCESSING

I. Purposes of Use. We use personal information for the following purposes:

A. Account and Service Operations:

1. Creating, maintaining, and securing customer accounts.
2. Processing Hashrate Contract purchases, payments, contract assignments, mining accruals, and Bitcoin payouts.
3. Providing access to and operating the customer dashboard, portal features, and account management tools.
4. Delivering customer support, responding to inquiries, and managing account communications.

B. Compliance and Security:

1. Verifying customer identity and satisfying KYC, AML, sanctions screening, fraud prevention, and other legal and regulatory requirements.
2. Protecting Ridgeline, our users, infrastructure, and legal rights against fraud, security threats, and unlawful activity.
3. Complying with tax, accounting, regulatory reporting, subpoena responses, and recordkeeping obligations.

C. Service Improvement and Development:

1. Operating, maintaining, and improving our website, portal, products, mining infrastructure, and Services.
2. Monitoring performance of Forge and Frontier equipment and deployment operations.
3. Conducting analytics, research, product development, and AI-assisted analysis to enhance user experience and operational efficiency.

D. Marketing and Communications:

1. Sending promotional emails, text messages, newsletters, and product updates.
2. Personalizing advertisements and measuring advertising performance.
3. Creating and distributing marketing materials, including customer testimonials and case studies.

E. Corporate Transactions:

1. Supporting corporate transactions such as financing, mergers, acquisitions, asset sales, or other business combinations.

II. Legal Bases for Processing (GDPR, UK GDPR, and Similar Regimes). For users in the European Economic Area, United Kingdom, and other jurisdictions requiring a legal basis for processing, we rely on the following:

A. Contractual Necessity: Processing necessary to perform our contract with you, including account creation, Hashrate Contract fulfillment, payment processing, dashboard access, and customer support.

B. Legal Obligation: Processing required to comply with applicable laws, including KYC/AML requirements, tax obligations, regulatory reporting, and responses to lawful requests from authorities.

C. Legitimate Interests: Processing necessary for our or a third party's legitimate interests, including:

1. Fraud prevention, security, and protection of our systems and users.

2. Service improvement, analytics, research, and product development.
3. Marketing to existing customers regarding similar services (subject to opt-out rights).
4. Corporate transactions and business operations.

We balance these interests against your rights and do not process personal information where your interests or fundamental rights override our legitimate interests.

D. Consent: Where required by law, we obtain your explicit consent for specific processing activities, including certain marketing communications, optional third-party integrations (e.g., Pura Vida Bitcoin OAuth), and use of non-essential cookies and tracking technologies. You may withdraw consent at any time without affecting the lawfulness of processing based on consent before withdrawal.

ARTICLE 5 – DISCLOSURE AND SHARING OF PERSONAL INFORMATION

I. Categories of Recipients. We disclose personal information to the following categories of recipients:

A. Service Providers and Processors: Third-party vendors that perform services on our behalf, including:

1. Payment processors and financial institutions.
2. Identity verification and KYC/AML and sanctions screening providers.
3. Blockchain wallet and Lightning Network service providers, including Pura Vida Bitcoin.
4. Cloud hosting, data storage, and infrastructure providers.
5. Customer support platforms and communication tools.
6. Analytics, marketing, and advertising service providers.
7. Security, fraud prevention, and monitoring services.
8. Equipment vendors and deployment contractors for Forge and Frontier services.

- B. Business Partners:** Commercial partners, affiliates, and co-marketing entities where you have consented to such sharing or where necessary to deliver requested services.
- C. Corporate Transaction Parties:** Potential or actual acquirers, investors, advisors, and other parties involved in corporate transactions such as mergers, acquisitions, financing, asset sales, or bankruptcy proceedings.
- D. Legal and Regulatory Authorities:** Government agencies, law enforcement, regulators, tax authorities, and courts when required by law, legal process, subpoena, court order, or to protect our rights, property, safety, or that of our users.
- E. Professional Advisors:** Attorneys, accountants, auditors, insurers, and other professional advisors in connection with legal, financial, compliance, and risk management matters.

