vertice

Vertice AI MCP Connector Privacy Policy

Vertice AI MCP Connector Privacy Policy

Last updated: 29.6.2026

This policy applies to Vertice Group Ltd and its global subsidiaries (collectively, "Vertice," "we," or "us") and describes how Vertice processes personal data when a customer connects an external AI assistant to Vertice through the **Vertice AI MCP server**, accessible at the per-tenant endpoint pattern `https://ai.vertice.one/accounts/<accountId>/mcp`. This server implements the open Model Context Protocol (MCP) specification.

This policy supplements the Vertice general Privacy Policy and the Vertice Master Data Protection Agreement (MDPA), which governs the underlying processing of Personal and Customer Data. Where this document is silent, the standard terms of the Privacy Policy and of the MDPA shall apply.

Connecting an external AI assistant does not change the scope of data Vertice stores or processes. The data accessible to the user via the connector is the same data that the user can already access through the Vertice web application.

This document is a privacy policy and does not by itself create a contractual relationship. Contractual data-protection commitments are set out in the MDPA.

1. Scope and roles

Role	Party
Data controller for customer business data	The customer (the Vertice account holder)
Data processor for that business data	Vertice
Data processor for the AI assistant provider's processing of prompts and responses	The AI assistant provider (e.g., Anthropic for the Claude.ai connector)

When a customer connects an external AI assistant to Vertice, two distinct processing relationships apply: (a) Vertice's processing of customer business data on behalf of the customer organization, and (b) the AI assistant provider's processing of the prompts entered by the user and the tool responses returned by Vertice. This policy covers (a). The AI assistant provider's own privacy policy and terms govern (b); we strongly encourage customers to read those documents before enabling the connector.

2. Data we process through the connector

2.1 Data received from the AI assistant

When a user invokes the connector, the AI assistant transmits to Vertice:

- **An access token** — a short-lived JSON Web Token (JWT) issued by Vertice's identity layer during the OAuth 2.1 authentication flow. The token carries the user's Vertice user identifier, the user's Vertice account membership, and a scope identifier used for audience binding. It does not carry any external personal data.
- **The MCP request envelope** — a JSON-RPC 2.0 message that specifies which Vertice tool to invoke and the parameters for that invocation, including any prompt text the user typed into the AI assistant.
- **Standard HTTP request headers** — `Origin`, `MCP-Protocol-Version`, `User-Agent`, and the source IP address as received by Vertice's load balancer for routing and abuse-protection purposes.

2.2 Data returned to the AI assistant

When the connector executes a tool, Vertice returns to the AI assistant:

- The tool's result content.
- JSON-RPC envelope metadata (request identifier, content type, MCP tool annotations indicating read-only or destructive intent).

The information returned is identical in scope to what the same user would see in the Vertice web application, subject to the same role-based access controls.

2.3 Data Vertice generates

In the course of operating the connector, Vertice generates:

- **Operational service logs** — request timestamps, account identifier, user identifier, tool name invoked, HTTP status code, latency, error class. Access tokens and prompt content are explicitly excluded from these logs by application configuration.
- **Aggregate service metrics** — pseudonymous counters used for service health monitoring and abuse detection.
- **Audit-trail entries** — created for every tool invocation that modifies customer data, written into Vertice's existing audit log alongside the equivalent web-application audit entries.
- **Rate-limit accounting records** — counters keyed by account and user, used solely to enforce per-user and per-tenant request limits.

2.4 Data Vertice does not collect

The Vertice AI MCP server does not:

- Collect conversation data beyond what is required to execute the requested tool call.
- Access the AI assistant's memory, chat history, conversation summaries, or files the user has uploaded to the AI assistant. The connector receives only the tool parameters the AI assistant explicitly sends as part of a tool invocation.
- Collect device identifiers, advertising identifiers, location data, or biometric data.
- Use connector data for advertising, retargeting, or resale to third parties.

3. Why Vertice processes this data (purposes and legal bases)

Vertice processes data through the connector for the following purposes, under the following legal bases (GDPR Article 6):

Purpose	Legal basis
Executing the tool the user requested and returning the result	Legitimate interests in providing the contracted service to our customers (Art. 6(1)(f)), or Art. 6(1)(b) if the end-user is directly the customer)
Authenticating the user via OAuth + single sign-on	Performance of the contract (Art. 6(1)(b)) and legitimate interests in preventing unauthorized access (Art. 6(1)(f))
Enforcing per-user and per-tenant rate limits	Legitimate interests in service availability and abuse prevention (Art. 6(1)(f))
Generating audit-trail entries for modifying actions	Legitimate interests in maintaining operational security, auditability, and compliance records (Art. 6(1)(f))
Monitoring service health via operational metrics	Legitimate interests in operating a reliable service (Art. 6(1)(f))
Investigating reported security incidents	Legitimate interests in protecting the service and customer data (Art. 6(1)(f))

Vertice relies on legitimate interests or contractual necessity to process this data. We do not rely on Consent (Art. 6(1)(a)) as our legal basis under GDPR for these processing activities. (Technical authorizations, such as OAuth scopes granted by the user or administrator, dictate system access but do not constitute the GDPR legal basis for processing).

4. Where data is processed

All connector processing performed by Vertice occurs within Vertice's AWS infrastructure in **Ireland (eu-west-1)** and Vertice's GCP infrastructure in **Belgium (europe-west1)**.

