Privacy Policy

INFINIFX NETWORK INC.
Revision date 3 November 2026

This Policy explains how INFINIFX NETWORK INC. handles personal information for its website, enquiries, business onboarding and agreed payment technology and exchange facilitation services. It also explains individual choices, access and correction rights, and how to raise a privacy concern. A business relationship does not remove the privacy rights of its representatives, owners, shoppers or beneficiaries.

1 Responsibility and contact

1.1 INFINIFX NETWORK INC., Ontario Corporation Number 1001203825, is responsible for personal information under its control. Contact the person responsible for privacy by writing Privacy Officer to business@infinifx.io or to 1270 Central Parkway West, Unit 102, Mississauga, Ontario L5C 4P4, Canada. Website: https://infinifx.io. Telephone: +1 888 586 3171.

1.2 This Policy covers visitors, enquiry contacts, applicants, business customers, Authorized Users, beneficial owners, directors, representatives, payers and beneficiaries whose information is processed through the agreed services. InfiniFX does not receive or hold customer Transaction Funds or cryptoassets. Transaction information may still be personal information even when funds do not pass through InfiniFX.

1.3 Applicable requirements include the Personal Information Protection and Electronic Documents Act, and provincial private-sector privacy law where it applies, including Quebec, Alberta or British Columbia requirements. Where we process information only on a business customer's instructions, that relationship also requires appropriate written privacy and security terms. Each party remains responsible for its own legal duties. A provider independently collecting information under its own contract must identify itself and its own privacy notice.

2 Information and sources

2.1 Enquiries and support. We collect the name, business affiliation, contact information, message and follow-up information you submit so we can respond and keep a record of the issue. Provide only what is needed. Do not send identity documents, full payment card details, bank credentials, private keys, seed phrases or unrelated sensitive information through the general contact form or ordinary email.

2.2 Business onboarding and compliance. Where necessary for the actual service or a legal requirement, information includes identity and contact details, date of birth, government identification details and verification results, authority to act, business activities, incorporation and address information, directors, ownership and control details, and relevant source of funds or wealth. We obtain it from the person or business, authorized representatives, relevant public registers, and verification or screening sources disclosed in the onboarding process.

2.3 Service and transaction records. Information may include user access records, the instructions we facilitate, payer and payee information, bank or wallet destination identifiers necessary for routing, transaction references, amounts, currencies, asset types, rates, charges and settlement status received from the executing party. Wallet addresses and blockchain records can identify individuals when linked with other information. Collection must be limited to our actual role.

2.4 Risk and legal records. Information may include sanctions and politically exposed person determinations, relevant public-source information, fraud indicators, supporting documents, records of

required reporting, complaints and investigation outcomes. A screening indicator must not be treated as proof of wrongdoing without appropriate assessment.

2.5 Website and technical information. Hosting and delivery of the website can involve IP addresses, browser and device details, request times, accessed pages and security or error logs. Cookies and external resources are addressed in clause 9. We do not need precise location for a general enquiry. A feature requesting location or other additional device permissions must explain the purpose before requesting permission.

2.6 Payment information and recordings. The provider responsible for accepting payment must explain which payment details it collects. Do not provide security codes or raw card data to InfiniFX unless an approved collection flow specifically requires them and has been disclosed. A call or session must not be recorded without prior notice explaining its purpose and an applicable lawful basis. Where practicable, a non-recorded contact route will be offered.

3 Purposes and consent

3.1 We use personal information to respond to enquiries; assess eligibility and authority; administer agreed business access; facilitate authorized instructions; provide service records and support; meet applicable identity, AML ATF, sanctions and reporting duties; prevent and investigate fraud and security incidents; handle complaints; and fulfil lawful recordkeeping obligations. Information must be relevant and limited to these stated purposes.

3.2 We explain the information required, the purpose, relevant recipients and material privacy consequences before collection, except where a specific legal exception permits otherwise. Sensitive information and unexpected or materially risky processing require express consent where required by law. Less sensitive, reasonably expected processing may use another lawful form of consent where appropriate. A contract, commercial interest or use of a website is not a general substitute for consent under Canadian law.

3.3 You can refuse optional processing without losing an unrelated service. If information is required for a particular service or a legal duty, we explain that requirement and the consequences of refusing it. We do not ask you to consent to a legal obligation that applies independently of consent. Any processing without consent must fit a specific statutory exception and remain limited to its scope.

3.4 We will seek fresh consent where required for a new purpose, material change or new disclosure. Acceptance of the Terms and Conditions does not itself authorize marketing, biometric processing, third-party advertising or public visibility of personal information.

