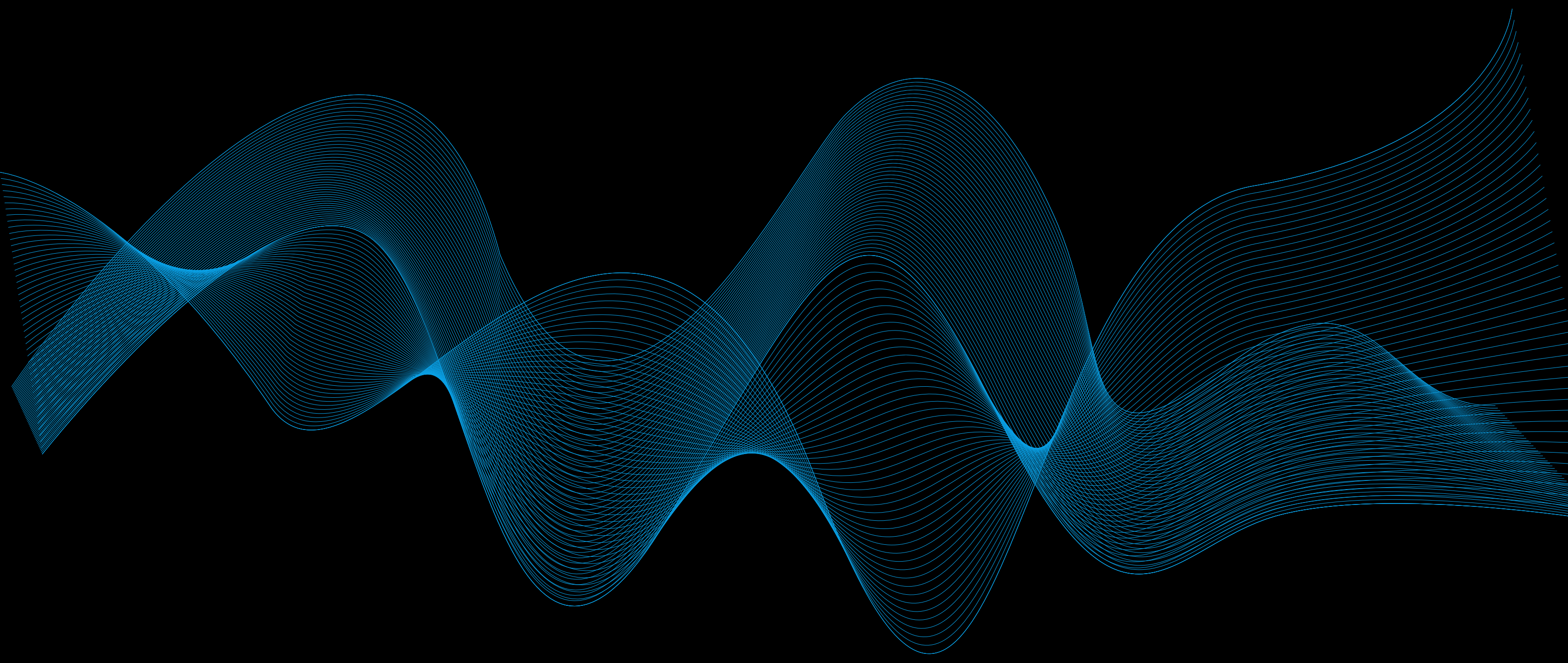
privatris



WHITE PAPER

UNCOVERING AND MITIGATING HIDDEN PRIVACY RISKS

A comprehensive AI-powered solution to detect and manage sensitive data in unstructured environments

■ OUR STORY

Privatris was founded with a clear vision:
“To make privacy compliance accessible, intuitive, and impactful. “
During our years of consulting in compliance and privacy, we witnessed a common struggle, organizations faced a patchwork of complex, siloed tools that made staying compliant a daunting task.
Many solutions lacked usability, or addressed only fragments of the compliance process, leaving companies burdened with navigating multiple platforms to achieve a single goal.

