Certivo

Privacy Policy

Company: Ready 4 Everything Training and Supplies Ltd.

Privacy Officer: Aaron Hoyte

Jurisdiction: Alberta, Canada

Date: March 2026 (Updated)

Applicable Law: PIPEDA, Alberta PIPA, Quebec Law 25

Ready 4 Everything Training and Supplies Ltd. Certivo — certivo.ca

Effective Date: March 1, 2026 **Last Updated:** November 1, 2026

Table of Contents

1. Introduction
2. Definitions
3. Scope and Application
4. Accountability (Principle 1)
5. Identifying Purposes (Principle 2)
6. Consent (Principle 3)
7. Limiting Collection (Principle 4)
8. Limiting Use, Disclosure, and Retention (Principle 5)
9. Accuracy (Principle 6)
10. Safeguards (Principle 7)
11. Openness (Principle 8)
12. Individual Access (Principle 9)
13. Challenging Compliance (Principle 10)
14. Types of Personal Information Collected
15. Third-Party Service Providers
16. Cross-Border Data Transfers
17. Cookies and Similar Technologies
18. Data Retention
19. Children's Privacy
20. Changes to This Policy
21. Contact Information

1. Introduction

Ready 4 Everything Training and Supplies Ltd. o/a Certivo (operating the Certivo platform, "Certivo," "we," "us," or "our") is committed to protecting the privacy and confidentiality of personal information entrusted to us. This Privacy Policy describes how we collect, use, disclose, and protect personal information through the Certivo ("Platform"), a multi-tenant software-as-a-service (SaaS) platform for safety training companies, accessible at certivo.ca.

This Privacy Policy is designed to comply with the **Personal Information Protection and Electronic Documents Act** (PIPEDA, S.C. 2000, c. 5), the **Personal Information Protection Act** (PIPA, S.A. 2003, c. P-6.5) of Alberta, the **Personal Information Protection Act** (PIPA, S.B.C. 2003, c. 63) of British Columbia, and Quebec's **Act respecting the protection of personal information in the private sector** (CQLR c. P-39.1), as amended by **Law 25**. Where these laws differ, we apply the standard that affords greater protection to the individual. Section 3 describes how each provincial law applies.

By using the Platform, you acknowledge that you have read and understood this Privacy Policy and consent to the collection, use, and disclosure of your personal information as described herein.

---

2. Definitions

For the purposes of this Privacy Policy:

- **"Personal Information" (PI)** means information about an identifiable individual, as defined under PIPEDA and PIPA, but does not include the name, title, business address, or telephone number of an employee of an organization.
- **"Tenant"** means a safety training company or organization that subscribes to the Platform to manage its operations.
- **"Tenant Administrator"** means an authorized user of a Tenant who manages the Tenant's account, staff, and operations through the Tenant Suite application.
- **"Instructor"** means an individual engaged by a Tenant to deliver safety training courses, who accesses the Platform through the Instructor Suite application.
- **"Client"** means a company or individual that contracts with a Tenant for safety training services and accesses the Platform through the Client Portal application.
- **"Student"** means an individual enrolled in safety training courses managed through the Platform.
- **"Platform Operator"** means Ready 4 Everything Training and Supplies Ltd. o/a Certivo in its capacity as operator of the Platform.
- **"Privacy Officer"** means the individual designated by Certivo to be responsible for compliance with this Privacy Policy and applicable privacy legislation.

---

3. Scope and Application

3.1 What This Policy Covers

This Privacy Policy applies to all personal information collected, used, or disclosed by Certivo through:

- The **Tenant Suite** application (administrative management)
- The **Instructor Suite** application (instructor operations and mobile access)
- The **Client Portal** application (client self-service access)
- The **Super Admin** application (platform operations, accessible only to Certivo staff)
- The Certivo website at certivo.ca
- Cloud Functions and backend services operated by Certivo
- Communications sent through or on behalf of the Platform (emails, notifications)

3.2 Multi-Tenant Data Processing

Certivo operates as both a **data controller** (for Platform account data, billing, and platform operations) and a **data processor** (for Tenant-managed operational data including student records, certification records, incident reports, and payroll data). Each Tenant is the data controller for the personal information of its instructors, clients, and students that it manages through the Platform.