4 Sensitive information and identity technology

4.1 Identity documents, financial records, biometric measures and related verification information can be sensitive. This Policy does not by itself authorize a biometric process. Before any collection or use of a face or voice template, biometric measurement or biometric liveness result, the specific process must explain the responsible organizations, purpose, information created, recipients, location of processing, retention, risks, available alternatives and consequences of refusal, and obtain separate express consent where required.

4.2 Any such process must be necessary and proportionate, use the least intrusive suitable method, limit access and retention, and prohibit unrelated reuse, model training or disclosure unless separately lawful and transparently authorized. The collection of a photograph or identity document is not unrestricted permission to derive or reuse biometrics. Mandatory identity verification must use a legally permitted method; Canadian AML law does not universally require biometrics.

4.3 If Quebec rules apply, required privacy assessments, express consent and notifications to the Commission d'acces a l'information must be completed before the relevant biometric process is used. Creation of a biometric database requires the applicable advance disclosure, including the 60-day rule where triggered. Where an eligibility decision is based exclusively on automated processing, the person must receive the legally required notice and an opportunity to obtain information, correct relevant data and make observations for review.

5 Recipients and service providers

5.1 Information is shared only as needed for an identified purpose and lawful basis. Relevant recipient categories include contracted hosting, communications, identity verification, screening, security and support providers; the execution provider, financial institution or counterparty needed for an authorized transaction; professional advisers under confidentiality; and authorities where a legal obligation or specific lawful exception applies.

5.2 Before a service shares information with an independent execution provider, that provider and its role must be identified in the Service Confirmation or collection notice. Necessary payer and payee information may accompany a transfer, including information required by the applicable travel rule. This does not authorize making user contact details generally visible to other platform users.

5.3 For processing we outsource, we remain accountable for information under our control and require appropriate contractual safeguards, limited instructions, access controls, incident cooperation, restrictions on further processing and return or deletion when permitted. Outsourcing does not mean that every supplier is an independent controller or that InfiniFX has no further responsibility.

5.4 A lawful business transaction involving the company may require limited disclosure under confidentiality and legal safeguards. It is not an unrestricted right to sell personal information or change its purposes. We do not sell personal information under this Policy or authorize third-party advertising use. Disclosure without consent for an investigation, business transaction or authority request is limited to the conditions of the applicable legal exception.

6 Processing outside Canada or a province

6.1 Online hosting, external resources, communications and providers can involve processing outside Canada or outside your province. Foreign authorities may obtain lawful access under the law of the place of processing. Canadian privacy protections do not make foreign law inapplicable, and we do not promise exclusively Canadian storage.

6.2 Before a service requires international processing of sensitive onboarding or transaction information, the collection notice must identify the relevant processing locations, provider roles and material implications. You may also ask the Privacy Officer about the locations and safeguards applicable to your information. We remain accountable for our transfers for processing and require protection appropriate to the information.

6.3 Where Quebec law applies, a required assessment must precede communication outside Quebec or the entrusting of collection, use, disclosure or keeping outside Quebec. Such communication must receive adequate protection and be governed by the required written agreement reflecting the assessment and risks. Any other applicable provincial transparency requirements also apply.

7 Retention and deletion

7.1 Information is retained only as long as reasonably needed for its stated purpose or a specific legal requirement. Closing a Customer Profile does not immediately erase lawful compliance records, but

does not justify indefinite retention of every item. Information no longer needed is securely destroyed, erased or, where lawful, irreversibly anonymized using appropriate standards.

7.2 Prescribed AML records commonly require at least five years, with the starting point depending on the record: for example, the transaction or report date, creation of a record, or the last relevant business transaction. We apply the applicable trigger for each category, rather than a blanket five years after closure for all information. Longer retention requires an identified legal, litigation or other justified purpose and appropriate access limits.

7.3 Enquiries, unsuccessful applications, technical logs and optional communications are not automatically subject to the same AML retention period. Their retention must reflect necessity, complaint handling and applicable law. Biometric source material or templates, if collected under a separate lawful process, require their own limited retention disclosure; they must not automatically be kept for the duration of the customer relationship.

7.4 Records of personal information breaches subject to PIPEDA are retained for at least 24 months after the breach is determined to have occurred; other applicable law may require longer. We preserve records relevant to an access request while it is being addressed and as required by law. Ask the Privacy Officer for the retention period or criteria applicable to a particular category.

8 Security and incidents

8.1 We must protect information through administrative, technical and physical safeguards appropriate to its sensitivity, quantity, format and risks, including appropriate access limitations, secure handling and oversight of contracted processing. No system can guarantee absolute security. This does not limit our responsibility to protect personal information or respond to a breach.