Inspired by this challenge, we set out to create a solution that brings it all together.
Our mission is simple but powerful: to provide a unified, adaptable platform that meets the unique needs of each organization we work with. By combining innovation with ease of use, we make compliance not just manageable, but empowering, so that businesses can focus on growth without fear of regulatory setbacks.

At Privatris, we´re not just building tools, we´re setting new standards in privacy solutions. With an eye on the future and a commitment to staying at the forefront of technology, we aim to become a leader in privacy compliance across North America. As we grow, our goal remains the same: to help organizations thrive by transforming privacy compliance into a seamless part of their success story.

MARKET LANDSCAPE

With global data projected to exceed 175 zettabytes by 2025, of which 80-90% is unstructured (IDC, 2018), organizations face an overwhelming challenge in managing data privacy. Unstructured data—like emails, scanned documents, and media files—complicates data governance due to its varied and fragmented nature (Datanami, 2023). This increasing volume, combined with stricter regulations, has driven demand for privacy solutions capable of managing unstructured data at scale.

Governments globally are tightening data privacy laws, raising both the risks and financial stakes of non-compliance. According to DLA Piper (2022), GDPR fines totaled over €1 billion in 2021, representing a seven-fold increase from the previous year. These fines can reach €20 million or 4% of annual global revenue, whichever is greater, creating significant financial implications for organizations that fall short in privacy practices. CCPA penalties also have steep fines, with intentional violations reaching $7,500 and unintentional violations at $2,500 per occurrence (California Office of the Attorney General, 2020). The regulatory landscape has grown even more complex with Canada's Law 25 and PIPEDA, which mandate specific storage requirements to protect national data sovereignty (Privacy Commissioner of Canada, 2021).

Beyond regulatory penalties, data breaches have additional financial impacts. IBM's Cost of a Data Breach Report 2022 estimates the global average cost of a data breach at $4.35 million, encompassing recovery costs, customer attrition, and reputational damage (IBM, 2022). With breach costs rising, organizations are increasingly seeking robust privacy solutions to mitigate these risks effectively.

THE HIDDEN RISKS OF UNSTRUCTURED DATA

Without automated, AI-driven tools, unstructured data risks remain hidden, exposing organizations to significant compliance and breach risks.