II. Blockchain Disclosures. Because Bitcoin and Bitcoin Cash transactions occur on public, decentralized blockchain networks, payout transactions to your wallet address are publicly visible and permanently recorded on the blockchain. We do not control blockchain networks and cannot modify or delete blockchain transaction records.

III. No Sale of Personal Information (U.S. State Law Context). Ridgeline does not "sell" personal information as defined under the CCPA/CPRA or other U.S. state privacy laws. We do not exchange personal information for monetary consideration. Certain data sharing with advertising partners or analytics providers may be considered "sharing" for cross-context behavioral advertising under some state laws; see Article 11 for opt-out rights.

IV. International Transfers. Ridgeline is based in the United States. Personal information collected from users worldwide may be transferred to, stored in, and processed in the United States and other countries where our service providers operate. These jurisdictions may have data protection laws different from those in your country of residence. Where required by applicable law (including GDPR and UK GDPR), we implement appropriate safeguards for international transfers, such as Standard Contractual Clauses approved by the European Commission or UK authorities, adequacy decisions, or other legally recognized transfer

mechanisms. For more information about our international transfer safeguards, please contact us at support@ridgeline mining.com.

ARTICLE 6 – COOKIES, TRACKING TECHNOLOGIES, AND ANALYTICS

- I. Types of Technologies Used.** We and our service providers use cookies, web beacons, pixels, local storage, log files, and similar tracking technologies to collect device and technical information, recognize returning users, analyze usage patterns, and deliver personalized content and advertising.
- II. Categories of Cookies and Tracking.**
 - A. Strictly Necessary:** Technologies essential for operating our Services, including authentication, security, session management, and dashboard functionality. These cannot be disabled without impairing core functionality.
 - B. Performance and Analytics:** Technologies that collect aggregated and anonymized usage data to understand how users interact with our Services, identify performance issues, and inform product improvements.
 - C. Functional:** Technologies that enable enhanced features such as language preferences, user settings, and customized dashboard displays.
 - D. Advertising and Marketing:** Technologies used to deliver targeted advertisements, measure advertising effectiveness, and track conversions across websites and platforms.
- III. Third-Party Analytics and Advertising.** We use third-party analytics services (such as Google Analytics) and advertising networks that may collect information about your online activities over time and across different websites. These providers may use their own cookies and tracking technologies subject to their respective privacy policies.
- IV. Your Choices.** Where required by law, we obtain consent before deploying non-essential cookies. You may manage cookie preferences through:
 - A. Browser settings** that allow you to refuse or delete cookies (note that disabling cookies may limit functionality).

ARTICLE 7 – BLOCKCHAIN TRANSACTIONS AND DASHBOARD DATA

- I. **Public Blockchain Nature.** Bitcoin and Bitcoin Cash transactions are processed on public, decentralized blockchain networks. Once a payout transaction is broadcast to the blockchain:
 - A. The transaction, including the recipient wallet address, amount, and transaction identifier, becomes publicly visible and permanently recorded on the blockchain.
 - B. Blockchain data is not controlled by Ridgeline and cannot be modified, deleted, or restricted after confirmation.
 - C. Blockchain records may be indexed by third-party blockchain explorers and analytics services.
- II. **Dashboard Data.** The Ridgeline web dashboard displays:
 - A. Detailed information about your Hashrate Contracts, mining allocations (Bitcoin vs. Bitcoin Cash), earnings, accruals, and payout history.
 - B. Account activity logs, login history, and parameter adjustment records.
 - C. Portfolio values and performance metrics.

Dashboard data is stored on our secure servers and accessible only to authenticated account holders and authorized Ridgeline personnel. We implement technical and organizational security measures to protect dashboard data as described in Article 9.

- III. **Wallet Address Privacy.** Your Bitcoin and Lightning wallet addresses are collected and used solely for payout processing. We do not publicly associate your wallet addresses with your identity except as visible on the blockchain. However, blockchain analysis techniques may allow third parties to infer connections between wallet addresses and identities.

