U.S. PRIVACY NOTICE AND PRIVACY POLICY

Effective date: September 29, 2026. Last updated: September 29, 2026.

Important scope note

This Notice is designed for Coingarage US LLC as a Montana-based U.S. digital-asset service provider and FinCEN-registered Money Services Business. It is intended to operate alongside the General Terms and Conditions and the Spot Market Terms. It addresses federal financial privacy and security requirements and, where applicable, Montana consumer privacy requirements. It does not create rights that applicable law does not require, and it does not limit rights that cannot lawfully be waived.

1. Who We Are and What This Notice Covers

1.1. Company. Coingarage US LLC ("Coingarage," "we," "us," or "our") is a Montana limited liability company with its principal office at 1001 S MAIN ST, STE 600, KALISPELL, MONTANA 59901, USA. Coingarage is registered with the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) as a Money Services Business (MSB), MSB Registration No. 31000336102485. FinCEN registration is not governmental approval or endorsement.

1.2. Scope. This Notice describes how we collect, use, disclose, retain and protect Personal Information when you visit https://coingarage.us, use the Coingarage application, create or use an Account, communicate with us, undergo identity or compliance checks, hold or transfer Digital Assets, or use spot trading or another Service made available by Coingarage.

1.3. Former customers and applicants. This Notice also applies, as relevant, to former customers, applicants whose Accounts are not opened, beneficial owners, authorized users, representatives of business customers, counterparties, and other individuals whose Personal Information we process in connection with the Services.

1.4. Relationship to other notices. Additional or just-in-time notices may apply to a specific feature, identity-verification process, cookie or tracking technology, promotion, jurisdiction, or legally required consent. If a more specific notice conflicts with this Notice for that activity, the more specific notice controls for that activity.

2. Privacy Framework Applicable to Coingarage

2.1. Federal financial privacy. Because Coingarage is significantly engaged in financial activities that include money transmission and related financial services, customer financial information may be subject to Title V of the Gramm-Leach-Bliley Act (GLBA), Regulation P, 12 C.F.R. Part 1016, and the FTC Safeguards Rule, 16 C.F.R. Part 314.

2.2. Montana Consumer Data Privacy Act. The Montana Consumer Data Privacy Act (MCDPA), Mont. Code Ann. Title 30, chapter 14, part 28, may apply to Personal Information that is not exempt from the Act and when the statutory applicability thresholds or other applicable provisions are met. The MCDPA exempts Personal Information collected, processed, sold or disclosed in accordance with Title V of GLBA, but that exemption does not necessarily remove every category of data processed by a non-bank financial-services company from Montana privacy law.

2.3. Other laws. We also process information to comply with the Bank Secrecy Act (BSA), applicable FinCEN regulations, U.S. sanctions administered by the Office of Foreign Assets Control (OFAC), tax and legal-process requirements, Montana security-breach notification law, and other applicable federal or state laws.

2.4. No automatic foreign-law extension. Unless we expressly offer a Service in another jurisdiction, this Notice does not represent that foreign privacy law applies to Coingarage. If we later offer Services in a jurisdiction that requires a separate privacy notice, we will provide an appropriate supplemental notice before or when required.

3. Personal Information We Collect

Category	Examples
Identity and KYC information	Name; date of birth; age; nationality/citizenship; residential address; government-issued identification details; document images; taxpayer identification information; signature; selfie or liveness information where identity verification requires it.
Contact and account information	Email address; telephone number; username; Account identifiers; language; preferences; authorized-user or representative information; business-customer role and authority.
Business and beneficial ownership information	Entity name and registration details; ownership and control structure; directors, managers, beneficial owners and authorized representatives; documents evidencing authority or ownership.
Financial and funding information	Bank-account or payment-method details; funding and withdrawal information; balances; payment references; transaction status; chargeback or return information; tax forms and reporting information.
Digital Asset and blockchain information	Wallet addresses; blockchain network; transaction hashes; Digital Asset type and amount; deposit and withdrawal information; custody records; blockchain analytics or wallet-risk indicators.
Trading and transaction information	Orders; execution time; price; quantity; fees; market or liquidity provider; settlement information; transaction history; account limits and restrictions.
Compliance and risk information	Sanctions and watchlist results; politically exposed person indicators where used; source-of-funds or source-of-wealth information; transaction purpose; risk scores; fraud signals; device and location indicators; case notes. Suspicious Activity Reports and information that would reveal their existence are subject to special confidentiality rules.
Device, network and security information	IP address; device and browser type; operating system; application identifiers; session information; authentication events; API activity; login history; security logs; approximate geolocation inferred from IP or device/network signals; fraud and abuse indicators.
Communications and support information	Emails; support tickets; complaint records; chat messages; call metadata and, where lawfully recorded, recordings; documents and information you provide to customer support or compliance.
Website and application usage information	Pages or features used; clicks; session duration; diagnostic data; crash logs; cookie and similar technology identifiers; consent or preference records.

