



Draft answers to common vendor security questionnaire topics, for [ORGANIZATION]'s reviewers ·

spertsuite.com/approval-kit

SPERT® Suite Approval Kit v1.0.0 (Release) · Content reviewed 2026-10-25 · Built 2026-10-26

Prepared for: [ORGANIZATION] · **Reviewing team:** [REVIEWING TEAM] · **Requested by:** [PROJECT MANAGER NAME]

Item	Value
Application reviewed	SPERT® Scheduler v0.79.26 (repo famousdavis/spert-scheduler , commit 86b3e49)
Shared backend reviewed	famousdavis/spert-landing v2.7.2 (commit 52b7fbf): Firestore rules, Cloud Functions, Connect AI server (version 1.14.1, confirmed live 2026-10-25)
Legal documents relied on	Terms of Service v1.4 (eff. 2026-10-26) · Privacy Policy v1.4 (eff. 2026-10-26) · AI Privacy Notice v2.3 (eff. 2026-10-26) · AI Connectivity Consent Notice v2.2 (eff. 2026-10-26)
Third-party sources	Firebase privacy and security page; Vercel Security & Compliance docs (page dated 2026-09-08). Both read 2026-10-24.
Review date	2026-10-25
Operator	famousdavis, LLC (Florida). Copyright holder: William W. Davis, MSPM, PMP

What this is. Ready-made answers to the questions a typical vendor security questionnaire asks (the topics found in CAIQ, SIG Lite and HECVAT-style forms), written from the current source code and legal documents. A project manager can copy answers into [ORGANIZATION]'s own form. This is not legal, compliance or security advice, and it makes no commitment on the operator's behalf beyond what the current legal documents already say. The operator has **not** completed any formal questionnaire (CAIQ, SIG, HECVAT) and holds no certification of its own.

HOW TO READ EACH ANSWER

Each answer carries a status:

- **Supported:** the answer is backed by code, configuration or the current legal documents, cited inline.
- **Partial:** the control exists but is limited, depends on a third party, or is documented but not independently tested.
- **Gap:** the control does not exist today. The answer says so plainly and suggests how [ORGANIZATION] can compensate.

File references are to [spert-scheduler](https://github.com/famousdavis/spert-scheduler) unless prefixed landing: (the [spert-landing](https://github.com/famousdavis/spert-landing) repo). "[Privacy](#) §x", "[ToS](#) §x", "[AI Notice](#) §x" refer to the legal documents above.

APPROVE IN TIERS

SPERT® Scheduler has three parts that can be approved separately. Many answers below differ by tier, so decide the scope first. The numbers are labels, not a ladder: tiers 2 and 3 are separate decisions.

Tier	Default?	What leaves the browser	Suggested approval scope
1. Local-only use	Yes, on by default	Page requests to the web host (IP, browser type). Optional holiday lookup sends a two-letter country code and a year. No project data.	[APPROVE / DECLINE]
2. Cloud Storage	Off; opt-in with sign-in	Name, email, project data and settings, stored in Google Firestore (US)	[APPROVE / DECLINE / NOT IN SCOPE]
3. Connect AI	Off; opt-in per session	Read Mode: a snapshot of the open project, sent to the relay and to the user's chosen AI provider	[APPROVE / DECLINE / NOT IN SCOPE]

1. COMPANY AND PRODUCT

1.1 Who provides the service?

famousdavis, LLC, a Florida limited liability company, has operated the service since 2026-09-12. The software copyright is held by William W. Davis individually, and the LLC operates the apps under a license from the copyright holder. It is a single-operator business. (ToS header and §1.1, §3; [Privacy](#) §1.1)

SUPPORTED

1.2 Describe the product and architecture.

A browser-based project scheduling tool built with React. Scheduling and Monte Carlo simulation run in the user's browser (in a Web Worker). There is no first-party application server for core features. Static pages are served by Vercel. Optional features use Google Firebase (Authentication, Firestore, Cloud Functions). (SECURITY.md "Architecture"; ARCHITECTURE.md)

SUPPORTED

1.3 Is the software open source? Can we inspect it?

Yes. GPL-3.0 with additional terms under GPL §7 (attribution kept, trademarks reserved, modified versions renamed). The full source for the app and the shared backend is public on GitHub, so [REVIEWING TEAM] can read the code that runs. (LICENSE; [ToS](#) §3)

SUPPORTED

1.4 What does it cost? Is there a contract?

Core functionality is free. No paid tier exists today; the legal documents mention Stripe only "if subscription payments are implemented". The relationship is governed by the clickwrap [Terms of Service](#), not a negotiated contract. ([Privacy](#) §2.4, §4.2)

SUPPORTED (no cost). Note: there is no negotiable enterprise agreement.