3.3 Alberta PIPA Compliance

Certivo is operated by Ready 4 Everything Training and Supplies Ltd., an Alberta corporation, and is subject to PIPA for the collection, use, and disclosure of personal information within Alberta. PIPA has been declared substantially similar to PIPEDA by the Governor in Council. Certivo complies with both statutes and applies the higher standard where they differ.

3.4 British Columbia PIPA Compliance

Where a Tenant, instructor, client, or student is located in British Columbia, Certivo applies the **Personal Information Protection Act** (PIPA, S.B.C. 2003, c. 63). BC PIPA has been declared substantially similar to PIPEDA. In practice this means parity on the core rights already provided under this Policy: the right to access one's own personal information (Section 12) and to request correction of inaccurate information (Section 9); consent-based collection limited to purposes a reasonable person would consider appropriate (Section 6); and notification of a privacy breach that could reasonably be expected to cause significant harm. Access and correction requests from individuals in British Columbia are handled on the same timelines and through the same Privacy Officer contact (Section 4.1) as elsewhere in this Policy.

3.5 Quebec Law 25 Compliance

Where a Tenant, instructor, client, or student is located in Quebec, Certivo applies Quebec's **Act respecting the protection of personal information in the private sector** (CQLR c. P-39.1), as amended by **Law 25** (formerly Bill 64). Specifically:

- **Person in charge of the protection of personal information.** The Privacy Officer designated in Section 4.1 (Aaron Hoyte) also serves as the "person in charge of the protection of personal information" for the purposes of Law 25. This individual's title and contact information are published in this Policy.
- **Confidentiality incidents.** Certivo maintains a register of confidentiality incidents. Where a confidentiality incident presents a risk of serious injury, Certivo will notify the Commission d'accès à l'information (CAI) and the affected individuals with reasonable promptness, take reasonable measures to reduce the risk of injury, and act to prevent recurrence. See Section 10 (Safeguards) and our Incident Response procedures.
- **De-identification and anonymization.** Where Certivo no longer requires personal information for the purposes for which it was collected, that information is destroyed, anonymized in accordance with generally accepted best practices, or de-identified for permitted serious-and-legitimate purposes. Anonymized information is processed so that it no longer allows the individual to be identified, directly or indirectly. See Section 8 (Limiting Use, Disclosure, and Retention) and Section 18 (Data Retention).
- **Consent and automated decisions.** Consent for collection is obtained as described in Section 6. Certivo does not make decisions about individuals based exclusively on automated processing; if that changes, affected individuals will be informed and given the opportunity to have the decision reviewed.
- **Transfers outside Quebec.** Personal information may be processed or stored outside Quebec (including in Google Cloud's US multi-region — see our Data Processing Agreement and Sub-Processor List). Before such a transfer, Certivo assesses the privacy-protection adequacy of the destination, taking into account the sensitivity of the information, the purposes of its use, the protective measures (including contractual) in place, and the legal framework applicable where the information will be processed.

These measures satisfy Law 25's designation, confidentiality-incident, de-identification, and cross-border-assessment requirements at the platform level. Each Tenant remains responsible for its own Law 25 obligations as data controller for the records it manages through the Platform.

---

4. Accountability (Principle 1)

4.1 Privacy Officer

Certivo has designated **Aaron Hoyte, Founder** as Privacy Officer, who is responsible for:

- Ensuring compliance with this Privacy Policy and applicable privacy legislation
- Receiving and responding to privacy inquiries and complaints
- Overseeing data breach response and notification
- Conducting and reviewing Privacy Impact Assessments
- Training staff on privacy obligations

Contact: Aaron Hoyte, Privacy Officer Ready 4 Everything Training and Supplies Ltd. 4952 Westbrooke Rd. Blackfalds, Alberta, Canada T4M 0L1 Email: aaron@certivo.ca

4.2 Accountability for Third Parties

Certivo uses contractual and other means to provide a comparable level of protection when personal information is processed by third-party service providers (sub-processors). A current list of sub-processors is maintained in our Sub-Processor List document, available upon request and at docs/legal/sub-processor-list.md.

