

NoLimit Payments

Privacy Policy

Website & Mobile Application — How We Collect, Use, Disclose, and Protect Your Personal Information

Issued by: NoLimit Payments Ltd.

Effective Date: June 8th, 2026

Governing Law: Province of Ontario, Canada

Last updated: June 8th, 2026

This Privacy Policy (this "**Policy**") explains how **NoLimit Payments Ltd.** ("**NoLimit**", "**we**", "**us**", or "**our**"), a corporation incorporated under the laws of Canada (corporation number 1444218-1) with its principal office at 325 Front St W, Unit 200, Toronto, Ontario M5V 2Y1, Canada, collects, uses, discloses, and protects Personal Information in connection with our websites, our mobile and web applications, and the payment and payment-related services we provide (together, the "**Platform**" and the "**Services**").

In this Policy, "**Personal Information**" means information about an identifiable individual, and includes "personal data", "personal information", and "nonpublic personal information" as those or equivalent terms are defined under the privacy laws that apply to you, including Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), Quebec's *Act respecting the protection of personal information in the private sector* (as amended by Law 25) ("**Law 25**"), the U.S. *Gramm-Leach-Bliley Act* ("**GLBA**") and applicable U.S. state privacy laws, and the EU *General Data Protection Regulation* ("**GDPR**"). This Policy forms part of, and should be read with, our Terms of Service. By using the Platform or the Services, you acknowledge the practices described in this Policy. Where we act as a service provider or processor on behalf of a business customer, that customer's privacy notice may also apply.

The following terms apply:

1. Who We Are and How to Reach Us

1.1 The Organisation Responsible. NoLimit is the organisation responsible for the Personal Information described in this Policy. For the purposes of the GDPR (where it applies), NoLimit is the "controller" of that Personal Information, except where we process it on behalf of a business customer, in which case we act as "processor" and the customer is the controller.

1.2 Privacy Officer. We have designated a Privacy Officer who is accountable for our compliance with this Policy and with applicable privacy law, and who is the "person in charge of the protection of personal information" for the purposes of Law 25. You may contact the Privacy Officer at

privacy@nolimit.money or by mail at NoLimit Payments Ltd., Attn: Privacy Officer, 325 Front St W, Unit 200, Toronto, Ontario M5V 2Y1, Canada.

1.3 Scope. This Policy applies to Personal Information we collect through the Platform and in providing the Services. It does not apply to third-party websites, applications, or services that we do not control, even if they link to or from the Platform (Section 16).

1.4 Relationship to the Terms of Service. Capitalised terms not defined here have the meanings given in our Terms of Service. If there is a conflict between this Policy and the Terms of Service on a privacy matter, this Policy governs to the extent of the conflict.

2. Personal Information We Collect

2.1 Information You Provide. We collect Personal Information you give us when you visit the Platform, create or use an Account, or contact us, including: identity and verification information (name, date of birth, nationality, residency, government-issued identifiers and identity documents); contact information (address, email, telephone number); account credentials and security information; for a business customer, information about the entity and its directors, officers, and beneficial owners; financial and account information (bank account, payment-card, and wallet details); transaction instructions and history; and the content of your communications with us.

2.2 Information We Collect Automatically. When you use the Platform, we automatically collect device and technical information (device identifiers, operating system, browser type, language, and app version), IP address and approximate or precise location, log and usage data, and information collected through cookies, software development kits (SDKs), and similar technologies (Section 4).

2.3 Information From Third Parties. We collect Personal Information from: identity-verification, credit-file, and identity-data providers; sanctions, politically-exposed-person, and adverse-media screening sources; fraud-prevention networks and device-intelligence providers; our banking, card, and crypto partners and other Third-Party Providers; referral partners; and public and commercial sources, in each case to provide the Services, verify your identity and eligibility, and meet our legal obligations.

2.4 Sensitive Information. Some of the information we collect is sensitive, including government-issued identifiers, identity documents, and precise geolocation, and may include biometric information used to verify your identity (for example, in a document-and-selfie check performed by a verification provider). We collect and use sensitive information only where permitted by law and, where required, with your express consent, and we apply heightened protection to it.