2. HOSTING AND DATA RESIDENCY

2.1 Where is the application hosted?

Web pages: Vercel, production origin <https://scheduler.spertsuite.com/>. Optional back end: Google Firebase project spert-suite. (SECURITY.md "Deployment Headers"; [Privacy](#) §1, §4.1)

SUPPORTED

2.2 Where is customer data stored at rest?

- Local-only use: in the user's browser `localStorage`, on the user's device. (`SECURITY.md` "Local Mode")
- Cloud Storage and Connect AI relay data: in the United States. [Privacy](#) §9 states: "Cloud Storage data and AI Connectivity relay data are currently stored at rest in the United States (Google Cloud Firestore multi-region `nam5`), and the Operator will give notice by updating this Policy before changing that location."
- Server functions run in `us-central1`. (landing: `functions/src/mcp/index.ts`, `pairing.ts`, `teardown.ts`; AI Notice §5)

SUPPORTED

2.3 Is any processing or logging outside that region?

Yes, in limited ways, and the policy says so. Operational logs are kept 30 days in Google Cloud Logging, "whose default storage location is not restricted to a specific country or region" ([Privacy](#) §2.3). Google's authentication, security and support operations "may involve processing elsewhere" ([Privacy](#) §9). Vercel may process request data wherever it operates (Vercel docs, "Where does my data live?").

PARTIAL

2.4 Can we choose an EU (or other) region?

No. The service is US-only.

GAP Compensate by approving tier 1 (local-only) only, or by self-hosting (see 13.3).

3. DATA COLLECTED AND CLASSIFICATION

3.1 What personal data is collected?

- Local-only: none by the operator. Vercel receives standard request data (IP address, browser type) to serve the pages. ([Privacy](#) §1, §2.4)
- Cloud Storage: name, email and profile-photo link from the Google or Microsoft account (with the time the profile was last updated), plus a record of which ToS and Privacy version was accepted, when, with which sign-in provider and in which app first. "No other personal information is collected during account creation." ([Privacy](#) §2.1)
- Firebase also collects IP address, browser and OS, and read/write timestamps; Firebase Authentication keeps logged IP addresses for a few weeks. ([Privacy](#) §2.3)
- Sharing: invitee email, inviter name and email, project id and name, role. ([Privacy](#) §2.6)

SUPPORTED

3.2 What business data is stored?

Project planning data: activity names, three-point estimates, dependencies, milestones, calendars, notes, descriptions and checklist items. Simulation results are stripped before cloud saves. ([Privacy](#) §2.2; `SECURITY.md` "Cloud Mode")

SUPPORTED

3.3 What data classifications are permitted?

The ToS prohibits storing third-party PII, protected health information, payment card data, government ID numbers "or other sensitive or regulated data", and recommends Cloud Storage "be used only for non-sensitive planning metadata". ([ToS](#) §5.3; [Privacy](#) §2.2) **[ORGANIZATION]** should map this to its own scheme: permitted classification for SPERT® Scheduler = [e.g., PUBLIC / INTERNAL]; prohibited = [e.g., CONFIDENTIAL and above].

SUPPORTED (the restriction is contractual; the app does not technically detect sensitive data).

3.4 Are cookies or trackers used?

No analytics, telemetry, advertising or tracking cookies. Authentication cookies and local storage are set only when Cloud Storage is enabled. ([Privacy](#) §7.7; SECURITY.md "Architecture")

SUPPORTED

4. ENCRYPTION

4.1 Is data encrypted in transit?

Yes. All traffic is HTTPS. Production sends Strict-Transport-Security: max-age=63072000 (two years), which comes from Vercel's platform configuration rather than the repo. ([Privacy](#) §5; SECURITY.md "Deployment Headers")

SUPPORTED HSTS is a platform default, not repo-controlled; [REVIEWING TEAM] can confirm with `curl -sIL https://scheduler.spertsuite.com/`.

