Privacy Policy

Promo CoWork and promoconsulting.com

Promo Consulting, LLC | https://promoconsulting.com

Effective date: November 11, 2026 | Last updated: November 24, 2026

1. Who we are and what this policy covers

Promo Consulting, LLC ("Promo Consulting," "we," "our," or "us") operates **Promo CoWork**, a business-to-business software-as-a-service platform whose AI agents assist distribution businesses, including promotional products distributors, with back-office work. Depending on the agents and settings a Customer selects, the agents may check orders, validate vendor acknowledgements, match vendor bills to purchase orders, record freight, prepare customer invoices and send them through the Customer's own business systems, post customer payments, summarize activity for accounting, and follow up on past-due invoices.

This Privacy Policy explains how we collect, use, disclose, retain, and otherwise process personal information through Promo CoWork, including the customer portal and our administration tools, and through our website at promoconsulting.com. It also describes the choices and rights that may be available. In this policy, "personal information" means information that identifies, relates to, describes, or can reasonably be linked with an identified or identifiable individual, subject to the definitions, exclusions, and exemptions under applicable law. Use of Promo CoWork is also governed by our Terms of Service at https://promoconsulting.com/terms.

Promo CoWork is offered to businesses in the United States and Canada for business purposes, not for personal, family, or household use. Accounts are created only by invitation: Promo Consulting sets up each Customer workspace and invites the Customer's administrator, who invites and manages the Customer's authorized users. This policy may nevertheless describe personal information about users and other individuals whose information appears in Customer Data.

2. Our role

The businesses that subscribe to Promo CoWork, such as promotional products distributors, are our "Customers." "Customer Data" means data that a Customer or its users submit to Promo CoWork or authorize Promo CoWork to access, including data in connected business mailboxes, order management systems, accounting systems, and other connected systems. Each Customer decides which systems and mailboxes to connect, which agents to enable, and the permissions and instructions that apply. When we process personal information in Customer Data on a Customer's behalf, we act as its processor or service provider, as those terms apply, and process that information to provide, secure, support, and maintain Promo CoWork, carry out the Customer's instructions, and comply with law. The Customer generally acts as the controller or business for that personal information and is responsible for its instructions, legal basis, notices, permissions, and responses to individuals. If our agreement with a Customer imposes stricter obligations, the agreement controls.

We act as a controller, business, or other responsible organization, as applicable, when we determine why and how personal information is processed for our own purposes. This includes personal information about website visitors and prospects and account, billing, security, support, and operational information relating to Promo CoWork. For Canadian privacy-law purposes, we are responsible for personal information under our control, including information transferred to a service provider for processing on our behalf.

3. Information we collect

3.1 Account and contact information

We collect a user's name, work email address, company, role, department, permissions, sign-in and multi-factor authentication settings, and notification preferences. We also collect contact and business relationship information for Customer administrators, billing contacts, prospects, and others who communicate with us. Customers and their administrators generally provide this information, and users may provide or update some of it directly.

3.2 Information from systems a Customer connects

At a Customer's direction, Promo CoWork reads from and writes to the business systems the Customer connects, within the permissions granted and as needed to run the agents the Customer has enabled. Depending on those connections, Customer Data may include the following:

- Email (Microsoft 365 or Google Workspace). We access only business mailboxes that the Customer or its administrator authorizes and connects, typically shared intake inboxes such as accounts payable or orders. Depending on the enabled features and granted permissions, we may process message identifiers, subject lines, senders, recipients, timestamps, folders, message bodies, signatures, forwarded or quoted text, plus attachment names and contents, such as vendor bills, acknowledgements, freight bills, and remittances. When a user enables message filing in their preferences and the granted permissions allow it, agents move messages from the inbox to a folder within that same user's connected mailbox, and back to the inbox if a message turns out not to be the agent's work. Messages and attachments may contain information about people who are not Promo CoWork users.
- **Order management and ERP systems,** such as Syncore: jobs, purchase orders, sales orders, line items, acknowledgements, invoices, payment and account status, shipping information, and business contact details for the Customer's vendors and customers.
- **Accounting systems,** such as QuickBooks Online: account mappings, customer and vendor records, invoices, payment records, and the summary journal entries that authorized agents read, prepare, or post.
- **Supplier and carrier systems:** supplier data such as PromoStandards acknowledgements, invoices and order status, and shipping data (ship dates, tracking numbers and freight costs) from carriers and shipping tools.
- **Payment sources:** transaction and remittance information from merchant or other payment sources a Customer connects, such as card payments received, so enabled agents can match and post customer payments. Promo CoWork does not connect to Customers' bank accounts or move money from them.