The categories of Personal Information we collect are summarised below:

Category	Examples
Identity and verification	Name, date of birth, nationality, residency, government identifiers, identity documents, and any l

Contact	Mailing address, email address, telephone number
Account and security	Username, credentials, authentication and security data, account preferences
Business-customer data	Entity details, and identity and ownership information for directors, officers, beneficial owners, and
Financial and transaction	Bank-account, payment-card, and wallet details; balances; Orders; transaction history
Compliance and risk	KYC/KYB records, source-of-funds and source-of-wealth data, sanctions and PEP screening results
Technical and usage	Device and browser data, IP address, location, log and usage data, cookie and SDK identifiers
Communications	Messages, support tickets, call recordings (where notified), and marketing preferences

2.5 Children. The Services are intended for individuals who are at least the age of majority in their jurisdiction (and in any event 18 or older). We do not knowingly collect Personal Information from children (Section 15).

3. Why We Use Your Personal Information

3.1 Purposes. We use Personal Information to: provide, operate, and administer the Platform and the Services; verify your identity and eligibility and complete onboarding; conduct know-your-customer (KYC), know-your-business (KYB), customer due diligence, and beneficial-ownership checks; meet anti-money-laundering and counter-terrorist-financing, sanctions-screening, Travel-Rule, and related regulatory obligations; detect, prevent, and investigate fraud, security incidents, and prohibited or excluded use (including enforcing the residency and geographic exclusions in our Terms of Service); process and settle transactions; provide customer support; secure the Platform; comply with our legal and regulatory obligations and respond to lawful requests; manage risk and our business; analyse and improve the Platform and the Services; and, where you have consented or as otherwise permitted by law, send you marketing communications.

3.2 Legal Bases and Consent. In Canada, we rely on your consent (express or implied) and on the bases on which PIPEDA and applicable provincial law permit collection, use, or disclosure without consent (for example, to detect or prevent fraud, to comply with a legal requirement, or where seeking consent would compromise an investigation). Where the GDPR applies, we rely on one or more of the following lawful bases: performance of a contract with you; compliance with a legal obligation; our legitimate interests (such as securing the Platform, preventing fraud, and operating our business), balanced against your rights; your consent; and, in limited cases, protection of vital interests. Where we rely on consent, you may withdraw it as described in Section 10, subject to legal and contractual limits.

The principal purposes and the bases for them are summarised below:

Purpose	Typical Personal Information	Basis
Provide and administer the Services	Identity, contact, account, financial, transaction	Contract; consent (PIPEDA)
Identity verification and onboarding	Identity and verification, sensitive identifiers	Legal obligation; consent
AML/CTF, sanctions, Travel Rule, reporting	Identity, compliance, transaction	Legal obligation
Fraud prevention and security	Technical, usage, transaction, risk signals	Legitimate interests; fraud-prevention (PIPEDA)
Customer support	Contact, account, communications	Contract; consent
Product analytics and improvement	Technical, usage	Legitimate interests; consent
Marketing communications	Contact, marketing preferences	Consent (CASL; GDPR)

4. Cookies, SDKs, and Similar Technologies

4.1 What We Use. We and our service providers use cookies, SDKs, pixels, and similar technologies on the Platform. These fall into categories: strictly necessary (required to operate the Platform and keep it secure); performance and analytics (to understand how the Platform is used); functional (to remember your preferences); and, where applicable, advertising or targeting technologies.

4.2 Managing Your Choices. Where required by law, we obtain your consent to non-essential cookies and similar technologies through a consent banner or in-app control, and you can change your choices at any time. You can also manage cookies through your browser settings and manage device identifiers through your device settings. Disabling some technologies may affect how the Platform functions.

5. Electronic Communications and Marketing (CASL)

5.1 Service Messages. We send you transactional and service messages necessary to provide the Services, administer your Account, and meet our legal obligations. We may send these on the basis of an existing business relationship or as otherwise permitted under Canada's Anti-Spam Legislation ("CASL").

