OrderPilot

LEGAL

Privacy Policy

Bevy Commerce Inc. Version 1.1 This Privacy Policy explains how Bevy Commerce Inc., operating OrderPilot, collects, uses, discloses and retains personal information. It covers merchants, their staff, their customers, vendor contacts and visitors to our marketing website. “You” means the store using OrderPilot, and “your customers” means that store’s shoppers. The rights described here belong to individuals whether or not they have an OrderPilot account.

EFFECTIVE	LAST UPDATED
November 2, 2026	November 2, 2026

1 Who we are

1.1 OrderPilot is a business software service operated by Bevy Commerce Inc., 3093 Bathurst St., Unit 690, Toronto, Ontario, M6A 2A3, Canada. It operates through Shopify Admin, Shopify POS and merchant-facing and customer-facing tools connected to Shopify.

1.2 Our privacy and legal contact is **privacy@meetorderpilot.com**. Support is available at **support@meetorderpilot.com**. Our Terms of Service contain the contractual terms for merchants, including our data-processing obligations.

2 Key definitions

2.1 The following terms have these meanings:

2.1.1 **Personal information:** information about an identified or identifiable individual, also called Personal Data under some laws.

2.1.2 **Merchant information:** information supplied by a store, collected for it or processed on its instructions through OrderPilot.

2.1.3 **Controller or business:** the person or organization that determines the purposes and means of processing, using the applicable law's terminology.

2.1.4 **Processor or service provider:** an organization that processes personal information on another organization's instructions under applicable legal and contractual restrictions.

2.1.5 **Processing:** collecting, using, storing, accessing, disclosing, correcting, exporting, deleting or otherwise handling information.

3 Our privacy roles

3.1 For customer information and other personal information we handle on a merchant's instructions, the merchant is normally the controller or business and we are its processor or service provider. The merchant decides why it uses the information for its sales, communications, purchasing and service activities. Its own privacy notice also applies.

3.2 We act as controller for our own merchant business relationship, website, business administration and other processing for which we determine the purposes. Staff and vendor information may fall into either role depending on its use. A person's job title or the source of a record does not, by itself, decide the role.

3.3 Your customers do not need a separate OrderPilot subscription or account. Access through a signing link, portal link or portal security check still involves processing personal information. Questions about a store's sale, messages or customer records should normally be directed to that store.

4 Information we collect

4.1 We receive information from Shopify and merchant-authorized integrations, from merchants and their staff, directly from customers and vendors using the tools, and automatically through service operation. We also receive information when someone contacts us directly.

4.2 The categories depend on the features used:

4.2.1 **Store and staff information:** store identity and contact details, locations, Shopify identifiers, staff names and emails, roles, permissions, subscription information and activity showing who changed a record.

4.2.2 **Customer and transaction information:** names, emails, phone numbers, billing and delivery addresses, product choices, quotes, orders, prices, deposits, balances, delivery details and payment status or references.

4.2.3 **Messages and attachments:** customer and vendor correspondence, portal messages, change requests, purchase-order replies, uploaded documents, warranty photographs and related delivery or engagement records.

4.2.4 **Signing evidence:** signer name and email, signature image or recorded signing method, signing and recording times, IP address and forwarding information, browser/device information, consent wording, the exact document and terms signed, document fingerprints, signing-link activity and signed-copy delivery records.

4.2.5 **In-store and paper evidence:** relevant staff and location details, staff attestations, and any uploaded scan or photograph of a signed paper document.

4.2.6 **Purchasing and accounting information:** vendor contacts, purchase orders, receiving records, costs, credits, vendor payment records, accounting mappings and related information exchanged with QuickBooks when connected.

4.2.7 **Access and diagnostic information:** session and device identifiers, portal authentication information, IP-derived approximate location, page views, feature use, browser interactions, session recordings, errors, logs and security events.

4.2.8 **Direct business communications:** contact information and the contents of support, privacy, legal or other enquiries sent to us.

4.3 Shopify and its payment providers handle shopper payments. OrderPilot does not receive shopper funds or process full payment-card numbers for checkout or POS payments. We receive relevant transaction information made available through Shopify.

4.4 We do not ask for government identification numbers, health information or biometric identifiers for identity recognition. Signatures are used as agreement evidence, not for biometric identification. Do not include unnecessary sensitive information in messages, notes or attachments.

5 How we use information

5.1 We use merchant information to provide the features you enable, including quotes, signing, payment links, purchasing, customer and vendor communications, order tracking, warranty work, accounting connections and data exports. We also use necessary information to maintain access controls, investigate problems, protect the Service and assist with privacy requests.

5.2 For our own business purposes, we use relevant information to administer subscriptions, provide support, communicate service changes, diagnose errors, improve usability, prevent abuse, meet legal obligations and establish or defend legal claims. We limit these uses to what is permitted by applicable law, our agreements and Shopify's requirements.

