PRIVACY POLICY

NOTAM PAY LTD.

Last updated: 05 May 2026

This Privacy Policy explains how NOTAM PAY LTD. collects, uses, discloses, stores, protects and otherwise processes personal information in connection with its over-the-counter digital asset exchange services, including cryptocurrency-to-cryptocurrency and cryptocurrency-to-fiat exchange transactions.

This Privacy Policy should be read together with our Terms and Conditions for NOTAM PAY LTD. OTC Services and any other notice, disclosure, consent form or agreement provided to you in connection with our services.

By requesting a quote, submitting an instruction, completing onboarding, providing personal information, sending Digital Assets or fiat funds to us, or otherwise using our OTC Services, you acknowledge that we may collect, use, disclose and retain your personal information as described in this Privacy Policy and as permitted or required by applicable law.

1. ABOUT NOTAM PAY LTD.

1.1. NOTAM PAY LTD. is a company incorporated under the laws of the Province of British Columbia, Canada, with incorporation number BC1575404 and Business Number 706910965BC0001, having its registered office at 1783 Manitoba St, Vancouver, BC V5Y 0K1, Canada.

1.2. NOTAM PAY LTD. is registered as a Money Services Business with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) under MSB Registration Number N300000181.

1.3. In this Privacy Policy, “NOTAM PAY”, “we”, “us” and “our” refer to NOTAM PAY LTD.

1.4. For privacy-related questions, access requests, correction requests or complaints, you may contact our Privacy Officer at:

Privacy Officer’s email: legal@notampay.com

Address: 1783 Manitoba St, Vancouver, BC V5Y 0K1, Canada

Website: Notampay.com

2. SCOPE OF THIS PRIVACY POLICY

2.1. This Privacy Policy applies to personal information that we collect, use, disclose or retain in connection with:

(a) onboarding and verification of clients;

(b) provision of OTC Services;

(c) crypto-to-crypto transactions;

(d) crypto-to-fiat and fiat-to-crypto transactions;

(e) transaction monitoring, blockchain analytics, sanctions screening and AML/ATF compliance;

(f) client support and communications;

(g) complaints, disputes, investigations and legal matters;

(h) operation of our website, platform, communication channels and related systems.

2.2. The OTC Services are intended primarily for individual clients. Where we provide services to a Business Client in cases permitted by applicable law, this Privacy Policy also applies to personal information about the Business Client's representatives, directors, officers, shareholders, beneficial owners, authorized signatories, employees, contractors and other related individuals.

2.3. This Privacy Policy does not apply to personal information processed by third-party websites, wallets, exchanges, banks, payment service providers, custodians, liquidity providers or other third parties acting independently from NOTAM PAY. Such third parties are responsible for their own privacy practices.

3. DEFINITIONS

3.1. Unless otherwise defined in this Privacy Policy, capitalized terms have the meaning given to them in our Terms and Conditions.

3.2. **"Personal Information"** means information about an identifiable individual, including information that can reasonably be linked to an individual, whether directly or indirectly.

3.3. **"Sensitive Personal Information"** means Personal Information that, due to its nature or context, requires a higher level of protection. This may include identity documents, financial information, source of funds/source of wealth information, biometric or liveness-check data where used, blockchain analytics results, sanctions screening results, fraud indicators, transaction history and compliance records.

3.4. **"Applicable Privacy Laws"** means applicable Canadian federal and provincial privacy laws, including the Personal Information Protection and Electronic Documents Act, the British Columbia Personal Information Protection Act and any other privacy or data protection laws applicable to NOTAM PAY.

4. PERSONAL INFORMATION WE COLLECT

4.1. We may collect the following categories of Personal Information, depending on your relationship with us, the OTC Services requested, the transaction type, risk profile and legal requirements.

4.2. Identity information

We may collect:

(a) full legal name;

(b) date of birth;

(c) nationality;

(d) country of residence;

(e) residential address;

(f) government-issued identification document details;

(g) copies or images of identification documents;

(h) photo, selfie, video, liveness-check or biometric-related information, where required for identity verification;

(i) signature or electronic signature.

4.3. Contact information

We may collect:

(a) email address;

(b) phone number;

(c) messaging application handle or identifier;

(d) mailing address;

(e) preferred communication channel;

(f) records of communications with us.