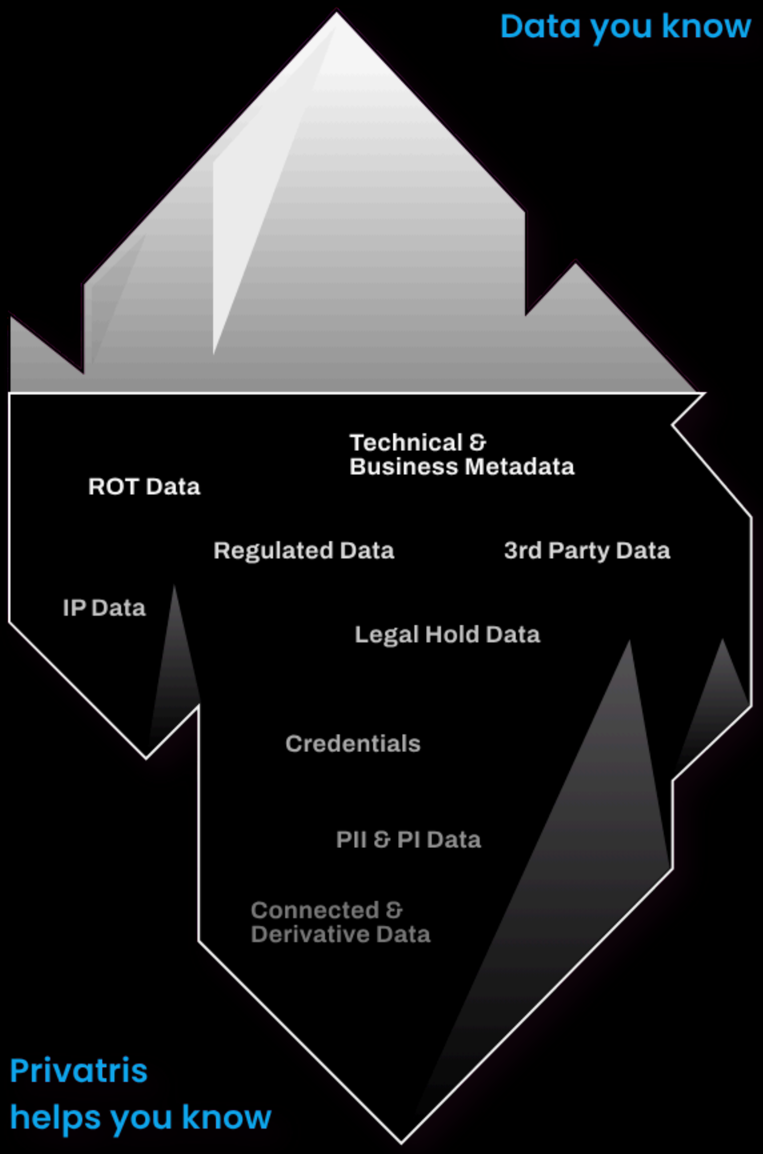


Figure 1: How Privatris can help organizations to comply with regulations

■ THE HIDDEN RISKS OF UNSTRUCTURED DATA

Unstructured data has become a central issue in privacy management:

1. Data Fragmentation and Visibility: Unlike structured data, unstructured data is fragmented across emails, chat logs, PDFs, and other free-form formats, making it difficult to locate sensitive information. Gartner (2022) reports that over 60% of companies struggle to identify and classify unstructured data, leaving them vulnerable to privacy risks.

2. Increasing Data Volume: Enterprises now handle an average of 300 terabytes of data, with nearly 90% of that data unstructured, per Veritas (2023). Manually managing such vast data volumes is unrealistic, prompting a shift toward automated solutions.

■ THE SHIFT TOWARD AI-DRIVEN PRIVACY SOLUTIONS

With traditional data management tools falling short, the demand for AI-driven privacy solutions has soared. MarketsandMarkets (2022) projects that the AI in Data Privacy Market will grow from **$5.2 billion in 2022** to **$13.3 billion by 2027**, with a CAGR(Compound Annual Growth Rate) of 20.6%. AI solutions can dynamically analyze complex unstructured data, enabling organizations to:

1. Automate Detection and Classification: AI systems use machine learning and natural language processing to scan and categorize sensitive data in varied formats, a task difficult for rule-based systems.

2. Offer Real-Time Compliance Monitoring: With real-time risk assessment and alerts, AI systems can help organizations proactively address privacy concerns, enabling immediate responses to compliance risks.

This evolution to AI-based privacy management represents a shift toward scalable, real-time solutions that address the challenges of unstructured data.

$25B

Projected Market Growth by 2033

120K

Canadian Businesses with Compliance Need

4%

Fine on worldwide turnover under Law 25

Data sovereignty remains a critical consideration, particularly in countries with stringent localization laws like Canada. Under PIPEDA and Law 25, Canadian organizations must store sensitive data domestically, ensuring data security within national boundaries. This trend reflects broader global concerns over data sovereignty, with 60% of U.S. companies similarly citing data localization as a key priority (Privacy Commissioner of Canada, 2021; MarketsandMarkets, 2022).

Privatris's on-premise deployment addresses these concerns by keeping all data within the client's ecosystem, helping clients meet localization requirements while minimizing the risk of third-party data exposure.

The privacy management market, valued at approximately $10 billion, is expected to grow to $25 billion by 2026, largely driven by regulatory demands and changing consumer expectations (MarketsandMarkets, 2022). According to Cisco's Consumer Privacy Survey, 81% of consumers state that they would disengage with a brand if they felt their data was being mishandled (Cisco, 2021). Effective privacy solutions are thus not only necessary for regulatory compliance but also for maintaining customer trust and loyalty.

