GDPR Compliance with Rsam: Solution Brief

It’s Time to Get Serious about GDPR

Effective May 25th, 2018, the General Data Protection Regulation (GDPR) imposes a broad set of privacy requirements aimed at providing EU residents more control over their personal information. Expanding on the Data Protection Directive (1995) to better account for all the ways that today’s organizations collect, transfer, and utilize data, the GDPR is characterized by its broad scope, challenging complexity, and massive potential impacts for non-compliance.

Who is Affected?

The GDPR applies not only to all organizations within the EU, but also to any organization that collects or processes the personal information of EU residents, regardless of that organization’s physical location(s). It covers the collection and processing of personal data not only as it relates to the delivery of products and services but also to the targeting of communications to EU residents, the monitoring of their behaviors, etc. The GDPR makes a distinction between organizations acting as “data controllers” (those who collect personal data) vs. “data processors,” (those who process that data on behalf of data controllers), but both are responsible for maintaining compliance.

What are the Impacts?

The most obvious impacts of non-compliance are the massive fines - up to the greater of €20 million or 4% of global annual revenue. But beyond the financial penalties, there are significant strategic business incentives for achieving and maintaining compliance with the GDPR, including:

- **Competitive advantage in business-to-business markets:** GDPR-compliant data processor organizations will be favored by sourcing data controller organizations evaluating potential vendors and business partners.
- **Competitive advantage with end-consumers:** GDPR-compliant organizations will be favored by the segment of their target consumer market comprised of EU residents.
- **Competitive advantage in the labor market:** Employee privacy is as important as customer privacy under the GDPR, and EU residents in the labor market will expect employers to be GDPR compliant and will favor those who are.

The impacts of the GDPR are significant and varied, and so with its broad scope and complexity and looming effective date, the GDPR has organizations scrambling to define and begin executing on their compliance plans.

GDPR Brings Unique Challenges

Like most broad-sweeping regulatory frameworks, the GDPR requires all of the usual high-level requirements: designating compliance roles and responsibilities, assessing risks and related controls, and demonstrating ongoing monitoring and remediation around GDPR program effectiveness. However, the GDPR also imposes a number of uniquely challenging requirements. In order to better understand those, it’s helpful to look at the specific data rights to which it entitles all EU residents.

Right to be Forgotten

The right to be forgotten specifies that EU residents have the right to request that an organization remove all of their personal information from its custodianship. This requires that organizations not only know where all that data resides within the organization, but also that they have appropriate business processes and tools in place to respond to right-to-be-forgotten requests in an effective and timely manner and to communicate dispositions to requestors, regulators, and other stakeholders. Other special considerations include:

- The right to be forgotten may require the ability to document exceptions in cases where personal data cannot be removed because it is required for legal, tax, or other conflicting obligations.
- Recalling the roles of data controllers vs. data processors, the right to be forgotten creates a need for effective communication procedures between the controllers that receive right-to-be-forgotten requests and the downstream data processors, many of whom will be external to the organization, that may need to take action and report on the status of those requests.

Right to Data Portability

In order to support EU residents' ability to freely move between competing products and services, the right to data portability requires that organizations be able to package up and deliver customer information in a machine-readable format. This requires that organizations know not only those systems in which personal information resides, but also whether that information can be packaged from those systems into an acceptable format. Like the right to be forgotten, the right to data portability requires both process and tools in order to effectively meet such request, but it also requires an assessment of which systems and which data do not currently support the right to data portability, as well as the ability to document remediation activities for resolving such insufficiencies.

Right to Breach Notification

In the event of a personal data breach, organizations under the GDPR have 72 hours to notify local authorities and, in turn, those EU residents whose data may have been compromised. The clock starts ticking for both data controllers and data processors as soon as the breach is detected, and that clock doesn't stop for evenings, weekends, or holidays. This requires that organizations have highly effective security incident response plans. Those response plans should include playbooks that specify who should be notified (internal resources as well as data processors, forensics, legal counsel, regulators, customers, etc.), how they should be notified (email, phone, etc.), and relevant contact information. What's more, incident response plans need to be periodically reviewed and updated to ensure that they remain aligned with changing business, regulatory, and threat environments. If and when a breach occurs, you want your incident response team to be focused on managing and diffusing the incident.

