April 2018

Aravo for GDPR

Technology Innovator in Third Party Management

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.

Aravo for GDPR

Technology Innovator in Third Party Management

GDPR in Third Party Relationships Stretches Resources

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, and others around the world. The latest, most comprehensive, and the one that is the front and center of concern to organizations globally 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 which means it applies everywhere in the world (so long as an EU data subject PII is involved).

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 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 data subjects. It does not matter if the organization resides in the EU. Fines can be stiff, going as high as €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 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).

It is this last bullet, the requirement to ensure third parties are compliant, that is becoming one of the most challenging elements for organizations in GDPR compliance. The dependence on third parties processing data for organizations is becoming critically important and common. Competitive markets are forcing companies to evaluate and potentially outsource more processing to specialist and cost efficient providers to improve margins and/or become more agile in product and service delivery. These third parties who either process employee or customer data need to safeguard this

information, particularly in the scope of GDPR. Third party suppliers represent some of the weakest links to a company's employee and customer data. More than 63% of data breaches can be attributed to third parties, but the organization is still accountable and liable for these breaches.

Organizations will need to take a much stricter approach when dealing with third parties in context of GDPR as they need to ensure that potential contractors handle data privacy and security in a way that is compliant to the regulation. Organizations need to complete due diligence and question their third parties' data handling practices, how they store and delete data, who has access, their encryption policies, and essentially anything relevant to how applicable structured and unstructured digital data is handled and processed. This will also require more documentation and audit trail capabilities in order to be able to demonstrate compliance to the regulators and their EU data subjects.

This is a program that needs to be managed on a continuous basis to be compliant and minimize risk of exposure in the GDPR regulation in context of third party relationships. 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 compliance in third party relationships, organizations should avoid manual processes encumbered by documents, spreadsheets, and emails. They should look to implement a solution that can manage the assessment, communication, and awareness of GDPR requirements and processes in and across third party relationships to manage compliance consistently and continuously in the context of distributed and dynamic business.

Aravo for GDPR

Technology Innovator in Third Party Management

Aravo is a GRC solution that GRC 20/20 has researched, evaluated, and reviewed that is agile for use in complex, distributed, and dynamic business environments to govern third party relationships. Their solution, Aravo for GDPR, delivers an innovative approach to streamline GDPR compliance across an organization's third party relationships – vendors, suppliers, outsourcers, contractors, service providers, consultants, temporary workers, agents, and more. Aravo for GDPR makes GDPR compliance in third party relationships more efficient, effective, and agile. The solution delivers significant business value and brings a contextual understanding of GDPR compliance and control across an organization's distributed business environment. In this context, GRC 20/20 has recognized Aravo for GDPR with a 2017 GRC Innovation Award for the technology innovation in third party management.

Aravo is headquartered in San Francisco, with offices and partners across the US, Europe, and Asia. The overall Aravo solution supports a user base of over 115,000 users,

managing 4 million third party relationships across 33 languages and 154 countries. Founded in 2000, Aravo delivers SaaS/cloud solutions for managing third party risk and compliance across the world's most demanding and distributed organizations. Their solutions enable organizations to protect business value and reputation by managing risks associated with third parties and suppliers, and to build business value by ensuring that third party relationships are optimized.

While the GDPR regulation is new, the model and approach for Aravo for GDPR leverages domain expertise and best practice approaches from nearly two decades of experience delivering successful implementations to global companies with highly complex supply and third party networks. The breadth of the Aravo solution goes beyond GDPR to cover a range of requirements such as anti-bribery and corruption, data privacy, information security, responsible sourcing, and registration and qualification/know your supplier programs.

Aravo for GDPR is a new turn-key solution designed to drop into existing client deployments with minimal provisioning. It can also be implemented as a stand-alone application for new clients – particularly those needing to stand up a GDPR solution for third party compliance quickly and confidently. In the lead-up to this regulation coming into effect, Aravo worked with one of the largest, most complex software firms in the world, to determine their GDPR TPRM requirements as part of a wider global supplier security and privacy assurance compliance program. Taking the best practices developed for their largest clients, Aravo for GDPR is a distillation of technology and domain expertise into a turn-key application. Some of the specific innovative features that GRC 20/20 has identified in Aravo for GDPR are:

- **GDPR data model.** Aravo for GDPR delivers a complete and integrated data model for GDPR compliance in third party relationships. This includes elements for third party engagement, EU GDPR declarations, and a data protection impact assessment (DPIA).