As organizations confront the dual challenges of data volume and regulatory pressure, AI-powered privacy solutions like Privatris offer a comprehensive approach to unstructured data privacy. By addressing data sovereignty, compliance, and privacy risks, Privatris empowers organizations to secure sensitive information effectively, supporting both regulatory and operational requirements.

PROBLEM STATEMENT

Privacy laws, such as Law 25 in Quebec, PIPEDA across Canada, GDPR in the European Union, and CCPA in California impose strict requirements for handling personal information, regardless of its location or format.
Emails, scanned documents, images, spreadsheets, and cloud-stored files , which contain unstructured data, constitute a vast majority of today's organizational data. Unlike structured data, which is organized and easily searchable within databases, unstructured data lacks a consistent format, making it extremely difficult to identify and monitor.
This gap creates vulnerabilities that leave organizations exposed to severe compliance risks.

- **What are the key challenges in privacy compliance ?**

- **Hidden and fragmented data:** Sensitive information is often buried within free-form text, embedded in images, or dispersed across various systems and departments. This lack of visibility leaves organizations unaware of the extent and location of personal data, making it nearly impossible to enforce compliance.

- **Inadequacy of traditional tools**: Privacy management solutions have historically been designed for structured data, relying on rule-based detection and keyword searches. Such tools struggle with the complexity and inconsistency of unstructured data, leading to false negatives (missed detections) and false positives (irrelevant results), which hinder effective compliance.

- **Volume and diversity of data:** With organizations storing vast amounts of unstructured data across disparate platforms—emails, cloud storage, document management systems—manual oversight is impractical. The sheer scale and variation make it challenging to systematically detect and secure personal information.

- **Compliance complexity across jurisdiction:** Each regulation has its own unique provisions, including but not limited to :

Privacy Law Legal Requirements	Legal Requirements	How Privatris helps fulfill these requirements
GDPR (EU)	**Data Minimization:** Limit personal data processing to necessary purposes. **Data Subject Rights:** Provide access, correction, and deletion rights for personal data. **Data Privacy Impact Assessments (DPIA):** Assess high-risk data processing. **Breach Notification**: Notify authorities and individuals in case of a breach.	**Data Scanning and Categorization**: Identifies only necessary data within unstructured sources, ensuring compliance with minimization. **Data Subject Rights Support:** Tracks data locations for quick responses to access, correction, and deletion requests. **Continuous Risk Assessment:** Identifies high-risk processing activities, aiding DPIA compliance. **Breach Prevention and Response:** Detects vulnerabilities and provides tools for timely notification if breaches occur.

Privacy Law Legal Requirements	Legal Requirements	How Privatris helps fulfill these requirements
CCPA (California)	**Consumer Rights:** Allow access to, deletion of, and opt-out of data sales. Security: Implement adequate protections for consumer data. **Breach Notification:** Notify residents in case of significant breach risks.	**Consumer Data Management:** Categorizes consumer data for streamlined handling of access, deletion, and opt-out requests. **Data Security:** On-premise deployment secures data within the client's environment, meeting CCPA's security requirements. **Breach Prevention and Response:** Proactively monitors vulnerabilities and offers rapid response tools for managing breaches.
PIPEDA (Canada)	• **Consent:** Obtain informed consent for data collection. • **Access and Correction:** Provide individuals access to and correction of personal data.	• **Consent Tracking and Categorization:** Organizes data by consent type, supporting informed data processing. • **Access and Correction Support:** Facilitates easy retrieval of personal data for timely responses to access and correction requests.

