Security review pack

Where your data goes

Connector Central connects your firm's systems to your chosen AI assistant. The application and databases are **hosted in the EU**. Your AI and connected software providers have their own processing locations and data policies.

Connected systems <-> Connector Central <-> Your chosen AI

Your AI assistant sends a tool request to Connector Central. We check workspace access, use the provider credentials on the server, call the connected system, and return the result to your AI assistant. The assistant receives the data needed for the request; it never receives your provider credentials.

What we process

- **Provider credentials:** API keys and OAuth tokens, stored encrypted so the server can authenticate to connected systems.
- **Workspace and personal information:** names, email addresses, memberships, settings, and any profile images or workspace logos you upload.
- **Tool inputs and results:** processed transiently to fulfill the request. We do not store the raw inputs or returned provider data.
- **Operational evidence:** who invoked which tool, timing, outcome, access decisions, and hashes of inputs or results. These records do not contain raw tool payloads.
- **Analytics:** page views and product events. Signed-in PostHog events can include your email and name; cookie-free analytics does not mean anonymous analytics.

Processing locations

The application and databases run on Hetzner infrastructure in Nuremberg, Germany. PostHog uses EU analytics hosting; browser analytics pass through a Cloudflare proxy. Hatchbox manages deployment, Postmark delivers email, and Honeybadger receives error reports; those providers are based in the United States. Cloudflare provides network security, proxying, and object storage, with global processing.

Google Ads, and Google Analytics where configured, process website and conversion events. The sub-processor list gives provider purposes, locations, and policy links; the Cookie Policy explains analytics and advertising. These third-party services are distinct from EU application hosting.

Your firm chooses and contracts with its connected software and AI providers separately. Review their terms, processing locations, retention, and model-training settings. Connector Central cannot guarantee how those providers retain or use data after receiving it.

Protection and access

Encrypted credentials

Provider credentials are encrypted at rest and used only server-side. Saved secrets are not displayed again. HTTPS protects traffic to Connector Central. This is a claim about the controls described here, not a promise that every stored data category has the same encryption controls.

Per-person access and action limits

Owners and Admins manage which connectors each person can use. Tools are classified as read, write, or destructive, and access can be limited by tier.

Access limits can restrict which connected provider accounts a person can reach. A provider account may contain many client records: account reach is not a guarantee of restrictions on individual clients, records, or fields. Owners retain owner-level access; owner action caps can limit their tool tiers. These controls do not inspect the substance of an AI decision or provide a human approval step for each action.

Live checks and revocation

Provider verification checks whether credentials can be used and records the outcome. It is not continuous monitoring or an audit of the provider. Revoking access, disconnecting a connection, or changing an applicable limit takes effect on the next agent request. Requests already sent and sessions at the connected provider are not undone; revoke credentials with that provider when needed.

Workspace isolation

Workspace data is scoped in the application and protected by enforced row-level security in the database. Workspaces share infrastructure; they do not each have a physically separate database.

Staff identity and two-factor authentication

Workspaces have Owner, Admin, and User roles, with email invitations. Time-based one-time-password two-factor authentication is available to every user and is optional, including for Admins. Owners control workspace deletion.

OAuth consent binds an MCP-compatible AI client to one selected workspace and the authorizing person's access. It verifies their Connector Central identity and workspace membership. It does not prove that they belong to your firm's organization at the AI provider. Your firm must configure and check that separately.

Privacy, retention, and deletion

Our Privacy Policy, Data Processing Agreement, sub-processor list, and Terms of Service are public. They explain how WLS Labs Ltd processes information and the responsibilities of your firm. Using Connector Central does not by itself establish your firm's regulatory compliance.

Retention depends on the record

- **Tool inputs and results:** raw payloads pass through transiently and are not stored. Metadata and hashes are separate records.
- **Activity:** retained for your workspace's configured period, with a 30-day default. A daily cleanup removes expired Activity records.
- **Audit and execution evidence:** no automatic time-based deletion is configured. Workspace evidence remains until the workspace is deleted. Removing a member does not erase the audit history or its recorded actor name.
- **Platform usage facts:** workspace ID, tool identifiers, and timestamps are retained permanently, including after workspace deletion. These facts contain no member names or raw inputs/results.
- **Workspace records and credentials:** kept while the workspace exists. Disconnecting a provider stops its use but retains its encrypted connection record. Workspace deletion removes its live records and logo; revocation at the provider is separate.
- **Personal profile:** kept until account deletion. Deleting your account also deletes workspaces you own and removes your memberships elsewhere; those other workspaces and their audit history remain.
- **Analytics, error reports, and support messages:** handled separately from Activity. Contact support about access or erasure requests.
- **Backups:** may retain copies after live deletion. Contact support about data-return and deletion requests.

Data already held by your connected software or AI provider remains subject to that provider's policies. A deletion in Connector Central does not delete it there. The DPA's data-return and deletion obligations continue to apply; contact support to arrange a request.

Independent assurance

Status as of September 2026

- **SOC 2 Type I:** Preparing. Audit firm selection underway; report planned for late 2026.
- **SOC 2 Type II:** To follow the Type I report.

Our security review pack describes the controls in scope for the audit.

No auditor is engaged and no SOC 2 report is available yet. The scope describes our intended review; the timetable is a plan, not an assurance that a report will be issued by that date.

Review, access, and support

For security questions or a practice owner's, IT adviser's, or compliance reviewer's questionnaire, email support@connectorcentral.com. Tell us which controls or documents you need to assess.

Access, export, and removal

Review your profile in account settings and your workspace's records in Activity. Owners manage workspace deletion in workspace settings. Account deletion also deletes owned workspaces, so arrange an ownership transfer first if the firm needs to keep them.

There is no self-service workspace export. Request a copy, data return, correction, or erasure through support; we verify the requester's identity and authority and explain the available information and retention limits. We cannot export raw tool inputs or results that we do not store. Export client records directly from the connected software that holds them.

Responsible disclosure

Email support@connectorcentral.com with the subject “Security” and enough detail to reproduce a suspected vulnerability. Avoid accessing or changing anyone else's data. We investigate reports, keep you informed, and ask for reasonable time to address the issue before public disclosure. Our Privacy Policy describes the disclosure terms.

For sub-processor change notifications, email support@connectorcentral.com with the subject “Sub-processor updates”.