Collibra

USE CASE

Your consumer data is scattered. Your components are everywhere. Can you trace either one?

Using Collibra Model Context Protocol (MCP) for consumer privacy requests and payment data scoping in retail and consumer goods, export-control classification and recall traceability for manufacturing and supply chain.

Think about moments that compliance teams dread:

- A consumer emails asking you to delete every piece of data you hold on them
- Your payment provider launches a new Buy Now Pay Later (BNPL) integration and nobody is sure which tables now hold cardholder data
- An engineer shares a Computer-Aided Design (CAD) file with an overseas research partner without checking whether it is export-controlled
- The phone rings with a National Highway Traffic Safety Administration (NHTSA) investigator asking which vehicles contain a defective brake component, and you have five days to answer

Each moment has a deadline, a regulator and a penalty attached.

Each moment also shares similar data problems. The consumer's identifier appears in a primary customer record, a loyalty platform, a marketing model and a derived dataset nobody documented. The cardholder data column entered the new BNPL system without classification. The engineering file was uploaded without an Export Control Classification Number (ECCN) check. The component moves through a supply chain spanning dozens of suppliers with no end-to-end lineage. The truth is that the regulation isn't the hard part. But finding and governing the data is the real challenge.

Collibra MCP connects third-party large language models (LLMs) including Claude, ChatGPT, Microsoft Copilot and agents built on Databricks and Azure AI Foundry directly to governed metadata, data lineage, classification records and business context in the Collibra platform. Compliance, privacy, engineering and supply chain teams can ask questions in plain language and receive governed, audit-ready evidence assembled from the catalog automatically.

Collibra © 2026 Collibra. All rights reserved. | collibra.com

Where retail, manufacturing, and supply chain organizations face the greatest compliance data risk.

- **Consumer deletion requests span systems nobody has mapped:** Data deletion requests rose 82% year over year in 2025, surpassing access and do-not-sell requests for the fourth consecutive year. The consumer's identifier may appear in a primary customer record, a loyalty platform, a marketing segmentation model, a purchase history table and multiple derived datasets that were never explicitly documented. Finding and deleting all of it within 45 days requires a governed data map that most retail organizations do not maintain

- **New payment channels expand Payment Card Industry (PCI) scope without notice:** BNPL integrations, embedded finance features and digital wallet connections introduce new tables and systems that may contain Cardholder Data (CHD) or Sensitive Authentication Data (SAD). Before a Qualified Security Assessor (QSA) review, every column carrying cardholder data must be classified and every downstream system receiving it identified as in-scope for the Cardholder Data Environment (CDE). Without governed classification and lineage, the scope assessment is manual, incomplete, and unreliable

- **Technical data is shared internationally before export control status is confirmed:** The most common International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) violation is sharing controlled technical data before classification status has been confirmed. Civil penalties reach $1,271,078 per ITAR violation. The Bureau of Industry and Security (BIS) issued fines totaling more than $297 million as of September 2026, more than triple the five-year average, as the administration committed to a dramatic increase in enforcement

- **Recall traceability from component to vehicle identification number (VIN) is a manual exercise under a five-day deadline:** Under NHTSA 49 CFR Part 573, manufacturers must trace a defective component from raw material origin through every manufacturing step to every affected VIN. A single supplier production flaw in February 2026 impacted at least six international automakers simultaneously. Organizations with comprehensive supply chain traceability resolve recall investigations in hours using event-level lineage data alone. Organizations without it spend weeks reconstructing the chain manually at costs rising approximately 40% per event

- **Unstructured technical and quality records create a traceability blind spot:** Engineering specifications, quality inspection narratives, supplier audit reports and materials certifications exist as unstructured documents outside the reach of traditional data governance tools. Under both export control and recall traceability obligations, these documents carry the same evidentiary weight as structured data records and are the assets most likely to be shared or lost without governed classification.

 © 2026 Collibra. All rights reserved. | collibra.com

You can't honor a deletion request if you do not know where the data lives. You can' t classify an export-controlled asset after you have already shared it.

The gap between compliance policy and compliance evidence is a data classification, lineage and catalog problem.