Privacy Law Legal Requirements	Legal Requirements	How Privatris helps fulfill these requirements
	• **Breach Response:** Respond promptly to breaches to mitigate impacts.	• **Breach Mitigation Tools:** Detects vulnerabilities and offers quick response capabilities for breach incidents.
Law 25 (Quebec)	• **Privacy by Design:** Embed privacy protections in all data handling. • **Breach Notification:** Notify affected individuals and regulatory bodies of data breaches. **Accountability:** Ensure transparency and accountability in personal data handling.	• **Privacy by Default:** Integrates privacy measures at each data handling stage with an on-premise setup. • **Breach Documentation and Notification:** Logs data activity to support detailed breach documentation and prompt notifications. • **Continuous Risk Monitoring:** Assesses data handling risks, ensuring accountability and alignment with privacy obligations.

- **Operational and Security Vulnerabilities:** The dispersed nature of unstructured data across various systems and departments makes it difficult to enforce consistent privacy policies. This fragmentation heightens the risk of unauthorized access, unintentional exposure, and non-compliance with global privacy standards.

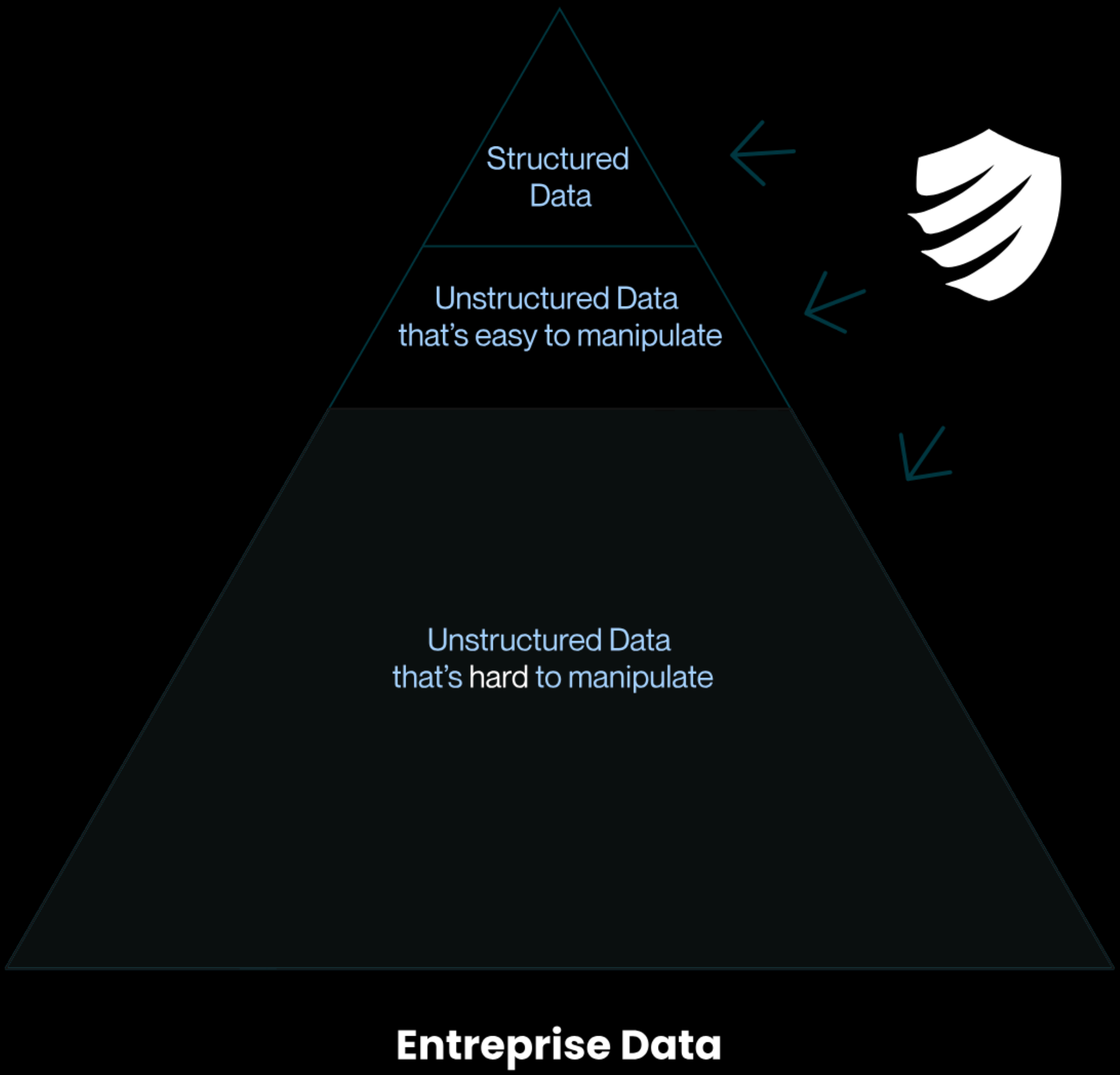

Structured Data
Unstructured Data that's easy to manipulate
Unstructured Data that's hard to manipulate
Entreprise Data

Figure 2: Types of data detectable by Privatris' solution

OUR APPROACH

Equipped with **400+ connectors**, our solution adapts to each organization’s unique data landscape, making compliance monitoring efficient and precise.

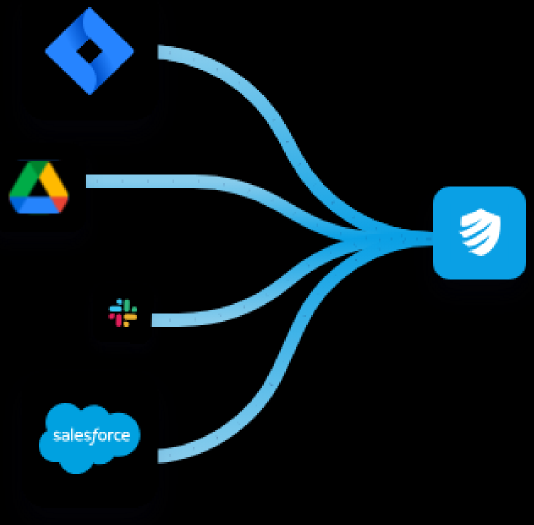
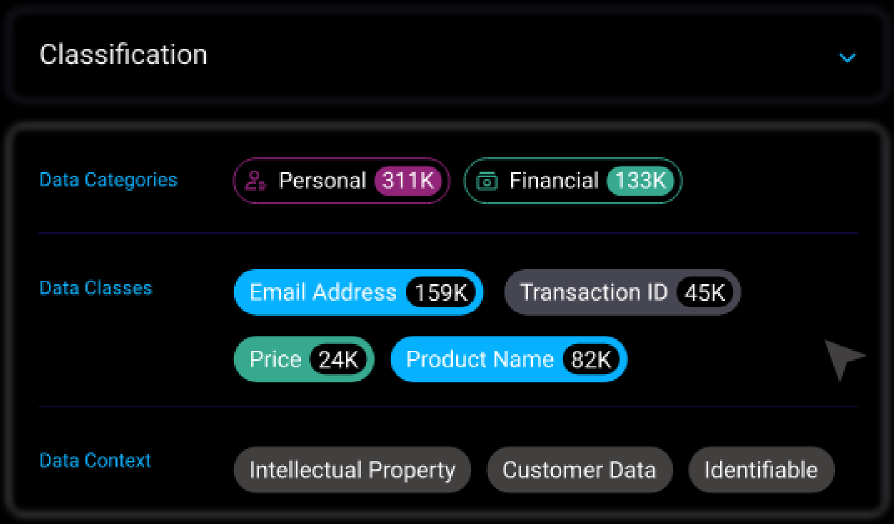


Figure 3: Effortless integration with hundreds of tools to streamline privacy management

Since all data processing occurs within the client’s ecosystem, organizations maintain full control and security over their sensitive information, reinforcing data protection and compliance without the need for external data transfers.