ARTICLE 8 – DATA RETENTION

- I. **Retention Principles.** We retain personal information for as long as necessary to fulfill the purposes described in this Policy, comply with legal obligations, resolve disputes, enforce agreements, and protect our legal rights.
- II. **Retention Periods by Category.**

- A. Account and Contract Data:** Retained for the duration of the customer relationship and for seven (7) years following contract termination or account closure to satisfy tax, accounting, and regulatory recordkeeping requirements.
- B. KYC and Compliance Data:** Retained for seven (7) years following account closure or transaction completion as required by AML, sanctions, and financial regulatory obligations.
- C. Payment and Transaction Records:** Retained for seven (7) years to comply with tax and financial reporting obligations.
- D. Communications and Support Records:** Retained for seven (7) years to resolve disputes, improve customer service, and satisfy legal hold or litigation requirements.
- E. Marketing and Analytics Data:** Retained until you opt out or withdraw consent, or for five (5) years if no active engagement occurs, unless longer retention is required by law.
- F. Employment Application Data:** Retained for five (5) years following application submission, or longer if required by employment law or if the applicant consents.
- G. Blockchain Data:** Permanently recorded on public blockchains and beyond our control; we retain off-chain references to blockchain transactions as part of account and payout records per the periods above.

III. Deletion and Anonymization. Upon expiration of applicable retention periods, we securely delete or anonymize personal information unless continued retention is required by law, legal hold, ongoing dispute, or legitimate business need. Anonymized data that cannot reasonably be re-identified may be retained indefinitely for analytics and research.

ARTICLE 9 – SECURITY MEASURES

- I. Technical and Organizational Safeguards.** We implement industry-standard technical and organizational measures designed to protect personal information against unauthorized access, disclosure, alteration, destruction, and loss, including:

- A. Encryption of data in transit using TLS/SSL protocols and encryption of sensitive data at rest.
 - B. Access controls, authentication mechanisms, and role-based permissions limiting access to personal information to authorized personnel and service providers with a legitimate need to know.
 - C. Regular security assessments and/or vulnerability scanning, penetration testing, and monitoring for security incidents.
 - D. Secure development practices, code reviews, and change management procedures.
 - E. Incident response plans and breach notification procedures aligned with applicable legal requirements.
- II. Third-Party Security.** We require service providers and processors to implement appropriate security measures and handle personal information in accordance with our instructions and applicable law. However, we cannot guarantee the security practices of third-party blockchain networks, wallet providers, or external platforms.
- III. User Responsibilities.** You are responsible for maintaining the confidentiality of your account credentials, securing your devices, and protecting your Bitcoin and Lightning wallet private keys. Ridgeline is not responsible for unauthorized access resulting from your failure to safeguard credentials or wallet keys.
- IV. No Absolute Security.** No method of transmission or storage is completely secure. While we strive to protect personal information, we cannot guarantee absolute security. You provide personal information at your own risk.

ARTICLE 10 – INDIVIDUAL RIGHTS AND CHOICES

- I. General Rights.** Depending on your jurisdiction, you may have the following rights regarding your personal information:
- A. Access:** Request confirmation of whether we process your personal information and obtain a copy of that information.
 - B. Correction/Rectification:** Request correction of inaccurate or incomplete personal information.

