October 2018

SureCloud GDPR Suite

Agile & Efficient GDPR 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.

SureCloud GDPR Suite

Agile & Efficient GDPR Compliance

Personal Data Protection is a Challenge in Today's Environment

Privacy and personal data protection is a highly dynamic and moving target. Personal data is pervasive across the data and processes of an organization (e.g., employee data, customer data, and sales data). Privacy management 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 an organization and its web of processes, transactions, relationships, and interactions. This is particularly challenging when organizations operate across jurisdictions and have to manage regulations on a global landscape, particularly with broad regulations such as the EU Global Data Protection Regulation (GDPR).

Privacy professionals struggle to interact with businesses to inventory all uses of personal data and ensure compliance to a set of requirements that are constantly evolving. 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 third-party relationships and interactions. This leads to an interconnected mesh of relationships and transactions that clouds privacy boundaries. 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.

Organization's 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, 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.

GDPR Adds to the Complexity of Privacy Compliance

As the years go by, there is increasing focus on the protection of personal identity information around the world. Over time we have seen new regulations such as US HIPAA, US GLBA, Canada's PIPEDA, the EU Data Protection Directive 95/46/EC etc.. The latest 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. All organizations – wherever they are in the world – that own or process the personally identifiable information (PII) of EU data subjects must comply with the Regulation. GDPR is not sector-specific, unlike privacy laws in other parts of the world (notably the US and Canada). It applies in all contexts and across all sectors. It is extra-territorial, meaning it applies everywhere in the world (so long as an EU data subject PII is involved).

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 organizational and process changes. This is a key component of managing information assets of individuals.

- **Conduct Data Privacy Impact Assessments.** The organization should do regular privacy impact assessments to determine risk of exposure to non-compliant management of personal identity information. When events occur, the regulation

specifically requires (Article 35) a data protection impact assessment. A new data privacy impact assessment is required if there is a change in the nature, scope, context, or purposes of the organization's processing of PII.

- **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 or those that may have occurred by the data processor.

- **Data Privacy by Design.** Each new service or business process that makes use of personal identity information within your organization must take the protection of such data into consideration when designing new or updating operational processes and technology builds.

- **Ensure Third Parties are Compliant.** Many data protection breaches happen with third-party relationships (e.g., vendors, contractors, outsourcers, law firms, 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. These data processors now have legal liability under GDPR and have direct legal compliance obligations. One additional requirement is the data processor cannot use a 'fourth party' to process any personal identity information without obtaining prior authorization from their client (i.e. data controller).

GDPR compliance is a complete program that needs to be managed on a continuous basis to minimize risk of exposure. 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 solution that can oversee ongoing GDPR requirements and processes to manage compliance consistently and continuously in the context of distributed and dynamic business.

Agile & Efficient GDPR Compliance

SureCloud's GDPR Suite 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 GDPR compliance, SureCloud addresses the range of GDPR related compliance processes and delivers effectiveness, efficiency, and agility to GDPR compliance and broader GRC management processes.

SureCloud is a GRC solution provider headquartered in London. The SureCloud Platform provides an intuitive and easy to use solution to replace manual processes encumbered by documents, spreadsheets, and emails. The solution is offered in a secure cloud Software as a Service environment. The GDPR Suite is a packaged offering on the SureCloud Platform, focused specifically on privacy and data protection compliance in context of GDPR and similar regulations around the world. Organizations can deploy the GDPR Suite for just GDPR compliance, but can also expand their implementation to the full range of the SureCloud Platform's GRC capabilities, which include:

- Information Asset Management
- Compliance Management
- Incident Management
- Internal Audit
- Policy Management
- Risk Management
- Third Party Risk Management
- Vulnerability Management

In context of researching SureCloud's GDPR Suite, GRC 20/20 has interviewed GDPR Suite clients and finds that the solution has helped these organizations increase efficiency in managing GDPR compliance in complex and dynamic environments. The GDPR Suite is being used in organizations of various sizes and across industries. The solution is highly agile and intuitive to meet the GDPR compliance management needs of a range of business functions, while providing the right information architecture to aggregate and see compliance at the enterprise level across departments and processes.

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

- **Before GDPR Suite:** Clients of the GDPR Suite typically are replacing manual processes for GDPR compliance 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 data that involves hundreds to thousands of documents and spreadsheets.

- **Why GDPR Suite:** Organizations choose the GDPR Suite as they are looking for a single integrated information architecture to automate and manage GDPR compliance management processes. Clients state they selected the GDPR Suite as the solution is highly intuitive and the acquisition, implementation, and ongoing maintenance costs were cheaper than the competition, and it is easy to maintain and configure to their environments.

- **How GDPR Suite is used:** The GDPR Suite's breadth of use cases is impressive. Typical use cases for GDPR Suite include:

  - GDPR & data protection program management
  - Data mapping
  - Data transfers
  - Data protection impact assessment
  - Incident management
  - Data access requests

- **Where GDPR Suite has excelled:** Organizations consistently state that the GDPR Suite has improved the quality of their GDPR compliance management related processes and information. This improves the organization's overall visibility into GDPR compliance, 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 requirements, has the core capabilities needed for GDPR compliance, and provides them with the ability to grow and mature their program over time to other GRC related areas. Overall, users find the solution intuitive to use, fast to deploy, and agile to meet diverse compliance process requirements.

What the GDPR Suite Does

GRC 20/20 has evaluated the features and capabilities of the SureCloud GDPR Suite and finds that it delivers an integrated and harmonized GDPR management information and technology architecture to meet the requirements of a complete GDPR compliance management program. The GDPR Suite 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 GDPR compliance programs in organizations of all sizes and complexity.

