Privacy Policy (shorted version)

Last updated: 05.08.2025

This privacy notice applies to **NEXT SOLUTIONS CORP.**, a federally registered Canadian company operating under Corporation Number **1001042225**, with its registered office at 155 East Beaver Creek Road, Suite 24-147, Richmond Hill, Ontario, L4B2N1, Canada.

This notice reflects our commitment to protecting your privacy rights in accordance with the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and other applicable provincial privacy laws in Canada. It sets out the basis on which we collect, use, disclose, and protect your personal information when you interact with us.

This Privacy Policy applies to the following contexts:

- your use of website features, user portals, and services made available when you visit website or any related pages, payment modules, or integrations embedded on third-party platforms that we power;
- your use of any desktop, mobile, or web-based applications (the “Applications”) offered by NEXT SOLUTIONS CORP.;
- any communication you engage in with us, including but not limited to: email, SMS, telephone, web chat, social media messages, or any other digital or voice channel.

Please read the following carefully to understand our policies and practices regarding your personal information and how we will treat it.

Our Approach to Transparency

NEXT SOLUTIONS CORP. takes a **"layered approach"** to explaining our privacy practices, in accordance with guidance from Canadian privacy regulators such as the Office of the Privacy Commissioner of Canada (OPC). This means:

- This document serves as our **Short-Form Privacy Notice**, giving you the key information upfront;
- Our **Comprehensive Privacy Policy** (available upon request or on our website) provides more detailed descriptions of our practices, including data retention, legal bases, international transfers, and your rights.

If you have questions, privacy concerns, or requests, please contact us using the contact information provided in the **“Contact Us”** section at the end of this notice.

INFORMATION WE MAY COLLECT FROM YOU

We may collect personal information in several ways, including directly from you, through automated technologies, or from trusted third parties.

Information you provide directly

You may voluntarily provide us with personal information in the following cases:

- when you inquire about or apply for our services;
- when you create a user profile or register an account;
- when you complete forms or applications on our website or through our partners;
- when you participate in our marketing campaigns, events, or surveys;
- when you communicate with us via email, telephone, live chat, SMS, or other messaging tools;
- when you interact with features of our Services that request or require your input.

This information may include (but is not limited to):

- your full name, contact details (email address, phone number), and mailing address;
- identification documents or government-issued IDs;
- payment information or banking details, when relevant to the services used;
- login credentials (if account-based access is provided);
- responses to surveys, customer feedback forms, or application questionnaires.

Information we collect automatically

When you use our website or applications, we may collect certain technical and usage data automatically through cookies, tracking pixels, scripts, and other web technologies. This may include:

- device identifiers (e.g., IP address, browser type, operating system, hardware model);
- session logs (e.g., pages visited, clicks, time spent, referring/exit URLs);
- location data (e.g., approximate geolocation based on IP address, if permitted);
- behavioral interaction data (e.g., heatmaps, scrolling behavior, user flow).

To learn more about how we use cookies and similar technologies, please refer to our [Cookie Policy].

Information from third parties

We may also obtain certain data about you from third-party sources, including:

- financial institutions or payment processors who confirm your account ownership or transaction history;
- credit reporting agencies (where applicable and permitted by law);
- publicly available records (e.g., corporate registries, sanctions lists);
- identity verification and fraud prevention providers;
- partners or referrers through whom you were introduced to us.

All such data is used in accordance with applicable legal requirements, and where necessary, subject to appropriate consent or notice.

HOW WE USE YOUR INFORMATION

We use the personal information we collect for the following purposes:

- **To deliver services to you**: including account creation, identity verification, onboarding, access to our products, and transactional support;
- **To communicate with you**: including service notifications, product updates, system alerts, and administrative messages;
- **To provide customer support**: responding to inquiries, complaints, and technical assistance requests;
- **To improve our services**: using analytics to understand usage trends, optimize platform performance, and enhance user experience;
- **To detect and prevent fraud**: including suspicious activity monitoring, transaction verification, and identity validation;
- **To comply with legal obligations**: such as anti-money laundering (AML) regulations, tax reporting requirements, or law enforcement requests;
- **To send you marketing communications**, where permitted by law and with your consent where required. You can opt out at any time.

If you are using one of our financial or transactional products, we may also use your personal information to:

- assess financial suitability and risk exposure (where applicable);
- investigate and take action against suspected fraudulent or unauthorized activities;
- cooperate with authorities and regulators in maintaining compliance with applicable laws.