5.3 Where the GDPR or UK GDPR applies to our controller activities, our lawful bases are:

5.3.1 **Contract:** where processing is necessary to perform a contract with the individual or take requested steps before entering one.

5.3.2 **Legitimate interests:** operating and securing the Service, managing business relationships and improving it, where those interests are not overridden by the individual's rights.

5.3.3 **Legal obligations:** complying with binding legal duties.

5.3.4 **Consent:** where required, including applicable nonessential tracking or optional marketing. Consent can be withdrawn without affecting processing that was lawful before withdrawal.

5.4 When acting as a processor, we follow the merchant's lawful instructions rather than substituting an independent lawful basis for its processing. The merchant is responsible for identifying its own lawful bases and giving the required notices.

5.5 We do not sell personal information, share it for cross-context behavioral advertising, or use it for targeted advertising. We do not use OrderPilot merchant personal information to train AI models or send it to AI providers. We do not publish merchant benchmarks or commercialize cross-store profiles.

5.6 OrderPilot applies workflow rules chosen by merchants. We do not use personal information for our own profiling or solely automated decisions that produce legal or similarly significant effects on individuals. Questions about a merchant's decisions should be directed to that merchant.

6 Cookies and recordings

App analytics and session replay

6.1 OrderPilot uses PostHog for product analytics and staff session replay, and monitoring tools for errors and operational diagnostics. Replay records interactions with the app, such as navigation, clicks and page content, to help understand and resolve problems. Depending on the page and recording configuration, displayed customer or business information may be included.

6.2 Cookies, local storage and similar technologies may maintain sessions, support portal access, remember settings and associate activity with a visit or store. These uses are separate from advertising tracking. An individual's browser settings may limit some technologies, but do not prevent all server-side processing needed to provide the Service.

6.3 Any legally required consent must be obtained before nonessential tracking or recording begins. Acceptance of a merchant contract does not replace an individual's required consent. Individuals may contact our privacy address to withdraw consent or object where applicable; we will explain the available options and any effect on the Service.

Messages

6.4 Store emails may include open and click tracking, and messaging providers return delivery and failure information. Signing tools also record relevant signing-link activity. These records help stores administer communications and preserve transaction evidence; they are not used by us for targeted advertising.

Marketing website

6.5 The marketing website currently has no analytics or advertising cookies. It uses presentation-related browser storage and loads fonts, scripts and media from service providers, which receive normal connection information such as an IP address and browser details.

6.6 When you request a demo on the website, the details you enter (your name, work email, store name, number of locations, store website and message) are sent to our team by email through Twilio SendGrid. We use them to reply to you and to arrange and prepare your demo. The website's newsletter form is not currently connected to a submission service. To contact us, email **support@meetorderpilot.com**. We will update the relevant disclosures before activating a new collection or marketing service.

7 Sharing and service providers

7.1 We disclose information to providers as needed for the stated services, to the merchant and its authorized users, and to recipients selected through merchant instructions. Examples include a vendor receiving a purchase order or a customer receiving an order update. We do not make customer messages or signing evidence public as a general practice.

7.2 The following list identifies the principal providers and connected platforms. Region descriptions reflect provider operating regions and account-dependent options; they are not a promise of dedicated storage in a particular country. A provider's support operations and subprocessors may involve additional countries.

PROVIDER	PURPOSE	REGION
Shopify	Platform, merchant data connections, app billing, checkout and POS.	International, including Canada and the United States.
Heroku / Salesforce	Application and worker hosting, database infrastructure and related recovery services.	United States or Europe, depending on deployment; international support.
Redis Cloud	Job queues and temporary operational data.	Account-dependent cloud region; international operations.
Cloudflare	Private file and image storage through R2, and website media and CDN delivery.	International; storage jurisdiction and delivery locations depend on configuration.
Twilio SendGrid	Outbound email, inbound replies, delivery records and message engagement.	United States for the integrated global service; international delivery.
Twilio Messaging	Text delivery, delivery records and opt-out processing.	United States for the integrated service; international carrier delivery.
Sentry	Error and performance monitoring.	United States or Germany, depending on the organization's selected region.
PostHog	Product analytics, staff session replay, errors and operational telemetry.	United States or European Union, depending on the selected project region.
Better Stack / Logtail	Application log collection and monitoring.	European Union or another configured service region; international operations.
Intuit QuickBooks Online	Optional merchant-authorized purchasing and accounting integration.	International, including the United States; account-dependent processing.
Google Fonts	Website font delivery and associated connection requests.	International.

7.3 Shopify and merchant-selected integrations such as QuickBooks also process information under their own agreements and privacy notices. Their role depends on the particular activity; they are not automatically our subprocessors for everything they do. We use contractual restrictions appropriate to the role when a provider processes personal information on our behalf.

