Privacy Policy

Xen Accounting Inc.

Effective Date: April 14, 2026 | Version: 3.0

Next Scheduled Review: April 14, 2027

1. Introduction

Xen Accounting Inc. ("**Xen Accounting**", "we", "us", or "our") is a Québec-headquartered online accounting firm. We are committed to protecting the personal information entrusted to us by our clients, website visitors, job applicants, and employees, and we treat privacy as a foundational element of our professional obligations.

This Privacy Policy explains what personal information we collect, why we collect it, how we use and share it, how we protect it, and the rights you have with respect to your personal information. It is designed to comply with Québec's Act respecting the protection of personal information in the private sector (commonly known as "Law 25"), the federal Personal Information Protection and Electronic Documents Act ("PIPEDA"), and other applicable Canadian privacy laws. As a professional accounting firm, we and our personnel are also bound by the professional confidentiality obligations of the Ordre des comptables professionnels agréés du Québec.

This Privacy Policy is the public-facing summary of our privacy practices. It is supported by an internal document titled "Policies and Practices Governing the Protection of Personal Information," which is maintained by our Privacy Officer in accordance with section 3.2 of Law 25 and is available on request where appropriate.

By engaging our services, visiting our website, or otherwise providing personal information to us, you acknowledge that you have read and understood this Privacy Policy.

2. Scope

This Policy applies to personal information we collect about:

- Clients and prospective clients, including their owners, directors, officers, employees, and authorized representatives;
- Visitors to our website and users of our online services;
- Job applicants and candidates;
- Current and former employees, contractors, and service providers; and
- Any other individual whose information is shared with us in the course of providing accounting, bookkeeping, payroll, tax, or advisory services.

This Policy does not apply to information about legal persons (corporations) or to de-identified or anonymized information that, on its own or in combination, cannot reasonably be used to identify an individual.

3. Our Privacy Principles

Our handling of personal information is guided by the following principles, which reflect Law 25, PIPEDA, and recognized international standards:

- **Lawfulness and transparency —** We collect and use personal information only for legitimate, clearly identified purposes that we disclose to you.
- **Purpose limitation —** We do not use personal information for purposes materially different from those for which it was collected without obtaining fresh consent, unless permitted by law.
- **Data minimization —** We collect only the personal information that is necessary to achieve the identified purposes.
- **Accuracy —** We take reasonable steps to keep personal information accurate, complete, and up to date.
- **Security —** We apply administrative, technical, and physical safeguards proportionate to the sensitivity of the information.
- **Accountability —** We maintain governance practices, assign clear responsibility to our Privacy Officer, and conduct Privacy Impact Assessments where required by law.
- **Privacy by default —** Where we offer technological products or services to the public, their privacy settings are configured to the highest level of confidentiality by default.

4. Personal Information We Collect

The categories of personal information we collect depend on the nature of our relationship with you. They may include:

4.1 Identification and Contact Information

- Name, title, and date of birth;
- Home and business address, email address, and telephone number;
- Government-issued identification numbers required for tax filings and regulatory compliance, including Social Insurance Numbers (SIN), business numbers, and GST/QST numbers.

4.2 Financial and Accounting Information

- Banking information, including account and transit numbers, for payment processing and pre-authorized debits;
- Bookkeeping records, invoices, receipts, and supporting documentation;
- Tax records, income information, and filings made on your behalf;
- Payment card information handled by our payment processors on our behalf — we do not store full payment card numbers on our systems.

4.3 Payroll and Employment Information (Where We Process Payroll for Clients)

- Employee names, addresses, dates of birth, SINs, and banking information;
- Salary, wage, benefit, deduction, and time-tracking information;
- Employment status, start and end dates, and Record of Employment (ROE) data;
- Provincial tax slip information, including Québec Relevé 1 forms.

4.4 Technical and Usage Information

- IP address, browser type, device identifiers, and operating system;

- Pages visited, time spent on our website, and referring URLs;
- Cookies and similar tracking technologies (see Section 11).

4.5 Communications

- Emails, support tickets, meeting recordings (where you have been notified and consented), and other correspondence.

Sensitive personal information. Some of the information we collect — such as SINs, banking details, and payroll records — is considered sensitive under Law 25, either because of its nature or the context of its use. We apply enhanced safeguards to this information, including strict access controls and encryption, and we collect it only where strictly necessary to deliver our services or meet legal obligations.

Biometric information. We do not currently collect or process biometric information. If this were to change, we would notify the Commission d'accès à l'information du Québec as required by law and obtain your express consent in advance.