3.1. Sensitive data. Some information used for identity verification, sanctions compliance, fraud prevention or jurisdiction controls may qualify as sensitive data under state privacy law, such as precise geolocation, citizenship or immigration information, or biometric data used to uniquely identify an individual. We process sensitive data only when reasonably necessary for a disclosed purpose and with consent where applicable law requires consent.

3.2. Biometric verification. If a verification provider uses facial geometry, liveness detection or another biometric identifier to verify identity, we will provide or cause to be provided any additional notice or consent required by applicable law before that processing occurs. A photograph or video is not treated as biometric data merely because it is a photograph or video; its legal treatment may change if measurements are generated to identify a specific individual.

4. Where Personal Information Comes From

- directly from you, including during registration, verification, funding, trading, withdrawals, customer support, complaints and privacy requests;

- from a business customer or other person you represent, or from an authorized representative acting for you;
- from banks, payment processors, custodians, trading venues, liquidity providers and other counterparties involved in a transaction;
- from identity-verification, sanctions-screening, fraud-prevention, blockchain-analytics and cybersecurity providers;
- from public records and lawful public sources, including company registers, sanctions lists and other official databases;
- automatically from your device, browser, application, network and use of the Platform; and
- from affiliates and service providers where lawful and reasonably necessary for the purposes described in this Notice.

5. Why We Use Personal Information

Purpose	Typical information used
Provide and administer the Services	Account, identity, contact, financial, Digital Asset, trading, device and communication information.
Verify identity and eligibility	Identity/KYC, business ownership, device, location, sanctions and verification information.
BSA/AML, sanctions and legal compliance	Identity, beneficial ownership, transaction, wallet, source-of-funds, sanctions, risk and supporting documentation.
Process funding and withdrawals	Financial, payment, identity, transaction and risk information.
Custody and transfer Digital Assets	Wallet, blockchain, account, security, transaction and compliance information.
Execute and settle spot transactions	Orders, balances, transaction history, execution and market data, compliance controls and account information.
Protect accounts and prevent fraud	Authentication, device, IP, security logs, behavioral and transaction signals, fraud and risk information.
Customer support and complaints	Account, communication, transaction, technical and complaint information.
Tax, accounting, audit and legal claims	Transaction, identity, tax, contractual, accounting, communication and evidentiary records.
Improve and operate the Platform	Technical logs, diagnostics, usage, performance, support and aggregated information.
Communications and permitted marketing	Contact details, communication preferences and service relationship information. We do not use KYC, account, financial or transaction information for third-party targeted advertising.

6. GLBA Financial Privacy Practices

Our baseline financial-privacy policy

Coingarage does not sell nonpublic personal information (NPI) and does not disclose customer NPI to nonaffiliated third parties for those third parties' own marketing. We may disclose NPI for everyday business purposes, to service providers, to process transactions, to protect against fraud, to comply with law, and for other purposes permitted by Regulation P. If our information-sharing practices change in a way that creates a statutory opt-out right, we will provide the required revised notice and a reasonable opportunity to opt out before the new disclosure occurs.

6.1. Everyday business purposes. We may disclose information as necessary to process or administer a transaction or Service you request, maintain or service your Account, verify identity, process payments, provide custody or transfers, execute trades, prevent fraud, secure systems, conduct audits, comply with legal process, or satisfy legal and regulatory obligations.