4.2 Is data encrypted at rest?

Cloud data relies on Google's default encryption at rest. Firebase states that Cloud Firestore, Firebase Authentication and Cloud Functions for Firebase encrypt data at rest (Firebase privacy and security page, read 2026-10-24). Vercel states it encrypts data at rest with AES-256 (Vercel docs, 2026-09-08). Local-only data sits in browser storage and is protected only as well as the user's device (disk encryption, OS account).

PARTIAL Provider defaults only; the operator makes no separate encryption statement beyond "HTTPS encryption for all data in transit" and "Google Cloud's infrastructure-level security controls" ([Privacy](#) §5).

4.3 Do you support customer-managed keys (BYOK/CMEK)?

No.

GAP Compensate with tier 1 only, where data never leaves the device.

5. AUTHENTICATION

5.1 How do users authenticate?

Local-only use needs no account. Cloud Storage uses Firebase Authentication with Google Sign-In or Microsoft Sign-In only, "including Microsoft Entra ID / Azure AD organizational accounts". ([Privacy](#) §2.1; `src/ui/providers/AuthProvider.tsx`)

SUPPORTED

5.2 Are passwords stored?

No. There is no username/password option; credentials stay with Google or Microsoft.

SUPPORTED

5.3 Is MFA supported?

Whatever [ORGANIZATION]'s Google or Microsoft identity provider enforces (MFA, conditional access, device compliance) applies at sign-in. The app has no MFA setting of its own.

PARTIAL (inherited from the identity provider).

5.4 Do you support SAML SSO, SCIM provisioning, or restricting sign-in to our tenant?

No SAML, no SCIM, and no way for [ORGANIZATION] to force users onto its tenant or block personal accounts. Also, the SPERT® Suite sign-in app is not yet a Microsoft "verified publisher": where Entra ID lets users consent only to verified publishers' apps, staff see "Need admin approval" and an administrator must grant consent first (operator's statement, 2026-10-25).

GAP Compensate by instructing staff to sign in with their [ORGANIZATION] Microsoft or Google work account (after granting admin consent in Entra ID if required), or by approving tier 1 only.

6. ACCESS CONTROL AND TENANT ISOLATION

6.1 How is customer data isolated?

Firestore security rules enforce role-based access: only members can read a project, only owners and editors can write, editors cannot change owner or members, a new project may list only its creator as a member, a member can remove themselves from a shared project, settings are owner-only, collection listing is limited to the caller's memberships, and profile lookups return at most one result per query to prevent bulk email harvesting. (The creator-only and leave rules shipped 2026-10-24 in landing v2.6.5 and SPERT® Scheduler v0.79.17.) (SECURITY.md "Cloud Mode"; canonical rules in landing: firestore.rules, tested in landing: rules-tests/)

SUPPORTED

6.2 How are access rules deployed and kept from drifting?

The canonical rules live in [spert-landing](#) and are deployed by CI on merge to main (landing: .github/workflows/deploy-firestore-rules.yml). A scheduled job compares the deployed rules with the repo every six hours (landing: .github/workflows/firestore-rules-drift.yml, cron 30 */6 * * *).

SUPPORTED

6.3 Are inputs validated server-side?

Access is enforced server-side by the rules. Since 2026-10-24 the rules also refuse a malformed project version number (landing v2.6.2), but most field-level validation (string lengths, enums) is still client-side only (Zod). The app now checks values before saving, never trusts simulation results from the cloud, and lists a project it cannot load with Export and Delete options instead of letting it vanish (v0.79.9, v0.79.20). (SECURITY.md "Known Limitations")

PARTIAL

6.4 Can the operator access our data?

The operator administers the Firebase project and so has technical access to Cloud Storage data. The ToS grants the operator a license "to host, copy, transmit, display, and make backups of that data solely as necessary to provide the Services". ([ToS](#) §5.6) No access-logging commitment exists for operator access. Local-only data is never accessible to the operator.

PARTIAL

6.5 Is there an admin console for our organization?

No organization admin console, no central user management, and no org-wide export.

GAP

7. LOGGING AND MONITORING

7.1 What is logged?

Google Cloud operational logs (request metadata such as IP, timestamp, requested URL) are retained 30 days and used "only to operate, secure, and troubleshoot the Services" ([Privacy](#) §2.3). Server logs redact invitation tokens (landing: `functions/src/logging.ts`) and Connect AI error logs record the operation type, not the user's content (`SECURITY.md` finding A7).

SUPPORTED

7.2 Are audit logs available to customers?

No. There is no customer-facing audit log of who viewed or changed a project.