5.2 Commercial Electronic Messages. Where we send commercial electronic messages, we do so in compliance with CASL: we obtain consent (express or, where permitted, implied) before sending, we identify ourselves clearly, and we include a functioning unsubscribe mechanism in each message.

5.3 Opting Out. You may unsubscribe from non-essential commercial electronic messages at any time, using the unsubscribe mechanism in the message or by contacting us. We will give effect to your request within the time CASL requires. We may continue to send you messages necessary to administer the Services.

6. How We Share and Disclose Personal Information

6.1 Service Providers and Processors. We share Personal Information with service providers that process it on our behalf and under contract, including cloud-hosting, identity-verification, analytics, communications, customer-support, and fraud-prevention providers. They are permitted to use it only to provide services to us and are required to protect it.

6.2 Financial and Payment Partners. To deliver the Services, we share Personal Information with our banking, card-issuing, card-network, crypto-custody, liquidity, and other financial partners and Third-Party Providers, as needed to process and settle your transactions and to meet their own legal and risk requirements.

6.3 Within Our Corporate Group. We may share Personal Information with QPX Inc. (doing business as QPexa) and its subsidiaries (the "QPexa Group") for the purposes described in this Policy, consistent with applicable law.

6.4 Regulators, Authorities, and Law Enforcement. We disclose Personal Information to regulators and authorities, including FINTRAC, FinCEN, the U.S. Office of Foreign Assets Control (OFAC), the Bank of Canada, tax authorities, courts, and law-enforcement agencies, where required or permitted by law. **Where the law restricts us from doing so, we will not tell you that a report has been made or is contemplated, and our doing so may be an offence.**

6.5 Corporate Transactions. If we are involved in a merger, acquisition, financing, reorganisation, or sale of all or part of our business or assets, we may disclose Personal Information to the parties and advisers involved, subject to appropriate confidentiality protections.

6.6 At Your Direction or With Consent. We share Personal Information where you direct us to, or where you otherwise consent.

6.7 We Do Not Sell Your Personal Information. We do not sell your Personal Information for money, and we do not "sell" or "share" it for cross-context behavioural advertising within the meaning of applicable U.S. state privacy laws, except as you may separately consent. If this changes, we will update this Policy and provide any opt-out the law requires (Section 12).

7. International Transfers and Storage

7.1 Where We Process Personal Information. We operate from, and your Personal Information may be processed and stored in, Canada, the United States, and other countries where we or our service providers operate. As a result, your Personal Information may be subject to the laws of those jurisdictions, including lawful access by their courts, regulators, and law-enforcement and national-security authorities.

7.2 Canada (PIPEDA). When we transfer Personal Information to a service provider for processing, including across borders, we remain accountable for it and use contractual and other measures intended to provide a comparable level of protection.

7.3 Quebec (Law 25). Before communicating Personal Information outside Quebec, we conduct a privacy assessment of the factors Law 25 requires, including the sensitivity of the information, the purposes, the protection measures, and the legal framework of the destination jurisdiction, and we use contractual measures designed to ensure the information receives adequate protection (Section 11).

7.4 European Union / EEA (GDPR). Where the GDPR applies and we transfer Personal Information outside the EU/EEA to a country without an adequacy decision, we rely on appropriate safeguards, principally the European Commission's Standard Contractual Clauses, together with any supplementary measures required, and you may request information about these safeguards (Section 13).

8. How Long We Keep Personal Information

8.1 Retention. We keep Personal Information only as long as necessary for the purposes described in this Policy and to satisfy our legal, regulatory, accounting, and reporting obligations, after which we securely delete or anonymise it. Certain records must be retained for minimum periods set by law — for example, identity and transaction records under the *Proceeds of Crime (Money Laundering)*

and Terrorist Financing Act (Canada) and under the U.S. *Bank Secrecy Act* are generally retained for at least five (5) years after the end of the relationship or the transaction. Where different periods apply, we retain the information for the longest applicable period.

