NowVertical

The hidden risks of misclassified PII:

Uncovering the True Cost to Enterprises

2024

We Transform Data into Business Value with AI, Fast

About Us

NowVertical Group is a leader in data analytics and governance, trusted by global enterprises for expertise in managing complex data challenges, including PII protection.

The Hidden Risks of Misclassified PII: Uncovering the True Cost to Enterprises

Enterprises today are stewards of vast amounts of PII, collected across multiple touchpoints and stored in increasingly complex data environments.

The stakes are high: misclassification of PII can expose organizations to severe financial penalties, operational inefficiencies, and enduring reputational damage. Despite the clear risks, many enterprises struggle to maintain accurate PII classification due to the sheer scale and complexity of modern data systems. The challenges are compounded by the dynamic nature of data, where information continually flows across various departments, systems, and jurisdictions, often outpacing the organization's ability to manage it effectively.

The difficulty of managing PII classification is not merely a technical issue but a strategic one. As enterprises grow and their data landscapes become more fragmented, the potential for misclassification—and the corresponding risk—grows exponentially. It is critical for organizations to understand that PII misclassification is not just an isolated data management problem but a systemic issue that requires an integrated, enterprise-wide solution.

The Complexity and Challenges of PII Classification

20%
of enterprises use 1000+ data sources

63%
of enterprises store over 100TB if data

>80%
of stored data is unstructured

The classification of PII is inherently complex, influenced by several factors that make it challenging to execute consistently across an organization. One of the primary challenges is the sheer volume and velocity of data generated by enterprises today. 63% of enterprises manage over 1PB of data, with 40% managing over 5PB.[1] 80-90% of that data is unstructured[2] and often less protected than structured data, making it a prime target for misclassification and potential breaches[3]. This data deluge makes it difficult for organizations to maintain accurate classification, particularly when dealing with large, heterogeneous datasets where PII may be embedded in various forms.

Adding to the complexity is the fragmented nature of modern data environments. Data is often dispersed across legacy systems, cloud platforms, and third-party applications, each with its own set of classification standards and security protocols. 20% of enterprises draw from over 1000 sources[4]. This fragmentation can lead to inconsistent classification practices, where PII is adequately protected in one system but left vulnerable in another. The challenge is further exacerbated by the dynamic nature of data; as information moves through its lifecycle—from collection and processing to storage and sharing—it often changes context, necessitating reclassification. However, many organizations lack the real-time capabilities needed to update classification status dynamically, leading to gaps in data protection.

Despite advances in automation, many enterprises continue to depend on manual processes to classify PII, particularly when dealing with complex or unstructured data. This reliance not only slows down the classification process but also increases the likelihood of errors, where sensitive data may be overlooked or incorrectly categorized.

The Hidden Costs and Risks of Misclassified PII

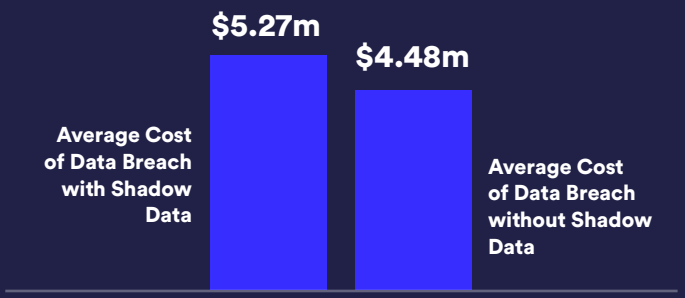
Misclassification of PII is not merely a compliance issue; it is a business risk with far-reaching implications. When PII is misclassified, it is often left unprotected, making it a prime target for cyberattacks.

The 2024 Cost of a Data Breach Report by IBM:

Breaches involving misclassified or unprotected PII are among the costliest, with the average breach costing enterprises $4.45 million[5]. The financial impact, however, is only part of the story. The hidden costs associated with these breaches—such as operational disruption, customer churn, and reputational damage—can be even more detrimental. IBM found 35% of breaches involved shadow data, showing theproliferation of data is making it harder to track and safeguard. Shadow data theft correlated to a 16% greater cost of a breach[5]. The immediate financial impact, however, is only part of the story. The hidden costs associated with these breaches - such as regulatory fines, operational distruption and reputational damage - can be even more detrimental.