GAP Compensate by keeping sensitive work out of scope, and by using the in-app JSON export as a point-in-time record.

7.3 Is the service monitored?

Yes, with limits. The operator checks the SPERT[®] Suite web apps every 5 minutes with UptimeRobot, an external uptime service (operator's statement, 2026-10-25; the monitor configuration is outside the repos and was not inspected). The Connect AI server is not on that 5-minute check: UptimeRobot's free tier could not be used for it (landing: `.github/workflows/external-health.yml`, header comments). Instead, a scheduled GitHub Actions job runs every six hours (best-effort timing). It sends a protocol ping to the server's direct Cloud Functions address and requires a valid response, and it checks that the TLS certificates of nine SPERT[®] Suite web hosts have at least 21 days left. That job does not test the public address `mcp.spertsuite.com` or its certificate. A failure emails the operator. There is no published status page and no 24×7 monitoring or response commitment.

PARTIAL A Connect AI outage could go unnoticed for up to about six hours, and a fault in the `mcp.spertsuite.com` address itself would not be detected by these checks. Local-only use does not depend on the server.

7.4 Is there abuse protection?

Invitations are capped at 25 per user per day (landing: `functions/src/rateLimiter.ts`), and the AI server applies a per-IP and per-session rate limit, held in memory per server instance (landing: `functions/src/mcp/rateLimit.ts`). Since 2026-10-24 the AI server rejects batched requests that could step around that limit, and pairing codes are one word plus 10 digits, closed about a minute after first use (landing v2.6.3; `functions/src/mcp/pairingCode.ts`). Vercel provides DDoS mitigation at the platform level (Vercel docs). Not yet built: Firebase App Check or other limits on unauthenticated writes to the Connect AI relay.

PARTIAL

8. APPLICATION SECURITY AND VULNERABILITY MANAGEMENT

8.1 What browser security headers are set?

Content-Security-Policy (as an HTML meta tag), X-Frame-Options: DENY, X-Content-Type-Options: nosniff, Referrer-Policy: strict-origin-when-cross-origin, Permissions-Policy denying geolocation, microphone and camera, and HSTS. Three unused CSP sources were removed in v0.79.21; the live policy was checked against `index.html` on 2026-10-25. (`index.html`; `vercel.json`; `SECURITY.md` "Deployment Headers")

SUPPORTED

8.2 Are there known weaknesses?

Yes, documented openly in SECURITY.md:

- CSP still allows 'unsafe-eval', needed only by the ExcelJS export library; removal is a deferred hardening item. Three broad CSP grants used by sign-in and cloud functions await a live test before they are narrowed.
- Most field validation is client-side only (see 6.3).
- The share dialog can reveal whether an email address is registered, and a signed-in user can still look up profiles one at a time.
- On a shared computer, acceptance of the Terms is remembered per browser, not per person. Local-only projects belong to the browser profile, so anyone using it can see them.
- A self-audit of v0.79.8 (2026-10-24) found 30 issues. Its three High findings were fixed and deployed the same day, and the SPERT® Scheduler side of the Medium and Low findings was fixed or decided by 2026-10-25 (v0.79.9 to v0.79.23). The remaining open items include the ones above and two Connect AI server items (see 11.7).

PARTIAL

8.3 What secure coding practices are used?

No first-party eval and no dangerouslySetInnerHTML; CSV exports guard against formula injection; imports are schema-validated with a 10 MB limit; holiday API responses are schema-validated. Targeted security audits are recorded in SECURITY.md (v0.20.2, v0.21.2, v0.57.4); the v0.79.8 self-audit's fixes are listed in the public changelog (v0.79.9 to v0.79.23). CI runs release and ship-gate workflows (.github/workflows/release.yml, shipgate.yml), and the repo uses mutation testing (stryker.config.mjs).

SUPPORTED for practices; these are self-reviews, not independent audits.

8.4 Has a third-party penetration test been performed?

No.

GAP Compensate: the source is public, so [REVIEWING TEAM] can review it or test its own copy. Do not scan or test the production apps without raising it with the operator first: the [Terms of Service](#) (§4) forbid attempting "to probe, scan, test, or circumvent the security or authentication measures of the Apps".