- C. Deletion/Erasure:** Request deletion of your personal information, subject to legal exceptions (e.g., compliance, legal claims, contractual obligations).
 - D. Restriction/Objection:** Object to or request restriction of certain processing activities, including processing based on legitimate interests or for direct marketing purposes.
 - E. Data Portability:** Receive your personal information in a structured, commonly used, machine-readable format and transmit it to another controller (where technically feasible).
 - F. Withdraw Consent:** Withdraw consent for processing based on consent without affecting the lawfulness of prior processing.
 - G. Opt-Out:** Opt out of certain data practices such as targeted advertising, profiling, or sale/sharing of personal information (see Article 11 for U.S. state-specific rights).
 - H. Lodge a Complaint:** Lodge a complaint with a supervisory authority or data protection regulator if you believe your rights have been violated.
- II. Exercising Rights.** To exercise these rights, please contact us at support@ridgeline mining.com. We will respond to verified requests within the timeframes required by applicable law (or 30 days, if earlier, with possible extensions to fully-perform our duties in satisfaction of such requests where permitted). We may request additional information to verify your identity before fulfilling requests.
- III. Limitations on Rights.** Certain rights may be limited by applicable law or where necessary to:
- A.** Comply with legal obligations, regulatory requirements, or lawful requests from authorities.
 - B.** Establish, exercise, or defend legal claims.
 - C.** Fulfill contractual obligations or process transactions you have requested.
 - D.** Protect the rights, property, or safety of Ridgeline, our users, or third parties.
 - E.** Maintain the integrity and security of our systems and Services.

Additionally, blockchain transaction data is publicly recorded and cannot be modified or deleted from the blockchain.

ARTICLE 11 – U.S. STATE PRIVACY RIGHTS

- I. Applicability.** This Article applies to residents of U.S. states with comprehensive privacy laws, including California, Virginia, Colorado, Connecticut, and Utah. Rights and obligations vary by state; consult your state's law for specifics.
- II. Categories of Personal Information.** For U.S. state law purposes, we collect, use, and disclose the categories of personal information described in Articles 2-5, which may include:
 - A.** Identifiers (name, email, address, IP address, account credentials).
 - B.** Financial information (wallet addresses, transaction records, payment confirmations).
 - C.** Commercial information (contract details, purchase history, portfolio values).
 - D.** Internet or network activity (browsing data, device information, logs).
 - E.** Geolocation data.
 - F.** Audio, electronic, or visual information (support call recordings, testimonial content).
 - G.** Inferences drawn from personal information to create user profiles or preferences.
- III. Consumer Rights Under U.S. State Privacy Laws.**
 - A. Right to Know:** Request disclosure of the categories and specific pieces of personal information we have collected about you, the categories of sources, the business or commercial purposes for collection, and the categories of third parties with whom we share personal information.
 - B. Right to Delete:** Request deletion of personal information we have collected, subject to legal exceptions.
 - C. Right to Correct:** Request correction of inaccurate personal information (California, Virginia, Colorado, Connecticut).
 - D. Right to Opt Out:**

1. **Sale of Personal Information:** Opt out of the "sale" of personal information. As noted in Article 5, Ridgeline does not sell personal information.
2. **Sharing for Targeted Advertising:** Opt out of "sharing" personal information for cross-context behavioral advertising or targeted advertising (California, Colorado, Connecticut, Virginia).
3. **Profiling:** Opt out of profiling in furtherance of decisions that produce legal or similarly significant effects (Virginia, Colorado, Connecticut).

E. Right to Data Portability: Request a portable copy of personal information (where applicable under state law).

F. Right to Limit Use of Sensitive Personal Information: Limit use and disclosure of sensitive personal information to purposes necessary to perform services or provide goods requested by the consumer, or as otherwise permitted by law (California CPRA).

G. Non-Discrimination: You have the right not to receive discriminatory treatment for exercising your privacy rights. We will not deny goods or services, charge different prices, or provide a different level or quality of services solely because you exercised your rights, except as permitted by law.

IV. Exercising U.S. State Privacy Rights. To exercise these rights:

- A. Submit a request via support@ridgelinemining.com.
- B. We will verify your identity using information you previously provided and may request additional information to confirm your identity and residency.
- C. You may designate an authorized agent to submit requests on your behalf by providing written authorization. We may require the agent to verify their authority and may require you to verify your identity directly with us.
- D. We will respond within 45 days (with possible extension to 90 days where permitted), providing the requested information or explaining any denial.

