GLOBAL PRIVACY POLICY

Effective Date: 21 November 2025

This Privacy Policy **("Policy")** explains how the entity responsible for operating the **Onramp.Money** platform **("we," "us," or "our")** collects, processes, uses, stores, shares, and protects your Personal Data. This Policy applies to your use of our website, mobile application, APIs, and all related products and services, including fiat-to-crypto and crypto-to-fiat conversions, swap functionalities, and gift card purchases (collectively, the **"Services"**).

We are committed to safeguarding your Personal Data and handling it in accordance with applicable data protection laws and globally recognized privacy standards. By accessing or using the Services, you acknowledge and agree to the data practices described in this Policy.

1. SCOPE, DEFINITIONS AND JURISDICTIONAL COMPLIANCE

1.1 APPLICABILITY

This Policy applies to all natural persons (**“Data Subjects” or “Users” or “You”**) who access or use the Services provided through the Onramp.money platform.

1.2 DEFINITIONS

For the purposes of this Policy, and in alignment with globally recognized data protection frameworks (including the GDPR and similar comprehensive privacy laws), the following terms shall have the meanings set out below:

1.2.1 “*Personal Data*” (or “Personal Information”) means any information relating to an identified or identifiable natural person (“Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier (e.g., IP address, device ID, cookie ID), or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.2.2 “*Processing*” means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or dissemination, alignment or combination, restriction, erasure, or destruction.

1.2.3 “*Data Controller*” means the legal entity responsible for determining the purposes and means of Processing Personal Data in connection with the Onramp.money platform. References to “we,” “us,” or “our” in this Policy refer to this entity.

1.2.4 “*Data Processor*” (or “Service Provider”) means any natural or legal person or entity that processes Personal Data on behalf of the Data Controller. Depending on the specific use-case or workflow, this may include third-party

vendors such as cloud infrastructure providers, analytics tools, payment partners, customer support platforms, compliance solution providers, or other service partners engaged to support or enhance the Services.

1.2.5 ***"Consent"*** means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which the Data Subject, through a statement or a clear affirmative action, signifies agreement to the Processing of Personal Data relating to them.

1.2.6 ***"Affiliates"*** means entities that may support the delivery or operation of the Services and that are under common ownership or management with the legal entity acting as the Data Controller.

1.3 JURISDICTIONAL COMPLIANCE

We Process Personal Data in accordance with the privacy and data protection requirements applicable in the regions where our Services are available. The jurisdictions in which we operate are reflected on our website and product interfaces, and we apply globally recognised principles of lawful, fair, transparent, and secure Processing across all such regions.

2. CATEGORIES OF PERSONAL DATA COLLECTED

We collect and process Personal Data only as necessary to provide the Services, verify identity, facilitate transactions, ensure platform security, and comply with mandatory regulatory requirements.

2.1 DATA YOU PROVIDE DIRECTLY

This includes information you submit when creating an account, completing verification steps (Know Your Customer/Anti-Money Laundering or KYC/AML), initiating transactions, or contacting support. We collect only the information strictly required for account setup, transaction facilitation, and compliance obligations. Depending on the Services used, this may include:

1. **Identity Information:** Full name, date of birth, nationality, gender (where legally required for compliance), email address, phone number, and residential address.
2. **Official Documentation:** Copies of government-issued identification and acceptable proof of address documents, necessary for mandatory verification procedures.
3. **Financial Information:** Payment method details, bank account information, and information about the source of funds or wealth required for compliance and risk assessment.
4. **Communications:** Records of interactions with customer support, feedback submitted through the platform..

2.2 DATA COLLECTED AUTOMATICALLY WHEN YOU USE THE SERVICES

We automatically collect certain technical and usage information when you access or interact with our Services. This data is essential for maintaining platform security, analyzing performance, and detecting fraudulent activity. This category includes:

1. **Technical Device Information:** Information about the device you use, such as its hardware model, operating system version, unique device identifiers, and mobile network information.
2. **Log Data:** Server logs that automatically record information about your interaction with the Services, including IP addresses, access times and dates, pages viewed, and the web page you visited before navigating to our Services.
3. **Location Data:** General location information derived from your IP address or, with your consent, precise geolocation data from your mobile device. This is used for security, fraud prevention, and regulatory adherence based on jurisdiction.
4. **Usage Data:** Details of how you use the Services, such as features used, links clicked, and transaction patterns, which help us optimize the user experience and ensure system stability.