8.5 How are dependencies kept up to date?

Since 2026-10-25, GitHub Dependabot alerts and CodeQL code scanning (default setup) are on for every public SPERT® repository, along with secret scanning and push protection. These are GitHub settings, not files, so they do not appear in the repo (verified for SPERT® Scheduler through the GitHub API on 2026-10-25). Updates are applied by hand after a 60-day soak period for new releases; for example, react-router-dom was updated for an advisory in v0.79.14, and a zod advisory fix waits for its soak period to end. Automatic update pull requests are off.

PARTIAL (alerts and scanning on; updates manual, and no written exception yet for urgent advisories).

8.6 How are vulnerabilities reported?

Privately, by email to security@spertsuite.com, or through GitHub's private vulnerability reporting on the repository's Security tab (SECURITY.md "Reporting Vulnerabilities"; turned on for all eight public SPERT® repositories on 2026-10-25). The operator's Security page (<https://spertsuite.com/security>) aims to acknowledge reports within 3 business days and says a short advisory is published after fixing an issue that could have affected users' data. RFC 9116 contacts: <https://spertsuite.com/.well-known/security.txt> and <https://scheduler.spertsuite.com/.well-known/security.txt>. (Security page and site-wide security.txt checked in the [spert-landing](#) source, v2.7.1; not fetched live from here.)

SUPPORTED

9. INCIDENT RESPONSE AND BREACH NOTIFICATION

9.1 Do you have an incident response plan?

No written plan is published. The commitment is in [Privacy](#) §5.1: "If we determine that the incident creates a material risk of harm to affected users, we will notify them by email or in-app notice and, where required by applicable law, notify relevant regulators within the timelines mandated by statute."

PARTIAL

9.2 What notification timeline do you commit to?

None beyond what statute requires ([Privacy](#) §5.1).

GAP for contractual timelines (e.g., 72 hours). Tier 1 has nothing for the operator to breach.

9.3 Who is liable in a breach?

The service is provided as-is. The operator "is not responsible for any loss, corruption, unauthorized access to, or unavailability of data stored in Cloud Storage" ([ToS](#) §5). Security obligations are "limited to the proper configuration of these Google Firebase tools and services" ([Privacy](#) §5).

SUPPORTED (as a statement of terms). **[REVIEWING TEAM]** should weigh this against the data classification in 3.3.

10. BUSINESS CONTINUITY, BACKUP AND AVAILABILITY

10.1 Is there an SLA or uptime commitment?

No. "The Operator makes NO representations or warranties regarding the availability, security, durability, accuracy, or fitness for any particular purpose of the Cloud Storage feature." ([ToS](#) §5)

GAP

10.2 Are backups taken?

Yes, for operator recovery only: daily backups kept up to 98 days and point-in-time recovery data up to 7 days, in the same US location, "not available to you as a restore service". ([Privacy](#) §6) The ToS says users are "solely responsible for maintaining independent backups". ([ToS](#) §5)

PARTIAL

10.3 What happens if the service goes away?

Local-only use keeps working from the user's browser data for as long as the site is served. Users can export at any time to JSON, CSV or XLSX. Because the code is GPL, **[ORGANIZATION]** could run its own copy (see 13.3).

PARTIAL There is no documented continuity plan; the operator is a single person.

11. AI USE (CONNECT AI)

11.1 Does the product use AI?

Not by default. SPERT[®] Scheduler has no built-in AI model. Connect AI is an opt-in feature that lets a user connect their own AI assistant (for example **[AI PLATFORM]**) to the open project. It is off when the app opens and starts only after a consent dialog and a single-use pairing code. (AI Notice §1; `src/ui/components/ConnectAI/ConnectAiConsentModal.tsx`)

SUPPORTED

11.2 What data does the AI receive?

- **Write Mode** (required to use Connect AI): the AI can send edits; "Your existing project data remains in your browser's local storage and is not uploaded to any server" (AI Notice §2.1).
- **Read Mode** (optional): "A snapshot of your current project content is uploaded from your browser to the SPERT® cloud relay (Google Firestore)" and "transmitted to your chosen AI provider's servers" (AI Notice §2.2). Technically, the browser writes the snapshot straight to Firestore (`src/ui/hooks/use-ai-connectivity.ts`); the AI provider's servers then call the Connect AI server, `https://mcp.spertsuite.com`, a Google Cloud Function (second generation, running on Cloud Run) in `us-central1`, which reads it. The browser never calls the AI server itself. This includes free-text notes, descriptions and checklist items, and excludes owner id, members, email, other projects and calendars (`SECURITY.md` "Read-Mode snapshot"). Only the project the session was opened for is shared; switching projects starts a fresh session (v0.79.19). **This applies even in local-only mode** ([Privacy](#) §1; AI Notice §2.2).