Cost of Data Breaches Including Shadow Data (USD)[5]

Shadow data refers to data that exists within an organization's network and information systems but is not actively monitored, managed, or controlled by the organization's IT or security teams.



Cost Per Record by Record Type[5]

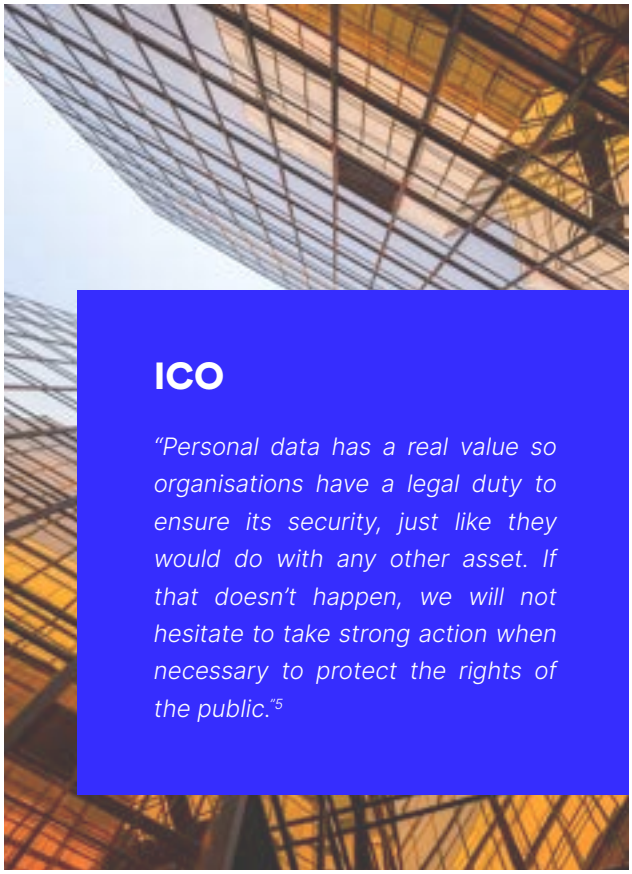
Types of Data Compromised

Compliance and Legal Liabilities

The regulatory environment surrounding PII is becoming increasingly stringent. With regulations such as GDPR, CCPA, and LGPD imposing heavy fines for non-compliance, the stakes for accurate PII classification have never been higher. Yet, despite the clear regulatory requirements, many organizations struggle to keep up. Misclassified PII can easily slip through the cracks, leading to compliance breaches that result in significant financial penalties. For example, under GDPR, fines can reach up to 4% of a company's annual global turnover or €20 million, whichever is higher. British Airways' €22 million fine in 2020 serves as a stark reminder of the potential financial impact of failing to protect PII.

However, the financial penalties are just the beginning. Organizations may also face regulatory sanctions, increased scrutiny, and the possibility of class-action lawsuits from affected individuals. These legal actions can result in further financial liabilities, as well as damage to the organization's reputation. The complexity of navigating these legal challenges underscores the importance of proactive data risk management strategies.

In today's digital marketplace, trust is a key differentiator. Customers expect that their personal data will be handled with care and protected from unauthorized access. When a breach involving PII occurs, it shatters that trust, often irreparably.



ICO

"Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."[5]

According to PwC, 85% of consumers will not do business with a company if they have concerns about its data security practices[6]. This loss of trust can lead to increased customer churn and lost revenue, far outweighing the immediate financial impact of the breach.

Moreover, the reputational damage caused by a data breach can have long-lasting effects on a company's market position. The Edelman Trust Barometer reports that trust in a company's ability to protect data is a critical factor in consumer decision-making, with 81% of respondents indicating that they would stop engaging with a brand if they no longer trust it to handle their data securely[7]. The erosion of trust can also have a cascading effect, leading to decreased investor confidence, lower stock prices, and increased scrutiny from regulators.