7.4 We may disclose necessary information to professional advisers, insurers, auditors, authorities or courts for legal compliance, protection against harm, or legal claims. We may also disclose it in a business transfer subject to appropriate confidentiality, lawful-purpose and privacy protections. A business transfer does not authorize incompatible new uses without the requirements of applicable law being met.

7.5 Mobile numbers and messaging consent are not sold, rented or disclosed to other businesses for their own marketing. Necessary messaging providers may process them to deliver the merchant's authorized messages and honor opt-outs.

8 International data transfers

8.1 Our team accesses information from Canada and Singapore. Our providers may process it internationally, including in the United States and the other operating regions described in clause 7. The laws and government-access rules in those places may differ from those where an individual lives.

8.2 We remain responsible for protections required when we transfer information to providers acting for us. Restricted transfers require a valid legal mechanism. Depending on the transfer, that may be an applicable adequacy decision or contractual safeguards such as EU Standard Contractual Clauses and the UK Addendum or International Data Transfer Agreement, with required assessments and additional protections.

8.3 Canadian adequacy applies only where its conditions are satisfied; it does not automatically cover every onward transfer. Contact **privacy@meetorderpilot.com** for information about the safeguards applicable to a transfer and how to obtain a copy, with necessary redactions. Using OrderPilot or reading this Policy is not blanket consent to an otherwise unlawful transfer.

9 Retention and deletion

Active stores and ordinary records

9.1 We retain information for the purposes described in this Policy and the merchant's lawful instructions. Ordinary order, purchasing and warranty records do not have a universal 30-day limit while the store uses the Service. Relevant criteria include ongoing transactions and warranties, the merchant's settings, privacy requests, security needs and legal obligations.

9.2 Notification and completed webhook logs generally have a 30-day application default, subject to configuration and specific exceptions. Diagnostic providers have their own configured retention schedules. Unresolved compliance requests and necessary opt-out records may be retained longer so they can be completed or respected.

9.3 Our own billing, tax, compliance and dispute records are kept for the applicable legal period or the period reasonably needed for their purpose. Backups may retain copies until their rotation or deletion cycle completes; their use is restricted to recovery, security and legal requirements. Deletion instructions apply again if information is restored.

Signature evidence

9.4 The default signature-evidence period is seven years, configurable by the merchant from one to thirty years. It is measured from the latest relevant signing, payment or shipment, pickup or delivery date. Routine deletion is deferred for relevant unpaid balances, unfinished fulfillment, continuing warranty obligations, unresolved warranty claims and active in-app legal holds.

9.5 Under the default deletion setting, eligible evidence receives 30 days' notice before its files and identifying details are removed. A limited verification record can remain. The active order may still retain its current signature image, signed terms and activity history under the order's separate retention rules.

9.6 A merchant may choose an available setting to keep evidence longer, but must have an ongoing lawful reason. No setting overrides applicable privacy rights, mandatory deletion or binding Shopify requirements.

9.7 After uninstall, signature evidence remains for up to six months unless the store reinstalls or earlier deletion is legally required. In-app legal holds do not extend that post-uninstall window. A binding preservation duty may require separate arrangements, and merchants should export their required records before uninstalling.

9.8 Ordinary signature exports expire seven days after preparation; uninstall export access lasts 30 days. Customer-data export files generally expire after seven days. Expiration of an export file does not, by itself, delete the underlying records.

Shopify privacy requests

9.9 We verify and acknowledge Shopify's mandatory privacy requests and complete the required action within 30 days of receipt, subject to legally required retention and any shorter applicable legal deadline:

9.9.1 **Customer data request (customers/data_request):** we make the customer information held by OrderPilot available to the merchant through its customer-data export process, so the merchant can respond to the individual.

9.9.2 **Customer redaction (customers/redact):** we delete or redact identifying customer information from the relevant records and files. Signed evidence follows the legally justified retention rules below.

9.9.3 **Shop redaction (shop/redact):** Shopify normally sends this request 48 hours after uninstall. We delete ordinary store records and files, while retaining only information covered by a valid exception, including applicable business records and signature evidence where justified.

9.10 Retention after an erasure request must have a valid legal basis and meet Shopify's requirements, including its narrower exception for legally required retention. A possible future use, merchant preference or configured retention period does not by itself establish an exception. Retained information is restricted to the relevant purpose and deleted when the basis ends.

10 Security and incidents

10.1 We use safeguards appropriate to the information and risks, including access controls, encrypted network connections, protection of integration credentials, controlled access to private files and monitoring. Diagnostic filtering is designed to reduce unnecessary exposure of personal information. No system can guarantee absolute security.

10.2 For a personal-data breach affecting information we process for a merchant, we notify the merchant without undue delay and provide available information and updates. We also meet separate Shopify notification requirements and any duties to notify individuals or regulators under applicable law. The applicable deadline depends on the duty and circumstances; a regulator's reporting window is not a waiting period before notifying a merchant.