9. How We Protect Personal Information

9.1 Safeguards. We maintain administrative, technical, and physical safeguards designed to protect Personal Information appropriate to its sensitivity, including access controls, encryption in transit and at rest where appropriate, network and monitoring controls, and due diligence and contractual controls over our service providers.

9.2 Breach Response. We maintain procedures to detect, assess, and respond to confidentiality incidents and breaches of security safeguards. Where a breach creates a real risk of significant harm (or meets the equivalent threshold under applicable law), we will notify affected individuals and the relevant regulators — including, as applicable, the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, applicable U.S. state authorities, and EU supervisory authorities — and keep records of breaches as the law requires.

9.3 No Absolute Security; Your Role. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. You are responsible for keeping your credentials and devices secure and for the matters described in our Terms of Service.

10. Your Privacy Rights and Choices

10.1 Core Rights. Subject to applicable law and to verification of your identity, you may: access the Personal Information we hold about you; ask us to correct inaccurate or incomplete information; and withdraw a consent you previously gave (subject to legal and contractual limits, which may mean we can no longer provide a Service). Depending on where you live, you may have additional rights, described in Sections 11 to 13.

10.2 How to Exercise Your Rights. Contact our Privacy Officer at privacy@nolimit.money. We may need to verify your identity before responding. We respond within the timeframes required by applicable law and, where the law allows a fee, we will tell you in advance. If we decline a request, we will explain why, to the extent we are permitted to do so.

10.3 Complaints. If you have a concern, please contact our Privacy Officer first so we can try to resolve it. You also have the right to complain to the privacy regulator that applies to you (Sections 11 to 13 and 18).

11. Additional Information for Quebec Residents (Law 25)

11.1 Services Not Offered in Quebec. As described in our Terms of Service, the Services are not offered to residents of the Province of Quebec. This Section 11 applies to the extent we nonetheless collect or hold Personal Information of individuals in Quebec — for example, when a person visits

the Platform or begins, but does not complete, registration before our residency checks apply — and we limit such collection accordingly.

11.2 Person in Charge. Our Privacy Officer (Section 1.2) is the person in charge of the protection of Personal Information for the purposes of Law 25.

11.3 Consent and Confidentiality. Where Law 25 requires consent, we obtain consent that is clear, free, and informed and given for specific purposes, and we obtain separate, express consent for sensitive Personal Information. Privacy settings that we offer are configured by default to the highest level of confidentiality.

11.4 Your Rights. Subject to Law 25, you may access and rectify your Personal Information, withdraw your consent, request that we cease disseminating your Personal Information or de-index a link where the legal conditions are met, and, for computerised Personal Information you provided to us, request a copy in a structured, commonly used technological format (portability).

11.5 Automated Decisions. Where we make a decision about you based exclusively on automated processing, we will, on request, inform you of that fact and of the Personal Information and principal factors used, and give you the opportunity to submit observations to a member of our staff who can review the decision (Section 14).

12. Additional Information for United States Residents (GLBA and State Privacy Laws)

12.1 Financial Privacy (GLBA). For the financial products and services we provide to individuals in the United States, NoLimit is a financial institution subject to the GLBA. We collect nonpublic personal information to provide those products and services, to process transactions, and to meet legal obligations, and we share it only as described in this Policy and as permitted by the GLBA. We restrict access to nonpublic personal information and maintain safeguards to protect it.

12.2 State Comprehensive Privacy Laws. Residents of California (under the California Consumer Privacy Act, as amended by the California Privacy Rights Act) and of other U.S. states that have enacted comprehensive consumer-privacy laws may have rights regarding their Personal Information. Importantly, Personal Information that is collected, processed, or disclosed under, and regulated by, the GLBA is generally exempt from these state laws; the rights below therefore apply mainly to Personal Information that is not subject to the GLBA (for example, certain website-visitor information).

12.3 State Privacy Rights. Where a state law applies, and subject to its exemptions and verification, you may have the right to: know about and access the Personal Information we collect and how we use and disclose it; request deletion; request correction; opt out of the "sale" or "sharing" of Personal Information and of targeted advertising; limit the use of sensitive Personal Information; and not be subject to discrimination for exercising your rights. As stated in Section 6.7, we do not sell your Personal Information or share it for cross-context behavioural advertising.

