Privacy Policy

Application: Gripper QuickBooks Integration | Effective date: November 3, 2026

This Privacy Policy (the “Policy”) describes how Gripper Logistics LLC (the “Company,” “we,” or “us”) handles information in connection with its internally operated integration with QuickBooks Online (the “Application”). The Application supports authorized business and accounting activities. This Policy applies to information processed through the Application, including information relating to Company personnel, customers, vendors, and other persons appearing in relevant business records.

1. Scope and intended audience

The Application is for authorized Company personnel and approved service providers; it is not a public-facing consumer service. This Policy covers the Application and its connection to QuickBooks Online, not every Gripper website, product, or service. Other Gripper privacy notices may apply to the Company’s broader operations.

2. Information the Application may process

Depending on the features enabled and the permissions approved, the Application may process: (a) business contact and identification details, such as customer or vendor names, company names, email addresses, phone numbers, and billing information; (b) transaction and accounting records, such as invoices, items, amounts, taxes, currencies, payment status, refunds, and reconciliation references; (c) authorized-user information, including account identifiers, access permissions, and activity records; and (d) technical data needed to operate and secure the connection, including authorization tokens, connection status, error messages, and relevant system logs. Data categories are limited to those reasonably needed for implemented functions.

3. Sources of information

Information may originate from a Company-authorized QuickBooks Online account, the Company’s operational and billing systems, authorized personnel, and technical records generated when the Application is used. The Application requests access to QuickBooks data only through permissions authorized by the Company’s designated account administrator.

4. Purposes for using information

We process information to connect and maintain authorized QuickBooks accounts; create, retrieve, update, or match customer records, invoices, payments, and related accounting entries as supported by the Application; facilitate reconciliation and internal financial administration; identify and resolve integration errors; safeguard systems and detect misuse; and satisfy applicable recordkeeping, tax, audit, and legal obligations. We do not use QuickBooks-connected accounting data for unrelated advertising or sell such data.

5. Legal grounds and responsible use

Where applicable privacy law requires a legal basis, processing may be supported by the Company's legitimate business interests in operating and securing its accounting systems, the performance of relevant business or contractual obligations, compliance with legal duties, or another lawful ground as appropriate to the data and jurisdiction. Information should be accessed only by personnel who need it for an authorized task.

6. QuickBooks access and authorization

The Application connects through Intuit's authorized integration mechanisms and may receive read or write permissions, depending on the scope approved. A designated administrator can manage or revoke the connection through available Intuit or Company controls. Revocation stops new authorized API access after it becomes effective, but does not automatically delete accounting records lawfully retained in the Company's systems or in QuickBooks. Intuit processes information under its own applicable privacy statement and terms.

7. Service providers and disclosures

Information may be accessed or processed by appropriately authorized Company personnel and service providers that support hosting, storage, security, integration, payment operations, or accounting workflows, only as necessary for those functions and subject to applicable obligations. We may disclose information when required by law, a valid legal process, or to protect legitimate legal rights. We do not disclose QuickBooks-connected data to third parties for their independent marketing purposes.

8. Payments and payment-card information

Accounting records may contain transaction amounts, payment identifiers, billing details, and payment status. The Application is not designed to collect or store complete payment-card numbers or card security codes. Where payments are handled by a separate payment processor, that provider's terms and privacy practices also apply. Payment information transferred into QuickBooks is limited to the accounting data needed for the relevant workflow.

9. Security safeguards

We seek to apply reasonable organizational and technical protections appropriate to the sensitivity of the information, including restricting access to authorized users, safeguarding connection credentials and tokens, using secure transmission methods, and reviewing operational access where appropriate. No electronic system is completely risk-free, and security practices should be assessed and updated as the Application evolves. Suspected unauthorized access or data exposure should be reported promptly through established Company channels.

10. Data retention and deletion

We retain information for as long as reasonably required to operate the Application, maintain accurate business and financial records, resolve issues, and meet applicable tax, accounting, audit, or legal obligations. Technical logs and temporary integration data should be retained only for an operationally justified period. When data is no longer needed and no legal obligation requires preservation, it should be deleted, de-identified, or handled under the Company's applicable retention procedures. Disconnecting QuickBooks may not remove information already stored in accounting records or required backups.

11. International processing

The Company and its technology providers may process information in the United States and other jurisdictions where relevant systems or providers operate. Where cross-border transfers are subject to legal requirements, the Company is responsible for applying the safeguards required by applicable law.

12. Individual privacy rights

Depending on the person’s location and applicable law, individuals may have rights to request access to, correction of, deletion of, or restrictions on certain personal information, or to object to particular processing. These rights may be subject to exemptions and legal record-retention duties. Requests concerning information processed by the Company through this integration may be submitted using the contact channel below. Requests relating to data maintained directly by Intuit should also be directed to Intuit where appropriate.

13. Children and sensitive information

The Application is not directed to children and is not intended to collect children’s information. The Application is also not designed to process sensitive personal information unless it is lawfully included in necessary Company records and appropriately authorized. Authorized users should avoid importing unnecessary personal or sensitive details into accounting records.

14. Updates to this Policy

We may revise this Policy to reflect changes to Application functionality, service providers, legal obligations, or data-handling practices. The current version will show its effective date. Material changes should be communicated through an appropriate Company channel and, where applicable, other legally required notices.

15. Contact

For questions about this Policy or privacy requests related to the Application, contact Gripper Logistics LLC using the Company’s published contact channels at https://gripper.co. Requests may be referred to the appropriate Company administrator or privacy contact. Please do not include passwords, API secrets, or full payment-card information in a privacy inquiry.

Issued by: Gripper Logistics LLC
Scope: Internal QuickBooks Online integration and associated business data processing.