When the connector returns a tool result to the AI assistant, that response is transmitted from Vertice's EU infrastructure to the AI assistant provider's infrastructure, which may be located outside the EU. The destination is determined by the AI assistant provider and is outside Vertice's control. Any cross-border data transfer that takes place at this step is governed by the customer's agreement with the AI assistant provider.

5. How long Vertice retains data

Data class	Retention
Operational service logs (redacted, no prompts, no tokens)	Per Vertice's standard service-log retention policy, as described in the MDPA
Aggregate service metrics (pseudonymous)	Per the standard retention of Vertice's metrics platform
Audit-trail entries for modifying actions	Per the audit-record retention clause in the MDPA
Rate-limit accounting records	Short-lived — retained only long enough to enforce the rolling rate window

Customer business data accessed by the connector (contracts, vendors, requests) follows the retention rules set out in the MDPA; the connector itself does not change those rules.

6. With whom Vertice shares data

In the connector data flow, Vertice shares data as follows:

- **With the external AI assistant provider** — by design. When a customer connects an AI assistant to Vertice, prompts entered into that assistant and tool responses returned by Vertice are transmitted to the provider's infrastructure. This transmission is essential to the core functionality of the MCP connector. Vertice does not control how the AI assistant provider processes or retains this data; such processing is strictly governed by the customer's separate agreement with the AI assistant provider.
- **With Vertice sub-processors** necessary to operate the connector. The list of sub-processors is documented in the MDPA.

- **With competent regulatory or judicial authorities** — only as required by enforceable legal process. Vertice will notify the customer of legal requests unless legally prohibited.

No data resell: Vertice does not sell, rent, or share data through the connector with advertisers, data brokers, or any other third party for commercial purposes.

No AI Training: Vertice strictly does not allow its sub-processors to use any customer data, connector data, or prompt inputs/outputs processed through the MCP connector to train, retrain, or fine-tune any foundational AI models or machine learning algorithms.

Please note that the core function of the connector is to route data to the external AI assistant provider authorized by the customer. Vertice does not control, and is not responsible for, whether that third-party AI provider uses the transmitted data for model training. The AI provider's use of data is governed solely by the customer's independent agreement with that provider.

7. Authentication and security overview

The connector is protected by a defense-in-depth security chain:

- HTTPS only; TLS is terminated at Vertice's AWS Application Load Balancer.
- `Origin` header validation to mitigate DNS-rebinding attacks.
- `MCP-Protocol-Version` header validation per the MCP Streamable HTTP specification.
- OAuth 2.1 with PKCE (S256), federated through the customer's existing single sign-on provider; personal API keys are not issued.
- JWT validation with three independent audience checks: the token issuer, the OAuth client identifier, and the required resource scope `https://mcp.vertice.one/invoke`.
- Per-user account-membership check: the token must explicitly authorize the requested account.
- Application-layer rate limiting (per-user and per-tenant), with spec-compliant HTTP 429 responses and `Retry-After` headers.
- WAF perimeter protection on the public discovery and dynamic client registration endpoints.
- No bearer-token pass-through to internal services — Vertice mints a separate short-lived internal credential for each downstream service call, scoped to the authenticated user's groups.
- Access tokens and prompt contents are excluded from Vertice's service logs by application logger configuration.

A description of Vertice's broader infrastructure security posture is set out in AI Security at Vertice document.

8. Data subject rights

If you are an individual whose personal data Vertice processes through the connector, users have the following rights under the GDPR and equivalent data protection laws:

- The right to know what data is processed and to access it
- The right to have inaccurate data corrected
- The right to have data erased (subject to legal retention obligations)
- The right to restrict or object to certain processing
- The right to data portability where applicable
- The right to lodge a complaint with a supervisory authority

The vast majority of your interaction with the connector is governed by the employer's customer relationship with Vertice. To exercise these rights, individuals should contact their employer's Vertice administrator first. They will route the request to Vertice's privacy team where required. You can also contact us directly at `data-privacy@vertice.one`.

Where Vertice acts as a data processor rather than a controller, requests will be routed to the relevant customer (the controller) for response.

For data the AI assistant provider processes about you (your prompts, the responses delivered through their interface), please refer to the AI assistant provider's privacy policy for the channel they provide for exercising your rights against them.

9. Changes to this policy

At our discretion, we may change our Privacy Policy to reflect updates to our business processes, current acceptable practices, or legislative or regulatory changes. If we decide to change this Privacy Policy, we will post the changes here at the same link by which you are accessing it.

If the changes are material (i.e., changes that significantly affect your rights or how we process your data), or if required by applicable law, we will provide a more prominent notice. This may include a notification sent to the email address registered with your account, or a clear announcement displayed on our platform.

Where required by law, we will obtain your consent or provide you with the opportunity to opt in to or opt out of any new uses of your personal information. We encourage you to review this Privacy Policy periodically to stay informed about our data practices.

Contact Us

For any questions or concerns regarding your privacy or this Privacy Policy, you may contact us at:

General privacy questions, data subject rights requests	data-privacy@vertice.one
Legal correspondence	legal@vertice.one
Security vulnerability disclosure	security@vertice.one — see also our Vulnerability Disclosure Policy and security.txt
Vertice customer support	Through your existing Vertice Customer Success contact, or via the in-product support channel
Business post address	Vertice Group Ltd, 3rd Floor 1 Ashley Road, Altrincham, Cheshire, UK, WA14 2DT