November 2021

Pathlock for Privacy & Data Protection

Enabling Continuous Privacy & Data Protection Compliance

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Pathlock for Privacy & Data Protection

Enabling Continuous Privacy & Data Protection Compliance

Personal Data Protection is a Challenge in Today's Dynamic Business

Privacy and personal data protection are a highly dynamic and moving target. Personal data is pervasive across the data and processes of an organization (e.g., financial data, employee data, customer data, patient data, and partner data). Privacy and data protection is about identifying and mitigating the compliance, brand, and business risks associated with processing personal data. It is about managing risks across the full lifecycle of data in the organization's web of business systems, processes, transactions, relationships, and interactions.

Privacy professionals struggle to interact with businesses to inventory personal data and ensure compliance to a set of requirements that are constantly evolving across business systems and processes. Continuously changing regulations and business environments encumber organizations as they aim to stay compliant. Trying to keep change in sync with growing, evolving, and shifting business needs and use of personal data bury privacy focused governance, risk management, and compliance (GRC) roles in mountains of tasks and processes in a struggle to keep pace with changes. Privacy is a significant GRC challenge that has specific requirements and associated content and processes that organizations should consider.

Consider that organizations are:

- **Distributed.** Organizations are a conglomeration of distributed operations and processes that are complicated by a web of business systems and data. This leads to an interconnected mesh of systems and transactions with varying privacy and data protection controls. The breadth of mergers, acquisitions, and expansion into new jurisdictions compound the distributed nature of the modern organization.

- **Dynamic.** Distributed operations and relationships are growing and changing as the organization attempts to remain competitive. Privacy risk environments of regulatory, legal, operational, and third-party risks are a moving target. The challenge with distributed organizations is that change is exponential and impacts many areas. A change in a process that uses personal data may intersect, impact, and/or conflict with changes in regulation or risk. An organization can go from being privacy compliant to non-compliant without knowing it.

- **Disrupted.** The intersection of distributed and dynamic operations brings disruption. Organizations manage high volumes of structured and unstructured

personal data across multiple systems, processes, and relationships in an attempt to stay compliant in a continuously changing environment. This disrupts the organization and slows it down at a time when it needs to be agile to remain competitive.

Organizations are confronting a growing array of complex rules and regulations that often look like an alphabet soup, resulting in managing privacy risk and keeping it in sync with organizational changes an increasingly critical burden. As privacy regulations and requirements pour out of all levels of governments, multinational organizations are dazed and overwhelmed in how to react when clarity is needed, when deadlines are not clear, and when audit and enforcement actions could be immediate or remain years in the future. This is particularly challenging when organizations operate across jurisdictions and must manage regulations on a global landscape, trying to meet the varying requirements in . . .

- Australia's Privacy Act
- Brazil's General Law for the Protection of Personal Data (LGPD)
- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Canada's Personal Protection in Electronic Documents Act (PIPEDA)
- EU Global Data Protection Regulation (GDPR)
- New Zealand's Privacy Act
- South Africa Protection of Personal Information Act (POPIA)
- US Fair Credit Reporting Act (FCRA)
- US Federal Trade Commission Act (FTCA)
- US Gramm Leach Bliley Act (GLBA)
- US Health Insurance Portability & Accountability Act (HIPAA)

. . . and that is scratching the surface of global privacy, state, and provincial laws.

Reactive, ad hoc, and manual assessments of privacy controls lead the organizations to inevitable problems as they fail to consistently and actively/continuously manage privacy risk across business systems and processes. Failure in privacy and data protection risk management comes about when organizations have:

- **Growing risk and regulatory concerns with inadequate resources.** Organizations are facing a barrage of growing privacy and legal regulatory requirements around the world. The organization is encumbered with insufficient processes and resources to manage privacy risk and requirements impacting the organization.

- **Silos of privacy oversight.** Monitoring privacy in different business systems and processes in different ways without any coordination, collaboration, or common technology architecture leads to greater privacy risk exposure. This leads to the unfortunate situation of the organization having no end-to-end visibility of privacy controls across the organization and its heterogenous business systems and processes.

