Collibra

USE CASE

Your network carries millions of decisions each second.

Can you govern and prove all of them?

Using Collibra MCP for compliance obligations in telecom, energy and the public sector under the European Union Artificial Intelligence Act, System and Organization Controls 2 (SOC 2) and Customer Proprietary Network Information (CPNI) rules.

Telecommunications providers and energy utilities sit at the intersection of two accelerating pressures. On one side, regulators are introducing some of the most demanding AI and data governance obligations ever imposed on private and public sector organizations. On the other, the data foundations those organizations depend on remain structurally ungoverned.

A survey of 1,270 information technology leaders conducted in early 2026, found that only 33% of telecom organizations report all of their data is fully governed. Sixty percent of telecom leaders cannot access the data required for their strategic AI initiatives despite near-universal confidence in their data visibility. For energy and utilities, the picture is comparable: 25% of respondents cited cost overruns as the leading reason AI and analytics investments fail to deliver expected returns, a direct consequence of ungoverned data foundations.

The regulatory timer is not waiting for data readiness. The EU AI Act's most demanding high-risk system obligations took effect Aug. 2, 2026, with penalties for non-compliance reaching €15 million or 3% of global annual turnover, whichever is higher, and up to €35 million or 7% of global turnover for prohibited practice violations. The U.S. Federal Communications Commission (FCC) issued Enforcement Advisory No. 2026-01 in February 2026, reminding carriers that CPNI annual certifications were due March 2, 2026, with monetary forfeitures of over $250,000 per violation or per day of continuing violation, up to a maximum of $2.5 million with no exemptions for smaller companies.

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

SOC 2 Type 2 compliance has become a non-negotiable requirement for enterprise customers and government procurement, with nearly 40% of companies reporting compliance as a condition of doing business.

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, data and governance teams can ask questions in plain language and receive governed, audit-ready evidence assembled from the catalog automatically, without manual reconstruction under deadline pressure.

Where telecom, energy and public utility organizations face the greatest regulatory evidence risk.

- **EU AI Act high-risk classification is broader than most expect:** AI systems used in critical infrastructure management, including grid control, smart grid management and network traffic routing that functions as a safety component, are subject to high-risk classification requirements under the EU AI Act. Energy companies operating AI in critical infrastructure face high-risk compliance obligations requiring documentation, conformity assessment and human oversight — all of which depend on a governed, traceable data foundation the underlying AI system relies on.
- **Customer Proprietary Network Information (CPNI) classification and access governance is manually maintained:** CPNI covers information relating to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service. Carriers must obtain customer approval to use or disclose CPNI, prevent unauthorized access and notify law enforcement and affected customers of a breach. The FCC's April 2024 forfeiture orders against the three largest mobile network operators (MNOs) for failing to safeguard CPNI signaled that the era of lax enforcement is over. Annual CPNI certifications require carriers to demonstrate that data governance controls are in place, while most carriers maintain manually, system by system.
- **SOC 2 evidence now requires demonstrated data lineage and classification, not just policy documentation:** After high-profile audit quality issues, SOC 2 examiners now require underlying evidence rather than a summary. For telecom and energy organizations, the relevant controls include data classification policies, data processing monitoring, data integrity verification and encryption for data at rest and in transit. First-year SOC 2 compliance costs range from $30,000 to $150,000 (or more when audit fees, readiness assessments, remediation and internal labor are included). Without governed metadata and lineage, organizations cannot produce the evidence auditors now expect.
- **AI governance under the EU AI Act requires traceable training data and model provenance:** The EU AI Act requires providers of high-risk AI systems to maintain technical documentation demonstrating that training data has been governed, access-controlled and validated for accuracy, relevance and representativeness. For telecom and energy operators deploying AI in network management, predictive maintenance, demand forecasting and customer service, that documentation must cover the full data lineage from source system through transformation to model input — a standard that ungoverned data estates cannot meet.

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

- **International equivalents extend obligations beyond the EU:** The United Kingdom's (UK's) AI Regulation and Data (Use and Access) Act 2025, Australia's AI Ethics Framework and Privacy Act 1988, and Canada's Artificial Intelligence and Data Act (AIDA) impose parallel or complementary governance obligations on telecom and energy operators in those jurisdictions. State-owned and nationally regulated utilities face additional obligations under public sector information governance frameworks including the UK Official Sensitive classification system and equivalent national security classification schemes.
- **Data governance gaps directly undermine AI return on investment:** 22% of telecom respondents in the Cloudera Data Readiness Index 2026 reported that data quality issues have led to poor return on investment for AI and analytics initiatives. Governance is not a compliance cost layered on top of AI investment; it is the foundation that determines whether AI investment delivers value at all.