DISCLOSURE OF YOUR INFORMATION

We respect the confidentiality of your personal information and will not disclose it unless it is necessary for the purposes described above, and permitted or required under applicable law. We may disclose your information to the following categories of third parties:

- **Service providers and vendors**: including IT support, cloud hosting, customer service tools, payment gateways, analytics platforms, KYC/AML screening services, and other operational partners;
- **Financial institutions**: when necessary to complete a transaction or process a service request;

- **Government authorities and law enforcement**: where disclosure is required under applicable legal processes such as subpoenas, warrants, or regulatory obligations;
- **Credit reporting and identity verification agencies**, when necessary to verify your identity or assess creditworthiness (if applicable to our services);
- **Corporate affiliates or successors**: in the event of a merger, acquisition, restructuring, or sale of our business assets.

All third-party service providers we engage are contractually required to maintain data protection standards consistent with applicable Canadian privacy legislation and to use your data only as instructed by us.

WHERE WE STORE YOUR PERSONAL DATA AND DATA SECURITY

The personal information that **NEXT SOLUTIONS CORP.** collects from you may be processed, stored, or accessed outside your province or territory of residence, including **outside Canada** — for example, by service providers located in the United States or other countries.

These jurisdictions may have privacy laws that differ from those in your province or territory. However, whenever we transfer or allow access to your information across borders, we ensure that appropriate safeguards are in place to protect it. This includes entering into data protection agreements with service providers and implementing technical and organizational security measures that meet Canadian standards.

If you would like more information about how we protect personal information when it is transferred internationally, you may contact us using the details at the end of this notice.

If you have been provided with (or have chosen) a password, access code, or any other secure authentication method for accessing parts of our Website or Services, **you are responsible for keeping these credentials confidential** and for adhering to all security instructions issued by NEXT SOLUTIONS CORP.

You must not share your login credentials with anyone. By using them, you authorize us to act upon instructions received via your access credentials, and we will assume any access or action taken using those credentials has been authorized by you.

Please note that while we take reasonable steps to protect your personal data, **no method of transmitting data over the Internet or storing it electronically is completely secure**.

Although we implement industry-standard safeguards and internal protocols to prevent unauthorized access, we cannot guarantee the absolute security of any information you transmit to us electronically.

Once we receive your information, we apply strict administrative, physical, and technical security measures to protect it against loss, theft, unauthorized access, disclosure, copying, use, or modification.

YOUR RIGHTS

Under applicable Canadian privacy laws, including **PIPEDA**, you have the following rights with respect to your personal information, subject to limited exceptions:

- The right to **access** the personal information we hold about you;
- The right to **request corrections** to your personal information if it is inaccurate or incomplete;
- The right to **withdraw your consent** to the collection, use, or disclosure of your information (subject to legal or contractual restrictions and reasonable notice);
- The right to **challenge our compliance** with applicable privacy obligations through a formal complaint process;
- The right to **request information** about how your personal data has been used or disclosed by us.

Please note that there may be exceptions to some of these rights under federal or provincial law. For example, we may retain certain data if required for legal, regulatory, or audit purposes.

To exercise any of these rights, please contact us using the information in the **Contact Us** section below.

AUTOMATED DECISION-MAKING

In certain cases, we may use **automated decision-making processes** to evaluate or process personal information. This means that a decision concerning you may be made solely based on an automated analysis, without human intervention.

For example, we may use automated tools:

- to assess your eligibility for certain services (e.g., during onboarding or identity verification),
- or to detect and flag potentially fraudulent transactions.

Where such processing has a significant impact on you, and where required by law, you will be informed of this automated decision-making and may have the right to **request human review** of the decision.

If you believe that an automated decision has been made in error, or wish to contest the outcome, you may contact us to request further explanation or review.

LEGAL BASIS FOR PROCESSING

NEXT SOLUTIONS CORP. will only collect, use, or disclose your personal information where we have a **valid legal basis** to do so under Canadian law. These may include:

- **Your consent**, for example, when you opt in to receive marketing communications;
- **A contract with you**, where processing is necessary to fulfill our obligations or provide the requested services;
- **A legitimate interest**, such as fraud prevention, service optimization, or protecting the security of our platform;
- **A legal obligation**, where we are required to collect or retain certain information (e.g., under anti-money laundering regulations);
- **Vital interests or public interest**, in rare cases where processing is necessary to protect someone's life, safety, or for law enforcement or regulatory investigations.

Where we rely on your consent, you have the right to withdraw it at any time by contacting us.

CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time in response to changes in our operations, regulatory requirements, or applicable laws.

If we make material changes, we will notify you by posting the updated version on our website and indicating the **"Last Updated"** date at the top of the page. In some cases, we may also notify you via email or through your account (if applicable).

We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information.

CONTACT US

We welcome your questions, comments, or requests regarding this Privacy Policy or our handling of your personal data.