8.2 If a breach meets the applicable legal notification threshold, we will notify the affected people and relevant authority in the required manner and time. Under PIPEDA, reporting to the Privacy Commissioner and notification to affected individuals are required as soon as feasible for a breach creating a real risk of significant harm. Applicable Quebec and other provincial incident duties must also be followed. An inability to guarantee absolute security does not remove these obligations.

9 Cookies external resources and website choices

9.1 Cookies and similar technologies can maintain a session, remember a choice or support security. Any such use must be limited to its identified purpose. Optional analytics, profiling or advertising technologies must be explained and obtain the consent required by applicable law before activation. Continued browsing alone is not blanket consent to optional tracking.

9.2 The public website loads hosted resources including Webflow assets and resources from Google Fonts, Google's hosted JavaScript service and Amazon CloudFront. Loading an external resource can send technical request information, including an IP address and browser information, to its operator even without a cookie. A provider's use of information for its own purposes must be disclosed and assessed separately from processing on our instructions.

9.3 You can block or delete cookies in your browser, although necessary functionality may be affected. Where optional technologies are offered, their notice must state the provider, purpose, information, duration and available choices, including a means to withdraw consent as easily as it was given. Browser controls do not replace a required consent choice before optional technology is used. Features enabling identification, location or profiling must meet applicable advance notice, consent and default-setting requirements, including Quebec rules where applicable.

10 Marketing and optional communications

10.1 We send marketing electronic messages only with valid consent or another basis permitted by Canada's Anti-Spam Legislation. We identify the sender, provide the required contact details and include a working unsubscribe route. Express marketing consent must be separate from a general enquiry or required service acceptance.

10.2 You may unsubscribe using the message link or by contacting us. We action unsubscribe requests without delay and no later than ten Business Days where CASL applies. Necessary non-promotional service, security or legal notices may still be sent on their applicable lawful basis. We do not make a service conditional on consent to unrelated marketing.

11 Access correction and other rights

11.1 Contact the Privacy Officer to request access to your personal information, information about its use and disclosures, or correction of inaccurate or incomplete information. We verify identity proportionately and do not demand unnecessary new sensitive information. Where PIPEDA applies, we respond within 30 calendar days, subject only to a lawful extension with the required notice and complaint information. Other applicable statutory deadlines prevail.

11.2 Access is supplied at little or no cost as required by law. If a charge is lawful, we explain it and obtain agreement before proceeding. If an exemption limits access, we explain the legal reason and recourse unless prohibited, and provide the remaining information where possible. Privacy complaints, access requests and mandatory disclosures are not subject to a discretionary document fee.

11.3 You may withdraw consent subject to applicable legal or contractual restrictions and reasonable notice. We explain the effect, including any service that cannot lawfully continue. Withdrawal does not erase processing already lawfully undertaken or records that must be retained. You may ask for deletion where permitted, but there is no general promise of immediate deletion of all compliance records.

11.4 Where applicable, Quebec law provides rights concerning computerized information in a structured, commonly used format, certain cessation of dissemination or de-indexing requests, and exclusively automated decisions. We assess requests under the legal conditions and exceptions. Other provincial rights and routes remain available.

12 Complaints and regulators

12.1 Send a concern to the Privacy Officer using clause 1.1. We will acknowledge within five Business Days, investigate and aim to provide a reasoned response within 30 calendar days, without extending a shorter mandatory deadline. If more time is lawfully needed, we explain the reason and expected response date. Raising a privacy concern does not justify retaliation or loss of an unrelated service.

12.2 You may complain directly to the Office of the Privacy Commissioner of Canada at https://www.priv.gc.ca/en/report-a-concern, or to the applicable provincial commissioner. Quebec's Commission d'acces a l'information is at https://www.cai.gouv.qc.ca; Alberta's commissioner is at https://oipc.ab.ca; British Columbia's commissioner is at https://www.oipc.bc.ca. You need not waive a legal remedy or exhaust an unrelated service complaint process to contact a privacy regulator.

13 Children and third party services

13.1 InfiniFX's business onboarding and Authorized User access are not intended for minors. A merchant's end customers are not automatically InfiniFX customers. If information about a minor is necessary for a particular transaction, the responsible organizations must first establish the applicable

lawful basis and any required guardian consent and safeguards. Please contact us if you believe information has been collected improperly.

13.2 Following an external link or separately using an execution provider brings that organization's privacy practices into consideration. We remain responsible for information we disclose and for providers processing on our behalf; a third-party label does not eliminate those duties.

14 Changes to this Policy

14.1 We publish the revised Policy with its revision date and bring material changes to affected individuals' attention in an appropriate way. A change does not retrospectively authorize an incompatible use or disclosure. Where fresh consent or a feature-specific notice is required, it must be obtained or supplied before the changed processing begins.