4.4. Financial and transactional information

We may collect:

(a) bank account details;

(b) payment details;

(c) source of funds information;

(d) source of wealth information;

(e) occupation, employment or business activity information;

(f) income range, asset information or other financial background information where required for due diligence;

(g) transaction amounts;

(h) transaction dates and times;

(i) Digital Asset type;

(j) Fiat Currency type;

(k) exchange rates, fees, spreads and transaction confirmations;

(l) wallet addresses;

(m) blockchain network information;

(n) payment references, memos, tags and settlement information;

(o) information about rejected, cancelled, delayed or suspended transactions.

4.5. Compliance and risk information

We may collect or generate:

(a) KYC verification results;

(b) AML/ATF risk assessment records;

(c) sanctions screening results;

(d) politically exposed person screening results;

(e) adverse media screening results;

(f) fraud prevention records;

(g) blockchain analytics results;

(h) wallet risk scores;

(i) transaction monitoring alerts;

(j) suspicious activity indicators;

(k) information relating to actual or attempted suspicious transactions;

(l) records required for FINTRAC reporting, record-keeping and compliance.

4.6. Technical and device information

Where you use our website, platform, electronic forms or online tools, we may collect:

(a) IP address;

(b) device identifiers;

(c) browser type and version;

(d) operating system;

(e) login and access timestamps;

(f) approximate location derived from IP address;

(g) usage logs;

(h) cookies and similar tracking information;

(i) security logs and audit trails.

4.7. Business Client-related personal information

Where we onboard or assess a Business Client, we may collect Personal Information about:

(a) directors;

(b) officers;

(c) beneficial owners;

(d) shareholders;

(e) authorized representatives;

(f) authorized signatories;

(g) controllers;

(h) employees or contractors involved in the relationship;

(i) other individuals relevant to due diligence, ownership, control, transaction approval or compliance checks.

This may include identity documents, contact details, ownership information, control information, source of funds/source of wealth information and screening results.

5. HOW WE COLLECT PERSONAL INFORMATION

5.1. We may collect Personal Information directly from you when you:

(a) request a Quote;

(b) apply for onboarding;

(c) provide identification documents;

(d) complete verification steps;

(e) submit transaction Instructions;

(f) send Digital Assets or fiat funds;

(g) communicate with us by email, phone, messenger, website, form or platform;

(h) submit a complaint, request or support ticket;

(i) provide documents or information requested by us.

5.2. We may also collect Personal Information from third parties, including:

(a) identity verification providers;

(b) sanctions screening providers;

(c) fraud prevention providers;

(d) blockchain analytics providers;

(e) banks and payment service providers;

(f) liquidity providers, exchanges and custodians;

(g) public registers and public databases;

(h) corporate registries;

(i) credit, background or risk databases where permitted by law;

(j) law enforcement, regulators or government authorities;

(k) publicly available sources, including open-source intelligence and adverse media sources.

5.3. We may collect blockchain-related information from public blockchains, blockchain nodes, blockchain explorers, analytics providers and other sources. Although blockchain wallet addresses may be pseudonymous, they may become Personal Information where they can reasonably be linked to an identifiable individual.

6. PURPOSES FOR WHICH WE USE PERSONAL INFORMATION

6.1. We collect, use and disclose Personal Information only for purposes that are reasonable in the circumstances and permitted or required by applicable law.

6.2. We may use Personal Information for the following purposes:

6.3. Onboarding and client verification

(a) to identify you;

(b) to verify your identity;

(c) to assess your eligibility to use the OTC Services;

(d) to determine whether you are acting on your own behalf or for another person;

(e) to verify ownership or control of wallets and bank accounts;

(f) to assess whether we may legally provide services to you.

6.4. Provision of OTC Services

(a) to provide Quotes;

(b) to receive and process Instructions;

(c) to execute crypto-to-crypto transactions;

(d) to execute crypto-to-fiat and fiat-to-crypto transactions;

(e) to process deposits, transfers and settlements;

(f) to provide transaction confirmations;

(g) to communicate with you regarding transactions;

(h) to provide customer support.

6.5. AML/ATF, sanctions and regulatory compliance

(a) to comply with anti-money laundering and anti-terrorist financing obligations;

(b) to comply with sanctions laws;

(c) to perform KYC and due diligence checks;

(d) to perform enhanced due diligence where required;

(e) to assess source of funds and source of wealth;

(f) to monitor transactions;

(g) to screen wallets and blockchain transactions;

(h) to detect suspicious or unusual activity;

(i) to prepare and submit reports to FINTRAC or other competent authorities where required;

(j) to maintain required compliance records;

(k) to comply with lawful requests, orders, inquiries or inspections by regulators, law enforcement or courts.