You may contact our **Privacy Officer** (responsible for ensuring our compliance with privacy obligations) at:

NEXT SOLUTIONS CORP.
Attention: Privacy Officer
155 East Beaver Creek Road, Suite 24-147, Richmond Hill, Ontario, L4B2N1, Canada
Email: info@next-solutions.io

If you are not satisfied with our response to a privacy-related concern, you have the right to file a complaint with the **Office of the Privacy Commissioner of Canada (OPC)**:
https://www.priv.gc.ca/en/report-a-concern/

Privacy Notice (Comprehensive Version)

Last Updated: 05.08.2025

This Comprehensive Privacy Notice, together with our [Terms of Use], governs the collection, use, disclosure, and retention of your Personal Information by **NEXT SOLUTIONS CORP.** ("NEXT", "we", "us", or "our").

NEXT SOLUTIONS CORP. is a federally registered Canadian corporation (Corporation Number: **1001042225**), with its principal place of business at 155 East Beaver Creek Road, Suite 24-147, Richmond Hill, Ontario, L4B2N1, Canada.

Scope and Application

This notice applies to any individual ("you", "your") who:

- accesses or uses our websites, portals, or online platforms;
- uses software solutions, including any mobile or desktop applications provided by NEXT;
- communicates with us via email, phone, SMS, chat, web forms, or other channels;
- interacts with NEXT as a customer, prospective customer, authorized user, partner, or as a representative of a business client.

This notice also applies to all processing of personal information by NEXT in the course of its financial services activities under **NAICS Code 522329 – Other Financial Transactions Processing and Clearing House Activities**.

Our Commitment

NEXT SOLUTIONS CORP. is committed to protecting your privacy and handling your Personal Information responsibly, in compliance with the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and applicable provincial privacy laws (e.g., **Ontario's Freedom of Information and Protection of Privacy Act**, as applicable).

This Privacy Notice outlines:

- What types of Personal Information we collect;
- How and why we collect and use your Personal Information;
- How we disclose your Personal Information to third parties;
- The measures we take to safeguard your Personal Information;
- Your rights under Canadian privacy law and how you can exercise them;
- How long we retain your Personal Information;
- How to contact us regarding any privacy concerns.

Definitions

For the purposes of this Privacy Notice:

- **Personal Information** refers to any information about an identifiable individual, including information that can be used alone or with other information to identify, contact, or locate a specific person. Examples include name, contact information, identification documents, and transaction records.
- **Processing** means any action performed on personal data, such as collection, use, storage, transfer, disclosure, or deletion.

- **PIPEDA** refers to Canada's federal privacy law for private-sector organizations.

If you are located outside Canada, including in the European Economic Area (EEA) or the United States, this policy still applies, but additional local rights may apply, and we endeavor to respect those where required.

1. Collection and Use of Personal Information

A. What Personal Information We Collect

At NEXT SOLUTIONS CORP. ("NEXT"), we collect, use, and retain your personal information to provide our services effectively, meet our legal obligations, and continually improve our offerings. The collection of certain data may be mandatory under Canadian laws and regulations, such as anti-money laundering (AML) legislation, while other information is collected with your informed consent.

We only collect personal information that is necessary for the purposes identified in this Privacy Notice or as required by applicable law. Providing some personal information is optional; however, declining to provide certain requested details may limit our ability to offer specific services.

Examples of When We Collect Personal Information:

- When you register for an account or complete identity verification;
- When you initiate or complete a financial transaction;
- When you subscribe to updates or marketing communications;
- When you contact our support team via email, phone, webchat, or online forms;
- When you participate in user surveys or promotional campaigns;
- When you engage with our services via our website or applications.

We also collect information from third parties, including but not limited to payment providers, identity verification services, business partners, fraud detection agencies, and publicly available sources.

Types of Personal Information Collected

Depending on your interaction with us, we may collect the following types of personal information:

1. Identification and Contact Information

- Full name, date of birth, nationality, and gender
- Residential and mailing address
- Telephone number and email address
- Signature and photographic ID
- Utility bills or other proofs of address

2. Account and Access Information

- Username and password
- Language preferences, notification settings
- Security questions and recovery options

3. Financial and Transactional Information

- Bank account or payment method details
- Transaction history (amounts, recipients, timestamps)
- Trading or account funding activity
- Tax identification number (TIN), Social Insurance Number (SIN)* — only where required by law

4. Identity Verification and AML-Related Information

- Passport, driver's license, national ID card details
- Visa, residency or immigration status
- Biometric identifiers (e.g. facial image, where required for verification)
- Screening results from AML/CTF systems and compliance tools

Note: Facial recognition or biometric data is collected and processed strictly in line with Canadian privacy law. We seek express or implied consent where required and ensure secure storage and limited use.