5. How We Collect Personal Information

We collect personal information:

- Directly from you, when you engage our services, complete forms, email us, or speak with our team;
- From your authorized representatives, such as your bookkeeper, lawyer, or business partners;
- From third parties with your consent, such as financial institutions, the Canada Revenue Agency, or Revenu Québec;
- Automatically, through cookies and analytics on our website (see Section 11).

6. Purposes for Which We Use Personal Information

We use personal information only for the purposes for which it was collected, or for compatible purposes that a reasonable person would expect. These purposes include:

- Providing accounting, bookkeeping, tax, payroll, advisory, and related professional services;
- Preparing and filing tax returns and government remittances;
- Processing payroll for clients, including direct deposits, source deductions, and year-end tax forms (T4, T4A, Relevé 1, ROE), delivered through platforms such as Wagepoint, Payworks, or Employeur D depending on client needs;
- Processing payments to and from your business, including accounts payable (via Plooto) and client payments (via Rotessa);
- Communicating with you about your file, our services, and service updates;
- Managing our client relationship, including billing, collections, and account administration;
- Meeting our legal, regulatory, and professional obligations, including anti-money-laundering and record-retention requirements;
- Recruiting, assessing, and managing employees and contractors;

- Operating, securing, and improving our website and internal systems;
- Preventing fraud, unauthorized access, and other security incidents.

We will not use your personal information for new purposes materially different from those listed above without obtaining your consent, except where permitted or required by law.

Use of artificial intelligence. We may use AI-enabled tools within our approved software stack (for example, features embedded in our accounting, email, or productivity platforms) to improve efficiency and accuracy. We do not submit client personal information to public or general-purpose AI services. Any AI feature that processes personal information must be reviewed by our Privacy Officer and operate under contractual terms that prohibit the vendor from using client data to train public models.

7. Consent

We collect, use, and disclose personal information with your consent, except where the law permits or requires us to do so without consent. Consent may be express (for example, when you sign an engagement letter) or implied (for example, when you provide information in the course of receiving our services). For sensitive personal information, we seek express consent.

You may withdraw your consent at any time, subject to legal or contractual restrictions and reasonable notice. Withdrawing consent may affect our ability to continue providing services to you. To withdraw consent, contact our Privacy Officer using the details in Section 14.

Consent for minors. We do not knowingly provide services directly to individuals under the age of 14. Where information about a minor under 14 is collected in the course of our engagement (for example, as a dependant on a tax return), we rely on the consent of the parent or person having parental authority.

8. Disclosure and Sharing of Personal Information

We do not sell personal information. We disclose personal information only as follows:

8.1 Service Providers and Processors

We use trusted third-party service providers to help us deliver our services. Each provider is subject to a written agreement requiring them to protect personal information, use it only for the purposes we specify, apply safeguards proportionate to the sensitivity of the information, and notify us of any confidentiality incidents. Our current key service providers are:

Service Provider	Purpose	Data Location
QuickBooks Online / Xero	Cloud accounting and bookkeeping software	United States
Wagepoint	Canadian payroll processing, direct deposit, and year-end tax forms	Canada
Payworks	Canadian payroll processing, HR, and time-and-attendance management	Canada

Employeur D (Desjardins)	Québec and Canadian payroll processing, source deductions, and tax slip preparation	Canada
Dext / Hubdoc	Receipt and source-document capture	United States / Canada
Google Workspace / Microsoft 365	Email, document storage, and internal collaboration	United States
Teamwork	Project and workflow management	United States / European Union
Rotessa	Pre-authorized debit processing for client payments	Canada
Plooto	Accounts payable and bill payment processing	Canada
Zendesk	Client support ticketing and communications	United States
Amazon Web Services / Microsoft Azure	Cloud infrastructure hosting	United States

We perform documented due diligence before engaging new service providers that will have access to personal information, and we review the relationship periodically. Where available, we give preference to providers with recognized security certifications (such as SOC 2, ISO 27001, or ISO 27701). If we materially change the set of service providers used to handle your personal information, we will update this Policy accordingly.

8.2 Government Authorities

We disclose personal information to the Canada Revenue Agency, Revenu Québec, and other tax, regulatory, or government authorities where required to deliver our services or comply with law (for example, filing tax returns or responding to a lawful production order).

8.3 Professional Advisors

With your express authorization, we may share information with your other professional advisors, such as lawyers, financial planners, or bankers, to the extent necessary for them to assist you.