4.3 Tenant Accountability

Each Tenant is responsible for ensuring that its own collection, use, and disclosure of personal information through the Platform complies with applicable privacy legislation. Tenants must obtain any required consent from their instructors, clients, and students before entering personal information into the Platform.

---

5. Identifying Purposes (Principle 2)

5.1 Purposes of Collection

Certivo collects personal information for the following identified purposes:

5.1.1 Account Administration

- Creating and managing user accounts (Tenant Administrators, Instructors, Clients)
- Authenticating users and maintaining session security
- Managing roles, permissions, and access controls
- Processing account recovery and password resets

5.1.2 Safety Training Operations

- Scheduling, managing, and recording safety training classes
- Tracking student enrollment, attendance, and completion
- Generating and managing safety certification records
- Recording and managing incident reports
- Tracking equipment and inventory for training purposes

5.1.3 Financial Operations

- Processing payroll calculations for instructors
- Generating invoices and processing payments
- Managing subscription billing for Tenants
- Processing payouts to instructors via Stripe Connect

- Maintaining financial records for tax and audit compliance
- Generating quotes and financial reports

5.1.4 Communication

- Sending transactional emails (invoices, certificates, booking confirmations)
- Sending operational notifications (schedule changes, reminders)
- Facilitating communication between Tenants and their clients
- Drip campaign communications (with consent)

5.1.5 Platform Operations and Improvement

- Monitoring platform performance and error detection
- Maintaining audit logs for security and compliance
- Analyzing usage patterns in aggregate to improve the Platform
- Providing technical support

5.1.6 Legal and Regulatory Compliance

- Complying with occupational health and safety record-keeping requirements
- Meeting Canada Revenue Agency (CRA) financial record retention requirements
- Responding to lawful requests from regulatory authorities
- Fulfilling contractual obligations

5.2 Notification of Purpose

The purposes for which personal information is collected are identified at or before the time of collection. If we identify a new purpose for previously collected information, we will obtain consent before using the information for that new purpose, unless the new use is required or authorized by law.

---

6. Consent (Principle 3)

6.1 Forms of Consent

Certivo obtains consent in the following ways, depending on the sensitivity of the information and the reasonable expectations of the individual:

6.1.1 Express (Explicit) Consent

Express consent is obtained for:

- Collection of sensitive personal information (payroll data, financial account details)
- Sharing personal information with third-party integrations (QuickBooks, Xero, Google Calendar)
- Marketing and drip campaign communications

- Cross-border data transfers to jurisdictions with different privacy protections
- Collection of incident report details that may include health or injury information

6.1.2 Implied Consent

Implied consent is relied upon where reasonable for:

- Basic account information (name, email, phone) when voluntarily provided during registration
- Operational use of information that is reasonably expected in the context of the service relationship
- Use of essential cookies required for Platform functionality
- Internal auditing and security monitoring

6.1.3 Deemed Consent (PIPA s. 8)

Under Alberta's PIPA, consent is deemed for:

- Collection that is reasonable for the purpose of an existing business transaction
- Use and disclosure for the purpose for which the information was collected
- Collection reasonably required for an employment relationship (instructors)

6.2 Withdrawal of Consent

Individuals may withdraw consent at any time by contacting our Privacy Officer at aaron@certivo.ca, subject to legal or contractual restrictions and reasonable notice. Certivo will inform the individual of the likely consequences of withdrawing consent, which may include:

- Inability to access certain Platform features
- Inability to process payroll or payments
- Inability to issue or verify safety certifications
- Termination of the user's account

Withdrawal of consent does not apply retroactively. Information collected and used prior to withdrawal, where retention is required by law (e.g., CRA financial records, OHS incident reports), will be retained for the required period.