6.6. Fraud prevention, security and risk management

(a) to prevent fraud, scams, unauthorized access, identity theft and misuse of the OTC Services;

(b) to protect NOTAM PAY, clients, counterparties and third parties;

(c) to maintain the security and integrity of our systems;

(d) to investigate suspicious, unlawful, fraudulent or high-risk activity;

(e) to detect attempts to evade sanctions, transaction monitoring, reporting or due diligence controls;

(f) to manage legal, financial, operational, banking and reputational risks.

6.7. Business administration and legal purposes

(a) to maintain business records;

(b) to administer client relationships;

(c) to manage complaints and disputes;

(d) to enforce our Terms and Conditions;

(e) to establish, exercise or defend legal claims;

(f) to obtain legal, tax, audit, accounting, compliance or professional advice;

(g) to support corporate transactions, restructuring, financing, acquisition, sale or transfer of business assets, where permitted by law.

6.8. Communications

(a) to send transaction-related notices;

(b) to provide updates regarding the OTC Services;

(c) to respond to inquiries;

(d) to notify you of changes to our Terms, Privacy Policy, fees, services or operational procedures;

(e) to send security alerts;

(f) to provide legally required disclosures.

6.9. Website, analytics and service improvement

(a) to operate our website or platform;

(b) to maintain security logs;

(c) to improve user experience;

(d) to diagnose technical issues;

(e) to understand how our services are accessed and used;

(f) to develop and improve compliance, security and operational controls.

7. CONSENT AND LEGAL BASIS FOR PROCESSING

7.1. We generally collect, use and disclose Personal Information with your consent, except where collection, use or disclosure without consent is permitted or required by applicable law.

7.2. Your consent may be express or implied, depending on the circumstances, the sensitivity of the information and the reasonable expectations of the individual.

7.3. By requesting a Quote, applying for onboarding, submitting information, accepting an OTC Transaction, sending Digital Assets or fiat funds, communicating with us, or using the OTC Services, you consent to the collection, use and disclosure of Personal Information for the purposes described in this Privacy Policy.

7.4. In some cases, we may collect, use or disclose Personal Information without consent where permitted or required by law, including for:

(a) AML/ATF compliance;

(b) sanctions compliance;

(c) fraud prevention;

(d) transaction monitoring;

(e) suspicious transaction reporting;

(f) record-keeping;

(g) law enforcement requests;

(h) court orders;

(i) regulatory inquiries;

(j) legal claims;

(k) emergencies involving safety, security or unlawful activity.

7.5. You may withdraw consent at any time, subject to legal, contractual and operational restrictions. If you withdraw consent, we may be unable to provide or continue providing OTC Services to you.

7.6. Withdrawal of consent does not affect Personal Information that we are required or permitted to retain, use or disclose for legal, regulatory, AML/ATF, sanctions, tax, audit, dispute resolution or record-keeping purposes.

8. DISCLOSURE OF PERSONAL INFORMATION

8.1. We may disclose Personal Information to the following categories of recipients where necessary or permitted by law.

8.2. Service providers

We may disclose Personal Information to third-party service providers that support our business, including:

(a) identity verification providers;

(b) KYC providers;

(c) sanctions screening providers;

(d) fraud prevention providers;

(e) blockchain analytics providers;

(f) wallet screening providers;

(g) cloud hosting providers;

(h) data storage providers;

(i) cybersecurity providers;

(j) communication and customer support providers;

(k) analytics providers;

(l) IT service providers;

(m) document management providers;

(n) professional advisers.

8.3. Financial, payment and transaction counterparties

We may disclose Personal Information to:

(a) banks;

(b) payment service providers;

(c) liquidity providers;

(d) exchanges;

(e) custodians;

(f) wallet infrastructure providers;

(g) blockchain infrastructure providers;

(h) intermediary financial institutions;

(i) counterparties involved in settlement of an OTC Transaction.

8.4. Regulators, government authorities and law enforcement

We may disclose Personal Information to:

(a) FINTRAC;

(b) Canadian federal, provincial or territorial authorities;

(c) foreign regulators or authorities where applicable;

(d) law enforcement agencies;

(e) courts and tribunals;

(f) tax authorities;

(g) sanctions authorities;

(h) other competent authorities.

8.5. Such disclosure may occur where required or permitted by law, including for AML/ATF reporting, sanctions compliance, suspicious transaction reporting, large transaction reporting, investigations, audits, court orders, subpoenas, production orders or other lawful requests.