6.2. Service providers. We may provide information to service providers that perform functions for us, including cloud hosting, customer support, identity verification, cybersecurity, compliance screening, blockchain analytics, payment processing, custody, execution, accounting, legal and professional services. We require appropriate confidentiality and security protections and limit use of customer information to the permitted purpose where required by law.

6.3. Affiliates. We may share information with affiliated companies for operational, technical, compliance, administrative or support purposes where lawful. Sharing with an affiliate does not authorize the affiliate to use the information for an unrelated purpose. We do not share consumer-report eligibility information with affiliates for affiliate marketing unless permitted by applicable law and any required notice and choice have been provided.

6.4. Government and legal disclosures. We may disclose information to FinCEN, OFAC, tax authorities, courts, law-enforcement agencies, regulators and other governmental authorities when required or permitted by law. We may be prohibited from telling you that certain reports, including Suspicious Activity Reports, have been filed or that certain investigations exist.

6.5. Former customers. We apply our financial privacy practices to NPI about former customers to the extent required by law.

7. Categories of Third Parties to Whom We Disclose Information

- banks, payment processors and other financial institutions involved in funding or settlement;
- Digital Asset custodians, wallet-infrastructure providers, trading venues, liquidity providers, market makers and execution or settlement providers;
- identity-verification, fraud-prevention, sanctions-screening, blockchain-analytics and compliance vendors;
- cloud hosting, software, cybersecurity, communications, customer-support and IT service providers;
- affiliates where the disclosure is lawful and necessary for operational, technical, compliance, accounting or administrative support;
- auditors, accountants, legal counsel, insurers and other professional advisers;
- governmental, regulatory, tax, judicial and law-enforcement authorities; and
- a buyer, successor, financing party or adviser in connection with a bona fide merger, acquisition, reorganization, financing, sale of assets or similar corporate transaction, subject to applicable confidentiality and legal requirements.

7.1. No sale of personal data. Our current policy is not to sell Personal Information for monetary consideration or to operate a data-broker business. We also do not disclose KYC, financial, transaction or Account information for cross-context behavioral advertising. If we later introduce processing that qualifies as a sale or targeted advertising under applicable state law, we will update this Notice and implement required opt-out mechanisms before that processing begins.

8. Cookies, Analytics and Online Tracking

8.1. Necessary technologies. We may use cookies, local storage, SDKs and similar technologies that are reasonably necessary for authentication, session management, fraud prevention, security, preferences, load balancing and operation of the Website and application.

8.2. Analytics. We may use first-party or service-provider analytics to understand performance, diagnose errors and improve the Platform. Analytics must be configured so that service providers do not use customer financial information for their own advertising or unrelated purposes.

8.3. Advertising technologies. Coingarage should not enable third-party behavioral advertising pixels or similar cross-context advertising technologies on authenticated Account pages. If such technology is introduced on public pages and applicable law treats the processing as targeted advertising or a sale, we will provide required notice, opt-out controls and, where applicable, honor recognized opt-out preference signals.

8.4. Browser and device controls. You may control cookies through your browser or device. Disabling necessary technologies may prevent portions of the Platform from functioning. Additional cookie controls may be provided through the Website or application.

9. How Long We Retain Information

We retain Personal Information only for as long as reasonably necessary for the purpose for which it was collected, to provide Services, to comply with BSA/AML, tax, accounting, security and other legal requirements, to investigate fraud, and to establish, exercise or defend legal claims. Retention periods vary by record type.

Record category	General retention approach
BSA/AML, MSB and regulatory records	Generally at least 5 years where required by applicable FinCEN/BSA rules or the Company's AML program, including applicable transaction, SAR-supporting and MSB registration records.
Contracts and material transaction records	Generally up to 8 years after termination or final settlement where reasonably necessary to address written-contract claims under Montana law, subject to longer legal holds or shorter periods where appropriate.
Tax and accounting records	For the legally required period and as reasonably necessary for audit or tax administration.
Account security and fraud records	For a period proportionate to security, fraud and evidentiary needs; incident-related records may be retained for the duration of an investigation and resulting legal hold.
Unsuccessful applications and ordinary support records	Normally no longer than reasonably necessary for compliance, fraud prevention, complaint handling and evidentiary purposes, with periodic deletion.
Cookies and analytics	According to the expiration period of the relevant technology and the purpose for which it is used; unnecessary identifiers should be minimized.
Marketing preferences and suppression records	Until consent is withdrawn or marketing ends; a minimal suppression record may be retained to ensure an opt-out remains effective.