Promo CoWork does not access a user's contacts or calendars as standalone data sources. Information from a contact or calendar may nevertheless appear in an email, attachment, or connected business record that the Customer authorizes us to process.

3.3 Information about people who are not Promo CoWork users

Business email, documents, and records may contain personal information about people who are not Promo CoWork users, including a Customer's employees, representatives, vendors, and customers. This information may include names, business contact details, signatures, job titles, company affiliations, invoice and order details, correspondence, shipping information, and financial information appearing in invoices, remittance advice, emails, and other business documents. Financial information may include bank-account, payment-card, routing, or other payment details included by the sender. We do not automatically redact such information before processing a document. We process it as Customer Data on the Customer's behalf and in accordance with its instructions to perform the enabled tasks.

Financial information in business documents. To perform an enabled task, Promo CoWork may temporarily submit an entire invoice, remittance advice, email, or other business document to an AI provider, including any bank-account, payment-card, or other financial information that appears in the document. Documents are not automatically redacted before submission. We do not intentionally extract full account or card numbers for an

unrelated purpose, use them to access a financial account, or intentionally include them in agent output. When our systems identify a document as containing a full bank-account or payment-card number, we use it to complete the task and then discard it rather than retaining it in persistent application document storage or application backups, subject to temporary processing and legal or security exceptions described in sections 7 and 10.

3.4 Onboarding and support information

We collect information a Customer or user provides during onboarding and support, including questionnaire responses, workflow descriptions, sample documents, process walkthroughs, communications, issue reports, and diagnostic information. Sample documents may contain Customer Data and are handled accordingly. System credentials are entered on a secure Promo CoWork page, stored encrypted, and not displayed again after entry.

3.5 Agent activity and AI records

For agent activity, we record the action or proposed action, the affected record, timestamps, status and result, exceptions or errors, the user who approved, edited, rejected, or reported it and any reason provided, and the AI model and instruction version used. These records support approvals, troubleshooting, security, audit history, and accountability.

3.6 Technical information and tracking signals

We collect technical and usage information such as IP address, browser and device type, operating system, pages or features accessed, timestamps, referral information, identifiers, sign-in and authentication events, security events, and application and diagnostic logs. We collect this information from users' devices, browsers, and interactions with the service. We use a bot-protection service on sign-in to detect and block automated attacks.

Cookies and similar technologies. The Promo CoWork portal uses essential cookies and similar technologies needed for authentication, security, session management, and core functionality. Our website uses only essential technologies and does not use analytics or advertising tools. Because these technologies are necessary to provide the requested service, disabling them may prevent parts of the portal or website from functioning.

Browser privacy signals. Some browsers transmit Do Not Track or Global Privacy Control signals. We do not sell personal information or share it for cross-context behavioral advertising. Because we do not engage in those activities, such signals do not change our current processing, except where applicable law requires otherwise.

4. How we use information

- To provide Promo CoWork and perform the tasks a Customer enables, including sorting and routing email and records; moving messages from the inbox to a folder within the same user's connected mailbox, and back to the inbox if a message is not the agent's work, when enabled in the user's preferences and allowed by the granted permissions; extracting and validating information; recording authorized results in connected systems; retaining permitted copies of processed documents in secure storage, subject to sections 3.3 and 10; drafting replies and messages and sending them through a connected business mailbox as authorized by the Customer; and preparing invoices, statements, and collection reminders for transmission through the Customer's own business systems.
- To administer accounts; authenticate users; apply permissions; present approvals, alerts, audit history, and results; and maintain the integrity of Customer workspaces.
- To provide onboarding, configuration, training, support, troubleshooting, and other Customer-requested services.
- To evaluate and improve service reliability, usability, workflows, and agent performance as described in section 8, subject to the limits in sections 5 through 8.

- To invoice Customers and administer the business relationship; communicate about the service; protect rights, safety, and property; prevent, detect, investigate, and respond to fraud, abuse, and security incidents; enforce agreements; establish, exercise, or defend legal claims; and comply with applicable law and lawful process.

We do **not** sell personal information or Customer Data, share it with advertisers or data brokers, use it for advertising, use it to determine creditworthiness or for lending, or use it to create, train, or improve AI or machine-learning models. Our AI providers are contractually restricted from using Customer Data to train or improve their models. These commitments do not prevent us from using deidentified process information as described in section 8.