8.6. Professional advisers and business transaction parties

We may disclose Personal Information to:

(a) lawyers;

(b) accountants;

(c) auditors;

(d) consultants;

(e) compliance advisers;

(f) insurers;

(g) prospective or actual purchasers, investors, lenders, successors or assignees in connection with a corporate transaction, restructuring, financing, merger, acquisition, sale or transfer of all or part of our business, where permitted by law.

9. INTERNATIONAL TRANSFERS AND PROCESSING OUTSIDE CANADA

9.1. Your Personal Information may be transferred to, stored in or processed in Canada, the United States, the European Economic Area, the United Kingdom or other jurisdictions where NOTAM PAY or its service providers operate.

9.2. Personal Information processed outside Canada may be subject to the laws of the foreign jurisdiction and may be accessible to courts, law enforcement, regulators or government authorities in that jurisdiction.

9.3. Where we transfer Personal Information to service providers outside Canada, we use contractual, organizational and technical measures designed to protect Personal Information in a manner consistent with applicable privacy laws.

9.4. By using the OTC Services and providing Personal Information to us, you acknowledge that your Personal Information may be transferred, stored and processed outside your jurisdiction of residence.

10. RETENTION OF PERSONAL INFORMATION

10.1. We retain Personal Information only for as long as reasonably necessary for the purposes for which it was collected, or as permitted or required by applicable law.

10.2. We may retain Personal Information for longer periods where necessary for:

(a) AML/ATF compliance;

(b) sanctions compliance;

(c) FINTRAC reporting and record-keeping;

(d) tax and accounting obligations;

(e) audit purposes;

(f) fraud prevention;

(g) dispute resolution;

(h) legal claims;

(i) regulatory inquiries;

(j) enforcement of our Terms and Conditions.

10.3. Certain AML/ATF, transaction, client identification and reporting records may be retained for at least five (5) years or for any other period required by applicable law.

10.4. When Personal Information is no longer required, we will securely delete, destroy, anonymize or de-identify it, unless continued retention is permitted or required by law.

10.5. We may retain de-identified, aggregated or anonymized information for analytics, compliance, security, risk management, service improvement or business purposes, provided that such information no longer identifies you.

11. SAFEGUARDS AND SECURITY

11.1. We use reasonable physical, organizational and technical safeguards appropriate to the sensitivity of the Personal Information we process.

11.2. These safeguards may include:

(a) access controls;

(b) authentication measures;

(c) encryption or secure transmission where appropriate;

(d) secure storage;

(e) role-based access restrictions;

(f) employee and contractor confidentiality obligations;

(g) security monitoring;

(h) audit logs;

(i) vendor due diligence;

(j) incident response procedures;

(k) staff training;

(l) internal policies and procedures.

11.3. No method of transmission, processing or storage is completely secure. We cannot guarantee absolute security of Personal Information.

11.4. You are responsible for maintaining the security of your own devices, email accounts, phone numbers, messaging accounts, wallets, bank accounts, private keys, passwords and other credentials.

11.5. You should notify us immediately if you believe that your Personal Information, communication channel, wallet, bank account or transaction details have been compromised.

12. ACCURACY OF PERSONAL INFORMATION

12.1. We take reasonable steps to ensure that Personal Information used by us is accurate, complete and up to date as necessary for the purposes for which it is used.

12.2. You are responsible for providing accurate, complete and current information.

12.3. You must promptly notify us of any change to your Personal Information, including changes to your name, address, contact details, residency, source of funds, source of wealth, wallet information, bank account information or other information relevant to your use of the OTC Services.

12.4. We may request updated information or documents at any time as part of ongoing due diligence, periodic review, transaction monitoring, sanctions screening or regulatory compliance.

13. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

13.1. Subject to applicable law, you may request access to Personal Information that we hold about you.

13.2. You may also request correction of Personal Information that you believe is inaccurate or incomplete.

13.3. To make an access or correction request, please contact our Privacy Officer using the contact details set out in Section 1.

13.4. We may require you to verify your identity before responding to an access or correction request.

13.5. We will respond to access and correction requests within the timeframe required by applicable law.

13.6. We may refuse or limit access where permitted or required by law, including where disclosure would:

(a) reveal Personal Information about another individual;

(b) reveal confidential commercial information;

(c) compromise security, fraud prevention or AML/ATF controls;

(d) interfere with an investigation;

(e) reveal information protected by solicitor-client privilege;

(f) breach legal or regulatory restrictions;

(g) disclose information that cannot be disclosed due to FINTRAC, AML/ATF, sanctions, law enforcement or tipping-off restrictions.