3. LEGAL BASIS AND PURPOSE OF PROCESSING

We Process Personal Data only where we have a valid legal basis and a clearly defined purpose for doing so. Depending on the nature of your interaction with the Services, we rely on the following grounds for Processing your data:

3.1 CONTRACTUAL NECESSITY

We process Personal Data that is necessary for the performance of the contract between you and us (the Terms of Service) or to take steps, at your request, prior to entering into a contract.

Purposes for Processing include, without limitation

1. To create, manage, and maintain your user account and profile.
2. To deliver the Services you request, including facilitating the execution and settlement of your transactions.
3. To provide ongoing customer support, troubleshoot issues, and manage service-related communications.
4. To send essential, non-marketing communications related to the operational status of your account or the Services.

3.2 COMPLIANCE WITH LEGAL OBLIGATIONS

We Process Personal Data where it is necessary for compliance with a mandatory legal or regulatory obligation to which we are subject.

Purposes for Processing include, without limitation

1. To conduct mandatory identity verification (Know Your Customer) and anti-money laundering (AML) checks, including screening against sanctions lists.
2. To detect, prevent, and report misuse of our Services or potential financial crime in adherence to global security standards.
3. To comply with tax-related obligations, financial crime reporting, and other mandatory disclosures to competent governmental or regulatory authorities.
4. To respond to lawful and valid requests, court orders, or subpoenas from governmental or judicial bodies.

3.3 LEGITIMATE INTERESTS

We Process Personal Data where it is necessary for the purposes of the legitimate interests pursued by us or by a third party, provided that those interests do not override your fundamental rights and freedoms. We have conducted assessments to balance these interests against your rights.

Purposes for Processing include, without limitation

1. To operate, secure, and monitor the Services, including preventing misuse, suspicious activity, and unauthorized access to your account.
2. To conduct analytics, research, and audits aimed at enhancing the performance, functionality, and user experience of the platform.
3. To manage and mitigate business risks, establish, exercise, or defend against legal claims, and handle internal disputes.
4. To share data with Affiliates for internal administrative and operational purposes necessary to provide the Services globally.

3.4 CONSENT

We rely on your explicit, informed, and voluntary consent (or opt-in) for Processing activities that are optional and not strictly required for delivering the core Services or complying with applicable laws.

***Note*:** Creating an account and using the core functions of the Services constitutes an acknowledgment that we will process data based on Contractual Necessity and Legal Obligations (as detailed in sections 3.1 and 3.2). However, it does not automatically constitute explicit consent for the optional activities listed below.

Purposes for Consent-Based Processing include;

1. **Marketing Communications:** Sending you promotional updates, tailored offers, or service-related announcements where such communications are optional and not essential to the management of your account.
2. **Non-Essential Tracking:** Using non-essential cookies or similar tracking technologies for personalized analytics, targeted advertising, or advanced profile building that goes beyond essential service monitoring.

Right to Withdraw Consent and Account Implications:

1. You may withdraw your consent at any time. Withdrawal does not affect the lawfulness of Processing carried out prior to the withdrawal.
2. Upon receiving a valid withdrawal request, we will discontinue any Processing activity that relies solely on your consent.
3. If the withdrawal of consent affects your ability to use a feature or functionality that requires such Processing, access to that specific feature may be limited or disabled. Where the withdrawal impacts our ability to maintain required security standards or meet contractual or regulatory obligations, we will inform you of the implications and any necessary next steps. In certain cases, this may include temporary

suspension or closure of your account if continued operation is not possible without the relevant Processing.

4. Instructions for withdrawing consent would be made available within your account settings or through our support channels.

4. DATA SHARING AND DISCLOSURE PROCEDURES

We share Personal Data only to the extent necessary to operate the Services, fulfil legal and regulatory obligations, or where you have expressly consented.