Right to Transparency

The right to transparency specifies that an organization must be transparent in communicating to data subjects what it will do with their personal information and it must in fact do with that information only what it said it would do. This requires that privacy notices be shown in a consistent and appropriate manner as customers engage with an organization's products and services. Privacy notices must be maintained as new products and services are deployed, and conversely, products and services should be periodically evaluated against published privacy notices to ensure they are aligned.

Right to Data Protection

At the end of the day, none of the above privacy rights can be guaranteed if an organization doesn't have appropriate security measures in place to protect the personal information of EU residents. The regulation is not specific about the security controls that an organization should have in place, but it does regularly refer to the implementation of controls that are "to industry standard" or "to industry best practice." As such, it is incumbent on organizations to assess their own unique data privacy and security risks, to implement controls as they deem appropriate to those risks, to periodically assess the design and operating effectiveness of those controls, and to remediate gaps as they are identified.

How Rsam Helps

At its most fundamental level, maintaining compliance with GDPR simply requires adherence to effective governance, risk, and compliance (GRC) management practices. To this end, other vendors highlight the ability of their existing solutions to independently address various elements of the regulation. However, what is quite different from other regulations is that the GDPR demands orchestration between, what are typically, siloed disciplines.

While many solution vendors tout otherwise, there is no out-of-the-box silver bullet that an organization can simply purchase to bring it into full compliance with the myriad of requirements imposed by the GDPR. As unique as organizations are, even more so are the programs, frameworks, and levels of maturity of their GRC practices. Rsam offers the industry's first truly integrated risk management GDPR solution. Our solution not only takes your uniqueness into consideration but provides a roadmap and actionable intelligence toward GDPR compliance.

Rsam's integrated risk management solution begins with providing Data Protection Officers (DPO) risk assessment intelligence on their programs ability to support the regulation's requirements. With the roadmap to compliance established, DPOs can then integrate existing program information from any Rsam module and/or external data sources into the plan. The resulting solution provides the ability to: demonstrate a path forward, collaborate and leverage current program practices, eliminate duplicative work, and provide on-demand integrated progress reporting.

Establish your GDPR Baseline

In order for an organization to begin effectively addressing its GDPR gaps, it first needs an informed understanding of what those gaps are. By combining Rsam's **Risk and Compliance Assessments Module** with an out-of-the-box **GDPR Control Library**, organizations can perform GDPR risk assessments against their various entities and the assets on which they rely.

- Assess departments and business units to determine their readiness to meet GDPR requirements.
- Leverage questionnaires, assessments, and control tests to identify gaps.
- Address and manage these gaps with powerful workflow and reporting features.

By starting with an effective GDPR risk assessment, you'll have a leg up when it comes to reporting GDPR readiness to stakeholders, prioritizing and justifying GDPR investments, and tracking your progress as you execute on a well-informed GDPR compliance road map.

Address your GDPR Gaps and Issues

GDPR risk assessments will expose shortcomings. Rsam's **Findings Management** module provides capabilities that allow organizations to not only identify issues, but also to track remediation plans and report on their review-and-approval status, relative prioritization, and implementation status. Additionally, this module provides workflow and reporting around the review, implementation, and ongoing monitoring of other mitigating factors such as compensating controls, exceptions, and risk acceptance requests.

Say what you Do

Governance is a critical component of any effective GDPR compliance program, and organizations need to be ready to manage GDPR-related policies and procedures throughout all levels of the organization. While corporate-level policies communicate your organization's commitment to privacy and security, each department and business line has to manage its own privacy and security policies to changing product and service offerings and define its own procedures for implementing GDPR requirements like tracking consent and responding to right-to-forgotten requests.