13.7. If we refuse access or correction, we will provide reasons where required and permitted by law.

14. COOKIES AND SIMILAR TECHNOLOGIES

14.1. If we operate a website, platform or online portal, we may use cookies, pixels, log files and similar technologies.

14.2. We may use these technologies to:

(a) operate the website or platform;

(b) maintain security;

(c) authenticate users;

(d) prevent fraud;

(e) remember preferences;

(f) analyze usage;

(g) improve services;

(h) comply with legal and regulatory requirements.

14.3. You may be able to control cookies through your browser settings. However, disabling certain cookies may affect the functionality, security or availability of the website or platform.

14.4. We do not knowingly use cookies to collect Sensitive Personal Information unless expressly disclosed and permitted by law.

15. MARKETING COMMUNICATIONS

15.1. We may send you service-related communications, including transaction notices, compliance requests, security alerts, operational updates and legal notices.

15.2. We may send marketing communications only where permitted by applicable law and, where required, with your consent.

15.3. You may opt out of marketing communications at any time by using the unsubscribe mechanism in the relevant message or contacting us.

15.4. Even if you opt out of marketing communications, we may continue to send you non-marketing communications related to transactions, compliance, security, legal notices or your relationship with NOTAM PAY.

16. AUTOMATED SCREENING, BLOCKCHAIN ANALYTICS AND RISK ASSESSMENT

16.1. We may use automated tools, manual review or a combination of both to support:

(a) identity verification;

(b) fraud prevention;

(c) sanctions screening;

(d) politically exposed person screening;

(e) adverse media screening;

(f) wallet screening;

(g) blockchain analytics;

(h) transaction monitoring;

(i) risk scoring;

(j) compliance review.

16.2. These tools may generate alerts, risk scores or recommendations that help us determine whether to onboard a client, process a transaction, request additional information, delay settlement, reject a transaction or report activity to competent authorities.

16.3. We do not rely solely on automated tools where human review is reasonably required by our internal policies or applicable law.

16.4. We may not be able to disclose details of automated screening rules, blockchain analytics results, risk indicators or internal compliance logic where disclosure would compromise security, fraud prevention, AML/ATF controls, sanctions compliance, investigations or legal obligations.

17. PUBLIC BLOCKCHAINS

17.1. Digital Asset transactions may be recorded on public blockchains.

17.2. Information recorded on public blockchains may include wallet addresses, transaction hashes, transaction amounts, timestamps, token types and network information.

17.3. Public blockchain records may be permanent, publicly visible and difficult or impossible to delete or modify.

17.4. NOTAM PAY does not control public blockchains and cannot delete, modify, hide or reverse information recorded on a public blockchain.

17.5. Blockchain data may be analyzed by third parties and, in some circumstances, linked to an identifiable individual.

18. THIRD-PARTY LINKS, WALLETS AND SERVICES

18.1. Our website, platform or communications may contain links to third-party websites, wallets, exchanges, payment providers or other services.

18.2. We are not responsible for the privacy practices, content, security or conduct of third parties.

18.3. You should review the privacy policies and terms of any third-party services before using them.

18.4. Your use of External Wallets, banks, payment providers, exchanges, custodians or other third-party services is subject to the privacy policies and terms of those third parties.

19. CHILDREN AND MINORS

19.1. The OTC Services are not intended for minors.

19.2. You must be at least nineteen (19) years old or the age of majority in your jurisdiction of residence, whichever is higher, to use the OTC Services.

19.3. We do not knowingly collect Personal Information from minors for the purpose of providing the OTC Services.

19.4. If we become aware that we have collected Personal Information from a minor in connection with the OTC Services, we may delete such information, terminate onboarding or refuse to provide services, unless retention is required or permitted by law.

20. BUSINESS CLIENT REPRESENTATIVES AND BENEFICIAL OWNERS

20.1. Where we provide OTC Services to a Business Client in cases permitted by applicable law, we may collect Personal Information about individuals associated with that Business Client.

20.2. This may include directors, officers, shareholders, beneficial owners, authorized signatories, representatives, employees, contractors and other individuals relevant to ownership, control, authorization, due diligence or transaction processing.

20.3. The Business Client must ensure that it has the authority to provide such Personal Information to NOTAM PAY and, where required, has provided all necessary notices and obtained all necessary consents.

20.4. Personal Information relating to Business Client representatives and beneficial owners may be used and disclosed for onboarding, verification, AML/ATF compliance, sanctions screening, transaction processing, risk assessment and regulatory reporting.

