YPulse Privacy Policy — MCP Section

6.1 YPulse MCP Integration — Data Handling

6.1A What is the YPulse MCP Integration?

YPulse subscribers can access YPulse research data, insights, and analytics through compatible third-party AI applications — such as Anthropic Claude — using a standard called the Model Context Protocol (MCP). When you use a connected AI application to ask questions about YPulse research data, your queries are routed through the YPulse MCP server, which authenticates your account and retrieves the relevant data from YPulse's research systems.

The MCP channel is available to registered YPulse subscribers only. Access requires authentication via your YPulse account credentials through YPulse's identity provider (FusionAuth). You cannot access YPulse MCP services without a valid YPulse account.

6.1B What Data Does YPulse Collect Through the MCP Channel?

When you use the YPulse MCP integration, the following data is collected and processed:

Data Type	What it is	How it is used
Account identifiers	Your user ID, email address, and username, read from your authentication token (JWT) at the time of your request.	To verify your subscription entitlements and to link your query to your account in YPulse analytics.
Natural-language query text	The question or search query you submit via your AI application (e.g. 'What do Gen Z think about brand X?').	Forwarded to Deepset (YPulse's AI search processor) to retrieve relevant research insights. Not retained by the MCP server after the request completes.
Tool parameters and filters	Structured filters you apply (e.g. regions, content types, brand names, demographic filters, metric types).	Forwarded to Deepset or Snowflake to retrieve filtered research data. Included in usage analytics.
IP address	Your IP address, derived from your connection to the MCP server.	Included in usage analytics metadata for security and fraud prevention. Not retained by the MCP server directly.
Client application identifier	The name or identifier of the AI application you are using to access YPulse MCP (e.g. Claude).	Included in usage analytics to understand how subscribers interact with different AI clients.
Session and event metadata	Session start and end times, tool names called, authentication events, result counts, and request outcomes.	Used for product analytics, service improvement, and security monitoring.

6.1C What the YPulse MCP Server Does Not Store

The YPulse MCP server operates in stateless mode by default. The following are explicitly not retained by the MCP server:

- Login tokens (JWTs) — validated and discarded at the time of each request; not stored.

- Query results and response content — results are returned to your AI application and are not logged or retained by YPulse's MCP server.
- Persistent session data — no session database or server-side session store is maintained.
- Full request/response logs — the MCP server does not maintain database or file-backed logs of individual user queries.

6.1C Third-Party Processors and Data Flows and Retention Periods

The following third-party processors receive data in connection with MCP requests. Each is bound by a Data Processing Agreement with YPulse:

Processor	Role and data received
Deepset GmbH	AI-powered semantic search and LLM pipeline. Receives your natural-language query text, tool routing parameters, and permission filters in order to retrieve relevant research insights. Deepset does not use YPulse query data to train its own AI models. Pipeline logs are accessible by the user for 2 days and retained for 2 weeks.
Snowflake Inc.	Structured brand metrics data warehouse. Receives SQL queries constructed from your filter parameters (brand names, regions, demographic filters, lookback periods) in order to retrieve aggregated brand data. Retained until our subscription ends.
FusionAuth	OAuth 2.0 identity provider. Handles authentication token issuance and validation for MCP access. Receives standard OAuth authentication flows. FusionAuth terms confirm MCP OAuth client coverage: Tokens are kept for 30 Days.
YPulse internal analytics	Internal event ingestion system. Receives identified usage metadata including account identifiers, IP address, client application identifier, tool usage events, and session data. Analytics event retention: Pendo retains subscription raw event data for a period of 7 years (84 months) from the date of collection, which serves as the data retention time limit. After a subscription surpasses the retention time limit, raw event data older than the specified period is automatically deleted from the Pendo database.

6.1D Third-Party AI Client Applications

When you access YPulse data via a third-party AI application (such as Anthropic Claude), your queries and the responses returned by YPulse are also processed by that AI application on its own systems, under that application's own privacy policy. YPulse is not responsible for how third-party AI applications process your queries or responses. We recommend reviewing the privacy policy of any AI application you use to access YPulse services.

The flow of data when using MCP is: you → your AI application → YPulse MCP server → YPulse research systems (Deepset / Snowflake) → response returned via MCP server → your AI application → you.

6.1E Legal Basis for Processing MCP Data (GDPR)

For users in the EU and UK, we process MCP-channel data on the following legal bases:

- **Contract performance (Article 6(1)(b)):** Processing of authentication tokens, query text forwarding, and tool parameters is necessary to perform the service you have subscribed to.
- **Legitimate interests (Article 6(1)(f)):** Usage analytics, session metadata, and security monitoring are processed on the basis of our legitimate interests in understanding product usage, improving our

services, and maintaining security. These interests are not overridden by your data protection rights given the limited nature of the data and the controls in place.

- **CCPA / U.S. State Privacy Laws:** MCP usage data is collected for the business purposes of service delivery, product analytics, and security. It is not sold or shared for cross-context behavioural advertising.

6.1F Your Rights Regarding MCP Data

Your data protection rights described in Section 10 of this policy apply equally to data collected through the MCP channel. In particular:

- **Opt out of MCP analytics tracking:** You may opt out of usage analytics collected through the MCP channel by contacting privacy@ypulse.com with the subject line 'MCP Analytics Opt-Out.' Note that opting out of analytics does not affect authentication or the delivery of research data.
- **Access and deletion:** You may request access to or deletion of MCP usage data held in YPulse's analytics system by contacting privacy@ypulse.com.
- **Query data forwarded to Deepset:** Where query text has been forwarded to Deepset, deletion requests relating to Deepset-held data will be handled in accordance with our Data Processing Agreement with Deepset. Contact privacy@ypulse.com to initiate a request.

Last updated June 15, 2026