JURISTAT

Smarter patent decisions start *here*
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, including if you have private data integration set up (formerly PAIR integration).

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, access timestamps, and records of specific activity.

Is customer data kept separate from other customers' data?
Yes. Your data is logically isolated from all other customers. Insights or outputs derived from your data cannot affect another customer's experience, and vice versa.

For Juristat's MCP, is any customer data sent offshore or processed by vendors outside the United States?
No, no customer data is sent offshore.

What third-party subprocessors or AI providers does Juristat use, and what data do they have access to?
Juristat uses Amazon Bedrock to power its AI models. These models only receive the information that is directly relevant to your current session, either content you link in yourself or content the system pulls in as part of a specific workflow (for example, Office Action Strategy Briefs automatically include similar office actions for context).

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.

Security Frequently Asked Questions (Data Layer MCP)

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 uses industry-standard threat detection tools and conducts at least one external penetration test per year. If an incident occurs, Juristat follows a formal incident response policy that is audited annually by an external firm. Juristat also runs tabletop exercises at least once a year and conducts drills with its cyber insurance provider. If an incident rises to the level of a breach, senior management is notified immediately, and external parties (including law enforcement, if appropriate) may be engaged.

Are attorney-client privileged communications or work product ever transmitted to or stored by Juristat?
Only if you explicitly upload them. Juristat does not pull in privileged materials on its own.

Could confidential prosecution strategy or claim drafts entered into the platform be exposed to opposing counsel or third parties?
No. Customer data is strictly isolated, and Juristat provides auditors with evidence of that isolation as part of its annual SOC 2 audit.

How does Juristat ensure that unpublished application 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 a Juristat product. Is that available?
Yes. Reach out to the Juristat team to arrange a full security review tailored to your organization's requirements.