5. Employment and Business Information

- Job title, employer name, and office location
- Description of role and authorization to act on behalf of an organization
- Corporate ownership and control structures (for business clients)

6. Technical and Usage Data

- IP address, device identifiers, browser type, and OS
- Cookie identifiers, geolocation data (where enabled)
- Session duration, page interactions, clickstream data
- Login timestamps and security logs

See our **Cookie Statement** for additional details on cookies, tags, and tracking technologies.

7. Communication Records

- Email, phone, SMS, and in-app chat messages
- Feedback forms, customer support records
- Voice recordings (if calls are recorded for quality assurance)

How We Use Your Personal Information

We use personal information for purposes directly related to providing and maintaining our services, including but not limited to:

- Verifying your identity, conducting due diligence and fraud prevention checks
- Processing your transactions and ensuring secure account access
- Providing customer support and managing inquiries or complaints
- Sending service-related communications and product updates
- Meeting legal, regulatory, and compliance obligations (e.g. FINTRAC reporting)
- Conducting audits, internal controls, and legal investigations
- Improving user experience, website functionality, and service personalization

Where required by PIPEDA or applicable provincial law, we will obtain your consent before collecting, using, or disclosing your personal information for secondary purposes, such as marketing.

Information from Third Parties

We may obtain information about you from trusted third-party sources, such as:

- Financial institutions and payment processors
- AML/CTF compliance vendors
- Identity verification providers
- Public registries (e.g. corporate or sanction databases)
- Credit bureaus and fraud prevention agencies
- Social media platforms and publicly available online data

This information helps us validate your identity, assess risk, comply with legal obligations, and detect unusual or unauthorized activity.

Retention and Legal Basis

Your personal information will be retained for as long as necessary to fulfill the purposes outlined in this Privacy Notice, and as required by:

- The **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**
- The **Income Tax Act** and other financial recordkeeping obligations
- Any contractual obligations or regulatory audits

In most cases, this means we will retain account data for at least **five (5) years** from the date of last transaction or account closure.

We may also retain data where necessary to investigate or defend legal claims, respond to law enforcement inquiries, or comply with court orders.

Legal Ground for Processing (Canada & International)

While PIPEDA is based on **reasonableness** and **purpose limitation**, our processing activities may also align with GDPR Article 6 legal bases for EEA residents. These include:

- Consent (where applicable and revocable)
- Contractual necessity
- Legal obligation
- Legitimate interests (balanced against your rights and expectations)
- Public interest or legal investigations

Use of Cookies and Similar Technologies

NEXT SOLUTIONS CORP. ("NEXT") automatically collects certain technical and behavioral information when you interact with our website or platform. This is done through cookies and similar tracking technologies in order to ensure platform functionality, enhance user experience, and meet regulatory obligations under Canadian privacy laws such as PIPEDA. Cookies are small text files stored on your device's hard drive or browser when you visit our website. They help us recognize your device, understand how our services are being used, improve security, personalize content, and provide relevant advertising. We also use technologies like clear GIFs (web beacons), pixel tags, and local storage objects in conjunction with cookies.

The types of data collected through cookies and similar technologies may include:

- **Technical data**: IP address, browser type and version, operating system, device identifiers, browser plug-ins, and time zone.
- **Usage data**: Pages viewed, duration of visit, click behavior, navigation paths, and referral source.
- **Interaction data**: Mouse movements, scrolling activity, clicks, and how users respond to pop-ups or interface changes.
- **Email behavior**: Whether you open or click through marketing or service emails sent by us.
- **Location data**: When enabled, we may collect approximate or real-time geolocation data via browser or mobile app permissions.

We may engage **third-party analytics providers** (e.g., Google Analytics or similar services) to help us understand user behavior and trends. These providers may place their own cookies or similar identifiers on your device, but are contractually obligated to process such data only for our benefit and in accordance with applicable privacy laws.

You can manage your cookie preferences via your browser settings or device controls. Disabling cookies may impact your ability to use certain features, such as logging into your account or completing transactions. By continuing to use our services with cookies enabled, you agree to our use of such technologies in accordance with this notice and our Cookie Policy.

How We Use Your Personal Information

We collect, use, and retain your personal information for a variety of purposes in accordance with the principles of **fairness, necessity, and reasonableness** under the **Personal Information Protection and Electronic Documents Act (PIPEDA)**. Our processing is guided by legal obligations, contractual necessity, your consent, or our legitimate interests.