SUPPORTED

11.3 What can the AI change or delete?

Through the scheduler's AI tools (landing: `functions/src/mcp/tools/scheduler.ts`), an AI can create activities, dependencies and milestones, and modify existing ones. Overwrite or delete capabilities are:

- Rename an activity; update estimates; update a milestone; bulk-update activities (patch named fields).
- Set an activity description, which overwrites it; an empty string clears it.
- Remove a dependency (requires Read Mode); unassign a milestone; reorder activities; toggle checklist and deliverable items.

No AI tool deletes an activity, a milestone or a project. Edits are written only by the server (clients cannot write AI operations under the rules), the server refuses estimates that are infinite or longer than 3,650 days (landing v2.6.5), and the browser re-validates each one with bounds checks before saving (`SECURITY.md` "Write-op validation", findings A1 to A6).

SUPPORTED

11.4 Is our data used to train models?

"The Operator does not use your data to train machine learning models." ([Privacy](#) §3) What the AI provider does is governed by that provider's terms ([Privacy](#) §4.5; AI Notice §3).

SUPPORTED for the operator. **Partial** overall: it depends on which **[AI PLATFORM]** and account type the user connects.

11.5 How long is AI session data kept?

Relay data expires seven days after the session's last activity, including requests from the AI assistant (so a session an AI keeps using does not expire) and is deleted from the live relay, "typically within 24 hours of expiry"; sooner on disconnect or sign-out (sign-out ends the session in the browser since v0.79.11 and on the server since v0.79.25; if the server cannot be reached at sign-out, the app tells the user and retries; if it cannot be reached at Disconnect, the app does not say so, and the data stays until a later attempt succeeds or the session expires); the Read Mode snapshot is deleted when Read Mode is turned off. Copies may remain in backups (up to 98 days). (AI Notice §2.2, §4) Session data uses a random identifier not tied to an account unless the user is signed in.

SUPPORTED

11.6 Can we turn Connect AI off for all our users?

No. There is no organization-level switch. Consent is per app, per browser, per user (AI Notice §1, §6).

GAP Compensate with an acceptable-use rule ("Connect AI may be used only with [AI PLATFORM], and Read Mode only for [CLASSIFICATION] data"). If [AI PLATFORM] lets administrators restrict which custom connectors (MCP servers) users can add, that is the most effective technical control. Blocking the Connect AI server (`mcp.spertsuite.com`) on [ORGANIZATION]'s network does not work, because the AI provider's servers call it, not the user's device. Starting Connect AI does need the user's browser to call SPERT® Suite's pairing function at `us-central1-spert-suite.cloudfunctions.net/generatePairingCode`, so blocking that path, or that whole host (which also stops sharing invitations), may stop Connect AI from starting. This is untested, so [ORGANIZATION]'s IT team should test any block it relies on.

11.7 Has the AI feature been security reviewed?

Two self-audits. The first is recorded in `SECURITY.md` (v0.57.4, findings A1 to A7 and C1 to C2, all addressed). The second, of v0.79.8 on 2026-10-24, raised eight Connect AI findings: guessable pairing codes (High), a session surviving sign-out, sessions following the user to other projects, consent edge cases and an unbounded estimate were fixed by 2026-10-25 (landing v2.6.3 to v2.6.5; SPERT® Scheduler v0.79.11, v0.79.15, v0.79.19). Three remain open on the server side: stronger protection of session identifiers, limits on unauthenticated relay writes (App Check is the named plan), and a hard limit on session lifetime (each AI request extends a session). No independent review.

PARTIAL

12. SUBPROCESSORS AND THIRD PARTIES

No standalone subprocessor list is published. The list below is built from [Privacy](#) §4 and the app's Content-Security-Policy `connect-src allow-list (index.html)`, which names every endpoint the browser may contact.

