Privacy Policy

How Commersive collects, uses, protects, shares, and retains personal information.

Effective date	June 2022 (last updated September 15, 2026)
Privacy Lead	Amy Lerman, COO
Privacy contact	amy@commersive.ca
Applies to	Commersive websites, hosted applications, retail experiences, business communications, and related services

Commersive Solutions Corp. ("Commersive", "we", "us", or "our") respects privacy and is committed to handling personal information responsibly. This Privacy Policy explains our practices for personal information collected or processed through our websites, digital experiences, hosted applications, client and partner interactions, and related business activities.

This Policy is intended to support compliance with applicable Canadian privacy laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA) where it applies, as well as applicable provincial privacy requirements.

1. Accountability and privacy contact

Commersive has designated **Amy Lerman, Chief Operating Officer**, as its Privacy Lead. The Privacy Lead is responsible for overseeing our privacy program, responding to privacy inquiries and requests, coordinating privacy incident assessments, and escalating material privacy risks where appropriate.

Privacy questions, access or correction requests, deletion requests where applicable, and complaints may be directed to **amy@commersive.ca**. We may ask for reasonable information to verify identity before disclosing or changing personal information.

2. Personal information we may collect

The personal information Commersive handles depends on the service, project, or relationship. We aim to collect only information reasonably necessary for an identified business purpose.

Business and client contacts

- Name, business email address, company, job title, telephone number, and other contact details that a person chooses to provide.
- Correspondence, project communications, support requests, and records needed to manage a client, partner, supplier, or business relationship.

Authorized application users

- Email address or other account identifier used to provide access to applications created for authorized representatives, staff, or partners.
- Authentication, access, and security information such as login events, one-time-code activity, access status, administrative actions, and related security logs where applicable.

- Where passwordless or one-time-code authentication is used, Commersive does not need to store a traditional end-user password for that application.

Customer-facing digital experiences

Certain customer-facing experiences may request limited information to complete a user-requested action. For example, the Commersive 2D Kitchen Builder may ask a customer to enter an email address so the selected kitchen or product configuration can be sent to that customer. **The Kitchen Builder application does not intentionally retain that customer email address in its application database after the requested email is sent.**

Technical and security information

- Internet protocol address, browser or device information, timestamps, request information, diagnostic events, and security-related logs generated when a person uses a website or application.
- Information necessary to protect systems, detect abuse, troubleshoot errors, maintain service reliability, and investigate security events.

3. How we use personal information

- Provide and operate websites, applications, retail experiences, and client services.
- Authenticate authorized users and administer access to applications and systems.
- Send information specifically requested by a user, such as a product or kitchen configuration summary.
- Respond to questions, support requests, proposals, and business communications.
- Protect our systems, investigate suspected misuse or security incidents, and maintain logs needed for security and troubleshooting.
- Meet legal, regulatory, contractual, accounting, insurance, or dispute-resolution requirements.
- Improve the reliability and operation of our services using information that is appropriate for that purpose.

We do not use personal information for an unrelated purpose unless permitted by law or appropriate notice or consent is provided.

4. Consent and limiting collection

Where consent is required, Commersive seeks consent appropriate to the sensitivity of the information and the context in which it is collected. We limit collection to information reasonably necessary for identified purposes and design workflows to avoid persistent storage when information is needed only transiently.

5. Sharing and service providers

Commersive does not sell personal information. We may disclose personal information only as reasonably necessary for the purposes described in this Policy, as authorized by the individual, as required by a client relationship, or as permitted or required by law.

We may use service providers that perform functions such as cloud hosting, infrastructure, security, communications or email delivery, and operational support. Providers are expected to receive only the information needed to perform their services and to protect information appropriately.

Commersive currently uses cloud infrastructure that may include **Cloudflare** services for application hosting and data storage. **AWS S3** may be used for approved asset storage such as images and logos. The authoritative list of material service providers is maintained internally and may change as our technology evolves.

We may also disclose information when required by law, court order, lawful government request, or where reasonably necessary to protect legal rights, investigate fraud or security incidents, or protect the safety of individuals and systems.

