

DATA NAPPING: KNOW WHERE YOUR SENSITIVE DATA RESIDES

In the modern data-driven enterprise, organizations rely on ever-growing volumes of information to drive business value. This includes vast amounts of sensitive data such as personally identifiable information (PII), financial records, healthcare data, intellectual property, and more. While this data is critical for business operations, it also introduces significant privacy, security and compliance risks if not properly managed.

Recent years have seen dramatic rises in damaging data breaches, along with skyrocketing regulatory penalties for noncompliance with laws like GDPR and CCPA. To minimize risk exposure, understanding exactly where sensitive data resides throughout your technology infrastructure is essential. This requires developing a comprehensive map of data assets, flows and handling.

This process of identifying, categorizing and mapping out sensitive data is known as data mapping. A data map serves as an inventory of all the places confidential data is stored, processed, and transmitted across your systems. It illuminates how this data moves into, within, and outside your organization. Data mapping provides complete visibility so you can pinpoint areas of highest risk.

With this knowledge, you can implement targeted safeguards to lock down sensitive data flows and systems. A data map also feeds into key functions like security audits, breach response, privacy impact assessments, user access requests and demonstrating regulatory compliance. Maintaining an accurate, up-to-date data map enables smart data governance tailored to true sensitivities rather than guesses. In today's data security landscape, neglecting thorough data mapping severely heightens an organization's exposure. This article explores what building a comprehensive data map entails, its critical use cases, and best practices for sustaining it as a core component of your data governance strategy.

CONDUCTING A DATA MAP

Compiling a fully detailed data map involves cataloging and analyzing all data assets, locations, classifications, applications, movement and dependencies. Key steps include:

CATALOGING DATA SYSTEMS AND SOURCES

The first phase is creating a catalog of all systems and sources where data is collected, processed, transmitted or stored. This inventory should be exhaustive, encompassing:

- All servers, databases, file shares and data repositories
- Cloud-based infrastructure like laaS, PaaS, SaaS applications
- Endpoints and edge devices handling data
- Legacy systems still housing sensitive datasets
- Backups, archives, and data warehousing systems
- Third party systems operated by vendors and business partners
- Any additional technologies handling confidential data



CLASSIFYING DATA TYPES AND SENSITIVITY

With an inventory established, the next stage is identifying and classifying the types of data present on these systems. This examines characteristics like:

- Personal data like names, government IDs, contact details, demographics
- Financial information such as payment cards, bank account numbers, credit records, insurance details
- Special categories including health data, religious/ethnic details, sexual orientation, biometrics
- Business confidential data like trade secrets, contracts, strategic plans, intellectual property
- Operational data such as system logs, network traffic, security artifacts

Each data type should be mapped to an appropriate sensitivity classification like high, moderate, low, or unclassified based on its inherent level of risk and impact of exposure. Sensitivity factors include regulatory obligations tied to the data, contractual controls, data criticality for the business, and privacy risks to individuals.

IDENTIFYING DATA OWNERS, CUSTODIANS AND PROCESSORS

The next key mapping step is to identify personnel associated with controlling and handling the data. This includes:

- Data owners Executives, managers or other staff ultimately accountable for specific data assets.
- Data custodians IT professionals, DBAs, system administrators responsible for technical storage and security.
- Data processors Employees, departments, vendors or other third parties who access and use the data as part of business processes.

Determining the human elements across the data lifecycle enables appropriate security and access controls tailored to each audience. It also clarifies responsibilities around data management to support policy and compliance initiatives.

MAPPING DATA FLOWS

With clarity on data types and personnel established, the connections between systems must be mapped. This entails illustrating how data flows across your architecture as it is:

- Ingested from external sources
- Transmitted between internal systems and departments
- Accessed and processed by various personnel
- Exchanged with vendors and partners
- Backed up or archived
- Analyzed for insights with analytics tools
- Removed via deletion and destruction processes

Data flow diagrams should highlight all system integrations, data pathways, connections to external entities, and sign-off points within processes that handle sensitive data. This illuminates how data traverses the organization and where it lands, exposing potential blind spots or inadequately secured access points.







DOCUMENTING DATA PROCESSING ACTIVITIES

In addition to the technical flow of bits and bytes, it's critical to understand exactly how data is handled at each processing point from a policy and compliance perspective. This requires assessing:

- Why data is collected and what it is used for
- How retention and destruction schedules align to policy
- What employee roles access and use the data, authorized vs. actual
- Whether consent is required for processing and attained
- What controls govern data sharing with third parties

Documenting these data handling nuances identifies gray areas where processes deviate from formal policy protections based on access needs or norms. It also highlights processing activities that introduce compliance risks.

EVALUATING JURISDICTIONAL APPLICABILITY

Finally, the geographic locations where data flows and resides must be analyzed to determine governing laws and obligations. Key considerations include:

- Country and state jurisdictions where data is physically stored
- Locations of personnel handling and accessing the data
- Nationalities and geographic distribution of data subjects
- Cross-border data transfer mechanisms in place

This evaluation identifies which regulations around data protection, privacy, security and industry standards apply based on where and by whom data is processed. Understanding jurisdictional scope is essential for ensuring compliant data management and transfers. By undertaking this comprehensive assessment, a detailed data map emerges identifying sensitive information, associated systems and personnel, data pathways and hand offs, jurisdictional applicability, and processing activities.

