November 2017

Mitratech PolicyHub

Addressing Policy Management in Context of GDPR

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

The Challenge of GDPR 4

Mitratech PolicyHub 5
- Addressing Policy Management in Context of GDPR 5
- What PolicyHub Does 7
- Benefits Organizations Have Received with PolicyHub 9
- Considerations in Context of PolicyHub 11

About GRC 20/20 Research, LLC 12

Research Methodology 12

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.

Mitratech PolicyHub

Addressing Policy Management in Context of GDPR

The Challenge of GDPR

As the years go by, there is increasing focus on the protection of personal information around the world. Over time we have seen US HIPAA, US GLBA, Canada's PIPEDA, the EU Data Protection Directive 95/46/EC, and others around the world. The latest, most comprehensive, and the one that is the front and center of concern to organizations is the EU General Data Protection Regulation 2016/679 (GDPR), which replaces the former directive. While this is an EU regulation, it has a global impact. Organizations interacting with EU citizen data no matter where they operate need to pay very close attention to compliance.

The GDPR strengthens and unifies data protection of individuals in the EU. Where the former directive required each country to pass national legislation that was not consistent, the GDPR is a regulation and not a directive and does not require further national legislation.

Full compliance for organizations starts May 25, 2018, and applies to any organization that stores, processes, or transfers the personal data of EU residents. It does not matter if the organization resides in the EU. Fines can be stiff, going above €20 million or 4% of global revenues of an organization, whichever is greater.

The regulation defines personal data as: "Personal data is any information related to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

To be compliant and mitigate the risk of data protection incidents, organizations should:

- **Establish a Data Processing Officer.** In fact, this is required in the regulation (Articles 37-39) for all public authorities and organizations that are processing more than 5,000 data subjects in a 12-month period. This role is also called a Chief Privacy Officer.

- **Define & Communicate Policies & Procedures with Training.** The foundational component of any compliance program is outlining what is expected of individuals, business processes, and transactions. This is established in policies and procedures that need to be communicated to individuals and proper training.

- **Document Data Flows & Processes.** Organizations should clearly document how individual data is used and flows in the organization and maintain this documentation in context of organization and process changes. This is a key component of managing information assets of individuals.

- **Conduct Privacy Impact Assessments.** The organization should do regular privacy impact assessments to determine risk of exposure of personal information. When events occur, the regulation specifically requires (Article 35) a data protection impact assessment.

- **Implement, Monitor & Assess Controls.** Define your controls to protect personal data and continuously monitor to ensure these controls are in place and operating effectively.

- **Prepare for Incident Response.** The regulation requires data breach notification to supervisory authorities within 72 hours of detection. Organizations need defined processes in place and be prepared to respond to, contain, and disclose/notify of breaches that occur in the organization.

- **Ensure Your Third Parties are Compliant.** Many data protection breaches happen with third-party relationships (e.g., vendors, contractors, outsourcers, and service providers). Organizations need to make sure their third parties are compliant as well and follow strict policies and controls that are aligned with the organizations policies and controls.

This is a complete program that needs to be managed on a continuous basis to be compliant and minimize risk of exposure in the GDPR regulation. Organizations that attempt to manage this in documents, spreadsheets, and emails will find that this approach will lead to inevitable failure. Manual spreadsheet and document-centric processes are prone to failure as they bury the organization in mountains of data that are difficult to maintain, aggregate, and report on, consuming valuable resources. The organization ends up spending more time in data management and reconciling as opposed to active data protection risk monitoring.

The Bottom Line: To address GDPR, organizations should avoid manual processes encumbered by documents, spreadsheets, and emails. They should look to implement a policy management solution that can manage the communication, compliance, and awareness of GDPR requirements and processes consistently and continuously in the context of a distributed and dynamic business.

Mitratech PolicyHub

Addressing Policy Management in Context of GDPR

Mitratech PolicyHub 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 policy management, Mitratech addresses policy management in

context of GDPR compliance and delivers effectiveness, efficiency, and agility to policy management processes.

The PolicyHub solution scales from the small organization with limited policy management requirements to global organizations that support policies around the world. Specifically, it enables:

- ***Policy lifecycle workflow process*** to ensure effective GDPR communication and implementation of policies across the organization.
- **Integration with common desktop word processing tools** so employees can develop GDPR related policies in the tools they already know how to use.
- ***Streamlined and efficient user experience*** that enagages all levels of the organization on GDPR policies.

Effective implementation of GDPR related policy starts with the manner in which the policies and procedures are written, and the PolicyHub solution enables this. The extent to which the policies have been understood and implemented by employees can be ascertained through configurable surveys, certifications, self-assessments, and questionnaires.