10.3 Contact **privacy@meetorderpilot.com** promptly about a suspected privacy or security issue. Provide enough detail for investigation without unnecessarily including sensitive records or access credentials.

11 Your privacy rights

11.1 Depending on the applicable law and our role, individuals may have rights to:

11.1.1 Know whether information is processed and obtain access to it and relevant information about that processing.

11.1.2 Correct inaccurate information, request deletion, or obtain a portable copy.

11.1.3 Restrict processing or object to processing based on legitimate interests.

11.1.4 Withdraw consent where processing relies on consent.

11.1.5 Opt out of applicable sale, advertising sharing, targeted advertising or qualifying profiling, and limit certain sensitive-information uses where the law provides that right.

11.1.6 Appeal a refusal where applicable and complain to a competent privacy regulator.

11.2 For merchant-controlled records, contact the store first. We assist the merchant and can help route a request received at our privacy address. For our controller activities, contact **privacy@meetorderpilot.com** directly.

11.3 We use proportionate steps to verify identity and authority before disclosing or changing information. An authorized agent may submit a request with appropriate proof of authority. We do not require unnecessary information or discriminate against an individual for exercising privacy rights.

11.4 We respond within applicable legal deadlines and explain any lawful refusal or permitted extension. Rights are subject to relevant exceptions, including protection of others' rights and valid legal-retention duties. An individual may appeal by replying to our decision with "Privacy appeal"; we explain the outcome and any available regulator complaint route.

12 Regional privacy information

EEA and United Kingdom

12.1 The lawful bases in clause 5, transfer information in clause 8 and rights in clause 11 apply where the GDPR or UK GDPR governs our processing. Individuals may complain to their local EEA supervisory authority or the UK Information Commissioner. Contact our privacy address for help identifying the relevant authority.

12.2 Providing information necessary for a transaction or access may be required to use the related feature; optional marketing consent is not required to purchase the Service. We explain the relevant consequences when information is requested or consent is withdrawn.

United States

12.3 For California purposes, the categories in clause 4 include identifiers, customer-record information, commercial information, internet or electronic activity, approximate geolocation derived from IP addresses, and professional or employment-related information. Signing records may include a signature, and some access credentials or financial information may be treated as sensitive personal information. We use such information only for necessary service, security and other legally permitted purposes, not to infer sensitive characteristics.

12.4 The collection sources, purposes, recipient categories and retention criteria are described in clause 4, clause 5, clause 7 and clause 9, including for the preceding twelve months to the extent OrderPilot operated during that period. We do not sell personal information or share it for cross-context behavioral advertising, and do not use it for targeted advertising. Accordingly, those opt-out rights do not correspond to an activity we currently undertake.

12.5 Other state-law rights, including applicable rights concerning recipients, portability and appeals, can be exercised through clause 11. We honor legally applicable opt-out preference signals; those signals do not require us to stop processing necessary to provide the requested Service. Merchant instructions and legally required service-provider restrictions apply to information processed for stores.

Canada and Singapore

12.6 Canadian individuals may request access and correction, challenge our compliance, and withdraw consent subject to legal or contractual restrictions and reasonable notice where applicable. They may complain to the Office of the Privacy Commissioner of Canada or another competent provincial authority.

12.7 Our team access from Singapore is covered by the protections described in this Policy. Where Singapore's Personal Data Protection Act applies, individuals may contact our privacy address about applicable access, correction, consent and complaint rights. We comply with the obligations applicable to our role.

13 Children and policy changes

13.1 OrderPilot is intended for businesses and authorized adult staff, not children. We do not knowingly seek children's information for our own marketing or account relationship. Merchants must ensure their use involving customer information complies with applicable age and consent requirements.

13.2 If we learn that information has been collected unlawfully from a child, we work with the relevant merchant or take other appropriate steps to address it, including deletion where required. Contact our privacy address to report a concern.

13.3 We update the dates above when this Policy changes. We ordinarily give at least 30 days' notice of material changes by email and an in-app notice where available, with appropriate website notice for visitors. Urgent legal or security changes may take effect sooner, with notice as soon as practicable.

13.4 We obtain any consent or other authorization required before introducing an incompatible new use. Continued use or publication of an updated Policy does not, by itself, replace legally required consent.

14 Contact us

14.1 For privacy requests, complaints, transfer-safeguard information or legal notices, email **privacy@meetorderpilot.com**.

14.2 Write to: Bevy Commerce Inc., Attention: Privacy Contact, 3093 Bathurst St., Unit 690, Toronto, Ontario, M6A 2A3, Canada.

14.3 For product support, email **support@meetorderpilot.com**. Customers asking about a store's order, refund, warranty or messages should contact that store.