5. Google user data

If a Customer or its Google Workspace administrator authorizes and connects a business mailbox, Promo CoWork processes Google user data only through the scopes granted for the Customer-enabled features. The Customer controls which business mailbox is connected and may revoke access through Google or Promo CoWork. We use the scopes listed below to:

- confirm the email address of the connected account (openid and userinfo.email);
- read messages and their attachments in the connected mailbox so the agents can sort and process them (gmail.readonly);
- file messages an agent has taken on by moving them from the inbox into a user predefined folder (in Gmail, a label such as “Promo CoWork / [agent] / Done”), and move a message back to the inbox if it turns out not to be the agent's work (mail.modify).

Where message filing is available and the connection has permissions that allow it, Promo CoWork moves messages from the inbox to a user predefined folder within the same user's connected Gmail mailbox, and back to the inbox if a message is not the agent's work, when enabled in the user's preferences. Although gmail.modify is a broad Google permission, Promo CoWork is configured to change messages in Gmail only by moving them into a mailbox folder and back to the inbox. It does not delete, draft, or send messages in Gmail. Messages it cannot handle remain in the inbox for the Customer to review.

Limited Use disclosure. Promo CoWork's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy (https://developers.google.com/terms/api-services-user-data-policy), including the Limited Use requirements.

In particular:

- We use Google user data only to provide the Customer-authorized, user-facing business features described above and to maintain their security and functionality.
- We transfer Google user data only as permitted by the Google API Services User Data Policy, including to service providers listed on our Service Providers page that are necessary to provide or secure the authorized features, to comply with applicable law, or in connection with a merger, acquisition, or sale of assets with any notice or consent required by Google policy and applicable law.
- We do not use or transfer Google user data to serve advertisements, sell it, share it with data brokers, or use it to determine creditworthiness or for lending.
- We do not use Google user data, or data derived from it, to create, train, or improve any AI or machine-learning model. Content from Google accounts is excluded from the shared learning described in section 8.
- Promo Consulting personnel do not read Google user data unless (a) the Customer affirmatively asks or agrees, such as when its administrator approves support, setup, or testing; (b) access is necessary to operate or secure the service, including investigating abuse; or (c) access is required by law. Access is limited to what the task requires and is logged.

6. Microsoft 365 data

If a Customer or its Microsoft 365 administrator authorizes and connects a business mailbox, Promo CoWork accesses it through Microsoft Graph using delegated permissions consented to by the user or administrator, as applicable. Delegated permissions allow Promo CoWork to act for the signed-in business user within the access that user already has and the Customer has authorized, including authorized shared mailboxes. The Customer may revoke the connection through Microsoft 365 or Promo CoWork. We use the delegated permissions listed below to:

- sign the user in and read their name and email address (openid, profile, email, User.Read);
- keep the connection active without asking the user to sign in again (offline_access);
- read messages and attachments in connected mailboxes, including shared mailboxes (Mail.Read, Mail.ReadWrite.Shared);

When message filing is enabled in the user's preferences and the connection has delegated write permission that allows filing, Promo CoWork moves messages from the inbox to a folder within the same user's connected Microsoft 365 mailbox. Mail.ReadWrite and Mail.ReadWrite.Shared can provide mailbox write access. Read access alone, including read access to an authorized shared mailbox, does not authorize filing. Promo CoWork is configured not to delete messages in Microsoft 365 as part of these features. We apply the same substantive data-handling commitments described in section 5, including the limits on access by Promo Consulting personnel.

7. How AI is used

Promo CoWork uses large language models from third-party AI providers to read and sort email, extract and compare details from documents and business records, draft messages, and explain findings. For a task that requires document-level analysis, Promo CoWork may temporarily submit the full business document to an AI provider, not merely selected fields. The submission may include personal information, confidential business information, and any bank-account, payment-card, or other financial information appearing in the document because documents are not automatically redacted before submission. We do not intentionally extract full account or card numbers for an unrelated purpose or intentionally include them in agent output. Current AI providers, processing purposes, and locations are listed at https://promoconsulting.com/serviceproviders.