You can't certify CPNI compliance for data you have not classified and inventoried.

You can't demonstrate EU AI Act conformity for a model trained on untraced data.

Collibra MCP for Telecom, Energy and Public Utilities: Four regulatory workflows

EU AI Act High-Risk System Technical Documentation

The EU AI Act requires providers and deployers of high-risk AI systems to maintain technical documentation demonstrating that the training data has been governed, validated and access-controlled, and the AI system's inputs, outputs and decision logic are traceable. For energy and telecom operators, assembling that documentation manually (across multiple AI systems, data sources and jurisdictions) is operationally unsustainable.

With Collibra MCP, a data engineer locates all AI system assets in the catalog and retrieves their classification, risk level and associated training datasets through governed metadata. A privacy analyst confirms that training data assets carry appropriate classification tags, access controls and data quality validation records. A data steward traces the lineage of each dataset from source system through transformation to model input, generating the provenance documentation the EU AI Act requires. A catalog admin confirms that data contracts covering AI training pipelines include accuracy and representativeness validation provisions. The EU AI Act technical documentation package is assembled from governed records, not reconstructed from memory.

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

CPNI Classification and Annual Certification

FCC CPNI rules require carriers and interconnected Voice over Internet Protocol (VoIP) providers to classify CPNI, govern access to it, obtain customer approvals for its use or disclosure and file an annual certification demonstrating compliance. The FCC's forfeiture orders against major MNOs and its Feb. 2026 enforcement advisory make clear that annual certification is an evidence requirement, not a checkbox.

With Collibra MCP, a Privacy Analyst locates all data assets across network, billing and customer systems that contain CPNI and applies the correct CPNI data class to each asset through the catalog. A Data Steward confirms that access controls, customer approval records and disclosure restrictions are documented for each CPNI asset. A Privacy Officer generates an audit record demonstrating consistent CPNI identification, classification, access governance and breach notification procedures across the carrier's data estate. The annual CPNI certification is supported by governed catalog evidence rather than manual system attestations.

SOC 2 Type 2 Evidence Assembly

SOC 2 Type 2 audits require organizations to demonstrate that security, availability, processing integrity, confidentiality and privacy controls have operated effectively over a defined period. After recent audit quality scrutiny, examiners require underlying evidence — lineage records, classification documentation, access logs and data contract manifests — not summaries. For telecom and energy organizations, assembling that evidence manually for systems spanning network operations, billing, customer data and third-party suppliers takes months.

With Collibra MCP, a Catalog Admin locates all data assets in scope for the SOC 2 audit and confirms classification, ownership and control status through the catalog. A Data Engineer retrieves data lineage records demonstrating how data flows through processing systems, including transformation logic, access events and validation gates. A Privacy Analyst confirms that data classification policies, encryption controls and retention schedules are applied consistently across all in-scope assets. A Privacy Officer pulls data contract manifests covering third-party and supplier data feeds to verify that supplier controls meet SOC 2 requirements. The SOC 2 evidence package is assembled from governed records, reducing audit preparation from months to days.

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

AI Training Data Governance for Network and Grid AI Systems

Telecom and energy operators deploy AI across network traffic management, predictive maintenance, demand forecasting, outage detection and customer service automation. Each of these systems consumes training data that, under the EU AI Act and emerging international AI governance frameworks, must be documented, classified, lineage-traced and validated. Without a governed catalog, operators cannot demonstrate that their AI systems meet the technical documentation standard regulators now require.

With Collibra MCP, a Data Engineer locates all datasets feeding network and grid AI systems and retrieves classification, sensitivity labels and data quality validation records through the catalog. A Privacy Analyst confirms that data collected from network infrastructure, smart meters, and customer systems is classified correctly and that applicable CPNI, privacy and data protection restrictions are enforced before data enters AI training pipelines. A Data Steward traces full lineage from operational data sources through all transformations to the AI model training environment, generating the provenance and accuracy documentation the EU AI Act requires. The AI technical documentation package is current, governed and defensible.