9.1. Secure disposal. Customer information that no longer has a legal, regulatory, security, customer-service or legitimate business retention need is securely deleted, destroyed or de-identified in accordance with our information-security program.

10. Security

We maintain administrative, technical and physical safeguards designed to protect customer information. Our controls are designed with reference to the FTC Safeguards Rule and include risk assessment, access controls, encryption or approved compensating controls, multi-factor authentication, monitoring, secure development and change management, staff training, service-provider oversight, vulnerability management, incident response and secure disposal. No security control can eliminate all risk, and we cannot guarantee that unauthorized access will never occur.

11. Your Privacy Rights and Choices

11.1. Financial privacy choices. GLBA does not create a general right to require deletion of financial records that we are legally required to maintain. If Coingarage proposes to disclose NPI to a nonaffiliated third party in a manner that triggers a GLBA opt-out right, we will provide the required notice and a reasonable method to exercise that choice before the disclosure occurs.

11.2. Montana consumer rights. To the extent the MCDPA applies to Personal Information that is not exempt under GLBA or another statutory exemption, a Montana consumer may have the right to:

- confirm whether we process the consumer's Personal Information and access that information;
- correct inaccuracies;
- delete Personal Information, subject to statutory exceptions;
- obtain a portable copy of Personal Information previously provided to us when the statutory conditions are met; and
- opt out of targeted advertising, the sale of Personal Information, or profiling in furtherance of automated decisions that produce legal or similarly significant effects.

11.3. How to submit a request. A request may be submitted through your existing Account or by emailing support@coingarage.us with the subject line "Privacy Request." We may require information reasonably necessary to authenticate the request. We will not require you to create a new Account solely to exercise a privacy right.

11.4. Response timing. Where the MCDPA applies, we will respond without undue delay and no later than 45 days after receipt. We may extend the period by up to 45 additional days when reasonably necessary and will notify you within the initial period. If we decline to act, we will explain the reason and provide instructions for appeal. We will decide an appeal within 60 days where the statute applies.

11.5. Sensitive identifiers in access responses. For security reasons, an access response will not disclose full Social Security numbers, government identification numbers, financial account numbers, passwords, authentication secrets or biometric templates. Where required, we will instead confirm with sufficient particularity that we collect or process such information.

11.6. Limits on rights. We may retain or continue processing information when necessary to comply with BSA/AML, sanctions, tax, accounting, recordkeeping, fraud-prevention, security, legal-process or other legal obligations, to complete a transaction you requested, or to establish, exercise or defend legal claims. We may also deny or limit a request where applicable law permits or requires us to do so.

11.7. Authorized agents and opt-out signals. Where the MCDPA applies, an authorized agent may submit an opt-out request on your behalf if the statutory verification requirements are satisfied. If Coingarage engages in targeted advertising or sale of Personal Information subject to the MCDPA, we will implement the required opt-out mechanism and recognized opt-out preference signals before that processing is used.

12. Automated Tools, Fraud and Compliance Decisions

We may use automated tools to identify fraud, security threats, sanctions or compliance risk, to verify documents, to prioritize manual review, and to apply account or transaction limits. These tools may produce risk scores, flags or recommendations. We do not represent that every compliance or fraud decision is made solely by a human. Where applicable law gives a right to opt out of profiling in furtherance of an automated decision producing legal or similarly significant effects, we will provide that right for processing within the scope of the law.

13. Children and Minors

The Services are intended only for persons who are at least 18 years old. We do not knowingly permit a minor to open or operate an individual Account. If we learn that Personal Information was collected from a minor contrary to our eligibility rules, we will take reasonable steps to restrict the Account and delete or

retain the information as required by law, security, fraud-prevention or evidentiary obligations. The Platform must not be designed or marketed to children.