6.3 Consent by Tenant Administrators

Tenant Administrators who enter personal information of instructors, clients, and students into the Platform represent and warrant that they have obtained all necessary consents from those individuals for the collection, use, and disclosure of their personal information through the Platform.

7. Limiting Collection (Principle 4)

7.1 Collection Limitation

Certivo limits the collection of personal information to that which is necessary for the identified purposes. We do not collect personal information indiscriminately.

7.2 Means of Collection

Personal information is collected through:

- Direct input by users through the Platform's user interfaces
- Automated collection during authentication and session management
- Integration with third-party services when authorized by the user or Tenant Administrator
- Cloud Function processing of submitted data
- Error and crash reporting through Sentry (technical data only)

7.3 Information Not Collected

Certivo does not collect:

- Social insurance numbers or government identification numbers (unless required for specific payroll compliance, and only with express consent)
- Biometric data
- Genetic or health information (except as voluntarily included in incident reports)
- Information from children under the age of 18 (see Section 19)

---

8. Limiting Use, Disclosure, and Retention (Principle 5)

8.1 Use Limitation

Personal information is used only for the purposes for which it was collected, or for purposes that a reasonable person would consider appropriate in the circumstances, unless:

- The individual consents to another use
- The use is required or authorized by law

8.2 Disclosure

Certivo discloses personal information only:

- To the Tenant that is the data controller for that information
- To third-party sub-processors as described in Section 15 and the Sub-Processor List
- When required or authorized by law (e.g., court orders, regulatory requirements)
- In the context of a business transaction (merger, acquisition, or sale) with appropriate safeguards

Certivo does **not** sell, rent, or trade personal information to third parties for marketing purposes.

8.3 Multi-Tenant Data Isolation

The Platform enforces strict data isolation between Tenants through:

- **Client-side:** TenantGuard automatically scopes all database queries and writes to the authenticated organization
- **Server-side:** Firestore Security Rules enforce organization-level access control on every read and write operation
- **Cloud Functions:** All callable functions validate organization identity from authentication tokens
- No Tenant can access, view, or modify another Tenant's data

8.4 Retention

Personal information is retained only as long as necessary to fulfill the identified purposes or as required by law. Specific retention periods are documented in our Data Retention Policy. Key periods include:

- Active user accounts: Duration of the service relationship
- Payroll records: 6 years (CRA requirement)
- Financial transactions and invoices: 7 years (CRA requirement)
- Safety certification records: Duration of employment plus 3 years, or as required by provincial OHS legislation
- Incident reports: 10 years (OHS requirement)
- Audit logs: 3 years

8.5 Secure Destruction

When personal information is no longer required, it is securely destroyed using:

- Cryptographic erasure for cloud-stored data (rendering encryption keys irrecoverable)
- Secure deletion from database systems with verification
- Overwriting of backup data within the 90-day rolling backup retention window

9. Accuracy (Principle 6)

9.1 Accuracy Commitment

Certivo makes reasonable efforts to ensure that personal information is as accurate, complete, and up to date as necessary for the purposes for which it is used.

9.2 User-Maintained Accuracy

Users are responsible for maintaining the accuracy of their own profile information. Tenant Administrators are responsible for maintaining the accuracy of information they enter about their instructors, clients, and students.

9.3 Updating Information

Users may update their personal information at any time through the Platform's user interface, or by contacting their Tenant Administrator. Individuals may also contact Certivo's Privacy Officer to request corrections.

9.4 Accuracy for Decision-Making

When personal information is used to make a decision about an individual (e.g., certification status, payroll calculations), Certivo ensures that the information is sufficiently accurate and up to date. Certification expiry dates, financial calculations, and compliance records are subject to automated accuracy checks.