- Our AI providers are contractually restricted from using Customer Data to create, train, or improve their models. We enable zero-data-retention settings where a provider offers and supports them for the relevant service. Under those settings, the provider retains inputs and outputs no longer than necessary to return a response, subject to the provider's applicable security, abuse-monitoring, and legal obligations.
- Each AI request contains one Customer's data only.
- Email and document contents are treated as untrusted. Instructions found inside an email or attachment are never followed.
- Agents act only through permissions set for each Customer and cannot approve their own actions, change their own settings, move money out of a bank account, or act for another Customer.
- AI output is probabilistic and may be inaccurate, incomplete, or inappropriate, including by misreading a document or mismatching records. Customers choose how much each agent may do within configured rules and tolerances and remain responsible for reviewing output and approvals required by their settings. Human oversight and consequential-action controls are described in our AI Data Usage Policy, but those controls do not guarantee error-free output.

Details are in our AI Data Usage Policy at https://promoconsulting.com/aidata.

8. How the agents improve

Promo Consulting maintains shared best-practice rules for the service. To evaluate and improve those rules, workflows, and agent performance, we may use deidentified process information about how tasks and issues are handled across Customers. Before using information for this purpose, we remove or exclude Customer and client identifiers and do not include document or email contents, Google user data, Microsoft 365 content, or confidential details such as client names and order details. We use and maintain this information in deidentified form, do not attempt to reidentify it, and do not disclose one Customer's information to another Customer. Deidentified and aggregated information is not treated as personal information to the extent applicable law excludes it.

9. Who we share information with

Promo Consulting does not sell personal information or Customer Data. We may disclose information to the following categories of recipients for the purposes described below, subject to contractual, legal, and technical restrictions where appropriate.

- **Service providers.** We disclose information to vendors that provide cloud hosting, storage, backups, system email, security, bot protection, logging, credential management, and AI model or email-classification services. They process information for specified purposes under written terms that restrict use and require appropriate protection. Our current Service Providers page at https://promoconsulting.com/serviceproviders identifies each provider, its function, the data it processes, and its processing location.
- **Connected systems and recipients designated by the Customer.** At the Customer's direction, agents read information from and send information to connected email, order-management, ERP, accounting, supplier, carrier, and payment systems and may send Customer-authorized business communications to the Customer's own customers or other recipients through those systems. These systems and recipients are not our service providers merely because the Customer connects or directs us to use them. Each third-party system handles information under its own terms and privacy practices.
- **At the Customer's direction.** We disclose information as a Customer instructs or authorizes, including during onboarding, support, testing, integrations, exports, and offboarding, subject to applicable law and our agreement with the Customer.
- **Professional advisers.** We may disclose information to lawyers, accountants, auditors, insurers, and other professional advisers that need it to provide services to us and are subject to confidentiality obligations.
- **Legal and regulatory purposes.** We may disclose information to courts, regulators, law enforcement, government agencies, or other parties when we reasonably believe disclosure is required or permitted by applicable law or lawful process, or is necessary to establish, exercise, or defend legal claims. Where legally permitted and appropriate, we notify the affected Customer before disclosing Customer Data.
- **Security, safety, and enforcement.** We may disclose information as reasonably necessary to prevent, detect, investigate, or respond to fraud, abuse, unlawful activity, or security incidents; protect the rights, safety, and property of Promo Consulting, Customers, users, or others; enforce our agreements; or collect amounts owed.
- **Corporate transactions.** We may disclose or transfer information in connection with an actual or proposed merger, acquisition, financing, reorganization, bankruptcy, sale of assets, or similar transaction, including during due diligence, subject to appropriate confidentiality protections and any notice or consent required by applicable law or platform policy. A successor's handling of personal information remains subject to applicable law and the commitments that apply to the transferred information.
- **Deidentified or aggregated information.** We may disclose statistics or insights that cannot reasonably identify a person or Customer and are maintained in deidentified or aggregated form, as described in section 8 and as permitted by applicable law.

What we never share. Customer Data, including Google user data and Microsoft 365 data, is never sold, never shared for marketing or advertising, never shared with data brokers or for credit-risk purposes, and never used to train AI models.

10. Where data is stored, how long we keep it, and deletion

Promo CoWork is hosted in the United States, and our service providers may process and store information in the United States and other locations identified on our Service Providers page. Personal information relating to Canadian businesses and individuals may therefore be transferred outside Canada, including to the United States. While outside Canada, it is subject to the laws of the jurisdiction where it is processed and may be accessible to courts, law enforcement, national-security authorities, or regulators in accordance with those laws. We use contractual, organizational, and technical measures designed to protect information under our control during cross-border processing. Each Customer's data is logically separated from other Customers' data. Contact the Privacy Contact in section 17 for information about our service providers or cross-border processing.