21. DISCLOSURE WITHOUT CONSENT

21.1. We may collect, use or disclose Personal Information without consent where permitted or required by applicable law.

21.2. This may include situations where collection, use or disclosure is necessary to:

(a) comply with AML/ATF laws;

(b) comply with sanctions laws;

(c) report suspicious transactions;

(d) comply with FINTRAC obligations;

(e) respond to lawful requests from regulators, law enforcement, courts or government authorities;

(f) prevent, detect or investigate fraud;

(g) protect the security of our systems;

(h) collect a debt owed to us;

(i) respond to an emergency;

(j) investigate a breach of our Terms and Conditions;

(k) establish, exercise or defend legal claims;

(l) complete a business transaction where permitted by law.

22. PRIVACY INCIDENTS

22.1. We maintain procedures to assess and respond to privacy incidents involving unauthorized access to, or collection, use, disclosure, loss or disposal of, Personal Information.

22.2. Where required by applicable law, we will notify affected individuals, regulators or other parties of a privacy breach.

22.3. In determining the appropriate response, we may consider:

(a) the sensitivity of the Personal Information involved;

(b) the probability of misuse;

(c) the risk of identity theft, fraud, financial loss, reputational harm or other harm;

(d) whether the information was encrypted or otherwise protected;

(e) whether the information has been recovered;

(f) legal and regulatory notification requirements.

23. YOUR CHOICES AND RIGHTS

23.1. Subject to applicable law, you may:

(a) request access to your Personal Information;

(b) request correction of inaccurate or incomplete Personal Information;

(c) withdraw consent where processing is based on consent;

(d) ask questions about our privacy practices;

(e) make a complaint about our handling of Personal Information.

23.2. Some rights may be limited where Personal Information is required for AML/ATF compliance, sanctions compliance, transaction monitoring, FINTRAC reporting, legal claims, fraud prevention, security, audit, tax, accounting or record-keeping purposes.

23.3. If you withdraw consent or refuse to provide required Personal Information, we may be unable to onboard you, provide Quotes, execute OTC Transactions, settle transactions or continue providing the OTC Services.

24. COMPLAINTS AND PRIVACY QUESTIONS

24.1. If you have a question, concern or complaint about this Privacy Policy or our privacy practices, please contact our Privacy Officer first:

Email: legal@notampay.com

Address: 1783 Manitoba St, Vancouver, BC V5Y 0K1, Canada

24.2. Please include:

(a) your full name;

(b) contact details;

(c) a description of your request or complaint;

(d) any relevant transaction reference;

(e) supporting information or documents.

24.3. We will review and respond to privacy complaints in good faith and within the timeframe required by applicable law.

24.4. If you are not satisfied with our response, you may have the right to contact the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner for British Columbia, or another competent privacy authority, depending on the nature of the matter and applicable law.

25. CHANGES TO THIS PRIVACY POLICY

25.1. We may update this Privacy Policy from time to time to reflect changes in our services, technology, legal obligations, regulatory requirements, risk controls or business practices.

25.2. The updated Privacy Policy will be effective from the date stated at the top of the updated version.

25.3. Where required by applicable law, we will provide notice of material changes or seek consent.

25.4. Your continued use of the OTC Services after the updated Privacy Policy becomes effective means that you acknowledge the updated Privacy Policy, subject to any consent requirements under applicable law.

26. CONFLICT WITH TERMS AND CONDITIONS

26.1. This Privacy Policy forms part of the legal and compliance framework applicable to the OTC Services.

26.2. If there is a conflict between this Privacy Policy and the Terms and Conditions, the Terms and Conditions will prevail in relation to contractual matters, transaction execution, fees, limitations of liability and dispute resolution.

26.3. This Privacy Policy will prevail in relation to the collection, use, disclosure, retention and protection of Personal Information, unless applicable law requires otherwise.

27. CONTACT DETAILS

For privacy questions, access requests, correction requests or complaints, please contact:

NOTAM PAY LTD.

Registered office: 1783 Manitoba St, Vancouver, BC V5Y 0K1, Canada

Privacy Officer's email: legal@notampay.com

Website: Notampay.com

28. ACKNOWLEDGEMENT

By requesting a Quote, submitting an Instruction, completing onboarding, providing Personal Information, accepting an OTC Transaction, sending Digital Assets or Fiat Currency to NOTAM PAY, or otherwise using the OTC Services, you acknowledge that you have read and understood this Privacy Policy.