



exterro®

The Risks Hiding in Your Data

Prevent Costly Compliance Failures
with Automated Data Mapping

EXECUTIVE SUMMARY: UNSEEN DATA, UNMEASURED RISK

Organizations collect, store, and process more data than ever before, yet many lack full visibility and control over it. Without a clear understanding of where data is stored, how long it is retained, who has access, and how it is used, businesses face growing risks—especially in an era of strict privacy regulations and escalating cybersecurity threats.

Regulators demand accountability, but many companies still rely on outdated compliance methods such as spreadsheets, emails, and fragmented tracking systems. These manual processes are prone to inefficiencies, errors, and oversight, increasing the likelihood of regulatory penalties, security breaches, and reputational damage.

THE DATA DILEMMA: WHY PRIVACY COMPLIANCE IS BECOMING MORE COMPLEX

Increasing Data Privacy Regulations

Governments and regulatory bodies worldwide are imposing stricter data protection laws, requiring businesses to maintain comprehensive records of personal data, enforce strong security controls, and comply with complex data retention policies. Some of the most impactful regulations include:

GDPR (General Data Protection Regulation – EU)	Data minimization, transparency, and the right to be forgotten (Articles 30, 33, 35)
CCPA / CPRA (California, USA)	Consumer access to data, opt-out of data sales, and deletion rights
HIPAA (USA – Healthcare Sector)	Strict patient data protection and access controls
NYDFS Cybersecurity Regulation (USA – Financial Sector)	CEO & CPO accountability for cybersecurity compliance
LGPD (Brazil)	Justification for data collection, cross-border data transfer transparency
PIPL (China)	Data localization, mandatory compliance documentation
PIPEDA (Canada)	Tracking data flows, access & correction rights
POPIA (South Africa)	Data flow tracking, governance documentation
DPDPA (India)	Data transparency, cross-border data restrictions

The Expanding Data Landscape

Today's businesses rely on an ever-growing number of data storage solutions and digital tools. Data is no longer confined to on-premises servers; it is spread across a wide range of applications and on- and off-premises infrastructure. As data environments grow more fragmented, organizations must adopt robust mapping and governance strategies to maintain compliance.



Cloud Storage

Solutions like Amazon S3, Microsoft OneDrive, and Google Drive house [60% of corporate data, shifting storage from traditional servers to the cloud.](#)



SaaS Applications

Platforms like Salesforce, Workday, and Microsoft 365 hold sensitive customer and employee data, with [96% of companies using at least one public cloud service.](#)



Unstructured Data

Emails, shared drives, and legacy databases contribute to data sprawl. By 2025, [80% of the 175 zettabytes of global data will be unstructured.](#)



Third-Party Vendors

External service providers further complicate data tracking and compliance efforts.

Fragmented Data Environments

A dispersed data landscape creates significant compliance risks, including:



Hidden Data Silos

Sensitive data is often scattered across multiple locations without centralized tracking, making compliance difficult. Studies show that [70% of organizations struggle with fragmented data management](#), leading to inefficiencies and regulatory risks.



Cybersecurity Vulnerabilities

Unmonitored data is a prime target for cybercriminals. [Citigroup's weak data governance led to over \\$1.5 billion in fines](#), highlighting the dangers of poor oversight.



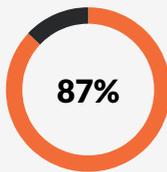
Inconsistent Data Retention

Many organizations lack clear retention and deletion policies, increasing regulatory and security risks.

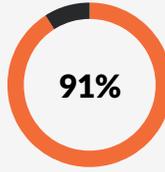
A well-structured data inventory and mapping strategy eliminates silos, enhances visibility, reduces redundancy, and ensures compliance. By taking control of fragmented data, enterprises can cut costs, boost efficiency, and turn data from a liability into a strategic asset. Without a centralized approach to data mapping and governance, businesses face mounting compliance challenges. Implementing automated data inventory and mapping solutions can mitigate these risks by improving visibility, security, and regulatory alignment.

With data growing exponentially, is your compliance strategy keeping up?

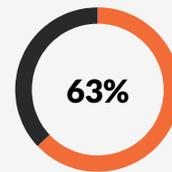
A recent Cohesity and Veritas report with IT leaders reveals the following



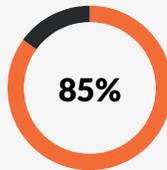
say secondary data is scattered across silos, making long-term management nearly impossible.



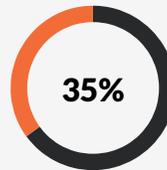
worry about poor visibility, with nearly half concerned about losing a competitive edge due to weak data insights



have between **4-15** duplicate copies of data, fueling unnecessary storage costs and complexity



struggle with data sprawl across multi-cloud environments. IT teams spend **16 extra weeks per year** managing fragmented data, straining resources and budgets.



of organizations use six or more point products for data management, while **10%** rely on 11 or more—creating inefficiencies and redundancy.

