Privacy Policy

Mosta · Last updated 2026-11-11

1. Introduction and Scope

1.1 Overview. This Privacy Policy ("Policy") describes how the licensed companies ("we," "us," or "our") collect, use, disclose, store, and protect personal information when you access or use the Mosta platform at https://mosta.io (the "Site"), the mobile application (the "App"), and all services provided or facilitated thereby (collectively, the "Platform" or "Services"). The licensed companies are the companies identified on the Licensing page at https://legal.mosta.io/v4/licensing. "Mosta" is the trade name of the website and platform at https://mosta.io, under which the licensed companies provide their services.

1.2 Acceptance. By accessing or using the Platform, creating an Account, or otherwise providing information to us, you acknowledge that you have read, understood, and agree to the practices described in this Policy. If you do not agree to this Policy, you must immediately cease all access to and use of the Platform.

1.3 Service Provision. The financial services available through the Platform are provided by the licensed companies. Where the licensed companies engage custodians or other third parties to help deliver those services, any personal information shared with them is processed under this Policy and applicable law, and no separate third-party privacy terms apply to you.

1.4 Scope. This Policy governs all personal information processed in connection with your use of the Platform and the financial services provided by the licensed companies.

2. Information We Collect

2.1 Information You Provide. We collect information you voluntarily provide, including: (a) account information such as full legal name, date of birth, email address, phone number, residential address, username, and password; (b) identity verification information such as government-issued identification documents, photographs, tax identification numbers, and other documentation required for verification; (c) business information for entity accounts such as registered business name, jurisdiction of incorporation, business address, nature of business, corporate documentation, and information about administrators and authorized users; (d) beneficial ownership information

including names, dates of birth, addresses, identification documents, and ownership percentages of Ultimate Beneficial Owners; (e) financial information such as bank account details, payment card information, transaction history, and source of funds documentation; and (f) communications including records of correspondence with us, support inquiries, and feedback.

2.2 Information Collected Automatically. When you use the Platform, we automatically collect: (a) device information such as device type, operating system, unique device identifiers, browser type and version, and mobile network information; (b) usage information such as pages viewed, features used, clickstream data, session duration, and interaction patterns; (c) location information such as IP address, approximate geographic location, and time zone; and (d) log data such as access times, error logs, and diagnostic information.

2.3 Information from Third Parties. We may receive information from: (a) identity verification providers including results of identity checks, document verification, and fraud screening; (b) financial service providers including transaction data, account status, and compliance-related information; and (c) public sources including publicly available information for verification and compliance purposes.

2.4 Cookies and Tracking Technologies. We use cookies, pixels, and similar technologies to collect information about your use of the Platform, remember your preferences, and improve your experience. We use: (a) essential cookies required for Platform functionality and security; (b) analytics cookies to understand how users interact with the Platform; and (c) preference cookies to remember your settings. You may manage cookie preferences through your browser settings; however, disabling certain cookies may affect Platform functionality.

3. Use of Information

3.1 Service Provision. We use your information to: (a) create and manage your Account; (b) provide and operate the financial services accessed through the Platform; (c) process and display transactions; (d) provide customer support; and (e) communicate with you about your Account and Services.

3.2 Compliance and Security. We use your information to: (a) verify your identity and comply with Know Your Customer ("KYC") requirements; (b) comply with Anti-Money Laundering ("AML") laws and regulations; (c) detect,

prevent, and investigate fraud, unauthorized access, and other illegal activities; (d) comply with legal obligations, court orders, and regulatory requests; and (e) enforce our Terms and Conditions and protect our rights.

3.3 Improvement and Analytics. We use your information to: (a) analyze usage patterns and improve the Platform; (b) develop new features and services; (c) conduct research and analytics; and (d) personalize your experience.

3.4 Communications. We use your information to: (a) send service-related notices and updates; (b) respond to your inquiries; and (c) send marketing communications where you have provided consent or as otherwise permitted by law.

4. Disclosure of Information

4.1 Regulated financial partners. We share personal information with regulated financial institutions and partners that provide accounts, payments and card services to you, including custodians and banks that the licensed companies engage to deliver the financial services accessed through the Platform. These partners receive identity verification and transaction information to provide their services and to meet their own anti-money laundering obligations. Such disclosures are made under this Policy and applicable law.

4.2 Service providers. We use service providers, such as our identity verification provider, that process personal information on our behalf and under our instructions, including: (a) cloud hosting providers; (b) analytics services; (c) identity verification providers; (d) customer support tools; and (e) payment processors. Such providers are contractually obligated to protect your information and use it only for the purposes for which it was disclosed. We share only the information necessary for the purposes in Sections 4.1 and 4.2, under written agreements, and protect it with encryption in transit and at rest.

4.3 Legal and Compliance. We may disclose your information where required or permitted by applicable law, including: (a) to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), to the Bank of Canada under the Retail Payment Activities Act (RPAA), and to comply with other applicable laws, regulations, or legal processes; (b) to law enforcement or other government authorities in response to a lawful request; (c) to protect our rights, privacy, safety, or property, or that of our users or third parties; and (d) in connection with investigations of suspected fraud, illegal activity, or violations of our Terms and Conditions.