Data	How long we keep it
Email and attachment contents and uploaded or generated documents not identified as containing full bank-account or payment-card numbers	Only as long as needed to complete the agent's task, and at most 30 days. The Customer's mailbox, order management system, and accounting system remain the systems of record.
AI prompts and responses retained by Promo CoWork, excluding discarded full financial-number documents	90 days in Promo CoWork. Where an AI provider offers and supports zero-data-retention settings for the relevant service, we enable them so the provider retains inputs and outputs no longer than needed to return a response, subject to applicable security, abuse-monitoring, and legal obligations.
Agent execution traces and error logs	90 days
File metadata, file fingerprints, and access history (no file contents)	2 years
Agent action history and security/access audit logs	7 years, because they record agent actions on invoices and payments
Approved knowledge, search indexes, and caches derived from Customer content	Deleted with the source content or when the Customer leaves
Backups	35 days, rolling. Documents identified as containing full bank-account or payment-card numbers are not included in application backups.

When access is revoked. A Customer administrator can disconnect a mailbox or system at any time through Promo CoWork or the applicable provider, such as Google Workspace or Microsoft Entra. Disconnection revokes future access once the revocation takes effect. At the Customer's request, we delete information previously obtained from that connection within 30 days, except for information retained under the periods above or as reasonably necessary for legal, security, fraud-prevention, dispute, or recordkeeping purposes. Ordinary content already present in rolling backups is removed as those backups expire, within up to a further 35 days, and is not restored to active use except for disaster recovery or security purposes. Documents subject to the special handling above are not placed in application backups when identified by our systems.

Special handling for full financial numbers. When our systems identify a document as containing a full bank-account or payment-card number, the document is used to complete the Customer's task and then discarded rather than retained in persistent application document storage or application backups. The document may be processed temporarily, including by an AI provider as described in section 7. Promo Consulting does not intentionally extract full account or card numbers for an unrelated purpose, use them to access financial accounts, or intentionally include them in agent output. Legal, security, or incident-response obligations may require limited preservation where applicable.

When a Customer leaves. We turn off its agents, revoke its connections, make an export of Customer Data available as provided in our agreement, and delete its content, indexes, and caches in accordance with the periods and exceptions above. Audit logs and agent-action history remain for their stated periods and are then deleted or deidentified. Residual copies in rolling backups expire under the backup schedule. Documents subject to the special handling above are discarded after the task when identified by our systems and are not retained in persistent application document storage or application backups.

11. Access by Promo Consulting staff

Authorized Promo Consulting personnel may access a Customer's account or Customer Data when reasonably necessary to provide Customer-requested support, setup, or testing; operate, maintain, troubleshoot, or secure the service; investigate suspected abuse or incidents; or comply with law. Customer approval is obtained for support, setup, or testing where required by our procedures or platform commitments. Access is role-based, limited to the information and duration reasonably needed for the task, and logged. Customer account owners can review applicable staff-access records through the service.

12. Security

We maintain administrative, technical, and organizational safeguards designed to protect information against unauthorized access, use, alteration, disclosure, or destruction. These measures include access controls, encryption, multi-factor authentication, logical separation of Customer data, and audit logging, as described in our Trust Center at https://promoconsulting.com/trustcenter. Safeguards are proportionate to the nature of the information and risks, but no system, transmission, or storage method is completely secure. We investigate suspected incidents and provide notices as required by applicable law and our agreements.

13. Your choices and rights

- Customer administrators choose which authorized business mailboxes and systems are connected, which agents run, and the permissions, rules, tolerances, and autonomy settings that apply. Where message filing is available and permitted, users choose whether to enable it in their preferences. Customer administrators can pause an agent or disconnect a mailbox or system at any time. Disconnection stops future access once revocation takes effect; deletion of information already processed follows section 10.
- Customers may request an available export of Customer Data, manage users and permissions, and submit privacy or deletion requests through the Promo CoWork portal or by contacting us. Individuals may contact us about personal information we control or process for our own purposes. Account and notification settings may also be managed through the service where the relevant feature is available.
- If personal information about you was submitted by or for a Customer, including where you are the Customer's employee, representative, vendor, or customer, the Customer generally controls that information. Please direct your request to the Customer first. If you send the request to us, we may refer it to the relevant Customer and will assist the Customer as required by our agreement and applicable law. We generally cannot fulfill a request concerning Customer Data without the Customer's instructions unless law requires otherwise.
- Rights vary by jurisdiction and apply only where the relevant law covers Promo Consulting, the individual, and the processing at issue, including any statutory thresholds, business-to-business or employment exemptions, and other exceptions. Where applicable, U.S. residents may have rights to confirm processing; access, correct, or delete personal information; obtain a portable copy; and opt out of sale, targeted advertising, or certain profiling. We do not currently sell personal information or process it for targeted advertising. Individuals in Canada may request access to personal information under our control, an account of its use and disclosure where required, and correction of information that is inaccurate or incomplete. We will not discriminate or retaliate for exercising a right protected by applicable law.

