

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Personal Data Location Mapper MCP

Track exactly where your sensitive information lives.

Personal Data Location Mapper helps you map, audit, and query the physical and digital locations of your personal data. It tracks information across your devices, cloud services, and physical storage so you can maintain a clear picture of your digital footprint and backup status.

A+ Quality Score 100/100

personal-data

audit

mapping

privacy

backup



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

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

Firewall & DLP

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

Agent Activity

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

Tool Health

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

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.

Personal Data Location Mapper MCP

4 tools available

Cloud-hosted on Vinkius

You can't protect what you can't find. This MCP gives your AI client the ability to act as a personal data auditor. Instead of guessing which cloud provider holds your tax documents or which old hard drive contains your identity files, you can ask your agent to locate them instantly. It bridges the gap between your physical storage and your digital accounts, providing a unified view of your data landscape. You can use it to verify if critical files are actually backed up or to see which specific entities are managing your most sensitive information. It's a practical way to manage privacy and ensure your data redundancy is actually working.

Core Capabilities

01 — Data Mapping

Your agent identifies the physical and digital locations of specific data types.

02 — Custodian Auditing

Your agent reviews the specific data inventories held by different service providers.

03 — Backup Verification

Your agent checks if your critical data categories have active redundant copies.

04 — Location Intelligence

Your agent pulls specific details regarding the management and backup status of folders or devices.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/personal-data-location-mapper — connect your AI agent in three steps.

- 01 Connect the MCP to your preferred client like Claude or Cursor via Vinkius.
- 02 Ask your agent a question about your data locations or backup status.
- 03 The agent invokes the necessary tool to query your data map.
- 04 You receive a direct answer about where your data is or if it is backed up.

Connecting this MCP to your AI client gives your agent immediate access to your data map.

Built For

This is for individuals and professionals who need to maintain strict control over their personal information footprint.

Privacy-conscious individuals

People who want to audit where their sensitive documents are stored across various clouds.

Digital organizers

Users managing complex digital lives who need to verify backup integrity.

Security researchers

Professionals mapping out data exposure and custodian management.

What Changes When You Connect

- 01 Reduces the time spent searching for specific digital or physical files.
- 02 Provides a clear view of data redundancy through backup checks.

-
- 03 Identifies which entities are managing your sensitive information.
-
- 04 Centralizes the oversight of your data across multiple platforms.
-

Real-World Applications

Identity Protection

Locate all instances of your identity documents to ensure they aren't sitting in unencrypted folders.

Custodian Review

See exactly what data a specific cloud provider or device is currently holding for you.

Backup Auditing

Check if your financial records are actually being synced to your secondary storage.

Digital Cleanup

Find old data locations to help manage your digital footprint and privacy.

Patterns to Avoid

Vague data searches

❌ AVOID

Asking your agent to find all your important files without specifying what they are.

✓ INSTEAD

Be specific about the data type. Use ``get_data_category_locations`` to find every location tied to a specific category like financial or identity documents.

Ignoring backup status

❌ AVOID

Assuming your tax documents are safe just because they are in a cloud folder.

✓ INSTEAD

Verify your redundancy. Use ``verify_backup_integrity`` to confirm that a specific category of data actually has valid redundant copies.

Blind custodian trust

❌ AVOID

Assuming a service provider only holds the files you recently uploaded.

✓ INSTEAD

Audit what they actually hold. Use ``audit_custodian_exposure`` to review the full data inventory managed by a specific entity.

The Right Fit

Connect this MCP if you need to audit where your sensitive files live or verify your backup redundancy. Do not connect it if you only manage a single, local folder of non-sensitive data. The decision depends on whether you need to bridge the gap between physical storage and digital cloud accounts.

Personal Data Location Mapper: 4 Specialized Tools

These tools give your agent the ability to map, audit, and verify the physical and digital locations of your sensitive information.

#	TOOL	DESCRIPTION
01	find_location_details	This tool retrieves specific details about a data location. It shows you the custodian and backup status for a particular device or folder.
02	get_data_category_locations	This tool finds all storage locations tied to a specific category. Use it to see every place your financial or identity data is kept.
03	verify_backup_integrity	This tool checks your backup status. It confirms if a specific category of data has valid redundant copies.
04	audit_custodian_exposure	This tool reviews the data inventory managed by a specific entity. It helps you see exactly what a custodian is holding for you.

See It in Action

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

U Where is my Identity data located?



Your Identity data is in your Passport (Physical Safe Box) and your Birth Certificate (iCloud).

U What is the backup status for my Work Laptop?



The Work Laptop is managed by you, and its data is backed up to your Google Drive.

U Is my Health data safely backed up?



Yes, your Health data is covered with backups available in your Dropbox account.

Frequently Asked Questions

01 What can this MCP do with my data?

It maps and queries the locations of your data across devices and cloud services. It does not move or change your data, it only reports on its location and backup status.

02 Which AI clients can use this MCP?

You can use this with any MCP-compatible client, including Claude, Cursor, Windsurf, and VS Code.

03 How does it help with privacy?

It helps you audit which custodians manage your data and ensures your sensitive information is stored in intended locations.

04 Can I check if my files are backed up?

Yes, you can use the tool to verify if specific data categories have valid redundant copies.

05 Do I need to host this myself?

No, Vinkius hosts and manages the MCP for you. You just connect your client and start using the tools.

06 How can I find where my financial records are stored?

You can use the ``get_data_category_locations`` tool and specify 'Financial' as the data category to see all associated locations.

07 Can I check if my data is properly backed up?

Yes, the ``verify_backup_integrity`` tool allows you to check the backup coverage for any specific data category.

08 How do I see what data a specific service provider manages?

Use the ``audit_custodian_exposure`` tool by providing the name of the service provider or person acting as the custodian.

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 <code>"personal-data-location-mapper": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Personal Data Location Mapper 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 Personal Data Location Mapper. 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	September 2026
MCP Server	Personal Data Location Mapper MCP
Server ID	01a0dabf-5e2f-7216-8343-cd5630e72183
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/en/ai-agent-connect/personal-data-location-mapper.