---

10. Safeguards (Principle 7)

10.1 Security Measures

Certivo protects personal information with security safeguards appropriate to the sensitivity of the information, including:

10.1.1 Technical Safeguards

- **Encryption in Transit:** All data transmitted between users and the Platform is encrypted using TLS 1.2 or higher (HTTPS enforced)
- **Encryption at Rest:** All data stored in Google Cloud Firestore and Cloud Storage is encrypted at rest using AES-256 encryption managed by Google Cloud
- **Authentication:** Firebase Authentication with email/password for all users, including Tenant Suite administrators, Instructor Suite users, and Client Portal users; custom claims for session management and organization scoping
- **Authorization:** Role-based access control (RBAC) enforced at three layers: client-side UI, Firestore Security Rules, and Cloud Functions

- **Multi-Tenant Isolation:** TenantGuard enforces organization-level data isolation at the application, database rule, and server function layers
- **Rate Limiting:** All Cloud Functions are protected by rate limiting to prevent abuse
- **Input Validation:** Server-side validation on all form submissions to prevent injection and data corruption
- **Error Monitoring:** Sentry integration for real-time error detection and crash reporting (no personal information is transmitted to Sentry beyond technical context)

10.1.2 Organizational Safeguards

- Privacy Officer designated with clear responsibilities
- Privacy Impact Assessments conducted for new features and integrations
- Data Breach Response Plan maintained and tested annually
- Principle of least privilege applied to all system access
- Audit logging of administrative actions and data access

10.1.3 Physical Safeguards

- All data is hosted on Google Cloud infrastructure, which maintains SOC 2 Type II, ISO 27001, and ISO 27017 certifications
- No personal information is stored on local servers or physical media controlled by Certivo

10.2 Employee and Contractor Access

Access to personal information is restricted to Certivo personnel and authorized Tenant Administrators who require access to perform their duties. Access is granted on a need-to-know basis and is subject to audit.

---

11. Openness (Principle 8)

11.1 Availability of Policies

This Privacy Policy is publicly available at certivo.ca and within the Platform. Certivo makes information about its privacy policies and practices readily available to any individual upon request.

11.2 Information Available

Upon request, Certivo will provide:

- The name and contact information of the Privacy Officer
- A description of the types of personal information held by Certivo
- A general description of the purposes for which personal information is used
- A description of how to access personal information held by Certivo
- A description of the complaint process

---

12. Individual Access (Principle 9)

12.1 Right of Access

Upon written request to the Privacy Officer, an individual has the right to:

- Be informed of the existence, use, and disclosure of their personal information
- Be given access to their personal information held by Certivo
- Challenge the accuracy and completeness of their personal information and have it amended as appropriate

12.2 Response Timeline

Certivo will respond to access requests within **30 calendar days** of receipt. If Certivo is unable to respond within 30 days, we will:

- Notify the individual of the expected response date
- Provide reasons for the delay
- Inform the individual of their right to complain to the applicable Privacy Commissioner

12.3 Format of Access

Personal information will be provided in a commonly used electronic format (e.g., PDF, CSV) at no cost to the individual, unless the request is manifestly unfounded or excessive.

12.4 Exceptions to Access

Certivo may refuse access to personal information in the following circumstances, as permitted by PIPEDA and PIPA:

- The information is protected by solicitor-client privilege
- Disclosure would reveal confidential commercial information
- The information was collected for a legal investigation or proceeding
- Disclosure could reasonably be expected to threaten the safety of another individual
- The information was generated in the course of a formal dispute resolution process

Where access is refused, Certivo will provide written reasons and inform the individual of their right to challenge the refusal.

12.5 Correction of Information

If an individual demonstrates that personal information held by Certivo is inaccurate or incomplete, Certivo will amend the information as required. Where a correction is not made, the individual's objection will be noted and attached to the information.

13. Challenging Compliance (Principle 10)

13.1 Internal Complaint Process

Individuals may challenge Certivo's compliance with this Privacy Policy by contacting the Privacy Officer:

Step 1: Submit a written complaint to: Aaron Hoyte, Privacy Officer Email: aaron@certivo.ca Address: 4952 Westbrooke Rd., Blackfalds, Alberta, Canada T4M 0L1

Step 2: The Privacy Officer will acknowledge receipt within 5 business days and investigate the complaint.

Step 3: The Privacy Officer will provide a written response, including any corrective actions taken, within 30 calendar days.