- **Documents, spreadsheets, and email centric approaches.** When organizations assess privacy risk and controls in a maze of documents, spreadsheets, and emails, it buries risk and compliance management in mountains of data that is difficult to maintain, aggregate, and report on. Managing and reconciling documents and controls requires a tremendous amount of staff time and resources to consolidate, analyze, and report on privacy risk. When things go wrong, the organization is exposed as it lacks a robust audit trail of who did what, when, how, and why.

- **Inability to actively and continuously assess privacy controls.** Privacy control assessments are often only done on a cyclical calendar schedule to validate that the organization has everything in place to meet data protection requirements. This approach fails to recognize that additional privacy risk and compliance exposure can occur at any time with any change to business systems and processes.

THE BOTTOM LINE: Privacy and data protection compliance requires an integrated process and architecture to provide full situational awareness of privacy controls across business systems, processes, and transactions. Organizations that attempt to manage this in documents, spreadsheets, and emails will find that this approach will lead to inevitable failure. The organization ends up spending more time in data management and reconciling, as opposed to continuous privacy risk and control monitoring and active data protection enforcement. Organizations should implement processes and technology that can continuously document, monitor, enforce, and ensure privacy controls in the context of a distributed and dynamic business system environment.

Enabling the Core of Privacy & Data Protection Compliance

Pathlock's solution for privacy and data protection is a solution in the GRC market that GRC 20/20 has researched, evaluated, and monitored over years. By enabling collaboration, accountability, and process automation for privacy compliance and control automation, Pathlock addresses the range of privacy related compliance processes across heterogenous business systems and processes to ensure complete situational awareness and enforcement of privacy and data controls across the enterprise. This delivers greater efficiency, effectiveness, and agility for privacy compliance and broader GRC management processes.

Pathlock, for privacy and data protection, gives organizations full insight into employee, customer, and partner data protection and controls across business systems. Pathlock supports integration for control monitoring, enforcement, and assurance across over 140 business systems (both on-premise and cloud). Where traditional privacy and protection solutions focus on a single application or business system, providing a siloed and incomplete view, Pathlock delivers a 360° view of privacy across all sensitive data including systems, transactions, and interactions of data.

The Pathlock platform provides an intuitive solution that integrates with other business systems and applications to replace manual privacy control processes encumbered by documents, spreadsheets, and emails. The solution increases efficiency, effectiveness, and agility in documenting, monitoring, assessing, and providing assurance on privacy and data protection controls across business systems. The Pathlock solutions can be used in organizations of various sizes and across industries. The solution is highly agile and intuitive to meet the privacy compliance management needs of a range of business functions, while providing the right information architecture to integrate with a variety of business systems to continuously and actively enforce privacy controls at the enterprise level down into departments and processes.

What the Pathlock Solution for Privacy & Data Protection Does

GRC 20/20 has evaluated the features and capabilities of the Pathlock solution and finds that it delivers an integrated and harmonized privacy control management information and technology architecture that integrates to enforce controls across business systems and processes. Pathlock provides an agile solution that is adaptable to the organization's business systems across employee/HR management (e.g., Workday), financial transactions (e.g., SAP, Oracle), partners (e.g., Ariba), patients (e.g., Epic, Cerner) and customer relationship management (e.g., Salesforce.com). The solutions can grow with the privacy requirements and controls of the organization as they change, and processes evolve.

The Pathlock platform is a solution that can grow and expand with the organization and adapt as the organization and its environments change. It can be easily implemented to meet privacy requirements of a single jurisdiction or business system for organizations starting off on their privacy journey or can be implemented as a backbone of an

enterprise privacy architecture to monitor and enforce controls across a heterogenous business environment. The Pathlock solution is designed to make privacy compliance and control management processes efficient, effective, and agile in a dynamic business environment. Pathlock enables the full privacy compliance lifecycle of the organization.

Foundational Privacy Capabilities Delivered in the Pathlock Solution

The Pathlock solution scales from the small organization with limited privacy compliance processes and resources to global organizations that support privacy and data protection compliance around the world. Specifically, it includes the following capabilities:

- **Discovery.** The Pathlock solution enables the organization to identify and inventory personally identifiable and sensitive information across business systems. The solution supports integration with over 140 different business systems in use today. This is an ongoing process of discovery to ensure that the inventory of data is complete and accurate as the business, its systems and processes change.