Your personal information may be used to:

- **Create and administer your account**, including user authentication, password management, preferences, and security settings;
- **Process transactions**, including payment facilitation, receipt issuance, and reconciliation;
- **Verify your identity**, fulfill KYC/AML obligations, and prevent fraud, in compliance with Canadian financial legislation, including the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act**;
- **Maintain legal and regulatory documentation**, including logs, agreements, and audit records;

- **Respond to your support requests** and resolve complaints or inquiries through our customer service team;
- **Customize your experience**, including interface preferences and personalized suggestions;
- **Conduct analytics and internal research** to improve service quality and system performance;
- **Enforce platform terms of use** and detect unauthorized or harmful activity;
- **Communicate with you**, including operational notices, policy updates, or legally required disclosures;
- **Comply with legal requirements**, law enforcement requests, or court orders, as applicable.

Some of these processing activities are required by law; others are based on your explicit or implied consent or on our legitimate interest in improving our service delivery.

Automated Decision-Making

We may use **automated decision-making technologies**, including algorithms and data models, to assess your eligibility for certain services or to identify potentially suspicious activity (e.g., fraud detection, credit risk scoring, or transaction blocking). These systems allow us to act promptly, improve risk management, and comply with regulatory standards.
Examples of automated decisions include:

- Denying or flagging suspicious account registration attempts;
- Rejecting transactions that deviate from your normal behavior patterns;
- Applying tiered service limits based on identity verification status or jurisdiction.

We do not rely on solely automated decisions that produce legal or similarly significant effects on you without meaningful human oversight, unless such processing is:

- Necessary to perform a contract with you;
- Authorized by law; or
- Based on your explicit consent.

Your Rights: If you disagree with an automated decision, you may request human review by contacting us at info@next-solutions.io or another designated privacy contact. We will review the decision manually and provide you with an explanation or alternative resolution, where appropriate.

Marketing Communications

We may use your contact information (e.g., name, email address, phone number) to send you **marketing materials**, promotional offers, service updates, newsletters, surveys, or invitations to events, if you have opted in or where permitted by applicable Canadian anti-spam laws (e.g., **Canada's Anti-Spam Legislation – CASL**).
Our marketing may be conducted via:

- Email campaigns;
- Push notifications or in-app messages;
- SMS (where permitted);
- Online advertising through our site or third-party platforms.

We may also engage third-party service providers or advertising networks to manage and deliver our campaigns. These third parties are contractually bound to use your personal data only for our purposes and are prohibited from selling or repurposing it.
Opt-Out Options:
You can withdraw your consent or opt out of receiving promotional communications at any time by:

- Clicking the "Unsubscribe" link in our emails;
- Updating your communication preferences in your user account;
- Contacting our privacy team at info@next-solutions.io

Please note that opting out of marketing does not affect communications that are **transactional** or **service-related**, such as billing notices, security alerts, or legal updates.

Disclosure and Transfer of Personal Information

We may disclose your personal information to third parties or governmental/regulatory authorities and transfer such information outside of Canada when necessary for the operation of our business, legal compliance, risk mitigation, or service provision. We ensure all such transfers are compliant with the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and other applicable Canadian privacy and financial legislation.

A. Disclosures to Third Parties

We may disclose your personal data in the following circumstances:

1. **Intra-Group Transfers**
   We may share personal information with other companies within our corporate group, including affiliates, subsidiaries, or parent entities. These entities may process your information to assist in providing services or support, subject to privacy safeguards consistent with this Policy.
2. **Service Providers and Contractors**
   We engage third-party service providers who assist us in areas such as:

- Information technology infrastructure and cybersecurity
- Marketing, analytics, and customer support
- Data storage and disaster recovery
- Transaction processing and payment gateways
- Identity verification and anti-fraud systems

These third parties act as "agents" or "service providers" under PIPEDA and are contractually obligated to maintain confidentiality, process data only on our behalf, and implement appropriate security measures. Your data is shared solely for the purpose of fulfilling their functions.

3. **Strategic Partners and Industry Databases**
   We may disclose personal data to third parties such as:

- Credit reporting agencies
- Fraud detection and prevention networks
- AML/KYC compliance partners
- Financial institutions and correspondent banks

This may occur in connection with your onboarding, creditworthiness assessment, or transaction monitoring. These disclosures are made on a "need-to-know" basis and are subject to security and confidentiality obligations.

4. **Marketing and Business Development**
   We may share anonymized or pseudonymized data with advertising partners or business development collaborators to analyze trends, test new services, or assess user engagement. We may also use partially completed web forms to improve customer experience or reach out with tailored support.
5. **Corporate Transactions**
   Your personal information may be disclosed in the context of a merger, acquisition, financing, restructuring, bankruptcy, or sale of all or a portion of our assets, provided the recipient is bound by confidentiality and continues to use the data in accordance with this Policy.
6. **Legal or Regulatory Requests**
   We may be required to disclose your personal data to:

- Law enforcement agencies
- Canadian regulators (e.g., FINTRAC, OSFI)
- Courts or tribunals
- Other competent authorities

Such disclosure will only be made in response to lawful demands, court orders, subpoenas, or when required under applicable Canadian or foreign law.

