ometria

Deep Insights Agent Security Overview

As you evaluate Deep Insights Agent for your organization, we understand you may have questions about data security and privacy. This document addresses the most common questions we hear from retail leaders.

Your customers' personal data is not accessible through Deep Insights Agent

Deep Insights Agent operates on a dedicated, optimised dataset built from your data, which excludes personally identifiable information by default. Personal data is not accessible through the agent — this includes:

- No customer names
- No street addresses (only city, state, and postal code for geographic analysis)
- No email addresses or phone numbers

Ometria does not process payment card data within PCI DSS scope. We do not handle card numbers, CVV codes, or card expiration dates anywhere within our platform, including Deep Insights Agent.

What Deep Insights Agent can access are analytics metrics like purchase history, campaign performance, customer segments, and product catalogues — the same data your marketing team uses for reporting and analysis.

Your data is not used to train AI models

Deep Insights Agent is built so that your data cannot be used to train AI models — this is a technical control enforced at the account level through how the Claude organisation is set up.

Your strategic insights, campaign performance data, and business metrics remain confidential to your organisation.

Access is controlled through your existing Ometria account

Deep Insights Agent is authenticated via your Ometria account credentials, with an explicit authorisation step that your administrators control. This ensures:

- Access can be granted and revoked at the account level
- Each query is authorised to ensure users can only access data they are permitted to see
- No separate credentials or external accounts are required

The system is designed for analysis, not data extraction

Deep Insights Agent cannot be used to extract your entire database. The system includes multiple technical safeguards:

- The agent operates in read-only mode and cannot modify data
- Query results are limited to 1,000 records
- Query complexity and execution time are restricted
- Each client's data is held in an isolated environment, with multiple layers preventing any cross-client access
- The underlying analytics data excludes personal information, so excluded data cannot be returned by a query

Enterprise-grade security, consistently applied

Ometria is ISO/IEC 27001 and 27701 certified and a member of the Cloud Security Alliance. Deep Insights Agent was built and is maintained under the same security standards as the broader Ometria platform, including:

- Mandatory security training for all engineers
- Security review and testing on every code change
- Regular penetration testing by independent CREST-certified specialists
- Continuous security monitoring
- Regular compliance audits by external reviewers
- Our Security and Privacy team has oversight of all new features

ISO/IEC 27001 | ISO/IEC 27701 | CSA Member | CREST Tested