8.4 Legal and Regulatory Disclosures

We may disclose personal information without consent where permitted or required by law, including to investigate fraud, enforce our rights, comply with court orders, or respond to lawful requests from public authorities.

8.5 Business Transactions

In the event of a merger, acquisition, reorganization, or sale of assets, personal information may be transferred to the successor entity, subject to appropriate confidentiality protections and applicable law. You will be notified of any such transfer where required.

9. Transfers of Personal Information Outside Québec

Important notice. Several of the service providers listed in Section 8.1 — specifically QuickBooks Online, Xero, Google Workspace, Microsoft 365, Teamwork, Zendesk, Amazon Web Services, and Microsoft Azure — store or process personal information outside of Québec, primarily in the United States. This means your personal information may be subject to the laws of the jurisdictions where it is stored, including lawful access by foreign courts, law enforcement, and national security authorities.

Our Canadian-resident service providers (Wagepoint, Payworks, Employeur D, Rotessa, and Plooto) store personal information within Canada.

Before transferring personal information outside Québec, we conduct a Privacy Impact Assessment ("PIA") as required by Law 25 to confirm that the information will receive adequate protection. Each PIA considers:

- The sensitivity of the information being transferred;
- The purposes of the transfer and the safeguards applied to it;
- The legal framework of the destination jurisdiction, including access by public authorities; and
- The contractual and technical protections in place with the service provider.

We enter into written agreements with our out-of-province service providers requiring them to apply technical, administrative, and organizational safeguards appropriate to the information entrusted to them, and we retain documentation of our PIAs for audit and regulatory purposes.

By engaging our services, you acknowledge that your personal information may be transferred, stored, and processed outside of Québec and Canada in accordance with this Policy.

10. Retention, Destruction, and Anonymization

We retain personal information only as long as necessary to fulfill the purposes for which it was collected, or as required by applicable tax, professional, and legal obligations. Accounting, tax, and payroll records are generally retained for a minimum of six (6) years from the end of the last tax year to which they relate, in accordance with CRA and Revenu Québec requirements; longer retention periods may apply where required by law or professional standards.

Our detailed retention schedule is maintained in our internal Policies and Practices document and is reviewed by the Privacy Officer periodically.

Once personal information is no longer needed and any applicable retention period has expired, we destroy it securely or anonymize it. Where we anonymize information for serious and legitimate purposes, the anonymization process follows the criteria prescribed under Québec law so that the information can no longer, at any time, be used to directly or indirectly identify an individual.

11. Cookies and Tracking Technologies

Our website uses cookies and similar technologies to operate the site, remember your preferences, analyze usage, and improve our services. Some cookies are strictly necessary for the site to function, while others (such as analytics cookies) are optional.

In accordance with Law 25, we request your express opt-in consent before activating non-essential tracking technologies, including technologies that may profile you or identify you across sessions. You can adjust your cookie preferences at any time through the cookie banner on our website or through your browser settings.

Where we offer technological products or services to the public, their privacy settings are configured, by default, to the highest level of confidentiality.

12. Automated Decision-Making and Profiling

We do not currently make decisions about you based exclusively on automated processing of personal information. We also do not use profiling technology to identify, locate, or build behavioural profiles of individuals.

If this changes, we will update this Policy, inform affected individuals in advance, and provide the rights required under Law 25, including the right to be informed of the principal factors and parameters that led to the decision, the right to submit observations, and the right to request human review.

Any new system or project that involves the collection, use, communication, retention, or destruction of personal information — including the introduction of new AI-enabled tools — will be subject to a Privacy Impact Assessment proportionate to the sensitivity of the data and the risks involved.

13. Your Rights

Subject to applicable law, you have the following rights with respect to your personal information:

- **Access.** You may request confirmation of whether we hold personal information about you and receive a copy of it.
- **Rectification.** You may request that we correct inaccurate, incomplete, or out-of-date information.
- **Withdrawal of consent.** You may withdraw your consent to our collection, use, or disclosure of your personal information, subject to legal and contractual restrictions.
- **Portability.** You may request that we release computerized personal information we hold about you in a structured, commonly used technological format, or transmit it to another organization you designate.
- **De-indexing and cessation of dissemination.** You may request that we stop disseminating your personal information or de-index any link that provides access to it, where the conditions set out in Law 25 are met.
- **Information about automated processing.** Where applicable, you may request information about any automated decision made about you and ask for human review.
- **Complaint.** You may file a complaint with us or with the Commission d’accès à l’information du Québec (see Section 15).