- Privacy rights are subject to verification and applicable exceptions. We may deny or limit a request where permitted by law, including where information is needed to provide a requested service, complete a transaction, protect security or prevent fraud, preserve legal privilege, establish or defend legal claims, comply with law or lawful process, meet tax, accounting, or recordkeeping obligations, or maintain records required by law or our agreements. Rights may not apply to deidentified information or information outside the scope of the relevant statute. If an exception applies, we will restrict further use as required by applicable law.

How to submit and verify a request. Email engage@promoconsulting.com with the subject "Privacy request," or use the request option in the Promo CoWork portal. Identify the right you wish to exercise, the information involved, your jurisdiction, and your relationship with us or a Customer. We use verification measures reasonably related to the request's nature and sensitivity, such as confirming control of an email address or matching information we already hold. We use information collected for verification only to verify and process the request, except as permitted by law. If we cannot reasonably verify identity, authority, or the information at issue, we may request additional information or deny the request and explain the basis where required. Where applicable law permits an authorized agent, we may require signed authorization or other proof of authority and may verify the individual's identity or instructions directly, subject to legally recognized powers of attorney.

Response timing and fees. For a verified request governed by an applicable U.S. state comprehensive privacy law, we respond within 45 days after receipt, unless that law specifies a different period. Where permitted and reasonably necessary, we may extend the response period by up to 45 additional days and will provide timely notice and an explanation. For a Canadian access or correction request, we respond within 30 days after receipt, subject to an extension authorized by applicable federal or provincial law. If we extend a Canadian response period, we will provide notice within the initial 30 days stating the reason, extension period, and any applicable complaint right. We do not charge a fee unless applicable law permits one, such as for manifestly unfounded, excessive, repetitive, or additional-copy requests, and we will provide any required advance notice.

Denials, appeals, and complaints. If we deny all or part of a request, we will provide the information required by applicable law, which may include the basis for denial and available appeal or complaint procedures. Where an applicable U.S. law grants an appeal right, you may appeal by replying to the decision or contacting the Privacy Contact in section 17. We will decide the appeal within the period required by that law and, where required, explain the outcome and how to contact the relevant attorney general or regulator. For a Canadian privacy concern, contact the Privacy Contact in section 17 and request escalation. We will investigate under our complaint procedure and communicate the outcome. If you remain dissatisfied, you may submit a complaint to the Office of the Privacy Commissioner of Canada or the applicable provincial privacy commissioner. Nothing in this section limits a right to contact a regulator directly.

14. Children

Promo CoWork is a business service and is not directed to children or intended for use by individuals under 18. We do not knowingly collect personal information directly from children through account registration or our website. Customer Data may contain information about minors if a Customer submits or authorizes access to that information; in that circumstance, the Customer is responsible for having the authority required by law, and we process the information on the Customer's behalf. If you believe a child has provided personal information directly to us without appropriate authorization, contact us using section 17.

15. Links to other websites

Our website and portal may link to or interoperate with third-party websites, systems, and services that we do not operate, including Customer-connected systems and service-provider websites. Their collection and handling of information are governed by their own terms and privacy notices, not this policy, except to the

extent they process information on our behalf. We are not responsible for independent third parties' privacy practices. Review their notices before providing information or authorizing a connection.

16. Changes to this policy

We may update this policy to reflect changes in the service, our practices, legal requirements, or other operational needs. We will post the revised policy on this page and update the "Last updated" date. For material changes, we will notify Customer administrators by email before the changes take effect and provide any additional notice or obtain consent where required by applicable law. Unless a shorter period is necessary for legal, security, or urgent operational reasons, we intend to provide at least 30 days' advance notice of material changes that materially reduce Customers' rights or expand our use of Customer Data.

17. Contact us

Promo Consulting, LLC

PO Box 8262, Breckenridge, Colorado, United States

Privacy Contact: engage@promoconsulting.com. Use this address for privacy questions, rights requests, complaints, appeals, and escalations, and include "Privacy request" in the subject line for a rights request.