6. Cross-border processing

Some service providers operate infrastructure in more than one jurisdiction. As a result, personal information may be processed or accessible outside the province or country in which it was collected. When information is processed in another jurisdiction, it may be subject to the laws of that jurisdiction. Commersive uses contractual, technical, and organizational safeguards appropriate to the service and the sensitivity of the information.

7. Safeguards and security

Commersive uses administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, use, disclosure, alteration, loss, or destruction. Safeguards are selected based on sensitivity, volume, context, and foreseeable risk. Measures may include:

- HTTPS/TLS for production web applications and internet transmission of personal information.
- Provider-supported encryption at rest for production cloud storage containing personal information.
- Multi-factor authentication for administrative access where supported.
- Least-privilege access controls and periodic review of privileged access.
- Protected handling of API keys, tokens, and credentials.
- Quarterly documented security and privacy reviews covering access, cloud configuration, secrets, updates, logging, recovery, vendors, retention, and open findings.
- Security logging, incident response procedures, and post-incident corrective actions.
- Controls intended to minimize or avoid local storage of personal information on public retail endpoints.

No security system can guarantee absolute protection. If Commersive becomes aware of a privacy breach, we assess the incident and provide notifications or reports when required by applicable law or contract.

8. Retention and deletion

Commersive retains personal information only for as long as reasonably necessary for the identified purpose, legal or contractual obligations, security and audit needs, dispute resolution, or another legitimate business requirement. When information is no longer required, it is securely deleted, anonymized, or allowed to expire from systems according to the applicable retention process.

For the 2D Kitchen Builder, the customer email address is used to send the requested configuration and is not intentionally retained in the application database after that purpose is completed. Other business contact or authorized-user information may be retained while the relationship or account remains active and for a reasonable period afterward where needed for legal, security, audit, or contractual reasons.

9. Cookies and similar technologies

Commersive websites or applications may use cookies, local storage, or similar technologies where needed for essential functionality, session management, security, or user preferences. If a Commersive service uses non-essential analytics, advertising, or similar technologies that require additional notice or consent, we will provide that notice or consent mechanism where required.

10. Access, correction, deletion, and other privacy rights

Subject to applicable law, individuals may ask Commersive to:

- Confirm whether Commersive holds personal information about them and request access to that information.
- Correct inaccurate or incomplete personal information.
- Request deletion of personal information where applicable and where no legal, contractual, security, or other legitimate retention requirement prevents deletion.

- Withdraw consent where processing is based on consent and withdrawal is legally available.
- Ask questions or make a complaint about Commersive privacy practices.

We may need to verify identity before completing a request. In some circumstances, applicable law may permit or require us to refuse, limit, or delay a request. Where appropriate, we will explain the basis for that decision.

11. Accuracy

Commersive takes reasonable steps to keep personal information accurate, complete, and up to date where accuracy is relevant to the purpose for which the information is used. Individuals may contact the Privacy Lead to request corrections.

12. Children and vulnerable users

Commersive does not intentionally design its general business services to collect unnecessary personal information from children. A project expected to involve minors or other vulnerable users requires additional privacy review and appropriate safeguards before launch.

13. Third-party websites and client environments

Commersive experiences may link to or operate within websites, stores, systems, or environments controlled by clients or third parties. Their privacy practices are governed by their own notices and policies. Commersive is responsible for personal information under its control but is not responsible for the independent privacy practices of unrelated third parties.

14. Changes to this Privacy Policy

Commersive may update this Privacy Policy to reflect changes in our services, technology, legal obligations, or privacy practices. The current version will identify its effective or last-updated date. Material changes will be communicated in an appropriate manner.

15. Contact us

Privacy Lead	Amy Lerman, Chief Operating Officer
Email	amy@commersive.ca
Organization	Commersive Solutions Corp.
Location	Toronto, Ontario, Canada

For written privacy correspondence, Commersive can also provide its formal business mailing address upon request.

Document note: This public Privacy Policy is separate from Commersive's internal Privacy, Information Security and Data Governance Manual, which contains detailed internal controls, procedures, evidence requirements, and incident-response processes.