4.1. INTRA-GROUP SHARING

We may share Personal Data with **Affiliates** and entities within our corporate group, including those under common ownership or operational control, for the purposes of account management, service delivery, operational continuity, security, and compliance. This sharing is necessary for the efficient and secure functioning of the platform and is based on our Legitimate Interests or Contractual Necessity. All intra-group Processing is subject to appropriate safeguards including the implementation of an Intra-Group Data Sharing Agreement and is carried out in accordance with this Policy.

4.2. THIRD PARTY SERVICE PROVIDERS

We engage vetted third parties to support essential operational, technical, and compliance functions. These parties act as Data Processors on our behalf. Depending on the Service, these may include without limitation:

1. **Identity and Verification Providers:** For KYC/AML checks and sanctions screening.
2. **Payment and Banking Partners:** To facilitate fiat currency transactions and payment processing.
3. **Security and Infrastructure Providers:** Including blockchain analytics tools, cloud hosting, IT infrastructure providers, and security service vendors.
4. **Customer Support Systems:** For managing communications and providing helpdesk functionality.

These providers are diligently onboarded, undergo due diligence, and are contractually required to treat Personal Data as confidential, Process Personal Data only on our documented instructions, and in alignment with applicable data protection obligations, including the imposition of security measures equivalent to our own.

4.3. LEGAL, REGULATORY, AND COMPLIANCE DISCLOSURES

We may disclose Personal Data where required to comply with applicable laws, lawful requests, regulatory obligations, financial crime prevention frameworks, or court orders. Such disclosures may also occur when necessary to protect our rights, investigate potential misuse of the Services, prevent fraud or security incidents, or safeguard the safety and interests of users or the public.

5. INTERNATIONAL DATA TRANSFERS

Due to the global nature of our operations, your Personal Data may be transferred to, stored in, or processed in countries other than your country of residence. A **"data transfer"** occurs whenever Personal Data is accessed, stored, or processed on servers or by service providers located outside your jurisdiction.

5.1 LEGAL BASIS FOR TRANSFER

All international transfers of Personal Data are conducted on a valid legal basis. Such transfers are necessary to:

- **a.** Perform our contractual obligations;
- **b.** Comply with legal and regulatory duties (including KYC/AML verification and reporting); or
- **c.** **Pursue legitimate interests**, such as maintaining platform security, system resilience, and global operational continuity.

5.2 SAFEGUARDS AND TRANSFER MECHANISMS

For Personal Data originating from the EEA, the UK, or other jurisdictions with strong data-protection laws, we ensure an equivalent level of protection by relying on approved international transfer mechanisms. These may include:

- **a.** **Standard Contractual Clauses (SCCs)** or other recognised contractual safeguards;
- **b.** **Adequacy decisions** issued by the relevant supervisory authorities;
- **c.** **Binding Corporate Rules (BCRs)** for intra-group transfers, where applicable.

These mechanisms ensure that your Personal Data receives the required level of protection regardless of where it is processed.

5.3 ADDITIONAL TECHNICAL AND ORGANIZATIONAL MEASURES

In addition to the legal mechanisms above, we implement robust security measures to ensure that Personal Data remains protected during and after transfer. These include:

- **a.** Encryption in transit and at rest
- **b.** Pseudonymization where appropriate
- **c.** Strict access controls, internal data-minimization protocols, and periodic security audits

Acknowledgment of Necessary Transfers

By using the Services, you acknowledge that certain cross-border transfers of Personal Data are essential for us to provide, maintain, and secure the Services as outlined in our Terms of Service. All such transfers are safeguarded in accordance with the mechanisms and protections described in this Section.

6. DATA SECURITY AND STORAGE MEASURES

We implement industry-standard technical and organisational safeguards designed to protect your Personal Data against unauthorised access, loss, misuse, alteration, or disclosure. These measures are continuously reviewed and updated to align with evolving security best practices. While no security measures can guarantee absolute protection, we take all reasonable and appropriate steps to maintain a secure environment and reduce risks to your Personal Data.