V. California-Specific Disclosures.

A. Categories of Personal Information Collected (CCPA § 1798.110): See Article 2 for detailed categories, which include identifiers, financial

B. Categories of Sources: See Article 3.

C. Business or Commercial Purposes: See Article 4.

D. Categories of Third Parties: See Article 5.

E. Retention: See Article 8.

F. Sensitive Personal Information: We collect the following categories of sensitive personal information as defined by the CPRA: government-issued identifiers (for KYC/AML), financial account information (wallet addresses, transaction records), and precise geolocation. We use and disclose sensitive personal information only for purposes permitted under CPRA § 1798.121, including performing services requested by you, security and fraud prevention, and compliance with legal obligations.

G. Shine the Light (California Civil Code § 1798.83): California residents may request information about personal information disclosed to third parties for direct marketing purposes. Ridgeline does not disclose personal information to third parties for their direct marketing purposes without consent.

H. Do Not Track: Our Services do not currently respond to "Do Not Track" browser signals. However, you may opt out of targeted advertising as described in Articles 6 and 11.

VI. Colorado, Connecticut, Virginia, and Utah Residents. Residents of these states have similar rights as described above. Virginia, Colorado, and Connecticut residents may appeal a denial of a rights request; we will provide appeal instructions in our response. Utah residents have a narrower right to opt out of targeted advertising and sale (as applicable).

VII. Opt-Out Preference Signals. To the extent required by applicable state law and relevant to our Services, we will honor opt-out preference signals such as Global Privacy Control (GPC) transmitted by your browser or device as a valid opt-out request for targeted advertising and/or sale/sharing of personal information.

ARTICLE 12 – GDPR AND UK GDPR RIGHTS (EUROPEAN ECONOMIC AREA AND UNITED KINGDOM RESIDENTS)

- I. Applicability.** This Article applies to individuals located in the European Economic Area (EEA), United Kingdom, and Switzerland whose personal data is processed under the GDPR or UK GDPR.
- II. Data Controller.** Ridgeline Mining, 30 N Gould St Ste N, Sheridan, WY 82801, is the data controller responsible for your personal data processed in connection with the Services.
- III. Legal Bases for Processing.** We process your personal data on the legal bases described in Article 4, Section II, including:
 - A.** Performance of our contract with you for account creation, Hashrate Contract fulfillment, dashboard access, payment processing, and customer support.
 - B.** Compliance with legal obligations, including KYC/AML requirements, tax obligations, and responses to lawful requests.
 - C.** Legitimate interests for fraud prevention, security, service improvement, analytics, business operations, and direct marketing to existing customers regarding similar services (subject to your right to object).
 - D.** Your explicit consent where required, including for certain marketing communications, optional third-party integrations, and non-essential cookies.
- IV. Your Rights Under GDPR and UK GDPR.** You have the following rights:
 - A. Right of Access (Article 15):** Obtain confirmation of whether we process your personal data and receive a copy of that data along with supplementary information about the processing.
 - B. Right to Rectification (Article 16):** Request correction of inaccurate or incomplete personal data.
 - C. Right to Erasure / "Right to be Forgotten" (Article 17):** Request deletion of your personal data where:
 - 1.** The data is no longer necessary for the purposes for which it was collected.

2. You withdraw consent (where processing is based on consent) and there is no other legal ground.
3. You object to processing based on legitimate interests and there are no overriding legitimate grounds.
4. The data has been unlawfully processed.
5. Erasure is required to comply with a legal obligation.

This right is subject to exceptions where retention is necessary for compliance with legal obligations, establishment or defense of legal claims, or other lawful purposes. Note that blockchain transaction data cannot be deleted from public blockchains.

D. Right to Restriction of Processing (Article 18): Request restriction of processing where:

1. You contest the accuracy of the personal data (for the period necessary to verify accuracy).
2. Processing is unlawful and you oppose erasure and request restriction instead.
3. We no longer need the data but you require it for legal claims.
4. You have objected to processing based on legitimate interests (pending verification of overriding legitimate grounds).