13.2 External Complaint Process

If an individual is not satisfied with Certivo's response, they may file a complaint with:

Office of the Privacy Commissioner of Canada (OPC) 30 Victoria Street Gatineau, Quebec K1A 1H3 Phone: 1-800-282-1376 Website: www.priv.gc.ca

Office of the Information and Privacy Commissioner of Alberta (OIPC) 410, 9925 - 109 Street NW Edmonton, Alberta T5K 2J8 Phone: 780-422-6860 Website: www.oipc.ab.ca

---

14. Types of Personal Information Collected

14.1 Account and Identity Information

Data Element	Collected From	Purpose
Full name	All users	Account identification, communications, certification records
Email address	Tenant Admins, Instructors	Authentication, communications, account recovery
Phone number	Tenant Admins, Instructors, Clients	Contact for scheduling, emergencies, two-factor authentication
Role and permissions	All users	Access control, platform security
Profile photo (optional)	Tenant Admins, Instructors	User identification within Platform
Password (hashed)	Client Portal users	Authentication for client self-service access

14.2 Employment and Payroll Information

Data Element	Collected From	Purpose
Salary/rate of pay	Instructors	Payroll calculations
Tax deductions and withholdings	Instructors	Payroll compliance
Banking or payout information (via Stripe Connect)	Instructors	Payment processing
Mileage and travel records	Instructors	Expense reimbursement, reporting
Hours worked and attendance	Instructors	Payroll and scheduling
Employment status	Instructors	Operational management

14.3 Safety and Certification Information

Data Element	Collected From	Purpose
Certification types held	Instructors, Students	Compliance tracking, qualification verification
Certification expiry dates	Instructors, Students	Automated renewal reminders
Training course completion records	Students	Certification issuance, compliance
Incident reports (may include injury details)	Instructors, Tenant Admins	Regulatory compliance, safety analysis
Safety compliance status	Clients, Students	Compliance monitoring and reporting

14.4 Financial and Transaction Information

Data Element	Collected From	Purpose
Invoices and payment history	Tenants, Clients	Billing, financial reporting
Subscription plan details	Tenants	Service delivery, billing
Payment card information (processed by Stripe, not stored by Certivo)	Tenants, Clients	Payment processing
Quotes and estimates	Clients	Sales process
Expense records	Instructors, Tenants	Financial reporting, reimbursement

14.5 Organizational and Business Information

Data Element	Collected From	Purpose
Company name and address	Tenants, Clients	Account management, invoicing
Company contact information	Tenants, Clients	Communications, service delivery
Business registration details	Tenants	Onboarding verification
Location and branch information	Tenants	Multi-location management

14.6 Technical and Usage Information

Data Element	Collected From	Purpose
Authentication tokens and session data	All users	Security, session management
Browser type and version	All users	Error diagnosis, compatibility
IP address (logged by Firebase)	All users	Security, abuse prevention
Error and crash reports	All users	Platform stability, bug resolution
Audit log entries (actions taken in Platform)	All users	Security, compliance
Theme preferences (dark/light mode)	All users	User experience personalization

15. Third-Party Service Providers

Certivo uses the following third-party service providers (sub-processors) to deliver the Platform. Each provider is contractually bound to protect personal information and use it only for the purposes specified by Certivo.

Provider	Service	Data Shared	Location
Google Cloud / Firebase	Infrastructure: hosting, database (Firestore), authentication, file storage, Cloud Functions	All Platform data	US (Cloud Functions: Toronto, Canada via northamerica-northeast2; Vertex AI/Gemini: Montréal, Canada via northamerica-northeast1)
Stripe, Inc.	Payment processing, subscription billing, Connect payouts	Names, email addresses, payment information, payout details	US
Resend, Inc.	Transactional and marketing email delivery	Names, email addresses, email content	US
Functional Software, Inc. (Sentry)	Error monitoring and crash reporting	Technical error data, browser information, anonymized user context	US
Google (Calendar API)	Scheduling integration (when enabled by Tenant)	Class schedules, instructor names, dates, locations	US
Intuit Inc. (QuickBooks Online)	Accounting integration (when enabled by Tenant)	Invoice data, expense data, client names, financial amounts	US / Canada
Xero Limited	Accounting integration (when enabled by Tenant)	Invoice data, expense data, client names, financial amounts	New Zealand / Global
Twilio Inc.	SMS delivery for class reminders and platform notifications (when enabled by Tenant)	Phone numbers, message content	US
Google (Analytics 4)	Marketing-website usage analytics (consent-gated; the logged-in applications are not tracked)	Pseudonymous usage events, coarse location	US