- **GDPR workflows.** Aravo for GDPR delivers pre-built workflows with full task management and a robust system of record to capture a full audit trail of who did what, when, how, and why in context of GDPR compliance. It includes workflow provisions for reporting breaches to the DPA within the appropriate timeframes and approved communication processes.

- **GDPR training.** Aravo for GDPR enables organizations to deliver GDPR training to third parties as well as specific individuals within third parties to ensure that policies are clearly understood and compliance requirements are communicated.

- **GDPR related integrations.** Aravo for GDPR leverages the integration capabilities of the full Aravo platform with a range of connectors available for integration with third party knowledge, content, and scorecard providers to ensure due diligence and ongoing monitoring in critical business relationships. Additionally, Aravo for GDPR will integrate with your firm's ERP and P2P platforms.

What Aravo for GDPR Does

GRC 20/20 has evaluated the features and capabilities of the Aravo for GDPR solution and finds that it delivers an elegant and streamlined GDPR compliance application that makes the GDPR compliance in third party relationships more efficient, effective, and agile. Aravo for GDPR provides a new breed of GRC software that is effective and easy to use in a cloud-based platform that centralizes all third party risk management and compliance activities in one place that enables the organization to collaborate, manage, analyze, and report on GDPR in this context.

This solution allows organization to get a head start on implementing a GDPR control framework that mitigates key third party security and privacy risks, which can otherwise result in GDPR non-compliance, breaches, fines and reputational damage. Aravo for GDPR provides pre-defined best practice questionnaires, templates and workflows designed to support third party compliance, in a simple, fast, and effective way. In context of the GDPR regulation, it is designed for organizations (Controllers) to manage their third party relationships (Processors) under the regulation, including the long tail which is where hidden risk lurks.

Aravo for GDPR specifically delivers:

- **GDPR compliance questionnaire.** This enables the organization to leverage pre-built content to collect GDPR compliance declarations and information from third parties and/or internal stakeholders, as well as proactive updates to GDPR declarations and information from approved third parties.

- **Workflow and task management automation.** This automates the review of GDPR compliance information and approvals for publishing or rejection back to third parties for further information or corrections and enables the notification and renewal of certifications as appropriate in these relationships.

- **Self-registration.** The GDPR questionnaire and workflow are integrated and enabled through the Aravo self-registration capabilities that process inbound self-registration requests from third parties on an organization's website.

- **Accountability for GDPR compliance.** The Aravo for GDPR solutions ensures oversight and accountability of compliance through up to five levels of approval for the validation of GDPR compliance information that has been provided by third parties or internal stakeholders.

- **Periodic/cyclical GDPR compliance evaluation with renewal.** Organizations can automate the renewal of GDPR compliance information annually/cyclically or based on associated certificate expiration dates as appropriate.

- **Incident reporting and corrective actions.** The solution captures incident reporting together with corrective action plans.

- **Reporting to Data Control Agencies.** The solution includes workflow provisions for reporting breaches to the DPA within the appropriate timeframes and approved communication processes.

- **Communications and compliance agility.** With Aravo for GDPR, organizations can communicate and process proactive updates to GDPR compliance information via the self-service portal to third party relationships. Further, organizations can publish approved third party GDPR compliance declarations and supporting information to a secure FTP site within an organization's infrastructure via Aravo Incremental Export (XML) integration.

Benefits Organizations Receive with Aravo for GDPR

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and acting with integrity [COMPLIANCE].[1] Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 measures the value of GRC initiatives around the elements of efficiency, effectiveness, and agility. Organizations looking to achieve GRC value will find that the results are:

- **GRC Efficiency.** GRC provides efficiency and savings in human and financial capital resources by reduction in operational costs through automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC achieves efficiency when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.