- Consumer personal information not lineage-traced to derived datasets and secondary systems across retail data estates
- Cardholder data columns unclassified and downstream CDE scope undefined when new payment channels launch
- Engineering and technical data assets uploaded without export control classification status confirmed before sharing
- Component supply chain data not cataloged with end-to-end lineage from raw material origin through manufacturing to finished vehicle
- Unstructured quality records, engineering documents, and supplier certifications outside the reach of governed classification

---

Collibra MCP for retail, manufacturing and supply chain: Four regulatory workflows

CCPA and GDPR right-to-delete fulfillment

A consumer submits a deletion request under the California Consumer Privacy Act (CCPA) or General Data Protection Regulation (GDPR). The Privacy Operations team has 45 days under CCPA and 30 days under GDPR to locate every data asset holding the consumer's personal information, including derived datasets, verify contractual holds and generate documented response evidence. With Collibra MCP, a privacy officer instructs a connected LLM in plain language to locate all data assets containing the consumer's identifier. A privacy analyst checks data contracts for terms prohibiting immediate deletion, then creates a documented privacy request audit record with all in-scope assets, their disposition and the deletion workflow. The response package is complete from governed records within the statutory window, at a fraction of the $1,524 per-request manual fulfillment cost.

Collibra © 2026 Collibra. All rights reserved. | collibra.com

PCI-DSS scope assessment for new payment channels

A new BNPL integration introduces database tables that may contain cardholder data. Before the QSA review, every CHD and SAD column must be classified and every downstream system entering PCI CDE scope identified. With Collibra MCP, a privacy analyst locates the new BNPL tables, calls for semantics to enumerate all columns and retrieves Payment Card Industry Data Security Standard (PCI-DSS) CHD and SAD data class definitions through search. A data engineer calls up lineage downstream to trace every system now receiving cardholder data, identifying new CDE scope.The QSA evidence package is completed from governed and cataloged records before the assessment begins.

ITAR and EAR technical data classification

An engineer uploads a CAD specification or materials specification to a collaboration environment. Before sharing with any international research partner, the file must be classified against the United States Munitions List (USML) or the Commerce Control List (CCL) and routed for export compliance review. With Collibra MCP, a privacy analyst locates the new technical data asset in the engineering domain, reads existing attributes and any prior ECCN or USML fields and retrieves applicable export control data class options, confirming no export classification has been applied. A catalog admin updates the ECCN code, Technology Control Plan (TCP) reference, export license type, Export Compliance Officer assignment and review status to Under Review. The asset is blocked from international sharing until export review completes, with a governed audit record of the classification decision.

Product recall traceability under NHTSA 49 CFR part 573

NHTSA opens a Preliminary Evaluation on a brake component defect. The manufacturer has five days to trace the affected part from raw material origin through every manufacturing step to every affected VIN range, file a Part 573 Safety Recall Report and begin owner notification within 60 days. With Collibra MCP, a Data Engineer locates the defective part number in the component catalog, reads lot codes, supplier and affected vehicle programs and finds the part in the manufacturing lineage graph. Traces the complete path to raw material origin and the original material supplier to reveal each manufacturing operation and quality inspection record.

© 2026 Collibra. All rights reserved. | collibra.com

Key outcomes

Governed data. Faster compliance. Smaller exposure.

Collibra MCP transforms compliance response across CCPA, GDPR, PCI-DSS, ITAR, EAR and NHTSA recall traceability from manual, deadline-driven processes into governed, repeatable, AI-assisted workflows. Consumer personal information is lineage-traced to derived datasets before the deletion request arrives. Cardholder data columns are classified before the QSA schedules the review. Technical data assets are classified before the sharing request is submitted. Supply chain component lineage is cataloged before NHTSA opens a Preliminary Evaluation. When the deadline arrives, the evidence is assembled from the catalog in hours, not days.

Collibra MCP and third-party LLMs

The Collibra MCP server provides a standardized access layer connecting third-party LLMs including Claude, ChatGPT, Microsoft Copilot, and agents built on Databricks and Azure AI Foundry to governed metadata, lineage, classification records and business context in the Collibra platform. Natural language questions from privacy, compliance, engineering and supply chain teams return governed, audit-ready answers drawn from the catalog, without requiring technical query skills or manual system-by-system searches.