The GDPR Suite, and broader SureCloud GRC 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 just GDPR requirements for organizations starting off on their GDPR journey, or can be implemented as a backbone of a broader enterprise GRC program. The GDPR Suite is designed to make GDPR compliance management processes efficient, effective, and agile in a dynamic business environment. SureCloud enables the full GDPR compliance lifecycle of the organization.

Foundational Capabilities Delivered in the GDPR Suite

The GDPR Suite scales from the small organization with limited compliance processes to global organizations that support privacy and data protection compliance around the world. Specifically, it includes the following applications (where an organization deploys the ones relevant for their organization's GDPR obligations):

- **GDPR Program Tracker.** This manages the entire spectrum of GDPR compliance from beginning to end, and is the backbone of the other capabilities to bring things together. Organizations start with a GDPR gap analysis, then identify and monitor GDPR risk, which then enables them to facilitate ongoing GDPR compliance.

- **GDPR Discovery.** SureCloud's GDPR Discovery data inventory solution allows an organization to kick-start their data gathering exercise through a simple set of questions - which can either be disseminated to functional heads via a questionnaire or completed in a workshop environment. The questions are designed to capture key data inventory elements, such as business processes, information assets, and systems.

- **GDPR Management.** The GDPR Suite comes with pre-packaged templates, controls, and forms to facilitate GDPR compliance. These enable the organization to automate the processing of GDPR related records, conducting data protection impact assessments, as well as facilitating subject access requests and data transfers.

- **Information Asset Management.** This module in the GDPR Suite is used to document and manage the data inventory of personal data - where and how it is used, data ownership, data mapping and process flows.

- **Compliance Management for GDPR.** It is with this module that organizations monitor ongoing GDPR compliance to defined requirements. This allows the organization to implement and monitor controls related to GDPR, and then demonstrate/validate compliance to GDPR requirements and controls

- **Risk Management for GDPR.** SureCloud's GDPR suite enables the documentation, management, monitoring, and mitigation of privacy related risks. This allows the organization to understand the range of privacy issues that could develop, document risks to rights and freedoms of individuals, and measure likelihood and severity of privacy related risk exposure.

- **Incident Management GDPR.** With this module, organizations document events and issues, and manage incidents related to GDPR and data protection. This module allows the complete documentation of evidence of incidents, identification of root causes, and manages the process report breaches as required by the regulation.

While not a part of the core GDPR Suite, the following modules in the broader SureCloud GRC Platform further enable a complete GDPR compliance program:

- **Policy Management.** With this organizations can manage the authoring, approval, communication, and awareness of GDPR related policies to the spectrum of employees that interact with personal data of EU citizens.

- **Third Party Management.** Here organizations can govern and manage the range of third party relationships (e.g., vendors, contractors, consultants, service providers, outsourcers etc.) that interact with GDPR related data in context of the services the organization engages them for.

Benefits Organizations Have Received with the GDPR Suite

Most SureCloud GDPR Suite clients that GRC 20/20 has researched and interviewed moved to the solution because they found that their manual document-centric approaches for compliance consumed too many resources, and things were going to slip through cracks as they started addressing GDPR compliance requirements. Clients consistent praise for the value of the ongoing cost of ownership, the speed of deployment, return on investment, and improved effectiveness and agility to reliably achieve objectives while reducing uncertainty and risk.

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

- *360° visibility into GDPR compliance management* - where all GDPR information is in one place, and gives complete situational and contextual awareness of GDPR compliance in context of business operations and processes.

- *Centralization and communication of GDPR information* for the organization, and the ability to maintain this information consistently across the organization.

- *Reduction in tasks and action items* related to GDPR slipping through cracks.
- *Easy access to reviews and approvals* that are centralized and easier to perform.
- *Ability to establish templates that streamlines GDPR* compliance management.
- Adaptability to a changing 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 management related activities and processes.
- *Significant efficiencies in time* through automation of workflow and tasks as well as reporting.
- *Increased awareness and accountability of GDPR* by business owners who are informed on risk in context of their role.
- *Greater assurance to board and stakeholders* that GDPR is properly understood and managed in context of the organization's objectives and strategy.
- *Consistency and accuracy of GDPR 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 GDPR 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 the GDPR Suite

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 SureCloud's GDPR Suite to enable organizations to achieve consistent GDPR management processes, readers should not see this as a complete and unquestionable endorsement of SureCloud or the GDPR Suite. The point is that any organization engaging a GRC solution provider, including SureCloud, 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 GDPR Suite has the core components of a complete and effective GDPR compliance management program. There are advanced features that the broader SureCloud GRC platform further offers to extend this, and builds a foundation for the organization to grow upon.

An area clients would like to see SureCloud address is the capture of older forms and data, so that when forms get updated or changed, old incidents and registers of data remain accurately intact. SureCloud has recognized this and is now in the process of rectifying the issue.

Overall, clients have shown a high degree of satisfaction with their use and implementation of the GDPR Suite and GRC management implementations, and find the organization to be agile and responsive to their issues and needs. Across interviews, clients reported the professionalism and ease of engagement with SureCloud. The solution itself is flexible and adaptable to GDPR specific programs as well as broader enterprise GRC processes - from the large global enterprise, to the small-localized organization. SureCloud delivers value by delivering the right features to get the GDPR compliance job done through a solution that is easy to use for GRC professionals as well as the line of business.

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