In context of researching PolicyHub, GRC 20/20 has interviewed several PolicyHub clients and finds that the solution has helped these organizations be efficient, effective, and agile in managing and communicating policies in complex and dynamic environments. PolicyHub is being used in organizations of various sizes and across industries and geographies. The solution is highly agile and intuitive to meet the policy management needs of a range of departments while providing the right information architecture to aggregate and see policies at the enterprise level across departments and processes.

GRC 20/20's evaluation, research, and interactions with PolicyHub clients has determined the following:

- **Before PolicyHub:** Clients of PolicyHub typically are replacing manual processes for policy management that are encumbered by documents, spreadsheets, and emails. Such approaches can be very manual, time-consuming, and prone to errors, particularly in aggregation and reporting on policy data that involves hundreds to thousands of documents and spreadsheets.
- **Why PolicyHub:** Organizations choose PolicyHub as they are looking for a single integrated information architecture to automate and manage policy management processes. They are looking for a single information architecture that can handle an array of policy management requirements, like GDPR. Clients state they chose PolicyHub as the acquisition, implementation, and ongoing maintenance costs were cheaper than the competition and it is easy to maintain and configure to their environments.

- **How PolicyHub is used:** PolicyHub's breadh of use cases is impressive, and exceeds much of its competition. Typical use cases for PolicyHub include:
  - GDPR policies and procedures
  - Code of Conduct
  - Other privacy related policies
  - IT security policies
  - HR policies
  - Anti-bribery and corruption policies
  - Certifications and attestations to policies
  - Vendor/supplier related policies
  - Quarterly questionnaires and attestations
- **Where PolicyHub has excelled:** Organizations consistently state that PolicyHub has improved the quality of their policy management related proceses and information. This improves the organization's overall visibility into policy management while eliminating the overhead of managing manual processes encumbered by hundreds to thousands of spreadsheets, documents, and emails. Clients find that the solution is flexible to adapt to their organization's breadth of policy management requirements, has the core capabilities needed, and provides them the ability to grow and mature their program over time. Overall, users find the solution fast to deploy and agile to meet diverse policy management process requirements.

What PolicyHub Does

GRC 20/20 has evaluated the features and capabilities of the PolicyHub solution set and finds that it delivers an integrated and harmonized policy management information and technology architecture to meet a wide range of policy management use cases, including GDPR. PolicyHub provides an agile solution that is adaptable to the organization's current requirements and grows with the organization as requirements change and processes evolve. The solution enables policy management programs at any level of the organization, whether for departments or enterprise-wide policy management programs.

PolicyHub 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 simplistic policy management requirements for organizations just beginning a GDPR and broader policy management journey. PolicyHub is designed to make policy management processes efficient, effective, and agile in a dynamic business environment. PolicyHub

enables the full policy management lifecycle of the organization from policy authoring, approval, communication, monitoring, and tracking to the maintenance of policies.

Foundational Capabilities Delivered in PolicyHub

GRC 20/20 finds that PolicyHub has the core capabilities to address policies in context of GDPR as well as for a broader enterprise policy management platform that scales from the small organization or department needs to a global enterprise. This includes:

- **Operationalizing policy management:** PolicyHub's approach to policy management integrates with standard Microsoft applications like Word to allow policy creation in the tools users know and work with every day while controlling the process through standardized templates, automation/task management, and workflow.

- **Content management:** PolicyHub is built on Mitratech's established content management engine and leverages these abilities to provide a robust solution to manage versions of policies across time. The content management component of the policy management system provides support for a range of document types as well as metadata (e.g., relevant dates, jurisdictions, programs, business units, vendors, status, and retention criteria). It also provides version control, audit trails, document links, and search capability.

- **Organization management:** All policies apply to something within the organization, whether it is a business process, a physical asset, an information asset, a business relationship, or the entire organization. PolicyHub enables the organization to map policies to where they apply.

- **Technology integration:** Policy management systems often require information from human resources, vendor management systems, and other sources to automatically maintain a single record. The PolicyHub solution allows for integration with LDAP directories and other enterprise applications.

- **Accessibility & Internationalization:** Policies are only of value if they are accessible. A policy management system must provide a complete system of record any individual can log into and find policies that apply to their role, along with required tasks, attestations, and training they must complete. PolicyHub supports internationalization capabilities to present user interfaces in different languages and meet the accessibility needs of a global organization. PolicyHub currently supports twenty-two different languages on its platform.

- **Workflow:** Core to the PolicyHub platform is workflow so policies, people, and process elements are accounted for as part of the overall policy management process. Automating workflow helps manage and monitor accountability and coordinate responsibilities in all phases of policy lifecycle management. Automating workflows is also valuable in creating audit trails and providing metrics for workloads, delays, assignments, and other measures to help manage resources, cost, and risk.