E. Right to Data Portability (Article 20): Receive your personal data in a structured, commonly used, machine-readable format and transmit it to another controller where processing is based on consent or contract performance and carried out by automated means.

F. Right to Object (Article 21):

1. Object at any time to processing based on legitimate interests (including profiling), unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or the processing is necessary for establishment, exercise, or defense of legal claims.
2. Object at any time to processing for direct marketing purposes (including profiling related to direct marketing); we will cease such processing upon objection.

G. Right to Withdraw Consent (Article 7): Withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing based on consent before withdrawal.

H. Right Not to be Subject to Automated Decision-Making (Article 22): Not be subject to decisions based solely on automated processing, including profiling, that produce legal effects or similarly significantly affect you, except where necessary for contract performance, authorized by law, or based on your explicit consent. See Article 14 for information about automated decision-making.

I. Right to Lodge a Complaint: Lodge a complaint with a supervisory authority in the EEA member state of your habitual residence, place of work, or place of the alleged infringement if you believe our processing violates the GDPR. For UK residents, you may lodge a complaint with the UK Information Commissioner's Office (ICO) at <https://ico.org.uk>.

V. Exercising Your Rights. To exercise your rights, contact us at support@ridgeline-mining.com. We will respond within one month of receipt of a verified request, with possible extension to three months for complex or numerous requests (we will inform you of any extension within one month).

VI. International Transfers. We are located in the United States, and information you provide to us is transmitted to, stored, and processed in the United States. U.S. law may not provide the same level of protection as the law of your jurisdiction. Where we engage service providers located outside the EEA, the United Kingdom, or Switzerland and a recognized transfer mechanism is legally required, we put appropriate safeguards in place.

You may request a copy of the applicable safeguards by contacting us at support@ridgeline-mining.com.

ARTICLE 13 – OTHER INTERNATIONAL PRIVACY RIGHTS

I. Canada (PIPEDA and Provincial Laws).

A. Applicability: This section applies to individuals in Canada whose personal information is subject to the Personal Information Protection and Electronic Documents Act (PIPEDA) or substantially similar

provincial privacy laws (e.g., Alberta's Personal Information Protection Act, British Columbia's Personal Information Protection Act, Quebec's Act respecting the protection of personal information in the private sector).

B. Accountability and Consent: We are accountable for personal information under our control and obtain meaningful consent for collection, use, and disclosure except where permitted or required by law.

C. Your Rights: You may:

1. Access your personal information held by Ridgeline, subject to limited exceptions.
2. Request correction of inaccurate or incomplete information.
3. Withdraw consent for certain processing activities where consent is the legal basis, subject to legal or contractual restrictions.
4. Challenge our compliance with PIPEDA or applicable provincial laws.

D. Complaints: You may file a complaint with the Office of the Privacy Commissioner of Canada at <https://www.priv.gc.ca> or the applicable provincial privacy commissioner.

E. Contact: Direct privacy inquiries to support@ridgelinemining.com.

II. Australia (Privacy Act 1988).

A. Applicability: This section applies to individuals in Australia whose personal information is subject to the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

B. Collection Notification: We collect personal information as described in Articles 2 and 3. We notify you of the purposes of collection, recipients of disclosure, and your rights at or before the time of collection.

C. Your Rights: You may:

1. Request access to your personal information held by Ridgeline (APP 12).

2. Request correction of inaccurate, out-of-date, incomplete, irrelevant, or misleading personal information (APP 13).
3. Make a complaint about our handling of your personal information.

D. Overseas Disclosures: We may disclose personal information to overseas recipients located in the United States and other countries as described in Article 5. We take reasonable steps to ensure overseas recipients comply with the APPs or are subject to substantially similar privacy protections.

E. Complaints: You may lodge a complaint with us at support@ridgelineining.com. If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at <https://www.oaic.gov.au>.

III. Other Jurisdictions. If you are located in a jurisdiction not specifically addressed in this Policy and your jurisdiction has data protection or privacy laws, we will process your personal information in accordance with applicable local law. Contact us at support@ridgelineining.com for jurisdiction-specific inquiries.