Third party	Tier	Purpose	Data received	Source	Published attestations (as of 2026-10-24)
Vercel Inc.	All	Hosts web pages	IP address, browser type	Privacy §1, §4.6	SOC 2 Type 2 (Security, Confidentiality, Availability); ISO 27001:2022; EU-U.S. DPF (Vercel docs, page dated 2026-09-08)
Google LLC (Firebase Auth, Firestore, Cloud Functions, Cloud Logging)	2, 3	Sign-in, storage, invitations, AI relay, logs	Name, email, project data, IP, timestamps	Privacy §2.3, §4.1; AI Notice §5	Firebase Auth, Cloud Firestore and Cloud Functions for Firebase list ISO 27001, 27017, 27018 and SOC 1, 2, 3 (Firebase privacy page)
Microsoft or Google identity	2	User's sign-in provider	Sign-in exchange	Privacy §2.1	[ORGANIZATION]'s own identity provider

Third party	Tier	Purpose	Data received	Source	Published attestations (as of 2026-10-24)
Resend	2	Sends invitation emails	Invitee and inviter email, project name	Privacy §2.6, §4.6	Not checked
Microsoft (Exchange Online)	Website and email only	Hosts the operator's spertsuite.com mailbox	Anything emailed to spertsuite.com addresses, and form messages	Privacy §2.7, §4.6	Not checked
Formspree	Website only	Delivers contact and training forms on spertsuite.com	Name, email, message	Privacy §2.7, §4.6	Not checked
Nager.Date (date.nager.at)	1 (optional)	Public-holiday lookup	Country list; two-letter country code and year; the request also exposes the user's IP	src/infrastructure/nager/nager-client.ts; CSP; Privacy Policy §1	Not checked
User's chosen AI provider ([AI PLATFORM])	3	Runs the user's AI assistant	Read Mode snapshot; AI-generated edits	Privacy §4.5; AI Notice §3	Depends on [AI PLATFORM] and account type
Stripe	None today	Only "if subscription payments are implemented"	None today	Privacy §4.2	Not applicable

PARTIAL The processors are disclosed in the policy, but there is no formal subprocessor list and no change-notification process for it. Nager.Date is described in [Privacy Policy](#) §1 rather than in the §4 provider list.

13. DATA RETENTION, DELETION AND PORTABILITY

13.1 How long is data kept?

Cloud Storage data is kept while the account is active. Invitations expire after 30 days, but invitation records remain until the operator purges them. Logs: 30 days. AI relay: see 11.5. Backups: up to 98 days. ([Privacy](#) §2.3, §2.6, §6)

SUPPORTED

13.2 How is data deleted?

By request through the contact form or the email in [Privacy](#) §12. "The Apps do not currently provide a self-service account-deletion control." Deletion is completed "within a commercially reasonable period, not to exceed thirty (30) days under normal circumstances", with backup copies expiring later. Local-only data is deleted by the user (delete the project, or clear browser site data). Switching off Cloud Storage does not delete stored data ([Privacy](#) §7.4).

PARTIAL (no self-service deletion; no deletion certificate).

13.3 Can we export our data or run our own copy?

Yes. In-app export to JSON, CSV and XLSX ([Privacy](#) §7.1). The GPL permits self-hosting with [ORGANIZATION]'s own Firebase project, but there is no self-hosting guide, and the trademark terms require a modified version to be renamed (LICENSE, GPL §7 terms).

PARTIAL

14. PRIVACY AND LEGAL

14.1 Which privacy laws do you address?

GDPR and UK GDPR (operator is data controller; lawful basis Art. 6(1)(b)), and CCPA. ([Privacy](#) §7.5, §7.6)

SUPPORTED

14.2 Will you sign our DPA or a BAA?

No DPA or BAA is offered. Under the current [Privacy Policy](#) the operator is a controller, not a processor for [ORGANIZATION]. PHI is prohibited ([ToS](#) §5.3).

GAP Compensate with tier 1 only, which processes no personal data on the operator's side.

14.3 Who must approve use inside our organization?

The user does. [ToS](#) §5.5: users acting for an organization represent "that your use of Cloud Storage complies with your organization's applicable data governance, information security, and cloud storage policies." AI Notice §7 says the same for Connect AI, and offers organizations "a summary of data flows for IT review purposes" on request.

SUPPORTED

14.4 Governing law and warranty?

Florida, United States. Service is provided as-is without warranty. (ToS header, §5)

SUPPORTED

15. CERTIFICATIONS AND AUDITS

15.1 SOC 2, ISO 27001, or similar for the operator?

None. The operator has not been audited.