Multi-factor authentication SMS codes are delivered by Firebase Authentication (Google), not Twilio.

A complete and current list of sub-processors, including change notification procedures, is maintained in our Sub-Processor List document (`docs/legal/sub-processor-list.md`).

16. Cross-Border Data Transfers

16.1 Transfer Locations

Personal information processed through the Platform may be transferred to, stored in, and processed in jurisdictions outside of Canada, including the United States. Specifically:

- **Google Cloud / Firebase:** Platform records are stored in the United States. The Firestore database is provisioned in Google Cloud's US multi-region (`nam5`), and Cloud Storage files and Firebase Authentication data are held in Google's US infrastructure. Application compute runs in Canada: Cloud Functions in Toronto (northamerica-northeast2) and Vertex AI in Montréal (northamerica-northeast1). Running compute in Canada does not keep the stored records in Canada.
- **Stripe, Resend, Twilio, SignNow (airSlate), and Sentry** are US-based companies and process data in the United States.
- **Xero** is a New Zealand-based company with global data processing.

16.2 Safeguards for Cross-Border Transfers

When personal information is transferred outside Canada, Certivo ensures that:

- Contractual protections are in place requiring the recipient to protect the information to a standard comparable to Canadian privacy law
- The transfer is necessary for the performance of the service
- Individuals are informed that their information may be subject to the laws of the foreign jurisdiction, including lawful access by courts, law enforcement, and national security authorities

16.3 Consent

By using the Platform, users consent to the transfer of their personal information outside of Canada as described in this section. Tenants are responsible for informing their instructors, clients, and students of these cross-border transfers.

---

17. Cookies and Similar Technologies

17.1 Essential Cookies

The Platform uses essential cookies that are strictly necessary for its operation:

- **Firebase Authentication session cookies:** Maintain authenticated user sessions
- **CSRF tokens:** Protect against cross-site request forgery attacks

These cookies cannot be disabled without rendering the Platform inoperable.

17.2 Functional Cookies

The Platform uses functional cookies to remember user preferences:

- **Theme preference:** Stores the user's dark/light mode selection
- **Sidebar state:** Remembers the sidebar collapsed/expanded state

17.3 Third-Party Cookies

Third-party services used by the Platform may set cookies:

- **Stripe:** Sets cookies during payment checkout for fraud prevention and payment processing
- **Google Calendar OAuth:** Sets cookies during the calendar integration authorization flow

17.4 Analytics on the Marketing Site

The signed-in Platform applications do not use analytics cookies or tracking pixels. The marketing site (certivo.ca) uses Google Analytics 4. Until a visitor makes a choice in the cookie banner, Google Analytics runs without cookies and every Google consent signal is set to denied. An analytics cookie is set only after the visitor chooses to accept analytics. Advertising signals stay denied in every case, because Certivo runs no advertising. Details are in the Cookie Policy.

For further details, see our Cookie Policy.

17A. REST API Data Access

17A.1 Tenants who subscribe to the REST API Access Add-On may authorize third-party applications to access their organization-scoped data through authenticated API keys. API access is limited to the subscribing Tenant's own data and is subject to the published rate limits and the Acceptable Use Policy.

17A.2 Certivo is not responsible for the privacy practices or data handling of third-party applications that access Tenant data through the REST API. Tenants are solely responsible for evaluating the privacy and security practices of any third-party application they authorize via API keys.

