

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

Family Photo Consent Register MCP

Keep photographic usage permissions organized and legally compliant.

Family Photo Consent Register MCP provides a structured way to handle photographic likeness permissions. Your AI client can use it to register new consent records, check if a person's permission is still valid, search through historical records, or process formal withdrawals of consent. It keeps your usage rights and revocation protocols in one place.

A+ Quality Score 100/100

consent

photography

privacy

compliance

records



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.

Family Photo Consent Register MCP

4 tools available

Cloud-hosted on Vinkius

Managing who can be photographed and how those images are used shouldn't be a manual headache. This MCP gives your AI client a direct way to handle photographic likeness permissions. Instead of digging through spreadsheets or emails, you can ask your agent to check if a specific person has granted permission for a shoot or to log a new consent agreement.

It handles the heavy lifting of maintaining a record of usage rights and durations. If someone changes their mind, you can process a formal revocation immediately. This ensures you stay compliant with privacy standards by keeping an accurate, searchable history of every permission granted or withdrawn. It's built for anyone who needs to maintain strict control over how people's likenesses are used in media or photography projects.

Core Capabilities

01 — Consent Registration

Your agent creates new, legally binding records for individuals.

02 — Permission Auditing

Your AI client checks the current validity and limitations of any person's consent.

03 — Historical Tracking

Your agent searches through all past and present consent records for a specific person.

04 — Revocation Management

Your AI client processes formal requests to withdraw permissions immediately.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/family-photo-consent-register — connect your AI agent in three steps.

- 01

Connect your AI client to the Vinkius-hosted MCP.
- 02

Ask your agent to register a new consent or check an existing one.
- 03

The agent executes the specific tool to update or query the registry.
- 04

Your agent provides you with the status, reference numbers, or history.

Connecting this MCP to your AI client gives you instant access to a managed consent database.

Built For

This MCP is designed for professionals who handle photography and need to maintain strict privacy compliance.

Photographers

They hand off the task of logging and checking client permissions to their AI.

Privacy Officers

They use the agent to audit consent records and ensure compliance.

Media Managers

They rely on the agent to verify usage rights before publishing content.

What Changes When You Connect

- 01

Maintains a searchable history of all consent actions.
- 02

Provides immediate verification of current usage rights.
- 03

Automates the logging of new permission agreements.

04 Ensures formal revocations are recorded accurately.

Real-World Applications

Pre-Shoot Verification

Ask your agent to check if a subject has active consent before you start a photography session.

Compliance Audits

Use the agent to pull a full history of permissions for a specific individual during a privacy review.

Permission Updates

Log new consent agreements as they are signed so your records stay current.

Handling Withdrawals

Process a person's request to stop using their likeness by recording a formal withdrawal.

Patterns to Avoid

Manual Spreadsheet Tracking

❌ AVOID

You keep a list of names in an Excel sheet and manually check it before every shoot. This leads to outdated info and missed revocations.

✓ INSTEAD

Let your agent handle the verification. Use ``get_consent_status`` to get real-time, accurate permission data before you pick up a camera.

Ignoring Permission Changes

❌ AVOID

A client emails you saying they no longer want their photo used, but you forget to update your records until the next audit.

✓ INSTEAD

Update your records immediately to stay compliant. Use ``withdraw_consent`` to process that request and keep your history accurate.

Fragmented Permission History

❌ AVOID

You have consent files scattered across different folders and emails, making it impossible to see a person's full history.

✓ INSTEAD

Centralize everything through the MCP. Use ``query_person_permissions`` to pull a complete timeline of every agreement for an individual.

The Right Fit

Connect this MCP if your work involves regular photography where privacy compliance is a legal requirement. Do not connect it if you only take casual photos with no formal usage rights to manage. The decision rests on whether you need a searchable, legally defensible record of likeness permissions.

Family Photo Consent Register 4 Tools

These tools manage the entire lifecycle of photographic likeness permissions, from initial registration to formal revocation.

#	TOOL	DESCRIPTION
01	query_person_permissions	This tool searches for all active and historical consent records for an individual. It's how you pull a full permission history.
02	register_consent	This tool creates a new, legally binding consent record for an individual. Use it to log a fresh permission agreement.
03	withdraw_consent	This tool processes formal requests to revoke photographic permissions. Use it when a person wants to pull back their consent.
04	get_consent_status	This tool checks if a specific person's consent is currently valid. It also returns any specific limitations on their permission.

See It in Action

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

U Register consent for Jane Doe for social media and editorial use, starting today, with contact jane@example.com and instructions to email support to withdraw.



Consent registered successfully. Permission Reference: REF-12345. Status: active.

U What is the current status of the consent for permission REF-12345?



The consent for Jane Doe is currently active. Allowed uses: social media, editorial.

U Find all consent records for John Smith.



Found 2 records for John Smith: REF-9876 (active) and REF-5432 (withdrawn).

Frequently Asked Questions

01 How do I add a new person to the consent register?

You can ask your AI client to use the `register_consent` tool to create a new, legally binding record for an individual.

02 Can I check if a person's permission is still valid?

Yes. Use the `get_consent_status` tool to check if a person's consent is active and to see any specific usage limitations.

03 What happens if someone wants to withdraw their consent?

You can use the `withdraw_consent` tool to process a formal request to revoke photographic permissions.

04 Is there a way to see all past permissions for a person?

Yes. The `query_person_permissions` tool allows you to find all active and historical consent records for a specific individual.

05 Which AI clients can use this MCP?

This MCP works with any compatible client, including Claude, Cursor, Windsurf, and VS Code.

06 How do I create a new consent record?

You can use the `register_consent` tool to create a new record by providing the person's name, allowed uses, and contact details.

07 Can I revoke a permission that was previously granted?

Yes, you can use the `withdraw_consent` tool to permanently revoke an existing permission using its unique reference ID.

08 How can I check if a specific consent is still valid?

Use the `get_consent_status` tool with the permission reference to see if the status is active, withdrawn, or expired.

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>"family-photo-consent-register": { "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

Family Photo Consent Register 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 Family Photo Consent Register. 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	Family Photo Consent Register MCP
Server ID	01a0de0a-a5ca-7059-868a-c0a9e3d86e01
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/family-photo-consent-register.