GAP What exists instead: the hosting providers' own attestations (section 12), public source code, the SECURITY.md self-audit record and the public changelog of fixes from the v0.79.8 self-audit, and a local-only mode that keeps data on the device. A suite-wide self-review was completed on 2026-10-25; its fixes are being released in stages. The operator is preparing security documentation (an overview, an IT-administrator guide, a sub-processor list and questionnaire answers). These are not published yet; ask the operator (contact@spertsuite.com) for their status. None of them is a certification or an independent audit.

SUMMARY OF GAPS

#	Gap	Affects tier	How [ORGANIZATION] can compensate
1	No SOC 2, ISO 27001 or pen test of the operator	2, 3	Rely on provider attestations; review the public code; start with tier 1
2	No DPA, BAA or negotiable contract	2, 3	Approve tier 1 only; keep personal data out

#	Gap	Affects tier	How ORGANIZATION can compensate
3	No SLA, support or continuity commitment	2, 3	Treat as a non-critical tool; export regularly
4	No SAML/SCIM, tenant restriction, admin console or audit log	2	Require work accounts by policy; limit to CLASSIFICATION data; blocking <code>spert-suite.firebaseio.com</code> may stop cloud sign-in (untested)
5	No organization switch for Connect AI	3	Acceptable-use rule naming AI PLATFORM ; restrict custom connectors in AI PLATFORM if it allows (blocking the Connect AI server does not work; blocking the pairing function may, untested, see 11.6)
6	US-only storage; logs not region-pinned	2, 3	Approve tier 1 only where residency matters
7	No customer-managed keys	2, 3	tier 1 only for higher classifications
8	Deletion by request only	2	Document the request process in the approval
9	Dependency alerts and code scanning are on, but updates are manual with a 60-day soak	All	Independent review of the public source, or of a separate copy, by REVIEWING TEAM if required (scanning the live apps needs the operator's agreement first, ToS §4)
10	No formal subprocessor list	All	Use the table in section 12
11	On shared computers, Terms acceptance is per browser and local projects belong to the browser profile	1, 2	Use only on assigned devices, or give each person their own browser or OS profile

REVIEWER NOTES

- **"It's open source with no vendor review behind it."** True: no third party has audited the operator. The trade-off is that every line that runs is public, the access rules are versioned and drift-checked, and the security history is written down in `SECURITY.md`, including its weaknesses. **REVIEWING TEAM** can verify claims directly rather than relying on a vendor's word.
- **"Our data will leave our environment."** Not in the default mode. Local-only use sends no project data anywhere. Cloud Storage and Connect AI are separate opt-ins, and this sheet lets you approve or decline each one.
- **"There's no audit trail."** Correct for tiers 2 and 3. If **ORGANIZATION** needs per-user audit logs, approve tier 1 only, or limit cloud use to data classified **CLASSIFICATION**.
- **"We've never heard of this vendor."** It is a small, single-operator tool, positioned here as a low-friction complement to **ORGANIZATION**'s existing scheduling tools, not a replacement. A time-boxed pilot with tier 1 only is the lowest-risk way to evaluate it.
- **"What if the AI deletes our schedule?"** No AI tool can delete an activity, milestone or project. The overwrite and removal actions are listed in 11.3, and Write Mode never uploads existing project data.

METHOD AND LIMITS

- **Scope.** Answers cover SPERT® Scheduler and the shared backend it uses. The other SPERT® Suite apps share the same Firebase project and legal documents, but their app-specific features and AI tools are not covered here.

- **Method.** As of 2026-10-25, facts were read from the public source code at the commits listed at the top of this sheet, and from the published legal documents. The live Content Security Policy, `security.txt`, served changelog and Connect AI server version were checked on 2026-10-25; other header and HSTS claims rest on the measurement recorded in `SECURITY.md` on 2026-08-22.
- **Not verified:** the Firebase billing plan and Vercel plan in use; Resend's, Formspree's and Nager.Date's security attestations; GitHub security settings on repositories other than SPERT® Scheduler (taken from the operator's change log of 2026-10-25, not checked one by one).
- **Third-party claims** are quoted from the providers' own pages as read on 2026-10-24 and can change. Re-check them before submission: Firebase, <https://firebase.google.com/support/privacy> ; Vercel, <https://vercel.com/docs/security/compliance> .

Attestation and approval decisions are for **[ORGANIZATION]** to complete.

Reviewer	Decision (tier 1 / 2 / 3)	Conditions	Date
[NAME, ROLE]	[] / [] / []	[CONDITIONS]	[DATE]