4.4 Business Transfers. In connection with any merger, acquisition, reorganization, sale of assets, or bankruptcy, your information may be transferred to the acquiring or successor entity.

4.5 With Consent. We may disclose your information for other purposes with your explicit consent.

4.6 No Sale of Personal Information. We do not sell your personal information to third parties.

5. Data Retention

5.1 Retention Period. We retain your personal information for as long as necessary to: (a) provide Services and maintain your Account; (b) comply with legal and regulatory obligations, including anti-money laundering record-keeping requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). We retain such records for at least five (5) years after Account closure; (c) resolve disputes and enforce agreements; and (d) meet audit and compliance requirements.

5.2 Deletion. When retention is no longer required, we shall securely delete or anonymize your information in accordance with our data retention policies and applicable law.

6. Data Security

6.1 Security Measures. We implement appropriate technical and organizational measures to protect your information, including: (a) encryption of data in transit and at rest; (b) access controls and authentication mechanisms; (c) regular security assessments and monitoring; and (d) employee training on data protection.

6.2 No Guarantee. While we implement reasonable security measures, no method of transmission over the Internet or method of electronic storage is completely secure. We cannot guarantee the absolute security of your information.

6.3 Breach Notification. In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will follow our incident response procedures and notify affected individuals and the relevant supervisory authorities as and when required by applicable law, without undue delay.

7. Your Rights and Choices

7.1 General Rights. Subject to applicable law and certain exceptions, you may have the right to: (a) access and obtain a copy of the personal information we hold about you; (b) request correction of inaccurate or incomplete information; (c) request deletion of your personal information; (d) request a copy of your data in a structured, machine-readable format; (e) request restriction of processing in certain circumstances; (f) object to processing based on legitimate interests; and (g) withdraw consent where processing is based on consent.

7.2 GDPR Rights. If you are located in the European Economic Area or United Kingdom, you have rights under the General Data Protection Regulation ("GDPR") and applicable local law, including the rights set forth in Section 7.1. Our legal bases for processing include: (a) performance of a contract; (b) compliance with legal obligations; (c) legitimate interests; and (d) consent.

7.3 CCPA/CPRA Rights. If you are a California resident, you have rights under the California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA"), including the right to: (a) know what personal information we collect, use, and disclose; (b) request deletion of your personal information; (c) opt-out of the sale or sharing of your personal information; (d) correct inaccurate personal information; (e) limit use of sensitive personal information; and (f) non-discrimination for exercising your rights. We do not sell your personal information.

7.4 PIPEDA Rights (Canada). If your personal information is processed under Canadian jurisdiction, the Personal Information Protection and Electronic Documents Act ("PIPEDA") and applicable provincial privacy laws govern that processing. We rely on consent, performance of a contract, or compliance with legal obligations as the basis for processing. Subject to legal and contractual restrictions, you may withhold or withdraw consent and request access to or correction of your personal information. If you have a privacy concern that we are unable to resolve, you may contact the Office of the Privacy Commissioner of Canada (OPC).

7.5 Other Jurisdictions. If you are located in another jurisdiction with applicable data protection laws, you may have additional rights under those laws.

7.6 Exercising Rights. To exercise any of your rights, submit a request to compliance@mosta.io. We shall respond within the timeframe required by applicable law and may require verification of your identity prior to processing your request.

7.7 Marketing Opt-Out. You may opt out of marketing communications at any time by: (a) clicking "unsubscribe" in any marketing email; or (b) contacting us at support@mosta.io. You shall continue to receive transactional and service-related communications.

7.8 Automated Decision-Making. We may use automated tools for identity verification, sanctions screening, fraud detection, and risk scoring as part of providing the Services and meeting our regulatory obligations. Where an automated decision produces a legal or similarly significant effect concerning you, we provide, where required by applicable law, information about the logic involved and its significance, and a means to request human review.

8. International Data Transfers

8.1 Transfer Locations. Your information may be transferred to and processed in countries other than your country of residence, including the United States, where data protection laws may differ from those in your jurisdiction.

8.2 Safeguards. When we transfer data internationally, we implement appropriate safeguards as required by applicable law, including standard contractual clauses approved by relevant authorities.

9. Children's Privacy

The Platform is not intended for individuals under eighteen (18) years of age or the age of majority in their jurisdiction, whichever is greater. We do not knowingly collect personal information from children. If we become aware that we have collected personal information from an individual under the required age, we shall promptly delete such information, subject to any retention required by applicable law, including the PCMLTFA.

10. Changes to This Policy

10.1 Modifications. We may update this Policy from time to time by posting the revised Policy on the Platform and updating the "Last Updated" date. Material changes shall be communicated via email or Platform notification where required by law.

10.2 Continued Use. Your continued use of the Platform after changes become effective constitutes acceptance of the updated Policy.

10.3 Version Control. We maintain version control and update logs for this Policy for at least five (5) years. Previous versions are available upon request to info@mosta.io.

11. Contact Information

Privacy Inquiries	The licensed companies · compliance@mosta.io
General Support	support@mosta.io

For inquiries regarding how your personal information is processed, please contact us using the details above.