7. **Anti-Fraud and AML Screening**
   We may share your information with:

- Fraud prevention bureaus
- Screening agencies
- Analytics services
- Law enforcement (in case of suspicious activity)

This helps us assess risk, comply with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, detect patterns of fraud, and fulfill our obligations under risk-based KYC protocols.

8. **Creditworthiness and Linked Accounts**
   When you apply for financial services, we may perform credit checks that affect both your personal profile and any associated business entities, such as directors, shareholders, or guarantors. These checks may result in "soft" or "hard" inquiries appearing on your credit file and could create associations with joint account holders. Such associations remain until you submit a formal request to the credit bureau for disassociation.

We also report on how you manage your obligations (e.g., repayment status), and this may impact your credit profile. Information remains on file with agencies for up to 6 years after closure.

9. **Risk Management and Dispute Resolution**
   We may disclose your personal data to:

- Debt collection partners
- Legal counsel or advisors
- Mediators or arbitrators
- Insolvency administrators

This helps enforce our Terms of Use, resolve billing disputes, manage claims, and recover outstanding balances.

10. **Anonymized or Aggregated Data**
    We may disclose data that has been anonymized or aggregated in such a way that it cannot be re-identified. This information may be used for research, reporting, or benchmarking without further notice to you.
11. **Other Cases with Consent**
    Outside of the above scenarios, we will never sell, rent, or trade your personal information to third parties. Any new category of data sharing will only be implemented with your informed consent.

International Transfers

If your personal information is processed outside of Canada (e.g., by a cloud provider or payment processor), we take steps to ensure that it receives an adequate level of protection. These may include:

- Entering into contracts with foreign service providers that incorporate model contractual clauses;
- Requiring adherence to internationally recognized security standards (e.g., ISO 27001);
- Limiting access to your personal data only to those who need it for service provision or legal compliance.

Where required by law, we will notify you of cross-border transfers and obtain your consent if the jurisdiction does not provide equivalent protections to those required under PIPEDA.

Disclosure to Legal and Regulatory Authorities

We may disclose your personal information to Canadian or international authorities when such disclosure is required or permitted by law, regulation, or public interest considerations. These disclosures are conducted in accordance with:

- the **Personal Information Protection and Electronic Documents Act (PIPEDA)**;
- the **Privacy Act** (for disclosures involving federal institutions); and

- other applicable provincial or federal legislation, including anti-money laundering and anti-terrorist financing laws (**PCMLTFA**).

We may share your personal data with law enforcement agencies, regulatory bodies, courts, or government authorities in the following cases:

- When compelled by **a court order, subpoena, search warrant, or other valid legal process**, including requests from Canadian federal or provincial regulators (e.g., FINTRAC, CRA, RCMP).
- Where there are **reasonable grounds to believe that a violation of Canadian or international law has occurred**, including fraud, financial crime, or threats to national security.
- Where required to **report suspected illegal activity**, money laundering, or terrorist financing.
- When necessary to **investigate actual or suspected violations of this Privacy Policy, our Terms of Use, or applicable agreements** with you.
- To respond to **formal inquiries** or **audits** from regulatory authorities to whom we are accountable under law or by virtue of industry self-regulation (e.g., financial service regulation).
- When deemed necessary to **protect the vital interests** of an individual, or in the public interest (e.g., in response to a declared emergency or threat).

All such disclosures are limited to what is strictly necessary and are documented in accordance with our internal compliance policies and audit requirements.

International Transfers of Personal Data

We may store, access, and process your personal data outside of Canada, including in jurisdictions where our cloud infrastructure, affiliates, or third-party service providers are located. These may include countries such as the United States, member states of the European Economic Area (EEA), the United Kingdom, and others.

Key points regarding such transfers:

- Transfers are conducted **only when necessary** for service provision, technical support, regulatory compliance, fraud prevention, or customer service.
- Where personal information is transferred outside of Canada, it may be **subject to access by foreign courts, law enforcement, or national security authorities** under applicable laws of those jurisdictions.

Safeguards for international data transfers include:

- Execution of **contractual agreements** with service providers that incorporate **Standard Contractual Clauses (SCCs)** approved by the European Commission, where applicable;
- Implementation of **binding contractual commitments** to comply with Canadian privacy laws and provide equivalent protections;
- Conducting **risk assessments** to evaluate the legal environment of recipient countries;
- Use of **data minimization, encryption, and pseudonymization** techniques to protect personal data in transit and storage;
- Ongoing **monitoring and auditing** of third-party compliance with our privacy obligations.

We ensure that all such transfers are in compliance with PIPEDA's cross-border data flow principles and, where applicable, the guidance of the **Office of the Privacy Commissioner of Canada (OPC)**.