17A.3 API access logs, including the requesting application, endpoint accessed, and timestamp, are retained for **twelve (12) months** for security and audit purposes.

17B. SMS Message Data

17B.1 When Tenants use the SMS Notifications feature, the Platform processes recipient phone numbers, message content, and delivery status. SMS message logs (including recipient phone number, message content, delivery status, and timestamp) are retained for **five hundred and forty (540) days** to support CASL compliance verification, after which they are securely deleted.

17B.2 SMS consent records (including the date, method, and content of consent) are retained for a minimum of **three (3) years** from the date of the last SMS sent in reliance on that consent, as required under CASL.

17C. Certification Marketplace Data

17C.1 Instructors who participate in the Certification Marketplace may publish portfolio profiles that are visible to all Platform users across organizations. Published portfolio data includes the instructor's name, qualifications, course offerings, ratings, and availability. Instructors consent to this cross-organizational visibility when they opt in to the Marketplace.

17C.2 Student enrollment data, payment information, and course completion records within the Marketplace remain private and are accessible only to the relevant Tenant, the enrolled student, and the delivering instructor.

17D. Community Forum Data

17D.1 Posts, comments, and other content submitted to the Community Forum feature are visible to all members of the posting user's organization. Forum content may include the poster's display name, role, and organization affiliation.

17D.2 Certivo may moderate Forum content in accordance with the Acceptable Use Policy. Removed content is retained in archived form for **ninety (90) days** for compliance review, after which it is securely deleted.

17E. White-Label Demo Environment

17E.1 Data entered into white-label demonstration environments is stored separately from production data and is used solely for demonstration and evaluation purposes.

17E.2 The public demonstration at certivo.ca/demo runs entirely in the visitor's own browser and stores nothing on Certivo systems: closing the tab ends it. The only demo interaction Certivo records is feedback a visitor chooses to submit through the demo feedback widget, which is retained under the ordinary feedback retention period in our Data Retention Policy. Data entered into an operator-led white-label demonstration tenant may be deleted by Certivo at any time without notice. Users should not enter real personal information into any demonstration environment.

> ***Corrected 2026-09-20.*** *This clause previously stated that demo environment data "is automatically purged thirty (30) days after creation". No code implemented that purge, no scheduled job performed it, and no field existed that would have made the thirty days computable. A stated commitment to data subjects with no technical enforcement behind it is worse than no commitment, so the clause now describes what the system actually does.*

18. Data Retention

Certivo retains personal information only as long as necessary for the purposes for which it was collected, or as required by law. Detailed retention periods for each category of data are documented in our Data Retention Policy. Upon expiry of the applicable retention period, personal information is securely destroyed.

When a Tenant's subscription is terminated, Certivo provides a 30-day window for the Tenant to export their data. After this window, Tenant data is securely deleted within 60 days, subject to legal retention requirements.

19. Children's Privacy

The Certivo is not intended for use by individuals under the age of 18. Certivo does not knowingly collect personal information from children. If we become aware that we have collected personal information from a child under 18, we will take steps to delete that information promptly.

Student records for individuals under 18 who are enrolled in safety training courses are the responsibility of the Tenant, who must obtain parental or guardian consent as required by applicable law.

20. Changes to This Policy

Certivo may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. When we make material changes:

- We will update the "Last Updated" date at the top of this policy
- We will notify Tenant Administrators via email or in-platform notification
- For changes that materially affect how we use previously collected personal information, we will obtain new consent where required

Continued use of the Platform after changes to this Privacy Policy constitutes acceptance of the updated terms, except where additional consent is required.

21. Contact Information

For questions, concerns, or requests related to this Privacy Policy or Certivo's privacy practices, please contact:

Aaron Hoyte, Privacy Officer Ready 4 Everything Training and Supplies Ltd. 4952 Westbrooke Rd. Blackfalds, Alberta, Canada T4M 0L1 Email: aaron@certivo.ca

---

This Privacy Policy is effective as of March 1, 2026.

Ready 4 Everything Training and Supplies Ltd. All rights reserved.

Last Updated: November 1, 2026