MCP SERVER | NO CODE | CLOUD HOSTED

Strict PII Redaction Engine MCP

Secure your data before AI ever sees it.

Strict PII Redaction Engine strips sensitive personal data from documents using deterministic regex patterns. Send raw legal or financial files to your AI client without risking a massive breach. It locally and permanently scrubs emails, SSNs, credit card numbers, and phone numbers, replacing them with [REDACTED] tags before any analysis occurs.

A+ Quality Score 100/100

pii-redaction | data-privacy | gdpr-compliance | regex | data-scrubbing | security-firewall

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/strict-pii-redaction-engine

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Strict PII Redaction Engine MCP

1 tools available
Cloud-hosted on Vinkius

Sending customer records or internal contracts directly to an LLM is risky business. You don't want your client data sitting exposed when it hits a general-purpose model. This MCP acts like a local firewall for your sensitive documents, ensuring compliance with regulations like GDPR and CCPA before the context ever reaches your agent. It uses high-performance algorithms to find and replace personal identifiers—emails, SSNs, credit cards, phone numbers, and more. The process is deterministic; it doesn't rely on the AI model 'remembering' or manually forgetting the data. You simply feed the document through this MCP, and you get a clean copy back that keeps all the valuable context but strips out the risk. By connecting this engine via Vinkius, your AI client can trust that the input it receives is safe to process. This means you can run complex analyses on sensitive files knowing the underlying data privacy rules were followed automatically.

Core Capabilities

01 — Scrub Sensitive Data

The MCP finds and replaces emails, SSNs, credit cards, phone numbers, and CPFs with a standardized [REDACTED] tag.

02 — Ensure Compliance Pre-Processing

You guarantee that raw documents meet strict data privacy standards before they are sent to any large language model or agent.

03 — Maintain Context Integrity

The redaction process keeps the surrounding text and structure intact, so your AI client still gets usable context after scrubbing.

04 — Handle Diverse Identifiers

It detects multiple types of personal data, including SSNs, CPFs, and various phone number formats.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/strict-pii-redaction-engine** — connect your AI agent in three steps.

01 You send the raw document (e.g., a PDF transcript or financial report) to this MCP using your AI client.

02 The engine runs the data through high-performance regex algorithms, identifying all specified sensitive patterns and replacing them with [REDACTED].

03 Your agent receives the resulting sanitized text, which is safe for analysis without having compromised personal information.

The bottom line is you get a clean version of your document that retains its meaning but eliminates every piece of identifiable private data.

Built For

Compliance officers, legal operations teams, and financial analysts need this. They deal with massive amounts of sensitive client documents daily and know that sending raw files to an AI agent is a compliance nightmare. This MCP gives them a required safety layer they can trust.

Legal Operations Specialist

They process deposition transcripts and contracts, needing to redact all names, SSNs, and private contact details before internal summaries are generated.

Financial Compliance Analyst

They review leak logs or transaction reports that contain 16-digit credit card numbers or account details, ensuring zero PII leaves the secured environment.

Data Privacy Officer (DPO)

They need a guaranteed, auditable method to scrub data for testing or development environments, proving that no raw PII ever reaches an external service.

What Changes When You Connect

01	Stops compliance risks cold. Instead of relying on the LLM to 'forget' private data, you use this engine to deterministically eradicate emails and SSNs locally.
02	Guarantees GDPR/CCPA adherence in your pipeline. You can confidently route sensitive legal documents through your agent knowing they are scrubbed before processing.
03	Keeps context intact while scrubbing. The redaction replaces the data with a tag, meaning the AI still sees where the information was, without reading it.
04	Handles multiple types of PII in one go. You don't need separate tools for phone numbers, credit cards, or national IDs; this MCP handles them all.
05	Speed and reliability matter. It uses fast, offline regex patterns, meaning scrubbing runs quickly and reliably every single time.

Real-World Applications

Handling a Litigation Discovery Dump

A paralegal receives a 50-page deposition transcript full of private phone numbers and emails. They run the document through the engine, getting back a clean file that preserves all quotes needed for summary generation without violating any privacy rules.

Analyzing Financial Leak Logs

A compliance analyst has a massive log containing thousands of credit card numbers from a breach. They use the engine to scrub every single 16-digit number, allowing their agent to analyze patterns without handling actual financial data.