ARTICLE 14 – AUTOMATED DECISION-MAKING AND PROFILING

I. Use of Automated Decision-Making. We may use automated systems and algorithms to:

- A.** Assess fraud risk, verify identity, and screen transactions for compliance with KYC/AML and sanctions requirements.
- B.** Personalize dashboard displays, recommend mining allocation strategies, and tailor communications based on your account activity and preferences.
- C.** Analyze usage patterns and conduct analytics for service improvement and product development.

II. Profiling. We may create profiles based on your interactions with the Services, including contract purchase history, mining preferences, dashboard activity, and communications, to personalize your experience, improve our Services, and deliver targeted marketing.

III. Solely Automated Decisions with Legal or Significant Effects. We do not make decisions based solely on automated processing, including profiling,

that produce legal effects concerning you or similarly significantly affect you, except where:

- A. Necessary for entering into or performing a contract with you (e.g., automated creditworthiness assessment if we offer financing options in the future).
- B. Authorized by applicable law with suitable safeguards.
- C. Based on your explicit consent.

In such cases, you have the right to obtain human intervention, express your point of view, and contest the decision (GDPR Article 22; similar rights under other laws).

IV. Your Rights. Where automated decision-making or profiling occurs, you may exercise your rights under Article 10, Article 11, or Article 12 (depending on your jurisdiction), including the right to object, request explanation of the logic involved, and challenge decisions.

ARTICLE 15 – CHILDREN AND AGE RESTRICTIONS

- I. **Age Limitations.** Our Services are not directed to children under the age of 18 (or the applicable age of majority in your jurisdiction). We do not knowingly collect personal information from children under 18 without verifiable parental consent as required by law, including the U.S. Children's Online Privacy Protection Act (COPPA) and equivalent international laws.
- II. **Parental Consent.** If you are under 18 and wish to use our Services, you must have the consent of a parent or legal guardian who agrees to be bound by this Policy and our Terms of Service on your behalf. By using the Services, a parent or guardian represents that they are at least 18 years old (or the age of majority) and authorize the minor's use and our collection of the minor's information.
- III. **Verification and Deletion.** If we learn that we have collected personal information from a child under 18 without verifiable parental consent (where required), we will take steps to delete that information promptly. If you believe we have inadvertently collected information from a child, please contact us immediately at support@ridgelinemining.com.

ARTICLE 16 – MARKETING COMMUNICATIONS AND OPT-OUT

- I. Marketing Messages.** We may send you promotional emails, text messages (SMS/MMS), push notifications, and other marketing communications regarding our Services, products, updates, offers, and related information.
- II. Consent and Legitimate Interest.** We send marketing communications:
 - A.** Based on your consent where required by law (e.g., for email marketing in certain jurisdictions, for SMS/text marketing under the U.S. Telephone Consumer Protection Act (TCPA) and similar laws).
 - B.** Based on legitimate interest where permitted (e.g., marketing similar services to existing customers under GDPR, subject to your right to object).
- III. Opt-Out Rights.** You may opt out of marketing communications at any time by:
 - A.** Clicking the "unsubscribe" link in promotional emails.
 - B.** Replying "STOP" to SMS/text messages.
 - C.** Adjusting notification preferences in your account dashboard settings.
 - D.** Contacting us at support@ridgeline mining.com with your opt-out request.

We will process opt-out requests promptly, typically within 10 business days. Note that opting out of marketing does not affect transactional or service-related communications (e.g., account notifications, contract confirmations, security alerts, customer support responses), which we may continue to send as necessary to provide the Services.

- IV. Third-Party Marketing.** We do not share your personal information with unaffiliated third parties for their own direct marketing purposes without your consent. If we partner with third parties for co-marketing activities, we will provide clear notice and choice mechanisms.