7. DATA RETENTION PROTOCOL

7.1 GENERAL RETENTION PRINCIPLE

We retain Personal Data only for as long as necessary to fulfil the purposes for which it was collected, including the provision of the Services, the maintenance of your account, fraud-prevention, dispute resolution, and compliance with legal and regulatory obligations. This period is determined on a case-by-case basis.

7.2 REGULATORY AND COMPLIANCE RETENTION

Certain categories of data, particularly those relating to financial transactions, identity verification (KYC), Anti-Money Laundering (AML) monitoring, tax obligations, and other statutory compliance requirements are subject to mandatory retention periods as required by competent authorities.

Depending on the jurisdiction and the nature of the transaction, these mandatory periods typically range from five (5) to ten (10) years or longer, often calculated from the date of account closure or the end of the business relationship, where required by applicable law.

7.3 DELETION OR ANONYMIZATION

Once the applicable retention periods expire, and where no further legal or legitimate operational need exists, Personal Data is securely deleted or irreversibly anonymized in accordance with industry-standard technical and organizational measures, making it no longer identifiable to any individual.

7.4 BLOCKCHAIN DATA LIMITATION

Blockchain transaction records (including wallet addresses, transaction hashes, and on-chain activity) are stored on public, decentralized networks that are not controlled by us and cannot be altered or deleted. We act as neither the Controller nor the Processor for this immutable, public ledger data. Such data is inherently pseudonymous and does not constitute Personal Data under our direct control.

Any platform-level metadata linked to blockchain transactions (e.g., internal logs or customer records) will follow the retention and deletion rules described above.

8. DATA SUBJECT RIGHTS

You have the right to request correction of any inaccurate Personal Data or completion of incomplete information. You may update certain details directly through your account settings, or you may submit a request to us through our designated support channels. We will act on such requests without undue delay, subject to any necessary verification steps required for compliance (including re-verification of identity information for KYC purposes).

9. ADDITIONAL INFORMATION

9.1 COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar technologies to enable essential functionality, enhance security, and improve performance.

a. **Essential Cookies:** Required for core functions such as login, security, and compliance. These operate based on our legitimate interests and do not require consent.
b. **Non-Essential Cookies:** Used for analytics, personalization, and marketing. These are activated only with your explicit consent via our cookie banner or preference center.

You may manage or disable cookies through your browser or our preference center. Disabling essential cookies may limit certain features of the Services.

9.2 AUTOMATED PROFILING

We use automated tools for fraud detection, transaction monitoring, risk scoring, and other compliance-driven processes. These are necessary for maintaining platform integrity and fulfilling our legal obligations (including AML/KYC).

Where an automated decision has a significant legal or similar effect on you, you may request human review, express your views, or contest the decision, as permitted under applicable laws.

9.3 MARKETING COMMUNICATIONS

We may send you service updates, promotional content, or product notifications based on your consent or our legitimate interests. You may opt out of marketing communications at any time using the unsubscribe option provided.

9.4 CHILDREN'S PRIVACY

Our Services are not intended for individuals under the age of majority. We do not knowingly collect Personal Data from minors. If such data is identified, we will delete it promptly.

9.5 THIRD PARTY LINKS AND INTEGRATIONS

Our platform may link to or integrate with third-party services. When you interact with these external services, you leave our platform. We are not responsible for the privacy practices or content of those third parties, and we encourage you to review their policies separately. This Policy applies only to Personal Data processed by us in our role as data controller.

10. CHANGES TO THIS PRIVACY POLICY AND CONTACT INFORMATION

10.1 CHANGES TO THIS POLICY

We may update this Privacy Policy from time to time to reflect changes in our services, operational practices, technological developments, or applicable legal and regulatory requirements. When we make material changes, we will notify you by updating the **"Effective Date"** at the top of this Policy and, where required, providing additional notice through our platform. Your continued use of the Services after such updates constitutes acceptance of the revised Policy.

10.2 CONTACT INFORMATION

For any questions about this Policy or to submit a request relating to your Personal Data, you may contact our Compliance Team via email at support@onramp.money.

Nothing in this Policy restricts any rights you have under applicable law. However, to the fullest extent permitted by law, we are not responsible for any data processing carried out by public blockchain networks, third-party platforms, external wallets, or any other services not operated or controlled by us.