Here is our solution works :

1. **Discover & Scan :**
    a. **Our solution securely** scans networks for both **structured and unstructured personal** or sensitive data while keeping all information secure within its environment.
    b. Periodic scans can be scheduled to continuously monitor and **protect sensitive data with minimal effort.**



Classification

Data Categories: Personal 311K, Financial 133K

Data Classes: Email Address 159K, Transaction ID 45K, Price 24K, Product Name 82K

Data Context: Intellectual Property, Customer Data, Identifiable

Figure 4: Efficient data classification for precise insights and robust control

2. Analyze & Comply :
  a. All detected data is **categorized by sensitivity** (e.g., Tier 1: Highly Sensitive, Tier 2: Sensitive) based on compliance requirements.
  b. Our AI-powered risk assessment tool evaluates the overall privacy risk by generating a **risk score and recommendations for the data to address identified risks**. A risk score is calculated using several key elements such as data sensitivity , data volume, data distribution and existence of potentially dangerous combinations.
  c. Our user-friendly dashboard provides privacy officers with the ability to monitor privacy risks, track metrics, and generate compliance reports.

■ CASE STUDIES : TACKLING PRIVACY CHALLENGES

Desjardins Privacy Breach: How Privatris could have made a difference

Background:

In 2019, Desjardins, one of Canada's leading financial institutions, experienced a significant privacy breach. A malicious insider exfiltrated sensitive information of nearly 9.7 million individuals, including names, addresses, and financial details. This breach resulted in an estimated cost of $108 million CAD, with $70 million CAD attributed to the initial assessment and response phase. The incident underscored the need for robust data protection measures to prevent and manage privacy risks effectively.

How Privatris could have supported Desjardins:

1. Streamlined PII detection across environments:

- Privatris' AI-powered detection system would have scanned Desjardins' internal databases, cloud storage, and file systems to identify all instances of Personally Identifiable Information (PII). By providing a comprehensive inventory of sensitive data—including names, contact details, and financial information—our solution ensures full visibility into PII. This proactive approach helps mitigate risks by identifying vulnerabilities before they can be exploited.

2. Proactive risk management and data classification:

- Privatris' automated data classification capabilities would have categorized PII based on sensitivity and regulatory requirements. High-risk data could then be anonymized or masked to render it non-identifiable. This step reduces the impact of breaches by ensuring that exposed data remains unusable to unauthorized parties.

3. Incident containment and seamless integration:

- With real-time detection and seamless integration into Desjardins' existing security infrastructure, Privatris would have enabled rapid prioritization and containment of the breach. By isolating affected datasets and identifying exposed members' data promptly, our solution minimizes response times and reduces assessment costs.

4. Detailed audit trails for compliance and trust :

- Privatris generates audit-ready reports documenting every step of data management and breach response. For Desjardins, these detailed records would have demonstrated due diligence to regulators, maintained transparency with affected individuals, and reinforced trust during a challenging period.

Outcome: Enhanced privacy breach management and prevention

By leveraging Privatris, Desjardins could have implemented a robust privacy breach prevention and management framework. From detecting and classifying sensitive data to mitigating breach impacts and streamlining compliance efforts, Privatris offers a comprehensive solution. The result? Reduced financial and reputational risks, stronger regulatory alignment, and sustained customer trust.

Proactive Privacy Governance: Empowering a growing tech Startup

Background:

A rapidly scaling tech startup specializing in customer analytics faced mounting challenges in aligning with stringent privacy regulations, including GDPR, CCPA, and PIPEDA. With data sourced from diverse platforms, including emails, cloud storage, and customer feedback forms, the startup struggled to maintain visibility into sensitive data and meet compliance obligations. Manual efforts to locate and classify Personally Identifiable Information (PII) were time-consuming, error-prone, and inadequate for audits.