USING THE DATA MAP

The data map provides immense utility to inform privacy, security and compliance programs. Primary use cases include:

GUIDING DATA PROTECTION AND MINIMIZATION

The detailed categorization of data types and sensitivity levels allows customized safeguards and access controls to match proper levels of protection to data criticality. By identifying the highest risk data flows, additional encryption, access controls, monitoring, and other countermeasures can be applied. Data mapping also aids minimizing unnecessary collection and retention based on value classification.



SUPPORTING COMPLIANT DATA HANDLING

The end-to-end mapping of data flows combined with processing details highlights potential areas of non-compliant handling according to governing regulations and policies. Any discrepancies between documented policies and actual inconsistent access, sharing or retention emerging from the map can guide corrective actions like tighter controls, reduced retention or increased oversight.

ENABLING DATA SUBJECT REQUESTS

Data mapping aids promptly fulfilling data subject rights requests around access, corrections or deletion as mandated by privacy laws like GDPR and CCPA. By delineating types of personal data tied to specific systems and databases, relevant records can be efficiently located and extracted to service requests.

RESPONDING TO DATA BREACHES

In the chaotic aftermath of a data breach, an accurate data map is invaluable for determining scope and guiding response. The mapping of data types and flows allows response teams to identify compromised systems, assess breach impact, and determine notification obligations based on sensitivities of exposed records.

FEEDING RISK ASSESSMENTS AND AUDITS

Data mapping provides input for preliminary risk assessments by highlighting areas of protected data flows and processing. Auditors can verify controls match defined protection levels per the map. It also demonstrates diligence to regulators requesting details on sensitive data footprints.

DRIVING DATA GOVERNANCE INITIATIVES

The map provides insights to shape broader data governance strategies around access policies, compliant handling, requisite controls, staff training, vendor management, privacy and archiving. Identifying data dependencies and flows is key for impact analysis when planning new processes or technologies.

SUPPORTING IT AND BUSINESS INITIATIVES

Beyond purely risk-based use cases, the data map aids IT teams with maintenance, troubleshooting and system changes by illuminating relationships and dependencies. It guides efficient migration by precisely identifying data holdings needing moved. For business teams, it enables analysis of how data underpins business functions and metrics to shape initiatives.

BEST PRACTICES FOR MAINTENANCE

While the upfront exercise of compiling a data map provides enormous insights, the map must be continually maintained to retain accuracy and value over time as an operational asset. Best practices for sustaining data mapping include:

Implementing a Central Repository

The data map should be maintained within a central repository accessible by any teams requiring the data inventory for their initiatives. This provides a single source of truth versus disparate, decentralized data mapping losing sync. Leading options include data governance tools with mapping features or a robust collaboration platform.

Assigning Responsibility for Updates

Keeping the data map current requires clearly defining stewardship responsibility. A data governance team is well positioned for oversight, partnering with IT leads, data owners and other key contributors to solicit map updates. Requests for additions or modifications can be routed to the governing team for review and inclusion in the central repository.







CONCLUDING THOUGHTS

In today's data security landscape, understanding exactly where sensitive information resides across your technology infrastructure is imperative. Comprehensive data mapping provides complete visibility so you can identify your most critical data, highest risk systems, and vulnerabilities that require urgent attention. A detailed data map is invaluable for:

- Implementing targeted data security and privacy controls tailored to true sensitivity rather than guesses
- Ensuring compliant data handling across collection, storage, usage and disposal
- Supporting efficient responses to data subject rights requests
- Quickly determining breach impact and notification duties
- Supplying auditors confirmation of diligent data protection programs
- Driving smarter data governance decisions aligned to organizational data risks

Without thorough mapping of data assets, flows and processing details, organizations are blind to risks plaguing their environment. Data mapping provides the essential foundation to build security, privacy and compliance programs firmly rooted in reality rather than assumptions.

However, while the initial mapping exercise delivers profound insights, maintaining a reliable inventory requires institutionalizing ongoing map maintenance. Data maps decay quickly without formal governance responsibility, scheduled reviews, update triggers baked into procedures, and centralized versioning. Keeping the map current based on industry best practices elevates its position as a strategic asset that delivers immense value over time.

With robust data mapping and diligent stewardship, organizations can protect sensitive information, preserve customer trust, avoid regulatory fines, and enable data-driven innovation. In contrast, without a comprehensive understanding and accounting of sensitive data, businesses face substantial exposure in today's turbulent data privacy and security landscape.

The threats and penalties grow more severe daily. Now is the time to prioritize mapping where data resides, classifying its sensitivities, locking down controls, and institutionalizing continuous updates. With progress in these areas, data risks become manageable versus catastrophic.