Collibra + Deasy Labs

Engineering specifications, quality inspection narratives, supplier audit reports, materials certifications and CAD documentation exist as unstructured documents that carry the same regulatory weight as structured data records under both export control and recall traceability obligations. They are also the assets most likely to be shared, modified or lost without governed classification. Deasy Labs extends Collibra's governance into this unstructured content. For recall traceability, Deasy Labs surfaces component certifications, material test reports and supplier quality documentation that would otherwise require weeks of manual search. For export compliance, it closes the classification gap between structured catalog assets and the unstructured technical content that engineers actually share across borders.

Learn more:
collibra.com/products/mcp-server

 © 2026 Collibra. All rights reserved. | collibra.com

Sources

1. Ketch, 'CCPA Right to Deletion: What Businesses Need to Know,' June 25, 2026. California's Delete Request and Opt-Out Platform (DROP) launched Jan. 1, 2026, with enforcement beginning Aug. 1, 2026. https://www.ketch.com/blog/posts/understanding-the-ccpa-right-to-deletion

2. Verizon 2026 Data Breach Investigations Report, cited in UpGuard, Aug. 10, 2026. 806 confirmed breaches in the retail vertical in 2025. Third-party involvement rose to approximately 48% of breaches; the human element featured in 62% of incidents. https://www.upguard.com/blog/biggest-data-breaches-in-retail

3. Total Retail, citing industry data breach reports, Oct. 2025. The cost of data breaches in the retail sector reached $3.54 million in 2025, a nearly 20% increase since 2023. https://www.mytotalretail.com/article/why-cybersecurity-month-is-the-right-time-to-re-evaluate-your-payment-data-compliance

4. Mohawk Global, 'Adjusted Civil Penalties for 2025,' Jan. 2025. ITAR maximum civil penalty as of Jan. 10, 2025: $1,271,078 per violation or twice the value of the transaction, whichever is greater. EAR maximum civil penalty as of Jan. 15, 2025: $374,474 per violation or twice the value of the transaction. https://mohawkglobal.com/trade-translation/adjusted-civil-penalties-for-2025/

5. Bureau of Industry and Security, U.S. Department of Commerce, EAR Penalties. Criminal penalties for EAR violations include up to 20 years of imprisonment and up to $1 million in fines per violation. https://www.bis.gov/enforcement/penalties

6. Center for Strategic and International Studies (CSIS), 'Trump Administration Ratchets Up Export Control Penalties,' Sept. 2026. As of September 2026, BIS issued fines totaling more than $297 million, more than triple the five-year average. https://www.csis.org/analysis/trump-administration-ratchets-export-control-penalties

7. Digital Dealer / Recall Masters, 'Recalls Were Up in 2025 But So Were Completed Repairs,' May 22, 2026. 447 NHTSA-mandated and 223 voluntary campaigns affected more than 28 million vehicles in 2025. https://digitaldealer.com/news/recalls-were-up-in-2025-but-so-were-completed-repairs-state-of-recalls-report/170858/

8. Willis Towers Watson, Insurance Marketplace Realities 2026: Product Recall, Oct. 2, 2025. Tariffs driving approximately 40% higher recall costs across imported and cross-border supply chains. A single vehicle recall in 2025 triggered a $600 million special charge and $2 billion in warranty expense. https://uatredesignp.wtwco.com/en/insights/2025/10/insurance-marketplace-realities-2026-product-recall

9. OpenText, 'The Recall That Didn't Have to Happen: When Traceability Becomes Liability,' 2025. 75% of manufacturers reported at least one product recall in 2025. Organizations deploying comprehensive product traceability achieve up to 50% reduction in recall-related costs. https://www.opentext.com/en/media/point-of-view/the-recall-that-didnt-have-to-happen-when-traceability-becomes-liability-pov-en.pdf

10. TMG, citing Sedgwick Q4 2025 State of the Nation Product Safety and Recall Index, March 30, 2026. 2025 was the seventh consecutive year of rising automotive recall activity. A single supplier production flaw in February 2026 impacted at least six international automakers. https://www.tmhcc.com/en/news-and-articles/thought-leadership/automotive-recall-risk-in-2025-why-the-trend-isnt-slowing-down

11. Collibra Product Innovations. Collibra MCP server generally available November 2025. https://www.collibra.com/products/innovations

12. Collibra Marketplace, Databricks MCP Marketplace: Collibra MCP Server. https://marketplace.collibra.com/listings/databricks-mcp-marketplace-collibra-mcp-server/

Collibra © 2026 Collibra. All rights reserved. | collibra.com