About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world’s leader in Enterprise Cloud Data Management, we’re prepared to help you intelligently lead—in any sector, category or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.
Table of Contents

Executive Summary........................................................................................................ 4
Introduction.................................................................................................................... 5
Four-Point Strategy for Mitigating Sensitive Data Privacy Risk ...................... 5
  Discovery and Classification ...................................................................................... 6
  Compliance ................................................................................................................ 6
  Protection .................................................................................................................... 7
  Audit Readiness and Response .............................................................................. 7
Conclusion.................................................................................................................... 7
Recommendations ......................................................................................................... 8
Executive Summary

To create a trusted, authoritative view of customer, product and service, operational and other business-critical enterprise information, organizations invest in Master Data Management (MDM) initiatives. MDM combines elements of essential data across the enterprise into consolidated records to create trusted data to be shared with the people and applications that need it. This has tremendous value for any business that wants to build more customer-centric offerings; improve customer service and loyalty programs; create efficiencies in product management and solutions; migrate to the cloud safely; and so on.

Trusted data becomes the crown jewels of the organization’s customer and product initiatives and provides competitive advantage. However, consolidation of sensitive data also provides an attractive target for outside attacks resulting in data security breaches and increases potential internal abuse, therefore is subject to privacy regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and beyond.

Natural questions arise for data protection and compliance for these environments:
• Where is all the data located and how does it proliferate?
• What is feeding the repository and who is accessing data with what applications?
• Does current access and use adhere to regulations and approved data use policies?
• Are data protections appropriate, and is data risk remaining at acceptable levels or are there conditions creating inappropriate risk that must be remediated?

The results of the discovery and classification of sensitive customer data become the foundation for decision support regarding the risk, protection, and privacy regulatory compliance of mastered data.

This white paper provides a framework of considerations and strategies for mitigating risk with a data-centric solution that:
• Applies analytics, metadata-driven intelligence, automation, and AI to identify and protect sensitive mastered data
• Complies with evolving data governance and privacy regulations
• Provides audit readiness to attest to controls in place, and
• Alerts stakeholders when anomalous user behavior occurs, requiring investigation
Introduction

According to research firm IDC, the world is predicted to create 175 zettabytes of data in 2025, up from 33 zettabytes in 2018.1 Organizations across all industries rely on the accuracy, availability, and protection of their data to generate revenue, serve customers, increase productivity, optimize operations, and conduct other mission-critical business processes.

The continued exponential growth in data volume and usage also includes sensitive master data across multiple silos, both on-premises and in the cloud, and in a variety of data formats. These conditions have rendered traditional data security methods obsolete,2 requiring a new approach to master data security across an organization.

However, most companies cannot accurately identify where all their sensitive master data is located and accessed, especially in unstructured format. This lack of visibility increases an organization’s risk, and as a result, a data security breach remains a top IT security risk.3

With data security breaches on the rise in tandem with the proliferation of sensitive master data used inappropriately, organizations must develop a risk mitigation strategy that includes a data-centric privacy solution with these key features:

• Visibility into all data sources to discover and classify sensitive master data located across the organization
• Ability to implement protection mechanisms for sensitive master data to mitigate data security breaches
• Compliance with current privacy regulations, including the use of metadata-driven intelligence, automation and AI to monitor user behavior and alert to anomalies in near real time
• Rich analytic visualization tools for risk assessment and sensitive data management
• Transparent and comprehensive reporting capabilities for demonstrating controls with audit readiness

Gartner predicts that integrated protection products will replace disparate siloed data security tools in 40 percent of large enterprises, up from less than five percent.4 These data-centric protection solutions provide a centralized view of at-risk data, so that all key stakeholders across a global organization can track sensitive data movement and apply protection mechanisms as required by governance policies and regulations.

A Four-Point Strategy for Mitigating Sensitive Data Privacy Risk

Sensitive data privacy risk is the impact of losing sensitive data with improper exposure, and the most common cause is a data breach or insider misuse. A common misperception is that simply locating sensitive master data is enough to remediate risk. However, locating and classifying this data is only the first step in a comprehensive risk remediation strategy.

The next steps involve assessing your organization's risk priorities to address, based on the results of the location and classification analysis. You need to determine a strategy for reducing the top risks—with automated controls that enforce data governance policies and involve all key stakeholders—not just IT. Your strategy should include implementing a reliable, data-centric privacy and protection solution that provides capabilities for regulatory compliance, including rich analytic visualizations of sensitive data for risk visibility dashboards and audit reporting of compliance controls; and protection for all sensitive mastered data types across the organization.