12.4 How to Exercise and Appeal. You may submit a request to privacy@nolimit.money, and you may use an authorised agent where the law permits. We will verify your request and respond within the statutory timeframe. Where a state law provides a right to appeal a refusal, we will tell you how to appeal, and if we deny your appeal you may contact your state Attorney General. California

residents may also have rights under California's "Shine the Light" law regarding disclosures to third parties for their direct-marketing purposes.

13. Additional Information for the European Union / EEA (GDPR)

13.1 When This Applies. The GDPR applies where we offer Services to, or monitor the behaviour of, individuals in the EU/EEA. As described in our Terms of Service, the Crypto Asset on/off-ramp Services are not offered to persons in the EU/EEA; this Section 13 applies to any other Personal Information processing to which the GDPR applies.

13.2 Controller and Representative. NoLimit is the controller of that Personal Information. Where required by Article 27 of the GDPR, we have appointed an EU representative for the purposes of Article 27 of the GDPR. Our EU representative is:

QPEXA OÜ

Narva mnt 13-27, Kesklinna linnaosa

Tallinn, Harju maakond, 10151, Estonia

Email: support@qpexa.com

You may contact our EU representative on matters relating to the processing of your Personal Information.

13.3 Lawful Bases. We process Personal Information on the lawful bases described in Section 3.2.

13.4 Your Rights. Subject to the GDPR, you have the right to access, rectification, erasure, restriction of processing, data portability, and objection to processing (including to processing based on legitimate interests and to direct marketing), the right to withdraw consent, and the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects, except as the GDPR permits (Section 14).

13.5 Transfers. We transfer Personal Information outside the EU/EEA only with appropriate safeguards (Section 7.4).

13.6 Complaints. You may lodge a complaint with a supervisory authority in the EU/EEA Member State of your residence, place of work, or the place of the alleged infringement.

14. Automated Decision-Making and Profiling

14.1 How We Use Automated Processing. We use automated processing, including profiling, to verify identity, screen for sanctions and politically-exposed persons, detect and prevent fraud, monitor transactions, and enforce eligibility and the geographic and residency exclusions in our Terms of Service. These processes may affect whether we open or maintain an Account or process a transaction.

14.2 Your Rights. Where Law 25, the GDPR, or other applicable law gives you rights in respect of automated decisions, we honour them, including telling you about the decision and the principal factors involved and giving you the opportunity to obtain human review and to contest the decision, except where an exception applies (for example, where disclosure would reveal a fraud-detection method or compromise a legal obligation).

15. Children's Privacy

15.1 Not Directed to Children. The Platform and the Services are intended for adults and are not directed to children. We do not knowingly collect Personal Information from anyone under the age of majority. If we learn that we have collected Personal Information from a child, we will delete it.

16. Third-Party Sites and Services

16.1 Third Parties. The Platform may link to, or integrate with, third-party websites, applications, and services that we do not control. This Policy does not apply to them, and we are not responsible for their privacy practices. Review their privacy notices before providing Personal Information.

17. Changes to This Policy

17.1 Updates. We may update this Policy from time to time. We will post the updated Policy on the Platform and update the "Last updated" date, and, where a change is material, we will provide additional notice as required by applicable law. Changes take effect when posted unless we say otherwise.

18. How to Contact Us; Complaints

18.1 Contact. For any question about this Policy or our handling of your Personal Information, or to exercise your rights, contact our Privacy Officer at privacy@nolimit.money or at NoLimit Payments Ltd., Attn: Privacy Officer, 325 Front St W, Unit 200, Toronto, Ontario M5V 2Y1, Canada.

18.2 Regulators. You may also contact the privacy regulator that applies to you, including: the Office of the Privacy Commissioner of Canada; the Commission d'accès à l'information du Québec; your U.S. state Attorney General; or an EU/EEA supervisory authority.