Privacy Policy

1. Introduction

This Privacy Policy explains how our cryptocurrency payment gateway service (the **"Company"**, **"we"**, **"us"** or **"Platform"**) collects, uses, stores, and discloses personal information of users. We are a Canada-registered company providing crypto-only merchant payment processing services globally. We are committed to protecting your privacy and safeguarding personal data. We implement all necessary legal, technical, and organizational measures to ensure the confidentiality, integrity, and availability of your personal information. Our data handling practices comply with applicable data protection laws, including the EU General Data Protection Regulation (GDPR) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

By using our Platform, you agree to the collection and use of information in accordance with this Policy. If you do not agree, please discontinue use of the services.

2. Personal Data We Collect

We minimize the personal data we collect, gathering such information mainly in cases where enhanced verification is required for compliance or security (e.g. high-risk transactions flagged under our Anti-Money Laundering (AML) procedures). The types of personal data we may collect include:

- **Account Information:** If you register for an account as a merchant, we collect basic contact details such as your name (or business name), email address, and password. In general, using our crypto payment services does not require extensive personal data.
- **Transaction Data:** Details related to cryptocurrency transactions processed through our gateway, such as blockchain wallet addresses, transaction IDs, and amounts. These by themselves usually do not identify individuals, but they are associated with your account activity.
- **High-Risk Verification Data:** In the event of a flagged high-risk transaction or account activity, we may require you to undergo identity verification. In such cases, additional personal data will be collected through our KYC provider (Sumsub). This may include your full name, date of birth, residential address, telephone number, email, and **Know Your Customer (KYC) documentation** – for example, government-issued identification (passport or driver's license), proof of address, a selfie or photograph for facial verification, and any other information necessary to confirm your identity.
- **Device and Technical Information:** When you interact with our Platform, we may collect technical data such as your IP address, browser type and version, operating system, device identifiers or fingerprinting data, and cookie data. We also record logs of your activity on the Website, including access times and pages viewed. This information helps us secure your account and prevent fraud.

- **Communication Data:** If you contact support or otherwise communicate with us, we will collect the information you provide (such as your contact details and the content of your communications) to assist you.

We do not intentionally collect any sensitive personal data (such as racial or ethnic origin, political opinions, health information, etc.), as our services are not designed to require such data. We ask that you not send us or upload any sensitive personal information unless specifically requested for compliance reasons.

3. Purpose of Data Processing

We process personal data for the following purposes, in accordance with the principles of necessity and proportionality:

- **Providing Services:** To **provide and maintain our services** to you as a user or merchant. For example, we use account information to set up your profile and authenticate your access, and we use transaction data to process payments or payouts. Without some basic personal or transactional data, we cannot perform the services you request.
- **Customer Support and Communication:** To contact you about your account, provide customer support, and respond to inquiries or requests. This includes using your contact information to notify you about important updates or issues related to the service.
- **Compliance with Legal Obligations:** To comply with applicable **legal requirements**, including AML/CFT (anti-money laundering and counter-terrorist financing) obligations and sanctions screening. Specifically, if certain transactions are flagged as potentially high-risk or suspicious, we will use your personal data to verify your identity and the legitimacy of the transaction (via KYC checks). We may also use personal data to fulfill record-keeping requirements (e.g. retaining transaction and identity records for a minimum period as required by law) and to cooperate with law enforcement or regulatory investigations, if legally obligated.
- **Security and Fraud Prevention:** To protect our Platform, you, and other users **from unauthorized access, fraud, spam, or other malicious activities**. For example, IP addresses and device information help us detect and block suspicious login attempts; transaction patterns help us identify potentially fraudulent activity. We may utilize automated decision-making and profiling as part of our fraud and risk prevention measures (for instance, automated algorithms may flag a transaction as high-risk based on predetermined criteria), but any decision to restrict services or require KYC will involve human review.
- **Service Improvements and Analytics:** To improve our services and user experience. We may analyze how users interact with our website (pages visited, features used, etc.) and use aggregate technical data and feedback to **develop new features or enhance functionality**. These analytics are generally performed on anonymized or aggregated data that does not identify individuals.
- **Marketing and Updates (Opt-in):** To send you newsletters, updates, or promotional communications about our services **only if you have expressly opted-in** to such

communications. Even after giving consent, you can opt out at any time. We do not sell or rent your personal data to third parties for marketing.

Our legal bases for processing personal data include: **Contractual necessity** (to provide the services you requested per our Terms of Use), **legal obligations** (compliance with laws such as AML regulations), **legitimate interests** (to secure and improve our platform, to prevent fraud, etc.), and **your consent** (for optional uses like marketing, or when you provide KYC information, as you consent by submitting the info for verification). Under GDPR, where consent is the basis, you have the right to withdraw consent at any time; however, this will not affect processing already carried out or any mandatory data processing under other bases.