Operational Disruption and Increased Costs

The operational impact of a data breach involving misclassified PII can be profound. In the immediate aftermath of a breach, organizations must reallocate resources to contain the breach, notify affected individuals, and implement remediation measures. This can disrupt normal business operations, leading to lost productivity and increased costs. Gartner estimates that the average cost of operational disruption following a data breach is $300,000 per hour[5], underscoring the significant financial impact of these disruptions.

In addition to the immediate costs, organizations may face long-term financial implications, including increased insurance premiums, higher costs for security and risk management, and the need to invest in new technologies to prevent future breaches. These costs can quickly add up, further eroding the organization's bottom line. Furthermore, the time and resources spent on managing the aftermath of a breach detract from other strategic initiatives, slowing down the company's growth and innovation efforts.

Managing PII outside of traditional databases presents unique challenges, particularly when dealing with unstructured data like documents, spreadsheets, presentations, and email attachments. These are often stored in collaborative environments such as shared drives, SharePoint, or cloud services like Google Drive and Dropbox, where the risk of misclassifying or overlooking PII is high.

Unlike structured data organized in databases, unstructured data lacks predefined formats, making it harder to search, categorize, and protect. This includes text files, images, and social media content, all of which may contain PII. The challenge lies in consistently identifying and safeguarding PII across all storage locations.

Many enterprises underestimate the volume of PII contained in unstructured data, leading to a false sense of security. However, studies have shown that unstructured data accounts for approximately 80-90% of all data within organizations, and this data is growing at a rate of 55-65% per year[2].

The lack of visibility into this data, coupled with the difficulty in applying traditional data governance practices, makes it a prime target for cyberattacks.

Proactive Solutions for Mitigating PII Risks

it is imperative for organizations to adopt a proactive, technology-driven approach to data risk management.

Given the complexities and risks associated with misclassified PII, it is imperative for organizations to adopt a proactive, technology-driven approach to data risk management. This approach should be comprehensive, addressing both structured and unstructured data across all storage environments—from traditional databases to cloud-based file sharing systems. The goal is to ensure that PII is consistently identified, classified, and protected, reducing the likelihood of compliance breaches, operational disruptions, and reputational damage.

Real-Time Data Discovery & Classification

One of the most critical components of a robust data risk management strategy is the ability to perform real-time data discovery and classification. In many organizations, PII is not static; it is constantly being created, modified, and shared across various systems. As such, traditional, manual approaches to data classification are often insufficient. They cannot keep pace with the dynamic nature of enterprise data environments, leaving gaps in protection that can be exploited by cyber threats.

NowVertical's Data Risk Mitigation solution leverages real-time scanning of all data sources. This includes structured data stored in databases as well as unstructured data found in documents, emails, and other files. The system automatically identifies and allows you to set up automated workflows to classify PII based on predefined criteria, ensuring that sensitive information is always accurately categorized and protected according to the organization's data governance policies.

This real-time capability is particularly important for managing unstructured data, which, as discussed, constitutes the majority of an organization's data and is often the most challenging to manage.

Automated Remediation & Compliance Assurance

Accurately classifying PII is only the first step; organizations must also ensure that once PII is classified, it is protected in accordance with relevant regulations. This includes applying appropriate encryption, access controls, and other security measures to prevent unauthorized access or exposure. However, given the volume and complexity of data that most organizations handle,

applying these protections manually is both time-consuming and prone to errors.

To address this challenge, NowVertical's solution enables automated remediation that can apply the necessary security measures as soon as PII is identified and classified. For example, if PII is found in an email attachment or document stored on a shared drive, automated workflows can apply appropriate protections to ensure that the data is not exposed to unauthorized parties.

These automated remediation processes are designed to be seamless and unobtrusive, minimizing the operational burden on IT and compliance teams. At the same time, they provide a critical layer of protection that reduces the risk of data breaches and ensures compliance with regulations such as GDPR, CCPA, and HIPAA.

