JURISTAT

Smarter patent decisions start *here.*
security@juristat.com

Security Frequently Asked Questions (Data Layer MCP)

What data does Juristat access, and what is included in the Data Layer MCP?
The Data Layer MCP gives you access to the same Juristat patent data you can already see when you log into the website. Your access is tied to your existing account permissions.

What types of customer data does Juristat collect beyond patent and prosecution data (e.g., usage logs, search queries, user behavior)?
Juristat collects standard usage telemetry (similar to most web platforms). We also maintain access audit logs as required by contract and applicable regulations. These logs may include user information (name and email address), access timestamps, and records of specific activity.

Is my organization's data kept separate from other customers' data?
Yes. Any non-publicly available data obtained from your organization is logically isolated from all other customers. Insights or outputs derived from your data cannot affect another customer's experience, and vice versa.

Where is customer data stored and processed in Juristat's MCP service, and are any subprocessors located outside of the United States?
Juristat's infrastructure and all of its USPTO data are hosted in the United States on AWS, US-East-1. Customer data processed by Juristat's MCP server including tool call parameters and any logs thereof, remain within US AWS regions.

Do you use customer data to train models?
Juristat does not use customer content, data, queries, or prompts to train AI models.

When I access Juristat's data through my LLM (CoPilot, Claude, ChatGPT, Harvey, etc.), who is processing my data?
Your LLM's AI processes your data: not Juristat. When you query Juristat's data through one of your AI tools, the AI tool (e.g. CoPilot) processes your query to determine what data is needed to respond. It then calls Juristat's MCP tools to obtain that data, which is then incorporated into your conversation with your LLM. The data you upload into a conversation is governed by your agreement with your AI provider.

Is Juristat SOC 2 certified?
Yes. Juristat holds SOC 2 Type II certification, which is the more rigorous, ongoing certification (as opposed to a one-time assessment). Upon signing an NDA, Juristat's security team will share the full audit report and any other reasonable supporting evidence upon request.

Has Juristat undergone third-party penetration testing?
Yes. Juristat conducts at least one external penetration test per year. Relevant findings and outcomes are documented in our SOC 2 Type II report.

Does Juristat support single sign-on (SSO) or multi-factor authentication (MFA)?
Yes. SSO is available to customers for a nominal fee to cover infrastructure and maintenance costs. MFA is supported through your SSO provider.

Who within Juristat can access user data on the Juristat platform, and how is access controlled?
Access to customer data is tightly restricted. Only a limited number of vetted, onshore engineers have "break-glass" emergency access, meaning they can only access customer data when necessary for emergencies or to respond to a specific customer inquiry, as outlined in your contract.

What is Juristat's process for detecting and responding to a data breach?
Juristat takes significant preventative measures to avoid any data breach or leak, including using industry-standard threat detection tools, conducting at least one external penetration test per year, and running simulated breach scenarios with its cyber insurance provide at least annually.
If a potential data security incident is detected, Juristat follows a formal incident response policy that is audited annually by an external firm. If said incident rises to the level of a breach, senior management is notified immediately, and external parties (including law enforcement, if appropriate) may be engaged. Juristat's incident response policy governs the notification of any affected parties.

Are attorney-client privileged communications or work product ever transmitted to or stored by Juristat?
The data Juristat returns through its MCP tools is sourced exclusively from USPTO public records. It originates from publicly available data that has been processed by Juristat. What Juristat receives from your MCP session should be limited to the parameters needed to fulfill each tool call (e.g. an application number, examiner name, CPC class, art unit, or similar identifier). Juristat should not receive your full prompts, your AI's reasoning, client communications, or documents you upload into your conversation with your AI.

Could confidential prosecution strategy or claim drafts entered into Juristat's MCP be exposed to opposing counsel or third parties?
No. When you use Juristat through an AI provider, your prosecution strategy and claim drafts live in your AI provider's session. Juristat receives only the tool parameters needed to fulfill each request (application numbers, examiner names, and similar identifiers). The data Juristat does hold is isolated per customer and validated annually under Juristat's SOC 2 Type II audit. Juristat does not use customer content to train AI models, and customer activity is never incorporated into the analytics products other customers see. Juristat's SOC 2 report is available under an NDA.

How does Juristat ensure that customer data remains confidential?
All data is encrypted both in transit and at rest. Internal access follows a least-privilege model, meaning employees only have access to the data they need to do their jobs. Customer data isolation prevents any merging or cross-contamination between accounts.

My organization requires a security review before adopting any AI product. Is that available?
Yes. Reach out to the Juristat team to arrange a full security review tailored to your organization's requirements.