4. How We Store and Protect Data

We take data security seriously and employ industry-standard security measures to protect your personal information from unauthorized access, alteration, disclosure, or destruction. These measures include encryption of data in transit (e.g., using HTTPS/TLS for our website), encryption of sensitive data at rest, firewalls and access controls on our servers, and regular security audits. We also limit internal access to personal data: only personnel with a legitimate business need (such as compliance or support staff) will access your data, and they are trained on confidentiality obligations. Our staff are made aware of their personal and legal obligations to protect user data and of the importance of compliance with privacy and security policies.

Personal data collected may be stored on cloud servers or databases that could be located in Canada, the United States, or other jurisdictions. In all cases, we ensure that appropriate safeguards are in place to protect the data. If you are located in the European Economic Area (EEA) or another region with data transfer restrictions, and your data is transferred to a jurisdiction not deemed "adequate" by regulators, we will rely on lawful transfer mechanisms. These may include **European Commission-approved Standard Contractual Clauses (SCCs)** or other safeguards to ensure an adequate level of protection for the transferred data. We also ensure any third-party service providers handling personal data on our behalf (e.g., cloud hosting, email service, identity verification processor) are bound by strict data protection obligations.

We retain personal data only for as long as necessary to fulfill the purposes described in this Policy or as required by law. In general, basic account data is kept for the duration of your use of our services. If you close your account or it becomes inactive, we will delete or anonymize your personal data after a defined retention period. However, **records related to transactions and any identity verifications performed are retained to comply with legal requirements** – typically, we keep such records for a minimum of five (5) years after the end of the business relationship or the date of a transaction, in line with AML record-keeping laws. This retention period may be extended if required by applicable law or if the data is needed for the establishment, exercise, or defense of legal claims. When personal data is no longer needed, we will securely destroy or anonymize it.

5. Disclosure of Personal Data

We do not disclose or share your personal information with third parties except in the limited cases described below, in accordance with this Policy:

- **Service Providers and Partners:** We may share necessary personal data with trusted third-party service providers who help us operate our business and the Platform. This includes, for example, our **KYC/identity verification provider** (Sumsub) which conducts document verification and fraud screening on our behalf when a high-risk transaction triggers a KYC requirement. We have partnered with Sumsub, a leading verification platform trusted by financial institutions worldwide, to ensure robust compliance checks. Sumsub and any similar providers are contractually obligated to protect your information and use it solely for the purposes of providing services to us (in this case, verifying your identity and assessing AML risk). We also use cloud hosting providers and may use analytics or email delivery services; any personal data shared with such providers (if at all) is limited to what is necessary and is protected by data processing agreements. All our service partners must comply with applicable privacy laws and maintain high standards of data security and confidentiality.
- **Affiliates and Corporate Transactions:** If our company expands into subsidiaries or affiliates, we may share data within our corporate family on a need-to-know basis under similar protections. In the event of a merger, acquisition, reorganization, or sale of all or part of our business, personal data may be transferred to the successor entity. In such cases, we will ensure the confidentiality of the personal data is maintained and give affected users notice before their data becomes subject to a different privacy policy.
- **Legal Compliance and Protection:** We may disclose personal information to government authorities, law enforcement, or other third parties **when we believe in good faith that such disclosure is required by law or is necessary to comply with our legal obligations**. For instance, we might be required to respond to valid legal process (such as a subpoena, court order, or official request) or to report certain transactions under anti-money laundering laws. Additionally, if in the course of our own AML compliance efforts we find evidence of illicit activity, we may report details (including personal data) to relevant authorities as permitted or required by law. We may also disclose information if necessary to **protect our rights, property, or safety, or that of our users or others**. This includes sharing information with other companies or organizations for fraud protection and security purposes.
- **With Your Consent:** We will share your personal data with third parties in any other situation where you have given your consent for us to do so. For example, if you opt-in to a co-marketing arrangement or request a referral to a partner service, we would share data only with your explicit consent and only the data needed for that specific purpose.

Importantly, we do **not** sell your personal data to third parties for profit. We may share anonymized, aggregated usage data (which cannot be linked back to any individual) with partners or publicly (for example, to report trends or statistics about cryptocurrency usage on our Platform), but such data contains no personal identifiers.

6. International Users and Cross-Border Data

Given the global nature of our services, personal data may be processed in or transferred to countries outside of your home jurisdiction, including Canada and the United States. If you are located outside of Canada, please be aware that data protection laws in the jurisdiction where your data is processed may differ from those in your country. However, as noted, we will ensure that appropriate safeguards are in place to protect your personal information consistent with the standards of your jurisdiction (for example, GDPR-compliant measures for EU residents).