1. Discovery and Classification
A common ad hoc approach to discovery is to review existing sources and send questionnaires. However, a manual approach is inadequate because it consumes valuable time and resources, and it is often inaccurate and out of date quickly, with reliance on self-reporting rather than actual monitoring in real time of user behavior and dataflow.

Organizations need to ask themselves:
• What data do you store, who has access to it, and for what purposes?
• How do you manage user privileges and provision data rights?
• How will you protect sensitive mastered data and ensure that the appropriate controls are in place?

Other considerations for discovery and classification compliance include:
• Defining and understanding your data landscape, including databases and unstructured data
• Mapping which systems contain sensitive mastered data and mapping data to identities
• Procuring a solution that can map the movement of this data across your ecosystem while maintaining a near real-time view with analytics and reporting tools

2. Compliance
Organizations struggle to identify, monitor, and remediate data risks to comply with data privacy regulations. Further, they must monitor, analyze, and alert on data access or movement that could jeopardize compliance.

The GDPR, having begun enforcement on May 25, 2018, was adopted with the intent to strengthen and unify data protection for all individuals within the EU, thereby simplifying the regulatory environment for international business. Similarly, the CCPA, having gone into effect as of January 1, 2020, raises the bar, extending privacy to include household data.

Many businesses have not fully prepared for either regulation and are not sufficiently compliant with noncompliance potentially resulting in significant fines and reputational damage. On the other hand, compliance can provide the opportunity for competitive advantage as a mastered data privacy differentiator to enhance customer loyalty, while also driving digital transformation outcomes. Moreover, companies that demonstrate diligence by protecting data can realize 5x access to personal information from their customers that trust them to handle it responsibly.5

5 Excerpt, Boston Consulting Group, "Bridging the Trust Gap in Personal Data"
Organizations need to develop intelligent policies that identify data stores that contain GDPR-, CCPA-, and similar privacy mandate relevant “data domains.” These policies are multifactor, with data intelligence logic that determines which combinations pose a privacy risk exposure threat.

3. Protection
In 2019 as of Q3, there were over 5,000 data breaches, with nearly 8 billion records exposed.\(^6\) Clearly, despite large investments in data privacy and security, critical personal data remains vulnerable. Organizations need to continuously protect high-risk data; identify suspicious behavior and unauthorized use or movement, while automating and orchestrating remediation.

Organizations should prioritize the most critical data risks and remediate these risks with data-centric controls that support data mobility, rather than relying on historical server access controls, firewalls and similar system-centric cybersecurity tools alone. For example, data-centric controls include masking, identity-based controls, and encryption.

In addition to data privacy controls, organizations must monitor identity-based data access and behavior. Excessive access or unusual behavior can indicate that users are not adhering to privacy policies or that user credentials have been compromised.

4. Audit Readiness and Response
Companies undergo more audits and assessments of sensitive data than ever before. They struggle to provide proof to auditors that they have visibility and protection of critical data.

Organizations should be able to immediately respond to auditors and provide evidence that they know where data exists, what is its risk, how the data is protected, and how the data is being used. They should consider that auditors will want reports and visualizations that are abstracted for departments or locations, and that provide the ability to drill down on specific data domains.

Conclusion
The power of MDM can help organizations transform their operations and services. The power of this data is clear, but it also represents a tempting target for internal or external actors to misuse. Coupled with the continued onslaught of data breaches and growing compliance requirements, organizations must rethink their processes and tools for identifying, analyzing, and protecting sensitive data.

In the current climate of heightened privacy risk and routine data breaches, companies now must develop a robust digital strategy to continuously monitor, analyze, and remediate the risk of their sensitive master data. They need to monitor data in near real time for signals of misuse or data security breach, unusual access and behavior, or improper cross-border transfers. With this diligence, organizations can leverage MDM and improve their data risk posture to help mitigate the impact of data breaches or internal misuse and meet the stringent requirements of regional and industry regulations.

\(^6\) Risk Based Security’s Q3 2019 Data Breach QuickView Report
Recommendations

1. Perform a data privacy risk assessment to gain a clear understanding of where your sensitive mastered data is located, how far it proliferates through your data ecosystem, and which sets of sensitive data are most vulnerable for remediation.

2. Based on the assessment results, prioritize your organization’s top sources of the most sensitive mastered data; determine a strategy and timeline for protecting these; and implement this strategy as a pilot solution for your approach to data privacy and protection.

3. Define, document, and distribute your organization’s privacy compliance policies and the key stakeholders that are accountable for privacy regulatory compliance. Build a strategic plan for this year and beyond.

Further Research

For more information about sensitive data security risks and protection considerations, refer to the following publications and videos:

Informatica Data Privacy Management
Informatica Master Data Management–Customer 360
White Paper: Intelligent Data Privacy
Bloor Research: Discovering Sensitive Data