You may request additional details regarding our data transfer arrangements or a copy of applicable safeguards by contacting us via the details provided in the "Contact Us" section of this Policy.

Your Rights Regarding Your Personal Information

Under applicable Canadian privacy laws, including the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and, where applicable, relevant **provincial privacy legislation** (such as Quebec's Law 25, Alberta's PIPA, or BC's PIPA), you have a number of important rights relating to your personal information. You may exercise any of these rights by contacting us at info@next-solutions.io

We will respond to your request within the timelines set out by law (typically 30 calendar days), and in a manner that is transparent and accessible.

1. Right to Access

You have the right to request whether we hold any personal information about you and, if so, to request access to such information. This includes information on how we collect, use, disclose, and retain it. Upon verified request, we will provide:

- A copy of your personal data in our custody or control;
- A description of how it has been used and shared;
- The identity of any third parties to whom it has been disclosed.

Note: If the request is extensive or involves a large volume of records, we may ask you to clarify your request or charge a reasonable fee (in line with Section 9(5) of PIPEDA).

2. Right to Rectification

You may request correction or updating of any inaccurate, incomplete, or outdated personal information we hold about you. We will correct such data and inform any third parties to whom we disclosed the inaccurate data (if applicable), unless it is impractical or prohibited by law.

3. Right to Erasure ("Right to be Forgotten")

You may request the deletion of your personal information in certain circumstances, such as:

- If the information is no longer necessary for the purposes for which it was collected;
- If you withdraw consent (where consent is the lawful basis for processing);
- If the processing is unlawful;
- If required by law.

However, we may retain your data where:

- It is necessary to comply with legal obligations (e.g., financial record-keeping under PCMLTFA);
- It is needed for internal auditing, dispute resolution, or investigation of potential violations;
- Retention is required under our contractual or regulatory obligations.

4. Right to Restrict Processing

You may request to restrict or limit the use of your personal data in the following cases:

- You contest the accuracy of the data (pending verification);
- You object to processing based on legitimate interests;
- The data is no longer needed for our purposes but is required by you for legal claims.

During the period of restriction, we will not process your data for any purpose other than storing it and maintaining its integrity, unless legally authorized to do so.

5. Right to Data Portability

Where technically feasible, and where the processing is based on your consent or a contract, you may request that we provide your personal data in a structured, commonly used, and machine-readable format, and/or transmit it directly to another organization (upon request). Please note that this right may be limited under Canadian law compared to the GDPR and may not apply to all types of data.

6. Right to Object

You may object to the processing of your personal data based on our legitimate interests, including for:

- Direct marketing purposes;
- Profiling related to marketing;

- Automated decision-making, where it produces legal or similarly significant effects.

We will cease such processing unless we can demonstrate compelling legitimate grounds to continue processing or if the processing is necessary for legal claims.

7. Right to Withdraw Consent

If we process your personal data based on your consent, you may withdraw that consent at any time. This will not affect the lawfulness of processing carried out before the withdrawal. However, withdrawal may affect your ability to access some or all of our services.

8. Right to Challenge Compliance

You have the right to challenge our compliance with Canadian privacy legislation by:

- Contacting our Privacy Officer at [insert contact];
- Filing a complaint with the **Office of the Privacy Commissioner of Canada (OPC)** at www.priv.gc.ca, or with the relevant provincial privacy authority.

Important Limitations:

These rights are subject to certain legal and operational limitations. For example:

- We cannot delete personal data that we are legally obligated to retain.
- We may refuse requests that are manifestly unfounded or excessive.
- We may require identity verification before fulfilling your request to protect your privacy and the security of your information.

Security of Personal Information

We take the protection of your Personal Information seriously and implement a comprehensive set of organizational, physical, and technological safeguards to help ensure the confidentiality, integrity, and availability of the data we process.

These measures are designed to protect your Personal Information from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks. Our approach includes, but is not limited to:

- **Encrypted communication protocols** such as TLS/SSL for data transmitted over the internet;
- **Password-protected systems and accounts**, with strong authentication requirements;
- **Role-based access control (RBAC)** limiting employee access to Personal Information strictly on a need-to-know basis;
- **Data encryption at rest and in transit**, including storage of sensitive financial data in encrypted environments;
- **Ongoing vulnerability assessments**, including regular security audits and penetration testing;
- **Data loss prevention (DLP) technologies** to monitor and prevent unauthorized transfer of information;
- **Firewalls and intrusion detection/prevention systems** on all critical infrastructure;
- **Multi-factor authentication (MFA)** for access to administrative areas and customer databases;
- **Monitoring and logging of access events** to identify and investigate potential security breaches;
- **Mandatory security and privacy training** for all employees and contractors with access to personal data.