- **Task management:** The PolicyHub solution tracks a variety of tasks at different stages of execution — drafting policies or procedures, providing approvals, handling exceptions, and performing policy reviews. The solution provides a collective overview of each individual's task list, including outstanding work items, due dates, and reminders of upcoming activities. It also escalates overdue tasks to the appropriate oversight and management personnel.

- **Notifications:** In PolicyHub, notifications are delivered when policy authors receive a new work assignment, when a due date draws near, or when a task is overdue and an escalation notice must be sent to management. It notifies individuals a person, or whole business units, when they have a need to read and attest to a policy, with built-in reminders and escalation. The PolicyHub solution provides configuration capabilities to customize messages, provide links to tasks, consolidate notifications, and help enforce goals, plans, and accountability. Notifications integrate with the organization's email system to deliver messages and drive accountability.

- **Audit trail:** If it is not documented, it is not done. Within PolicyHub a robust audit trail records each who, what, where, and when for every document, assignment, person, and piece of content collected, developed, changed, distributed, archived, surveyed, notified, and read. This ensures that when an incident occurs, an audit takes place, or a regulatory exam or investigation happens, you are prepared with accurate and timely evidence.

- **Policy relationships:** The PolicyHub solution enables cross-referencing and linking of related and supporting policies and procedures so users can quickly navigate to what they need to understand.

While PolicyHub has the core components of a policy management platform, what really sets the company apart is their customer service. Every client GRC 20/20 has interviewed and interacted with has raved about the responsiveness of Mitratech and how easy they are to work with. Mitratech excels at building strong client relationships and partnering with their clients to not only see that issues are resolved but also that features are built into new versions of the product. Clients are actively engaged as part of PolicyHub and feel vested in the product maturity and growth.

Benefits Organizations Have Received with PolicyHub

Most PolicyHub clients that GRC 20/20 has researched and interviewed moved to the solution because they found their manual document-centric approaches consumed too many policy management resources and they found things were slipping through cracks in the continuous barrage of policy management as well as regulatory and business change. Across these clients, there is consistent praise for the value of the ongoing cost of ownership in the speed of deployment and return on investment improved effectiveness and agility to reliably achieve objectives while reducing uncertainty and risk.

Specific benefits that clients of PolicyHub have told GRC 20/20 they have achieved in their implementations are:

- *360° visibility into policy management* where all policy information is in one place and gives complete situational and contextual awareness of policies in context of objectives and processes.
- *Centralization and communication of policies* to employees, and maintain them consistently for the organization.
- *Reduction in tasks and action items* related to policy management slipping through cracks.
- *Easy access to reviews and approvals* that are centralized and easier to perform.
- *Ability to establish templates* and a standard "policy on writing policies" that streamlines policy management.
- *Adaptability to change* in the business environment.
- *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 GDPR and other policy management related activities and processes.
- *Significant efficiencies in time* through automation of workflow and tasks as well as reporting.
- *Increased awareness and accountability of policies* by business owners who informed on risk in context of their role.
- *Greater assurance to board and stakeholders* that GDPR related policies be properly understood and managed in context of the organization's objectives and strategy.
- *Consistency and accuracy of GDPR and policy 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.
- *Accountability with full audit trails* of who did what and when; particularly this has delivered value in fewer things slipping through the cracks.
- *Reduction in headcount needed to govern and manage policies* that are freed from manual processes.

- *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.

Considerations in Context of PolicyHub

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 PolicyHub to enable organizations to achieve consistent GRC management processes, readers should not see this as a complete and unquestionable endorsement of PolicyHub. The point is that any organization engaging a policy management solution provider, including Mitratech, 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.

PolicyHub has the core components of an enterprise policy management platform. There are advanced features in policy management that the platform does not have such as a fully integrated learning management system (LMS) which GRC 20/20 is seeing come up more frequently in RFPs. The solution itself is fully integrated with the Microsoft Office suite which is something many clients and prospects praise it for while others find it limiting in non-Microsoft environments.

Overall, clients have shown a high degree of satisfaction with their use and implementation of PolicyHub for GDPR and broader policy management implementations and find the organization to be agile and responsive to their issues and needs. They find that the solution is agile by allowing distributed functions to get what they need when they need it. Across interviews, clients reported the professionalism and ease of engagement with Mitratech in context of PolicyHub. GRC 20/20 finds that PolicyHub has delivered on the core requirements for GDPR policies as well as a broader enterprise policy management platform. The solution is flexible and adaptable to policy management processes from the large global enterprise to the small-localized organization. It is built on a robust enterprise content management engine that is owned by Mitratech and has matured over years. Clients praise the platform for its simplicity and ease of use, and have further praise for the company itself in its support and responsiveness to client issues and requests. PolicyHub delivers value by delivering the right features to get the GDPR compliance job done through a solution that is easy to use for policy managers, authors, and most importantly the policy readers.

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