ARTICLE 17 – THIRD-PARTY LINKS AND SERVICES

- I. Third-Party Websites and Platforms.** Our Services may contain links to third-party websites, applications, blockchain explorers, wallet providers (including Pura Vida Bitcoin), payment processors, and other external platforms. This Policy does not apply to third-party services.

- II. No Responsibility for Third-Party Practices.** We are not responsible for the privacy practices, terms of use, security measures, or content of third-party services. Third-party services have their own privacy policies and terms, and your interactions with them are governed by those policies.
- III. Third-Party Integration.** When you connect third-party services (e.g., OAuth authentication with Pura Vida Bitcoin, linking external wallets), you authorize the sharing of information between Ridgeline and the third party as necessary to provide the integration. Review the third party's privacy policy before connecting.
- IV. Blockchain Explorers.** Public blockchain transaction data may be indexed and displayed by third-party blockchain explorers (e.g., Blockchain.com, Blockchair). We do not control these explorers and are not responsible for their use of publicly available blockchain data.

ARTICLE 18 – CHANGES TO THIS PRIVACY POLICY

- I. Right to Modify.** We reserve the right to update, modify, or replace this Policy at any time to reflect changes in our practices, Services, legal requirements, or for other operational, legal, or regulatory reasons.
- II. Notice of Changes.** When we make changes to this Policy:
 - A.** We will post the revised Policy on our website and update the "Effective Date" at the top of this Policy.
 - B.** For material changes that significantly affect your rights or our processing practices, we will provide additional notice, which may include:
 - 1. Prominent notice on our website or dashboard.
 - 2. Email notification to the email address associated with your account.
 - 3. In-app notification or banner.
 - 4. Other reasonable means appropriate to the nature of the change.
 - C.** Where required by applicable law (e.g., for processing based on consent or material changes under GDPR, CCPA/CPRA, or other

privacy laws), we will obtain your consent or provide an opportunity to opt in or object before the changes take effect.

III. Effective Date of Changes. Revised versions of this Policy take effect on the Effective Date stated at the top of the revised Policy, or as otherwise specified in the notice of changes.

IV. Continued Use. Your continued use of the Services after the Effective Date of a revised Policy constitutes your acceptance of the updated Policy, except where affirmative consent or opt-in is required by law.

V. Review Responsibility. We encourage you to review this Policy periodically to stay informed about our privacy practices. It is your responsibility to check for updates.

ARTICLE 19 – CONTACT INFORMATION AND PRIVACY INQUIRIES

I. General Privacy Inquiries. If you have questions, concerns, or requests regarding this Policy, our privacy practices, or the processing of your personal information, please contact us at:

Ridgeline [Ridgeline Mining]

Attn: Privacy Officer

Email: support@ridgelinemining.com

II. Response Time. We will acknowledge receipt of your inquiry and respond within the timeframes required by applicable law (or 30 days, if earlier, with possible extensions for full performance of our duties in response to inquiries where permitted).

ARTICLE 20 – SEVERABILITY AND INTERPRETATION

I. Severability. If any provision of this Policy is found to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be modified to the minimum extent necessary to make it valid and enforceable, or if such modification is not possible, severed from this Policy. The remaining provisions shall continue in full force and effect.

II. Interpretation. Section headings and article titles are for convenience and reference only and do not affect the interpretation or scope of this Policy. Use of "including," "such as," "e.g.," or similar terms shall be deemed to mean "including without limitation" unless expressly stated otherwise.

III. Language. This Policy is drafted in English. If this Policy is translated into other languages, the English version shall prevail in the event of any conflict or inconsistency.

IV. No Waiver. Our failure to enforce any provision of this Policy shall not constitute a waiver of that provision or any other provision.

ARTICLE 21 – EFFECTIVE DATE AND ACKNOWLEDGMENT

Effective Date: as stated at the top of this Policy.

By accessing or using the Services on or after the Effective Date, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy. If you do not agree to this Policy, you must not access or use the Services.

If you have questions or do not understand any part of this Policy, please contact us at support@ridgeline-mining.com before using the Services.

END OF PRIVACY POLICY