How Privatris supported the startup:

1. **Comprehensive data scanning across platforms:**
   - Privatris seamlessly integrated with the startup's data repositories, scanning unstructured data across email systems, cloud platforms, and internal documents. This automated process identified all instances of PII, such as email addresses, phone numbers, and behavioral data. The solution provided a complete inventory of sensitive data, categorized by risk level, ensuring full visibility into the data landscape.

2. **Automated data classification and sensitivity scoring:**

Privatris's AI-driven classification engine organized data into sensitivity tiers (e.g., Tier 1: Highly Critical, Tier 2: Sensitive). This enabled the startup to prioritize security measures for high-risk data, ensuring compliance with GDPR's data minimization and security principles.

3. Streamlined Response to Data Subject Requests (DSRs):

- With regulations requiring timely responses to Data Subject Requests (DSRs) for data access, correction and deletion. Privatris provided a centralized dashboard to locate relevant data efficiently. The solution reduced response times by 70%, ensuring the startup met regulatory deadlines while maintaining customer satisfaction.

4.**Continuous compliance monitoring & scalability to support growth:**

- Privatris offered real-time compliance insights, highlighting areas where the startup was at risk of non-compliance. Actionable recommendations included encrypting high-risk files, restricting access to sensitive data, and optimizing data retention policies.As the startup expanded its customer base and operations, Privatris scaled effortlessly to accommodate new data sources and jurisdictions. The flexible architecture ensured that compliance remained seamless, even as data volumes grew exponentially.

Outcome: A foundation for growth with Privacy built-in

By partnering with Privatris, the startup achieved:

- **Regulatory compliance**: Full alignment with GDPR, CCPA, and PIPEDA, avoiding potential fines and reputational damage.
- **Operational efficiency**: A 50% reduction in manual data management efforts, freeing resources to focus on core business objectives.
- **Customer trust:** Enhanced transparency and data handling practices, strengthening customer relationships and competitive positioning.
- **Scalability**: A privacy-first foundation that adapted to the startup’s growth, ensuring long-term sustainability.

■ CONCLUSION

Privatris stands as a pioneering solution, purpose-built to address these challenges by leveraging AI-driven capabilities for detecting, categorizing, and managing personal information within unstructured data.
By operating on-premise, Privatris not only provides clients with a powerful tool to maintain data sovereignty but also enables a secure, comprehensive view of privacy risks which is supported by real-time risk scoring and tailored compliance recommendations.

Through our approach, we empower organizations to transition from reactive data management to proactive privacy stewardship, transforming how they handle, secure, and comply with data protection requirements across industries. As demonstrated in our case studies, Privatris enables measurable improvements in efficiency, compliance responsiveness, and data protection, offering a tangible impact across sectors.

We invite you to explore how Privatris can support your organization’s privacy goals, help mitigate risks, and streamline compliance efforts. In a world where privacy expectations are higher than ever, Privatris provides the most advanced capabilities you need to navigate today’s complex privacy landscape with confidence and integrity.

Contact us to learn more and discover how Privatris can be a strategic asset in your privacy management.

REFERENCES

- California Office of the Attorney General. (2020). California Consumer Privacy Act (CCPA). Retrieved from California Consumer Privacy Act (CCPA)
- Cisco. (2021). Consumer Privacy Survey. Cisco Systems, Inc.
- DLA Piper. (2022). Data Protection Laws of the World: GDPR Fines. DLA Piper Global Data Breach Survey.
- Gartner. (2022). Top Trends in Privacy Management and Data Security. Gartner Inc.
- IBM. (2022). Cost of a Data Breach Report 2022. IBM Security.
- IDC. (2018). Data Age 2025: The Digitization of the World. International Data Corporation.
- MarketsandMarkets. (2022). AI in Data Privacy Market - Global Forecast to 2027. MarketsandMarkets Research Pvt. Ltd.
- Privacy Commissioner of Canada. (2021). PIPEDA and Canadian Privacy Standards. Office of the Privacy Commissioner of Canada.
- Veritas. (2023). Enterprise Data Management in 2023. Veritas Technologies LLC.