Key outcomes

Regulatory evidence assembled from governed records, not from manual reconstruction.

Collibra MCP transforms regulatory compliance responses across the EU AI Act, CPNI, SOC 2, and international AI governance frameworks from a manual, deadline-driven process into a governed, repeatable, AI-assisted workflow. CPNI is classified. AI training data is lineage-traced. SOC 2 evidence is drawn from the catalog. EU AI Act technical documentation is generated from governed records. When an FCC enforcement action lands, an EU AI Act audit is initiated, or a SOC 2 examiner arrives, the evidence is assembled in hours, not months.

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 compliance, data and governance teams return governed, audit-ready answers drawn from the catalog, without requiring technical query skills or manual system-by-system searches.

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

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

Sources

1. Cloudera, The Data Readiness Index 2026, June 2026. Only 33% of telecom organizations report that all of their data is fully governed. 60% of telecom leaders cannot access the data required for strategic AI initiatives. 22% report data quality issues have led to poor ROI for AI and analytics initiatives. https://portalerp.com/news/cloudera-report-finds-telcos-lack-access-to-their-own-ai-data

2. Cloudera, Data Readiness Index 2026, energy and utilities release, Sept. 17, 2026. 25% of energy and utilities respondents cited cost overruns as the leading reason AI and analytics investments fail to deliver expected returns. https://blog.pebblous.ai/blog/data-readiness-self-report/en/

3. Presencis, EU AI Act Enforcement Timeline, 2026. Penalties for high-risk AI system violations reach €15 million or 3% of global annual turnover. Penalties for prohibited practice violations reach €35 million or 7% of global annual turnover. Active enforcement of GPAI and penalties provisions began Aug. 2, 2025. https://presencis.com/regulations/eu-ai-act/timeline/

4. Baker Botts, legal analysis cited in Regulation Daily Brief, March 16, 2026. Energy companies operating AI in critical infrastructure face EU AI Act high-risk compliance obligations taking effect Aug. 2, 2026. https://techjacksolutions.com/ai-brief/eu-ai-act-news-august-2-2026-high-risk-deadline-looms-energy/

5. Deutsche Telekom, The EU AI Act at Deutsche Telekom, 2025. Timely EU-wide review of all AI applications for prohibited systems cited as a key milestone in compliance strategy. EU AI Act high-risk obligations for most applications take effect Aug. 2026. https://www.telekom.com/en/company/digital-responsibility/details/the-eu-ai-act-at-deutsche-telekom--1090710

6. FCC Enforcement Bureau, Enforcement Advisory No. 2026-01, Feb. 11, 2026. Annual CPNI certifications for calendar year 2025 due March 2, 2026. Monetary forfeitures of up to $251,322 per violation or per day of continuing violation, up to a maximum of $2,513,215. No exemptions for small companies. https://docs.fcc.gov/public/attachments/DA-26-139A1.pdf

7. Mondaq, citing FCC Forfeiture Orders of April 29, 2024. FCC issued forfeiture orders against the three largest MNOs for failing to safeguard CPNI, signaling the end of lax CPNI enforcement. https://www.mondaq.com/unitedstates/telecoms-mobile-cable-communications/1466908/dialing-up-accountability-fccs-warning-shot-to-mobile-network-operators-on-cpni

8. Sprinto, Business ROI of Compliance 2026. Nearly 40% of companies report that more than half of their enterprise buyers treat SOC 2 compliance as a non-negotiable condition of doing business. https://sprinto.com/soc-2/

9. Bright Defense, SOC 2 Audit Costs in 2026. First-year SOC 2 compliance costs range from $30,000 to $150,000 or more, including audit fees, readiness assessments, remediation, and internal labor. https://www.brightdefense.com/blog/soc-2-audit-costs/

10. Sprinto, SOC 2 Compliance: The Complete Guide, 2026. After high-profile audit quality issues, SOC 2 examiners now require underlying evidence rather than a summary. Controls including data classification, processing monitoring, and data integrity verification are central to the audit. https://sprinto.com/soc-2/

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. Addresses inconsistent context retrieval, fragmented integration workflows, and lack of standardized communication between Collibra and other information sources. https://marketplace.collibra.com/listings/databricks-mcp-marketplace-collibra-mcp-server/

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