Please note that no transmission of data over the internet is ever fully secure. While we make every effort to protect your Personal Information, including using secure channels when communicating with you, we cannot guarantee the absolute security of data shared online. We recommend that you use caution and verify the authenticity of any communication purporting to be from our company, particularly requests for payment information.

You are responsible for safeguarding your own login credentials (e.g., account passwords or PINs). If you believe that your account or personal information has been compromised, please contact us immediately using the contact details provided in this Policy.

Retention of Personal Information

We retain your Personal Information only for as long as necessary to fulfill the specific purposes for which it was collected, and to comply with legal, regulatory, accounting, or auditing obligations under applicable Canadian laws, including but not limited to:

- **Personal Information Protection and Electronic Documents Act (PIPEDA)**;
- **Canada's Income Tax Act**, **PCMLTFA**, and other financial compliance legislation;
- **Applicable provincial privacy laws**, where they apply.

The criteria we use to determine appropriate retention periods include:

- The nature of the services we have provided to you;
- Whether you still have an active account or ongoing relationship with us;
- Whether we are under a legal obligation to retain certain data (e.g., for tax, AML/CTF compliance, or dispute resolution);
- Whether retention is necessary to investigate or defend actual or potential legal claims;
- Whether your data has been aggregated or anonymized for analytic or research purposes (in which case it may be retained longer, provided it cannot identify you).

Retention periods may include:

- **5–10 years**: Account records, transaction data, identity verification records (as required by AML/CTF laws);
- **Up to 7 years**: Tax and billing documentation under federal and provincial financial record-keeping laws;
- **Until you withdraw consent**: Where consent was the basis for collection, and no other legal basis for retention applies;
- **Immediately upon closure of your account**: For non-essential or optional profile information, unless required otherwise.

Once the retention period has expired, or if the data is no longer needed, we will securely delete, anonymize, or de-identify it in accordance with industry standards and best practices. For any questions regarding our retention schedules or to request deletion of your Personal Information (where permitted by law), please contact our Privacy Officer.

Updates to this Privacy Policy

This Privacy Policy may be updated periodically to reflect changes in our practices, technologies, legal requirements, or for other operational reasons.

The **“Last Updated”** date at the top of this Policy indicates the date on which the latest changes were made. We recommend reviewing this page frequently to stay informed about how we process your Personal Information.

When significant changes are made, we will notify you in advance by appropriate means, such as:

- Posting a prominent notice on our website or platform,
- Sending you an in-app notification or email (where applicable),
- Updating the change log or version history of the Privacy Policy.

Unless otherwise stated, updates to this Policy become effective as of the date they are published on our website. If you continue to use our services after changes are implemented, you will be deemed to have accepted the revised Privacy Policy.

Definitions

- **Account**: A contractual relationship established when a user accepts our Terms of Use and Privacy Policy and is approved to access our services, including financial or crypto-related functionality where applicable.
- **Platform**: The technological infrastructure (including mobile apps, APIs, user interfaces, servers, and backend systems) we use to deliver our services.
- **DPL**: The applicable data protection law(s), which include:

    - **PIPEDA** – The Personal Information Protection and Electronic Documents Act (Canada),
    - The **EU GDPR** – Regulation (EU) 2016/679,
    - The **Swiss Federal Act on Data Protection (FADP)**,
    - and any successor or analogous legislation that governs our use of Personal Information.
- **Personal Information**: Any data that identifies or could reasonably identify an individual, either directly (e.g., name, email, address) or indirectly (e.g., IP address, device ID, usage data). This does **not** include anonymized or de-identified data that cannot be linked back to an individual.
- **Service(s)**: All tools, software, APIs, platforms, and related functionalities made available by us, including the facilitation of transactions involving cryptocurrency or other digital assets, financial services, customer support, account management, and community features.
- **Transaction**: Any financial or digital interaction made on our platform, including but not limited to:
    - The buying or selling of digital assets,
    - Transfers between user accounts,
    - Payments or withdrawals facilitated through the platform.

Global Notice

This Privacy Policy is intended to apply globally, but nothing in this Policy shall limit or override any local laws, consumer rights, or data protection provisions applicable in your jurisdiction. In the event of a conflict between this Policy and applicable regional or national data protection law, the latter shall prevail.

Contacting Us

If you have any questions, concerns, or complaints regarding how we handle your Personal Information, or if you would like to exercise any of your rights as described above, you may contact our Privacy Officer directly: info@next-solutions.io

Complaints

If you believe that your privacy rights have been violated or your data has been mishandled, you have the right to lodge a complaint with the appropriate data protection authority.
In Canada:
You can file a complaint with the Office of the Privacy Commissioner of Canada (OPC): https://www.priv.gc.ca