Building Safe Test Environments

A development team needs to test a new AI feature using real contracts but can't use live PII. They run the sample documents through the MCP, generating synthetic-looking redaction tags for safe testing.

Patterns to Avoid

Relying on LLM 'Memory'

✗ AVOID

Just sending a raw document and telling your agent to 'be careful not to expose PII.' The agent might summarize the data but still process or store the sensitive values.

✓ INSTEAD

Always run the input file through `redact_pii_strictly` first. This forces the model to only see scrubbed context, making compliance mandatory and auditable.

Using Manual Scrubbing

✗ AVOID

Opening a document, manually finding every phone number, copying it into a spreadsheet, and then re-pasting the clean text. This is slow and misses edge cases.

✓ INSTEAD

Use this MCP. It automatically identifies all standard formats—CPFs, SSNs, phones, etc.—and scrubs them with one function call.

Ignoring Data Format Differences

✗ AVOID

Assuming a simple find-and-replace will work on complex PDFs or structured data. Simple text replacement often fails to catch all variations.

✓ INSTEAD

This engine uses high-performance regex, designed specifically to handle the structural variation of emails and IDs across different document types.

The Right Fit

Use this MCP if your primary concern is that raw data cannot be processed by an AI agent. If you are working with legal transcripts, financial reports, or any internal documents containing SSNs, credit cards, or private emails, this engine is mandatory. Don't use it if your goal is simply to summarize text; you need it *before* the summarization happens. If your data already meets GDPR standards and contains no PII, then this MCP isn't necessary. You shouldn't use a general-purpose scrubbing tool for specific tasks like format validation—use a dedicated schema validator instead.

The Hidden Liability in Every Document

Think about it: you gather an account, maybe hundreds of pages of contracts or client transcripts. You have to get the AI agent to summarize them for a meeting, so what do you do? You open up tabs, manually highlighting every phone number and SSN in hopes that nobody notices before you paste it into your agent's prompt window.

With this MCP, you send the raw document first. The engine processes it locally, acting like an invisible security guard that strips out all private details—the emails, the card numbers, everything. You get back a clean version of the file ready for analysis, completely protected.

The redact_pii_strictly Tool Keeps Your Data Safe

You no longer have to worry about whether your agent missed an obscure format, like a foreign CPF or a non-standard email address. The tool handles the complexity of identifying and removing these specific PII types using highly reliable regex patterns.

It’s a one-step process that moves you from 'Are we compliant?' to 'Here is our clean data.' Your workflow instantly gains an audit trail for data security.

Strict PII Redaction Engine: 1 Tool

This engine allows you to process raw files through secure redaction algorithms using the available tools.

#	TOOL	DESCRIPTION
01	`redact_pii_strictly`	This tool quickly replaces emails, CPFs, SSNs, and credit card numbers in a document with the standard [REDACTED] tag.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Execute the strict redaction engine on this contract to remove all CPFs and Emails before we send the summary to Claude.

The computation has been executed with mathematical precision. All results are exact and ready for review.

U We have an extensive leak log. Process it through the engine to ensure every single 16-digit credit card number is destroyed.

The computation has been executed with mathematical precision. All results are exact and ready for review.

U Remove all standard phone numbers and SSNs from this 50-page deposition transcript before filing it to the public record.

The computation has been executed with mathematical precision. All results are exact and ready for review.

Frequently Asked Questions

01 **Does the Strict PII Redaction Engine MCP actually remove all phone numbers?**

Yes, it handles standard phone number formats. It uses advanced regex to find and replace these identifiers with [REDACTED] tags.

02 **What happens if I use redact_pii_strictly on a document that has no PII?**

The engine processes the file quickly, confirming there is nothing sensitive to scrub. It returns the original content unchanged but still processed through the secure pipeline.

03 **Can I use the Strict PII Redaction Engine MCP for legal documents only?**

No. While excellent for law (CPFs, SSNs), it works on any document type—financial logs, HR records, or customer support transcripts.

04 **Is this redaction process reversible?**

No. The engine deterministically replaces the data with a placeholder tag [REDACTED]. The original sensitive information is permanently scrubbed and unrecoverable from the output.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"strict-pii-redaction-engine": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Strict PII Redaction Engine is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Strict PII Redaction Engine. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Strict PII Redaction Engine MCP
Server ID	`019e38f4-fc89-73d8-847a-14b693938a50`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/strict-pii-redaction-engine.