SpecFlow

Privacy Policy

Seldon Data, operating SpecFlow
Effective and last updated: November 11, 2026

This Privacy Policy explains how Seldon Data, operating SpecFlow ("SpecFlow", "we", "us"), handles personal information when you visit usespecflow.com, use our business sales intelligence platform, or connect an external account. Questions and privacy requests can be sent to yusuf@usespecflow.com.

1. Information we collect

Account and business information: names, work email addresses, organization memberships, roles, product catalogs, target markets, campaign preferences, and information you provide when contacting us or booking a demonstration.

Workspace content: saved projects, business contacts, notes, outreach drafts and conversations, pipeline activity, CRM records, and other content you or authorized members of your organization enter or connect to SpecFlow.

Business research: professional contact details, employer and role information, project information, and source references obtained from public sources, customer-provided materials, and business data providers. This information may relate to people who do not have a SpecFlow account.

Technical information: IP addresses, browser and device information, authentication and security logs, cookies or similar identifiers, and product interaction and diagnostic information. Where configured, product analytics and session recording tools, including PostHog, help us understand usage and investigate problems. Recordings may include visible workspace content and interactions. Passwords are masked. Do not enter unnecessary sensitive personal information into the service.

Billing information: subscription and invoice details, payment status, and payment identifiers provided by payment processors. Payment providers process payment credentials under their own privacy notices.

2. Connected Google accounts

Connecting Google is optional and requires your authorization through Google's consent screen. We receive your connected email address and OAuth access and refresh tokens; we do not receive your Google password. We store OAuth tokens encrypted so the service can maintain the connection and perform authorized work when you are not actively using the browser.

The Google connection currently requests Gmail read access (gmail.readonly), Gmail draft and sending access (gmail.compose), read-only Calendar access (calendar.readonly), and read-only Contacts access (contacts.readonly). Gmail permissions allow access to message headers, recipients, subjects, message bodies, conversation identifiers and drafts. Calendar and Contacts permissions authorize access to calendar/event and address-book information; the current outreach implementation primarily uses Gmail. Any use of Calendar or Contacts information must support the connected account's visible contact or meeting features and this policy.

We use Gmail data to display and synchronize outreach conversations, create and update drafts, send messages when a user approves them or enables the relevant sending workflow, recognize replies, and track outreach and meeting progress. Authorized AI processing may analyze relevant conversation text to identify proposed, booked, completed, or cancelled meetings and provide related user-facing assistance. The service stores relevant message content, recipients, timestamps, thread identifiers, draft state, and derived outreach activity in your workspace.

3. Google API Limited Use commitments

SpecFlow's use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Google Workspace data is used only to provide or improve appropriate, prominent user-facing features of SpecFlow that you authorize.

We do not sell Google user data, use it for advertising or ad targeting, provide it to data brokers, use it for creditworthiness or lending decisions, or use it to train, fine-tune, or improve generalized or shared artificial intelligence or machine learning models. These restrictions also apply to raw, aggregated, anonymized, and derived Google data.

Google data may be transferred only as needed to provide or improve authorized user-facing features, with your consent where required, for security purposes, to comply with applicable law, or as part of a business transfer after obtaining the required explicit consent. An AI provider may process relevant Google content to deliver an authorized feature, subject to these same restrictions; this does not authorize generalized model training.

Human access to Google user data is limited to situations where you affirmatively agree to access to specific data, access is necessary for security or abuse investigation, access is required by law, or the data is aggregated and anonymized and used for internal operations as permitted by Google's policy.

4. Other integrations and organization sharing

If you connect Microsoft Outlook, LinkedIn, HubSpot, or another supported service, we process the account identifiers, credentials or tokens, and relevant messages, contacts, calendar information, or CRM records made available by the permissions you grant. We use these to provide the connected feature, such as sending outreach, displaying responses, or creating contacts and deals. The external provider's terms and privacy notice also apply.

SpecFlow is a shared business workspace. Authorized organization members may see shared contacts, messages, drafts, notes, connected account identities, and activity according to their access. If you choose to share a connection across represented brands or related organizations, it can be available in those workspaces. Connect only accounts you are authorized to use and share.

5. How we use information

We use information to operate and secure the service; authenticate users and manage organization access; research and match relevant projects and professional contacts; support outreach, CRM, and pipeline features; process billing; respond to requests; diagnose problems; and communicate service updates. AI-assisted features may process product, project, contact, and workspace information to generate research, rankings, drafts, or meeting assessments. Outputs can be incomplete or inaccurate and require human review.

Where applicable law requires a legal basis, we rely on performing our agreement with you, legitimate interests in providing and protecting a business service and relevant professional research, consent where required, and compliance with legal obligations. Google data remains subject to the narrower commitments in section 3.

6. Who receives information

We use service providers for hosting, cloud storage, databases, authentication, email delivery, payment processing, business research, customer support, analytics, and AI inference. They receive information relevant to the services they provide. Connected providers receive content you direct us to send or synchronize, such as an outreach email or a CRM contact. Workspace members receive shared information as described above.

We may disclose information when required by law, to address fraud or security incidents, to protect legal rights, or in connection with a merger, acquisition, financing, or sale of assets, subject to applicable law. Google user data remains subject to section 3, including its transfer and consent restrictions. We do not sell personal information or share it for cross-context behavioral advertising.

7. Retention, security, and international processing

We retain personal information for as long as reasonably needed to provide the service, maintain customer records, resolve disputes, protect security, and satisfy legal obligations. Retention depends on the information and purpose; we do not promise a single fixed period for all records. Information may remain temporarily in backups until those backups rotate out. Information retained for a legal or security reason is restricted to that purpose.

Disconnecting a Google account removes its stored mailbox credentials and stops future authorized synchronization; it does not automatically delete previously saved workspace messages, research, notes, or activity. Request deletion of those records using the contact below. Copies already delivered to recipients or exported to another service are controlled by those recipients or services.

We use access controls and other technical and organizational safeguards, including encryption of stored OAuth tokens. No system guarantees absolute security. Service providers and authorized personnel may process information outside your province, state, or country, where local laws may differ. We apply legally required safeguards for international transfers.

8. Your choices and privacy requests

You may disconnect an account through SpecFlow's integration settings. You can also revoke Google's access at https://myaccount.google.com/connections. Revocation stops future access; to delete information already stored in SpecFlow, email yusuf@usespecflow.com with the subject "Privacy request" and identify the relevant account or organization. Do not send passwords or access tokens.

Depending on your location, you may have rights to access, correct, export, or delete personal information, restrict or object to processing, or withdraw consent. We may verify your identity and authority before acting and will respond within applicable legal deadlines. Some information may be retained for lawful reasons, which we will explain where required. You may also contact the relevant privacy regulator.

Where your employer or another organization controls workspace information, contact its administrator as well. We will assist with requests within our role and legal obligations. People included in business research can use the same contact to request correction, removal, or suppression from future outreach. You can unsubscribe from marketing communications or ask us to stop sending them. Browser settings can restrict cookies and local storage, though this can affect sign-in and functionality.

9. Children and changes to this policy

SpecFlow is intended for adult business users and is not directed to children under 18. If you believe a child has provided personal information, contact us so we can investigate and take appropriate action.

We may update this policy as the service or legal requirements change. The date above identifies the latest revision. We will give notice of material changes where required and obtain any required consent before using Google data for a new purpose. The current policy is available at https://www.usespecflow.com/privacy-policy. Contact: Seldon Data, operating SpecFlow, yusuf@usespecflow.com.