COMPLIANCE RISKS HIDING IN PLAIN SIGHT



Regulatory Penalties Resulting from Poor Data Visibility

When companies fail to properly map and manage their data, they expose themselves to significant compliance failures. There have been multiple high-profile cases where businesses have faced millions of dollars in fines due to poor data tracking and retention practices.



CASE STUDY

Citigroup's Compliance Failures

Citigroup mistakenly credited \$81 trillion to a customer's account in April 2024, instead of \$280, due to an error detected 90 minutes later. The bank reversed the transaction, which did not result in any funds leaving the bank, hours later.

The error highlighted broader operational challenges Citi has been working to address. Citi recorded 10 near misses involving transactions of \$1 billion or more last year. In recent years, Citi has faced regulatory scrutiny over its risk management and compliance practices.

In 2020, federal financial agencies fined the bank \$400 million for failures in these areas, followed by an additional \$136 million fine in 2023 for insufficient progress in addressing those deficiencies. Citi Chief Financial Officer Mark Mason acknowledged the need for further investment in compliance and technology. He said that the bank has focused on enhancing data governance, on technology, on improving the quality of the information coming out of our regulatory reporting to avoid similar errors in the future.

CASE STUDY

2024 National Public Data breach

A massive data breach exposed 2.9 billion records containing sensitive personal information—including full names, current and past addresses, Social Security numbers, dates of birth, and phone numbers—of individuals in the US, UK, and Canada.

In August 2024, three class-action lawsuits were filed against the company, with over 14 complaints submitted in federal court, alleging that it failed to prevent hackers from stealing private data belonging to millions of people. In total, the company now faces more than a dozen lawsuits and could be held liable for providing credit monitoring to hundreds of millions of potentially affected individuals.

One lawsuit specifically claims that in April 2024, a hacker using the alias "USDoD" advertised the stolen data on the dark web, pricing it at \$3.5 million. The breach raised serious concerns about regulatory shortcomings in data protection.

On October 2, 2024, National Public Data filed for bankruptcy, and by December 2024, the company had shut down entirely, overwhelmed by mounting legal battles.

The breach was attributed to the company's failure to secure its data properly, highlighting the risks associated with inadequate data management practices.

Data Breach Risks from Unmonitored Data

Data breaches are often caused by organizations failing to track and secure their sensitive data properly. Without a clear and up-to-date data catalog, companies leave themselves vulnerable to cyberattacks and unauthorized data exposure. Organizations that fail to maintain a clear and up-to-date data catalog expose themselves to significant compliance risks, including data breaches and regulatory penalties.

When organizations lack a centralized system for tracking data, security teams cannot respond quickly to breaches, and legal and compliance teams struggle to assess the damage.

Lesson learned? Without **proper data tracking and centralized data catalog**, businesses are highly vulnerable to breaches, compliance failures, and financial losses.

Operational Inefficiencies and Compliance Challenges

Operational inefficiencies and compliance challenges often arise when organizations lack proper data mapping practices. Without a clear understanding of data flows, compliance teams frequently face long delays when responding to regulatory audits, legal requests, and Data Subject Access Requests (DSARs). Without proper data mapping, these teams:

Missed regulatory deadlines, rising penalties, and compliance risks are common consequences of poor data visibility. Teams also waste significant time and resources manually searching for scattered data, leading to operational inefficiencies.

If You Don't Know Where Your Data Is, How Can You Protect It?

To eliminate delays, reduce risk, and improve compliance, organizations must implement comprehensive data mapping strategies. A clear, centralized view of data flows enables faster responses, stronger data protection, and seamless regulatory compliance.

Even a single spreadsheet error can result in millions of dollars in penalties, data breaches, or regulatory violations. Relying on manual compliance processes—such as spreadsheets and email-based workflows—creates inefficiencies, compliance risks, and long-term sustainability issues. Organizations need a more robust and scalable solution to keep up with evolving regulations.



Locating Personal Data

Without a comprehensive data map, organizations struggle to identify where personal data is stored, processed, or transmitted. This lack of visibility delays responses to DSARs and compliance inquiries, increasing regulatory risk.



Meeting Regulatory Deadlines

Laws like GDPR require DSAR responses within one month. Failure to meet deadlines can result in fines and reputational damage, making timely compliance essential.



Resource Intensive Processes

Without automation, businesses rely on manual tracking, leading to higher labor costs, human error, and inefficiencies as teams waste time searching for scattered data across multiple systems.

The Alternative: Automated Data Mapping

Organizations that embrace automated data mapping position themselves for greater accuracy, efficiency, and long-term compliance success, reducing risk and improving operational resilience.