14. International and Cross-Border Processing

Coingarage is based in the United States. Information may be processed in the United States and, where reasonably necessary, in other countries in which our affiliates or service providers operate, which may include the Czech Republic or other jurisdictions. Those jurisdictions may have privacy laws that differ from Montana or U.S. federal law. We use contractual, access-control and security measures appropriate to the nature of the information and the service-provider relationship. If a foreign data-protection law requires a specific transfer mechanism because we offer Services in that jurisdiction, we will implement that mechanism before or when required.

15. Security Incidents and Breach Notifications

If a security incident affects Personal Information, we investigate the incident and provide notices required by applicable law. Montana law may require notice to affected Montana residents without unreasonable delay and simultaneous submission of a copy of the consumer notice to the Montana Attorney General's Office of Consumer Protection. The FTC Safeguards Rule may separately require notice to the FTC for a notification event involving the unauthorized acquisition of unencrypted customer information of at least 500 consumers, as defined by the Rule.

16. Communications and Marketing Preferences

We may send service, security, legal, transactional and Account communications that are necessary to administer the relationship and are not marketing choices. Commercial email or text marketing will be sent only as permitted by applicable law. Marketing messages will provide a reasonable method to unsubscribe or withdraw consent where required. Opting out of marketing does not stop service, security or legally required communications.

17. Changes to This Notice

We may update this Notice to reflect changes in law, Services, technology, service providers or information practices. We will post the current version through the Website or Platform and identify its effective date. If a change materially expands how we use or disclose Personal Information, we will provide any advance notice, consent or opt-out required by applicable law before the new practice begins.

18. Contact Us

Privacy requests and questions may be submitted through the Platform or by email to support@coingarage.us. Written correspondence may be sent to: Coingarage US LLC, 1001 S MAIN ST, STE 600, KALISPELL, MONTANA 59901, USA. Please include "Privacy" in the subject line or correspondence and provide only the information reasonably necessary for us to authenticate and respond to your request.

Montana residents may also submit a privacy complaint to the Montana Attorney General through the consumer-privacy complaint mechanism made available by the Montana Department of Justice, where applicable.

Primary Legal and Regulatory Framework

- Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809; Regulation P, 12 C.F.R. Part 1016.
- FTC Safeguards Rule, 16 C.F.R. Part 314.
- Bank Secrecy Act and FinCEN regulations applicable to Money Services Businesses, including 31 C.F.R. Chapter X.
- Montana Consumer Data Privacy Act, Mont. Code Ann. Title 30, chapter 14, part 28, as amended.
- Montana computer security breach law, Mont. Code Ann. § 30-14-1704.
- Montana contract limitation period, Mont. Code Ann. § 27-2-202, where relevant to record-retention decisions.
- Federal Trade Commission Act, 15 U.S.C. § 45, including the prohibition on unfair or deceptive acts or practices.

FACTS WHAT DOES COINGARAGE US LLC DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and account balances ▪ transaction history and account transactions ▪ checking account information and wire transfer instructions When you are no longer our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Coingarage US LLC chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Coingarage US LLC share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	**Yes**	No
For our marketing purposes— to offer our products and services to you	**Yes**	No
For joint marketing with other financial companies	**No**	We don't share
For our affiliates' everyday business purposes— information about your transactions and experiences	**Yes**	No
For our affiliates' everyday business purposes— information about your creditworthiness	**No**	We don't share
For our affiliates to market to you	**No**	We don't share
For nonaffiliates to market to you	**No**	We don't share

Questions?	Go to https://coingarage.us

Who we are	
Who is providing this notice?	Coingarage US LLC
What we do	
How does Coingarage US LLC protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. *We also use access controls, authentication, encryption where appropriate, monitoring, vendor oversight, and incident-response measures designed to protect customer information.*
How does Coingarage US LLC collect my personal information?	We collect your personal information, for example, when you ▪ open an account ▪ make deposits or withdrawals from your account ▪ provide account information ▪ give us your contact information ▪ show your government-issued ID We also collect your personal information from other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law.
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *Our affiliates include Coingarage s.r.o.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *Coingarage US LLC does not share with nonaffiliates so they can market to you.*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *Coingarage US LLC doesn't jointly market.*
Other important information	
Montana law may provide additional privacy rights for certain personal information that is not exempt under the Montana Consumer Data Privacy Act. For more information about applicable rights and how to submit a request, see our Privacy Policy at https://coingarage.us.	