For users in the European Union or United Kingdom: our Company acts as a data **controller** for your personal data. We rely on legal bases such as consent and legitimate interest for processing as outlined above. If we transfer your data out of the EEA/UK (for example, to Canada or the U.S.), we ensure such transfer is lawful. Canada has been recognized by the European Commission as providing an adequate level of data protection for personal data transferred from the EU to recipients subject to PIPEDA. For transfers to any country not covered by an adequacy decision (or to non-PIPEDA-regulated Canadian entities), we implement measures like Standard Contractual Clauses or obtain your consent where required.

7. Your Rights and Choices

We respect your rights to your personal data. Subject to applicable law (such as GDPR and PIPEDA), you have the following rights regarding your personal information:

- **Access and Portability:** You have the right to request a copy of the personal data we hold about you and to obtain information about how it is processed. Where applicable, we will provide your data in a portable format.
- **Rectification:** You have the right to ask us to correct or update any inaccurate or incomplete personal information. You can also update certain basic information yourself by logging into your account settings (if available).
- **Erasure:** You can request that we delete your personal data if it is no longer necessary for the purposes collected, or if you withdraw consent (where applicable) or object to processing, and we have no overriding legitimate grounds to continue processing. Note that we may need to retain certain information for legal compliance (for example, we cannot immediately delete records that we are required to keep by law) or to exercise or defend legal claims.
- **Restriction of Processing:** You have the right to ask us to limit the processing of your data in certain circumstances – for example, while we verify the accuracy of data you dispute or in lieu of erasure when you have a legitimate reason to retain the data.
- **Objection:** Where we rely on legitimate interests for processing, you have the right to object to that processing on grounds relating to your particular situation. If you make such an objection, we will consider it and respond in accordance with applicable law. You also have an unconditional right to object to your personal data being used for direct marketing purposes at any time.

- **Withdraw Consent:** If we are processing your personal data based on your consent, you have the right to withdraw that consent at any time. This will not affect the lawfulness of processing based on consent before its withdrawal. For example, if you consented to receive marketing emails, you can opt out and we will stop sending them. If you consented to a KYC identity verification, you can withdraw that, but note that we would then not be able to complete the verification or allow the related transaction.
- **Data Portability:** In certain cases, you may request to receive certain personal data in a structured, commonly used, machine-readable format, and have the right to transmit that data to another controller.
- **Complaints:** You have the right to lodge a complaint with a relevant data protection supervisory authority if you believe we have infringed your privacy rights. For example, EU users can contact their national Data Protection Authority; Canadian users can contact the Office of the Privacy Commissioner of Canada (OPC).

To exercise any of these rights, please contact us using the contact information in Section 9 below. We will respond to your request within the timeframe required by law (generally within 30 days for most requests). We may need to verify your identity (for example, by asking you to provide information or log in to your account) before fulfilling certain requests, to ensure we do not disclose data to the wrong person or make incorrect changes.

Please note that some rights may be subject to limitations or exceptions under applicable laws. For instance, we cannot delete data that we are legally mandated to keep, and once data is anonymized and aggregated, it may not be feasible to provide it to you since it's no longer associated with your identity.

8. Cookies and Tracking Technologies

Our Platform uses cookies and similar tracking technologies to enhance user experience and enable certain functionalities. Cookies are small data files stored on your device when you visit a website. We use cookies to remember your preferences (such as language or currency settings), to keep you logged into your account if applicable, and to gather analytic information about usage of our site. This helps us understand which features are most popular and improve our service.

We do not use cookies for advertising purposes on our site, and we do not engage in third-party behavioral advertising. You may control or delete cookies through your browser settings. However, note that disabling certain cookies (especially "essential" cookies used for login or security) may affect your ability to use the Platform's features.

For more details on cookies and how we use them, please see our Cookie Policy (if provided separately), or contact us with any questions.

9. Children's Privacy

Our services are **not directed to individuals under the age of majority** (which is typically 18 years old). We do not knowingly collect personal information from children. If you are under 18, please do not use our Platform or send us any personal information. If we learn that we have inadvertently

collected personal data from a minor, we will take steps to delete such information promptly. Parents or guardians who believe their child may have provided us personal data can contact us and request deletion.

10. Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or for other operational reasons. When we make significant changes, we will notify users by posting a prominent notice on our website or through other communication channels. The “Last Updated” date at the top of the Policy will indicate when the latest changes were made. We encourage you to review this Policy periodically to stay informed about how we are protecting your information.

If we make changes that materially affect how we handle personal data, we will take reasonable steps to let you know in advance (e.g., via email notification to registered users) and, if required by law, to obtain your consent.

11. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, you can contact us at:

PawPayments, Inc.
Email: support@paw.now
Mailing Address: **Office 150, 145 1/2 Church Street, Unit 5, Toronto, Ontario, M5B1Y4, Canada**

We will gladly assist you and address any issues you may have. Your privacy is important to us, and we welcome your feedback.