Manual Approach	Automated Data Mapping
✗ Requires constant manual input	✓ Automatically discovers & classifies data
✗ Difficult to track data flows across systems	✓ Provides real-time visibility across all data
✗ High risk of human error	✓ Reduces compliance gaps through automation
✗ Time-consuming & expensive	✓ Increases efficiency & reduces costs
✗ Fails to scale with growing data	✓ Adapts to expanding regulatory demands



Enhanced Accuracy

Automation eliminates human errors, ensuring consistent and precise data mapping across all systems.



Improved Efficiency

Automated tools streamline data discovery and classification, significantly reducing the time and resources required for compliance tasks.



Scalability and Adaptability

As data volumes grow and regulations evolve, automated solutions scale effortlessly, ensuring organizations remain compliant without manual intervention.

THE BUSINESS CASE FOR AUTOMATED DATA MAPPING

A well-documented data catalog ensures all data handling practices align with legal requirements, making audits and compliance checks more efficient. Regular updates help businesses adapt to evolving regulations and operational changes. Organizations with accurate, up-to-date data catalogs have greater control over compliance, can streamline operations, and can reduce risks associated with manual data management. Key benefits include:

Proactive Compliance is Key. The most successful organizations don't just react to regulations—they stay ahead. Transitioning from manual compliance methods to automated data mapping is critical for organizations seeking to maintain compliance, enhance efficiency, and secure sensitive data in an increasingly complex regulatory landscape.



Eliminating Data Silos

Gain a real-time, centralized view of personal and sensitive data across the organization, breaking down silos and ensuring consistency for better data integrity and decision-making.



Simplifying Compliance Audits

Automatically track regulatory obligations, retention policies, and cross-border data flows, making audits more efficient and reducing compliance workload.



Reducing the Time and Cost of Compliance Requests

Accelerate responses to data subject rights, requests, vendor assessments, and legal audits by quickly locating and retrieving relevant data, minimizing operational costs and non-compliance risks.



Enhancing Security and Preventing Compliance Failures

Enable continuous monitoring and policy enforcement and proactively detect risks, enforce data handling policies, and prevent breaches.

HOW AUTOMATED DATA MAPPING WORKS: A PRACTICAL GUIDE

Automated data mapping simplifies data identification, management, and monitoring, ensuring compliance while improving operational efficiency. The process involves four key steps:

STEP 1 Data Discovery & Classification

- » Identifies where personal and sensitive data resides across structured and unstructured environments.
- » Uses automated scanning tools to detect and classify data, such as Personally Identifiable Information (PII) and financial records.

STEP 2 Compliance & Risk Assessment

- » Maps data flows across systems, identifying regulatory risks and retention violations.
- » Analyzes how data moves within the organization, detecting compliance gaps and security risks.

STEP 3 Proactive Data Lifecycle Management

- » Enforces retention and defensible deletion policies to reduce unnecessary data risks.
- » Ensures consistent application of policies across all data repositories, aligning with regulatory and business requirements

STEP 4 Continuous Monitoring & Auditing

- » Provides real-time compliance insights via dashboards and reports.
- » Enables continuous auditing to keep organizations ahead of evolving regulations and compliance challenges

By following these steps, organizations enhance data management, minimize compliance risks, and improve operational efficiency. Automation empowers compliance teams, allowing them to focus on strategic initiatives rather than manual tracking.

Defensible Data Deletion

Uncontrolled data accumulation exposes enterprises to security threats, regulatory penalties, and operational inefficiencies. With data volumes expanding rapidly, organizations often store information indefinitely due to fear of deleting something valuable or uncertainty about regulatory requirements. However, excessive data retention leads to increased security risks, regulatory compliance challenges, operational inefficiencies, and unnecessary costs.

Defensible data deletion is a strategic approach that ensures unnecessary, outdated, or trivial data is systematically identified and removed while maintaining compliance with legal and business requirements. A well-structured deletion strategy helps enterprises enhance compliance, reduce cybersecurity risk, improve efficiency, and lower costs. By adopting defensible data deletion, enterprises can shift from reactive data management to a proactive, risk-reducing strategy—ensuring data remains an asset, not a liability.



PRIVACY GOVERNANCE: WHO OWNS COMPLIANCE IN YOUR ORGANIZATION?

Privacy Compliance is a Shared Responsibility

Effective privacy governance requires collaboration across multiple departments. Data protection is not just an IT or legal function—it's a company-wide effort involving leadership, security teams, HR, and every employee. Each role plays a crucial part in ensuring compliance with regulatory requirements and safeguarding sensitive data.