It is particularly important in today's rapidly evolving regulatory landscape, where new data protection laws are regularly introduced, and existing regulations are frequently updated tp automate compliance checks by evolving these automations with the latest standards, organizations can mitigate the risk of costly fines and legal liabilities.

Scalable Governance Frameworks

As organizations grow and their data environments become more complex, maintaining consistent data governance practices across all systems and locations becomes increasingly challenging. This is especially true for large enterprises with multiple departments, geographic regions, and third-party partners, each with its own data management practices.

Solutions need to be designed to scale with the organization, ensuring that data governance policies are enforced consistently across all environments. This includes not only internal systems but also external cloud services, third-party applications, and other data storage locations.

A centralized governance framework that enables organizations to define and enforce data classification, protection, and retention policies across the entire enterprise is critical. This ensures that PII is managed consistently and securely, regardless of where it is stored or how it is accessed. By providing a unified view of data governance across the organization, NowVertical's solution helps reduce the risk of misclassification and ensures that information is always protected appropriately.

Conclusion:
The Strategic Imperative of PII Classification and Protection

Find out more

Discover how our solutions can help you tackle complex data challenges and improve PII protection.

Find out More

In today's data-driven world, the accurate classification and protection of PII are not just regulatory requirements—they are strategic imperatives that directly impact an organization's financial health, operational efficiency, and market reputation. The hidden risks associated with misclassified PII can have profound implications, exposing organizations to compliance breaches, data breaches, a`nd significant financial penalties.

NowVertical's Data Risk Mitigation solution offers a comprehensive, technology-driven approach to managing these risks. By providing real-time data discovery and classification, automated remediation, and scalable governance frameworks, the solution ensures that PII is consistently identified, classified, and protected across all environments.

For organizations looking to safeguard their most valuable assets—customer trust and data integrity—NowVertical's Data Risk Mitigation solution provides the tools and expertise needed to navigate the complex landscape of PII management effectively. As the data landscape continues to evolve, proactive risk management will remain essential for ensuring that sensitive information is protected and that organizations are well-positioned to thrive in an increasingly regulated and security-conscious world.

Get in Touch

References

1. Komprise, 2022. State of Unstructured Data Management Report. [online] Available at: https://www.komprise.com/wp-content/uploads/Komprise-State-of-Unstructured-Data-Management-Report.pdf [Accessed 20 September 2024].

2. MongoDB, 2024. Unstructured Data. [online] Available at: https://www.mongodb.com/resources/basics/unstructured-data#:~:text=From%2080%25%20to%2090%25%20of,used%20to%20guide%20business%20decisions. [Accessed 20 September 2024].

3. Forcepoint, 2024. Gartner 2024 Strategic Roadmap for World-Class Security in Unstructured Data. [online] Available at: https://www.forcepoint.com/resources/industry-analyst-reports/gartner-2024-strategic-roadmap-world-class-security-unstructured [Accessed 20 September 2024].

4. Matillion, 2024. Matillion and IDG Survey: Data Growth is Real and 3 Other Key Findings. [online] Available at: https://www.matillion.com/blog/matillion-and-idg-survey-data-growth-is-real-and-3-other-key-findings [Accessed 20 September 2024].

5. IBM, 2024. 2024 Cost of a Data Breach Report. [online] Available at: https://www.ibm.com/security/data-breach [Accessed 20 September 2024].

6. PwC, 2024. Protect Me: Consumers and Cyber Security Report. [online] Available at: https://www.pwc.com.au/digitalpulse/report-protect-me-consumers-cyber-security.html [Accessed 20 September 2024].

7. Edelman, 2023. 2023 Edelman Trust Barometer Global Report. [online] Available at: https://www.edelman.com/sites/g/files/aatuss191/files/2023-01/2023%20Edelman%20Trust%20Barometer%20Global%20Report.pdf [Accessed 20 September 2024].

www.nowvertical.com

shailesh.mallya@nowvertical.com

545 King St. West, Toronto,
Ontario, M5V 1M1, Canada

NowVertical Group is a leader in data analytics and governance, trusted by global enterprises for expertise in managing complex data challenges, including PII protection.