- **Classification.** Once an inventory has been gathered, the Pathlock solution then creates and maps a universal data catalog of the organization in context of personal and sensitive information. This map includes where and how this data is stored and used across the range of an organizations diverse business systems and processes, enabling and delivering data and risk classification.

- **Universal Controls.** Pathlock allows the organization to have complete visibility into a singular and universal catalog of controls that can be enforced to personal and sensitive information wherever it rests in the organization. This allows for a consistent approach to privacy control documentation and assurance across data stores and compliance frameworks.

- **Monitoring & Enforcement.** Through agile data rules, Pathlock allows the organization to define business processes and system/technical rules to enforce preventive, detective, and responsive privacy controls to specific business systems and assets. This includes the ability to provide for control issue communications, the triggering of workflows and tasks, and responsive processes to lock accounts, mask/encrypt data, and more.

- **Assurance.** The Pathlock solution enables the organization to provide a complete system of record of user and process activity logs, transactions, and interactions for compliance evidence and/or forensic purposes should there be a breach.

- **Remediation.** When privacy control issues are found, or incidents happen, the Pathlock solution engages the ability to track and monitor response and remediation activities through to completion.

- **Reporting & Dashboards.** Pathlock enables ongoing privacy reporting and accountability to senior management functions and operational personnel to ensure privacy control compliance and assurance continuously. Control

effectiveness can even be sent to enterprise GRC platforms in real-time for organization-wide compliance reporting.

Benefits Organizations Receive with Pathlock

Pathlock clients move to this solution because they find that their manual document-centric approaches for privacy compliance consumed too many resources, and things were going to slip through cracks as they started addressing more and more privacy control requirements across business systems. Organizations considering Pathlock should find value in the ongoing cost of ownership, the speed of integration, return on investment, and improved effectiveness and agility to reliably achieve objectives while reducing uncertainty and privacy risk exposure.

Specific benefits that clients of Pathlock should expect are:

- *360° visibility into privacy control management* - where all privacy control information is in one place and gives complete situational and contextual awareness of privacy compliance in context of business operations and processes.
- *Centralization and communication of privacy information* for the organization, and the ability to maintain this information consistently across the organization.
- *Reduction in tasks and increased automation* related to manual privacy compliance work that often slips through cracks.
- *Easy access to reviews and approvals* that are centralized and easier to perform.
- *Ability to establish rules that streamlines privacy* control management across business systems.
- *Strength of the audit trail, and system of record* on what actions were performed and by who, on what date and time.
- *Elimination of hundreds to thousands of documents, spreadsheets, and emails* and the time needed to monitor, gather, and report on them to manage privacy control related activities and processes.
- *Significant efficiencies in time* through automation of workflow and tasks as well as reporting.
- *Increased awareness and accountability of privacy* by business owners who are informed on risk in context of their role.
- *Greater assurance to board and stakeholders* that privacy is properly understood and managed in context of the organization's objectives and strategy.

- *Consistency and accuracy of privacy information* as the organization conforms to consistent processes and information structures. It has increased quality of information that is more reliable and improves decision making.

- *Increased agility in context of change* that enables the organization to be proactive, and not just reactive - leading to less exposure and being caught off-guard.

- *Greater integrity in business processes* that ensures privacy controls are current within those processes.

- *Meet privacy requirements and avoid penalties* through active and continuous privacy control monitoring, enforcement, and assurance.

Considerations in Context of the Pathlock Solution

Every solution has its strengths and weaknesses, and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of Pathlock to enable organizations to achieve consistent privacy control management and enforcement processes, readers should not see this as a complete and unquestionable endorsement of Pathlock. The point is that any organization engaging a GRC solution provider, including Pathlock, needs to do their homework to ensure that they clearly understand what it is they need and are engaging the right solution provider to deliver on those needs.

The Pathlock solution for privacy and data protection has the capability to manage privacy across a range of business systems, processes, and transactions that makes them stand out among competitors. Overall, clients have shown a high degree of satisfaction with their use and implementation of Pathlock and find the solution to be agile and responsive to their privacy control documentation and automation requirements. The solution is flexible and adaptable to privacy specific programs as well as broader enterprise GRC control automation – from the large global enterprise to the small-localized organization. This is done by protecting personal and sensitive information from the inside out; where it is stored and used in business systems and processes.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com