Role	Responsibility
Executives & C-Suite	Define privacy strategy, allocate resources, and foster a compliance culture. Their leadership sets the tone for data protection across the organization.
DPO (Data Protection Officer) & Legal Teams	Oversee compliance with privacy laws, respond to regulatory inquiries, and enforce data governance policies. Under GDPR, appointing a DPO is mandatory for certain organizations.
IT & Security Teams	Implement technical safeguards, monitor for breaches, and manage secure data access. The Chief Information Security Officer (CISO) ensures data protection measures are enforced.
HR & Operations	Handle employee data, train staff on privacy policies, and embed compliance best practices into daily operations.
All Employees	Follow data protection guidelines and report potential security risks or compliance violations. Every employee plays a role in maintaining privacy and security.

Regulatory Accountability for Executives and Compliance Officers

Data privacy laws increasingly hold executives personally accountable for compliance. Under the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, financial institutions must ensure that CEOs certify compliance annually, while Chief Privacy Officers (CPOs) help implement data protection policies, incident response plans, and privacy training.

Failure to enforce proper compliance measures can result in personal liability for executives and fines for the organization. To mitigate these risks, companies must adopt robust data governance frameworks and integrate compliance into daily operations.

Privacy compliance is not a one-time initiative—it must be an ongoing commitment embedded into company culture and operations. By clearly defining roles, fostering collaboration, and ensuring continuous accountability, organizations can effectively navigate complex data protection laws and evolving regulatory landscapes.

Evolving Regulations Demand Greater Accountability

Privacy laws such as GDPR, CCPA, and HIPAA continue to evolve, imposing stricter requirements on data collection, storage, and sharing. Non-compliance can lead to financial penalties, legal action, and reputational damage.

New regulations, like the EU AI Act, introduce even tougher restrictions—banning high-risk AI applications like predictive policing and real-time biometric identification. To comply, organizations must implement robust risk management protocols and stay ahead of regulatory shifts.

AI-Driven Compliance Monitoring is the Future

With compliance regulations becoming increasingly complex, manual compliance management is no longer viable. AI-powered compliance tools are transforming data governance by offering:

- » **Continuous Monitoring** – AI tracks regulatory changes and automatically updates governance policies to ensure ongoing compliance.
- » **Real-Time Data Classification** – AI detects and categorizes sensitive data across structured and unstructured environments, strengthening security and compliance.
- » **Automated Risk Assessments** – AI analyzes compliance data to identify risks, detect anomalies, and reduce human error, making regulatory workflows more efficient.

Organizations That Embrace Automation Will Gain a Competitive Edge

Adopting Automated Data Mapping solutions provides key business advantages:

- » **Stronger Regulatory Compliance** – Ensures adherence to evolving privacy laws proactively and efficiently.
- » **Lower Operational Costs** – Reduces the time and resources needed for audits and legal inquiries.
- » **Improved Security** – AI-driven data lifecycle management prevents breaches and enforces consistent protection measures.
- » **Greater Customer Trust** – Advanced compliance strategies enhance transparency, strengthening customer confidence.

Privacy Compliance is No Longer Just About Avoiding Fines

Data compliance is now a critical element of responsible business and risk management. Organizations that integrate Automated Data Mapping into their data governance strategies will be better equipped to handle regulatory complexities, improve efficiency, and maintain a competitive advantage in a rapidly evolving market



TAKE CONTROL OF YOUR DATA WITH EXTERRO AUTOMATED DATA MAPPING

As data privacy regulations evolve, organizations must transition from manual, reactive compliance efforts to an automated, proactive approach. Companies that continue relying on spreadsheets and fragmented workflows will struggle to keep up with growing regulatory demands and rising security threats.

With its Automated Data Mapping Solution, Exterro helps organizations tackle compliance challenges with a real-time, comprehensive view of personal and sensitive data. Automated compliance workflows replace inefficient manual tracking, ensuring accuracy and regulatory adherence. Advanced security controls reduce the risk of data breaches, while seamless integration with IT, legal, and compliance teams enforces best practices in data governance, strengthening overall compliance.

AI-Driven Compliance Monitoring is the Future

- » **Data Source Discovery** – Automatically identifies structured and unstructured data across shadow IT, third-party storage, and internal systems.
- » **AI-Powered Classification** – Uses machine learning to accurately tag personal, financial, and health data, ensuring compliance with regulatory mandates.
- » **Centralized Data Catalog** – Establishes a single source of truth, providing quick access to sensitive data locations, access history, and retention schedules.
- » **Defensible Deletion Workflows** – Automates policy-driven data deletion, ensuring compliance with HIPAA, GLBA, and NYDFS retention mandates.
- » **Audit-Ready Reporting** – Generates real-time dashboards and compliance documentation, streamlining regulatory audits and reporting.

Experience firsthand how Automated Data Mapping can revolutionize your compliance strategy.

[Schedule A Demo](#)

exterro[®]