Rsam's **Enterprise Policy Management Module** makes it easy to manage the lifecycle of GDPR-related policies and procedures throughout all levels of your organization. Configurable workflow automates everything from policy development, review, and publication to attestation and exception tracking. Our relational data model allows policy managers to easily link policies to the GDPR risks and requirements they address as well as the controls that are in place to enforce them.

> "GDPR applies not only to organizations within the EU, but also to any organization that collects or processes the personal information of EU residents, regardless of that organization's physical location(s)"

Do what you Say

Rsam's **Continuous Control Testing Module** allows organizations to continuously ensure the design and operating effectiveness of privacy and security controls. The module's centralized control library allows organizations to capture and manage the lifecycle of GDPR controls and their related test definitions. Simply define a test plan for a specific entity or asset, and Rsam automatically manages testing activities according to each test's unique frequency and duration. Test results can also be generated automatically based on data that reside either in Rsam or in integrated tools, and real-time control testing reports can be generated either with a button click or on a scheduled basis to support attestation and certification requirements.

Get your Data Processors on Board

As organizations invest in beefing up their internal GDPR compliance programs, it's critical they remember that their measures are only as effective as their external data processors'. Some aspects of third-party considerations are more obvious, such as the need to determine which vendors constitute "data processors" and to assess their privacy and security control infrastructures. Other questions might be less obvious, such as:

- Do your existing contracts with data processors ensure that vendors will be compliant with GDPR requirements?
- Are your data processors prepared to handle "right to be forgotten" requests, and do your agreements specify how vendors must respond to and document such requests?
- Have you included breach reporting requirements in all agreements with data processors so that you can meet the 72-hour reporting window?

Rsam's **Vendor Risk Management Module** allows organizations to get their arms around third-party risk by automating the vendor classification, assessment, and remediation process. It also automates onboarding, contract management, and SLA management to make sure that you're asking and getting answers to all of the critical GDPR data processor questions.

GDPR Security Operations Management

If organizations are going to have a shot at meeting GDPR's 72-hour breach response requirement, they're going to have to address the inherent lag that comes with poor communication and siloed incident response processes. Rsam's **Security Incident Response Platform** automates incident and event triage and allows response teams to create, manage, and automatically execute collaborative response playbooks. In the event of an incident, the module ensures that all incident responders have clear communication channels to notify internal stakeholders as well as external data processors, legal counsel, forensics teams, regulators, and customers of required actions.

In addition to managing incident response plans, security operations teams also play an important role in ensuring that preventative and detective cyber security controls are in place. Rsam's **Threat and Vulnerability Management Module** provides security organizations with a centralized view of integrated cyber threat and vulnerability intelligence, allowing them to quickly triage and respond to cybersecurity risks and ensure that private data remains private.

GDPR Compliance and Beyond

Rsam also provides a rich set of configuration, integration, and reporting tools that provide customers the ability to easily modify and even build their own Rsam applications, allowing them to adapt to changing regulatory, risk, and business environments.

Build your Own

Rsam's **Build-your-Own** program allows customers to easily configure their own tailored applications that address requirements that are specific to a particular regulatory obligation or business process. In the case of GDPR, examples include a consent tracking tool or a ticketing application for managing right-to-be-forgotten requests. Build-your-own applications are inherently integrated with all other applications on the platform, allowing customers to tie their custom use cases to their foundational GRC infrastructure and taxonomy.

Integrated GDPR Technology Infrastructure

Organizations will rely on a variety of new and existing tools to solve specific GDPR requirements. Rsam's **Universal Connector** supports an integrated GDPR technology architecture by providing a wide range of inbound and outbound integration mechanisms, including a bi-directional RESTful API and a drag-and-drop data mapping interface.

Reporting

Rsam provides a rich set of searching and reporting options to meet the needs of all users and audiences. Rsam's RapidReports and powerful in-application searching and charting tools allow users to easily access, create, modify, and share meaningful views into critical day-to-day GDPR program information, while an integrated SQL Server Reporting Services (SSRS) engine allows users to create dazzling reports for executive management, the board, regulators, and other key stakeholders.

About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at http://www.rsam.com