To exercise any of these rights, contact our Privacy Officer using the details in Section 14. We will respond in writing within thirty (30) days of receiving your request. We may need to verify your identity before acting on your request, and we will only request the minimum information necessary to do so. Our response is provided free of charge, except where the law allows us to

charge a reasonable fee, in which case we will advise you in advance and you may withdraw or modify your request at no cost.

14. Privacy Officer

In accordance with section 3.1 of Law 25, we have designated a Privacy Officer who is responsible for ensuring our compliance with this Policy and applicable privacy laws, overseeing our governance practices, responding to requests, and managing confidentiality incidents. The Privacy Officer for Xen Accounting is:

Privacy Officer — Partner, Xen Accounting Inc.

Name: Joseph Steben, CPA Auditor

Email: admin@xenaccounting.com

Mailing address: 360 rue Saint-Jacques, Suite G101, Montreal, QC, H2Y 1P5

You may contact the Privacy Officer with any questions, requests, or complaints about this Policy or our handling of your personal information.

15. Complaints to the Regulator

If you are not satisfied with our response to a privacy request or complaint, you may contact the Commission d'accès à l'information du Québec (CAI):

Commission d'accès à l'information du Québec

Website: www.cai.gouv.qc.ca

Telephone: 1-888-528-7741

16. Security of Personal Information

We maintain administrative, technical, and physical safeguards designed to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. These safeguards are proportionate to the sensitivity of the information and the risks of processing, and include:

16.1 Technical Safeguards

- Encryption of personal information in transit using TLS and at rest where supported by our systems and service providers;
- Mandatory multi-factor authentication (MFA) for all employee and contractor access to systems holding personal information;
- Role-based access controls, applying the principle of least privilege so that team members can access only the personal information they need;
- Logging and monitoring of access to sensitive systems;
- Secure configuration of endpoints, including full-disk encryption and endpoint protection;
- Regular backup of business-critical systems and documented recovery procedures to support continuity of service.

16.2 Administrative Safeguards

- Written confidentiality obligations in every employee and contractor agreement, supplementing the professional secrecy obligations that apply to our personnel;
- Background checks on personnel with access to sensitive personal information, where permitted by law;
- Mandatory privacy and security training for all personnel at onboarding and at least annually thereafter;
- Documented onboarding and offboarding procedures that revoke access promptly upon role change or departure;
- Written agreements with all service providers who handle personal information on our behalf, including security, confidentiality, and incident notification obligations;
- Documented vendor due diligence and periodic review of service providers.

16.3 Governance Safeguards

- An internal Policies and Practices document governing the protection of personal information throughout its lifecycle;
- Defined roles and responsibilities for personnel involved in the processing of personal information;
- A complaints-handling process overseen by the Privacy Officer;
- Privacy Impact Assessments for new information systems, electronic service-delivery projects, new AI-enabled tools, and transfers of personal information outside Québec;
- Periodic internal review of our privacy and security practices.

Despite these measures, no method of transmission or storage is completely secure, and we cannot guarantee absolute security.

17. Confidentiality Incidents and Breach Notification

We maintain a documented incident-response process for suspected or confirmed confidentiality incidents (data breaches). Our Privacy Officer oversees the investigation, containment, and remediation of any incident.

Where a confidentiality incident presents a risk of serious injury to one or more individuals — assessed based on the sensitivity of the information involved, the apprehended consequences of its use, and the likelihood that it will be used for injurious purposes — we will:

- Notify the affected individuals with reasonable promptness and provide them with the information required by law;
- Notify the Commission d’accès à l’information du Québec with reasonable promptness;
- Take the measures necessary to reduce the risk of injury and to prevent recurrence.

We maintain a register of all confidentiality incidents, regardless of whether they trigger a notification obligation, and we retain each entry for at least the minimum period required by applicable regulation. A copy of the register is provided to the Commission on request.

18. Policy Governance and Updates

This Policy is reviewed and approved by the Privacy Officer at least annually, and more frequently where changes in our practices, our service providers, applicable law, or the threat landscape warrant it. Material changes will be communicated through our website and, where appropriate, directly to affected individuals.

Version history. Version 3.0 — Effective April 14, 2026. Current version supersedes all prior versions.

19. Contact Us

If you have any questions about this Privacy Policy or our privacy practices, please contact our Privacy Officer at **admin@xenaccounting.com**.