- **GRC Effectiveness.** GRC achieves effectiveness in risk, control, compliance, IT, audit, and other GRC processes. This is delivered through greater assurance of the design and operational effectiveness of GRC processes to mitigate risk, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the controls and policies set by the organization and provide greater reliability of information to auditors and regulators.

- **GRC Agility.** GRC delivers business agility when organizations can rapidly respond to changes in the internal business environment (e.g. employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g. external risks, industry developments, market and economic factors, and changing laws and regulations). GRC achieves agility when

1 *This is the official definition of GRC found in the GRC Capability Model and other work by OCEG at www.OCEG.org.*

organizations can identify and react quickly to issues, failures, non-compliance, and adverse events in a timely manner so that action can be taken to contain these and keep them from growing.

Aravo for GDPR is designed to make GDPR third party compliance efficient, effective, and agile in a dynamic and distributed business environment. This is done in an intuitive, easy to use user interface that delivers critical information to third parties and internal stakeholders who need it, when they need it, and in a format they can understand. Where most organizations have manual processes encumbered with documents, spreadsheets and emails for third party management, the Aravo solution streamlines this process making it more efficient for both parties.

The key value to organizations using Aravo for GDPR is their integrated and structured solution content and process for GDPR compliance in third party relationships. This is in a solution that can be implemented rapidly without a long project, consultation, and extended deployment time-frames. By providing pre-defined GDPR best practice questionnaires, templates and workflows designed to support third party compliance, Aravo has taken the hard work out of program design, and packaged it up in a way that supports rapid adoption – critical in a time-sensitive regulation such as GDPR.

Specific benefits and value organizations can expect to achieve with Aravo for GDPR include:

- *Agility to manage the full universe of third parties* and segment level of control based on GDPR risk indicators
- *Rapidly understand GDPR non-compliance exposure* within third parties, including the "long-tail"
- *Tier third parties* according to their data use and access rights
- *Gain insight* into and manage fourth party/subcontractor exposure
- *Triangulate assessment*, scorecard and content-provider data for a full picture of high-risk, critical third parties
- *Identify requirements* for virtual and/or on-site audits and schedule, record, and apply remediation actions within the system
- *Ensure required contractual terms* and conditions are included within agreements
- *Manage contract conformance* and performance, including SLAs
- *Guarantee breach reporting* escalation procedures and timeframes are met
- *Align and train third parties* on GDPR compliance expectations

- *Provide evidence or GDPR compliance* to the regulation with full audit trail and documentation

- *Integrate with ERP & P2P platforms* to share GDPR risk information across the enterprise

- *Deliver executive level analytics* and reporting

Considerations in Context of Aravo for GDPR

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 Aravo for GDPR to enable organizations to achieve consistent third party management processes, readers should not see this as a complete and unquestionable endorsement of Aravo.

Overall, organizations should find a high degree of satisfaction with their use and implementation of Aravo for GDPR and find that it delivers capabilities that are effective in identifying GDPR non-compliance issues in third party relationships while driving efficiency by reducing time and labor costs to manage third parties. The solution is intuitive and ease of use with implementation that is straightforward and rapid.

Some key differentiators GRC 20/20 sees in the use of Aravo for GDPR include:

- **Purpose built for third party management.** Aravo for GDPR is not trying to do everything for GDPR at a superficial high level. They go deep into managing GDPR compliance specifically in context of third party relationships rather than internal compliance.

- **Scalable to the most demanding environments.** Aravo has a proven track record in third party management implementations for some of the worlds largest and most demanding companies with tens to hundreds of thousands of third party relationships.

- **Lifecycle view of third party relationships.** Aravo does not simply send out GDPR questionnaires to third parties, their platform and solution is designed to manage the entire lifecycle of a third party relationship from on-boarding to off-boarding, and in that context meet the GDPR compliance needs across all phases of that lifecycle.

- **Part of a federated third party management approach.** While Aravo for GDPR can be implemented in a stand alone capacity for just GDPR, it is built on the Aravo platform that enables a fully federated, holistic enterprise view of third party risk and compliance across all third party relationships.

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