EU GENERAL DATA PROTECTION REGULATION COMPLIANCE WITH RSA ARCHER®

Solution Brief

Sanctions for GDPR non-compliance could include:

- *A written warning*
- *Periodic audits*
- *Fines up to 10 million EUR or up to 2% of the annual worldwide turnover of the preceding financial year, whichever is greater*
- *Fines up to 20 million EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher*

EU General Data Protection Regulation

ARRIVAL OF GDPR IN 2018

The European Union (EU) General Data Protection Regulation (GDPR) that takes effect in 2018 will bring changes for organizations that handle personal identifiable information of European citizens. This regulation is intended to strengthen and unify data protection of individuals within the EU, and the export of this personal data outside of the EU. The scope of the GDPR encompasses all European businesses as well as any business that controls or processes personal data related to the delivery of goods and services to individuals in the EU or is designed to monitor their behavior in some way. These requirements apply regardless of where the organization is based.
While there is some time before the EU GDPR is enforced, the significant breadth and complexity of the GDPR warrants starting the compliance strategy planning process now. Non-compliance with GDPR requirements is expected to result in fines up to 4% of an organization's annual world-wide revenue or 20 million Euros, whichever is greater. Without a holistic approach to GDPR compliance, organizations are likely to prematurely exhaust available human and capital resources and take an unnecessarily long time to prepare for the impending regulation.

PREPARATION IS ESSENTIAL

The EU GDPR imposes interrelated obligations for organizations handling personal data of EU citizens, including:

- Adopting policies and procedures to ensure and demonstrate that EU citizen personal data is handled in compliance with the regulation
- Maintaining documentation of all processing operations
- Assessing electronic and physical data security risk to personal data including accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Implementing appropriate technical and organizational controls to ensure a level of security appropriate to the risk
- Implementing procedures to verify the effectiveness of the controls which align with the results of the risk assessment
- Establishing control testing procedures
- Performing data protection impact assessments on planned processing of highly sensitive personal data
- Communication with EU citizens at the time information is collected, upon directed inquiry, and delivery of responses
- Appointment of a Data Protection Officer charged with the responsibility of ensuring the organization's compliance with the EU GDPR requirements

EU GDPR requires organizations to utilize a risk-based approach for compliance. To demonstrate compliance, organizations must document:

- The processes and infrastructure of the organization where EU personal data is handled or resides
- The risk assessment of these processes and infrastructure
- The controls and enforcement policies and procedures to ensure personal data is handled in compliance with the regulation
- The results of control testing
- The status of outstanding issues and remediation plans

RSA

By taking a holistic approach to EU GDPR compliance, you can better understand information security-related risk, how to prioritize investments to more effectively manage risk, establish accountability for risk management, and more quickly respond to identified gaps in the information security control framework. Consolidating these compliance efforts provides the executive team, regulators, and your board of directors with an accurate, real-time picture of the state of EU GDPR compliance across the organization, as well as proof that your organization has fulfilled regulatory obligations.

Taking a risk-based approach for EU GDPR compliance requires organizations to:

- *Understand if, where, and how much EU personal information is handled by the organization*
- *Have manual and technical controls in place to protect the information from unauthorized access, alteration, and unavailability commensurate with the risk*
- *Test manual and technical controls on a periodic basis to ensure they are operating effectively*

THE RSA ARCHER ADVANTAGE

RSA Archer® allows your organization to document and evaluate EU GDPR-related infrastructure, policies and procedures, risks, controls, third parties, outstanding issues and remediation plans. You can consolidate this information for relevant business processes to establish a sustainable, repeatable, and auditable EU GDPR compliance program. With RSA Archer, you get a clear view of the organization's state of EU GDPR compliance that allows you to prioritize activities that address the regulation's requirements. The RSA Archer Suite provides several use cases to help your organization address GDPR obligations, including the following options.

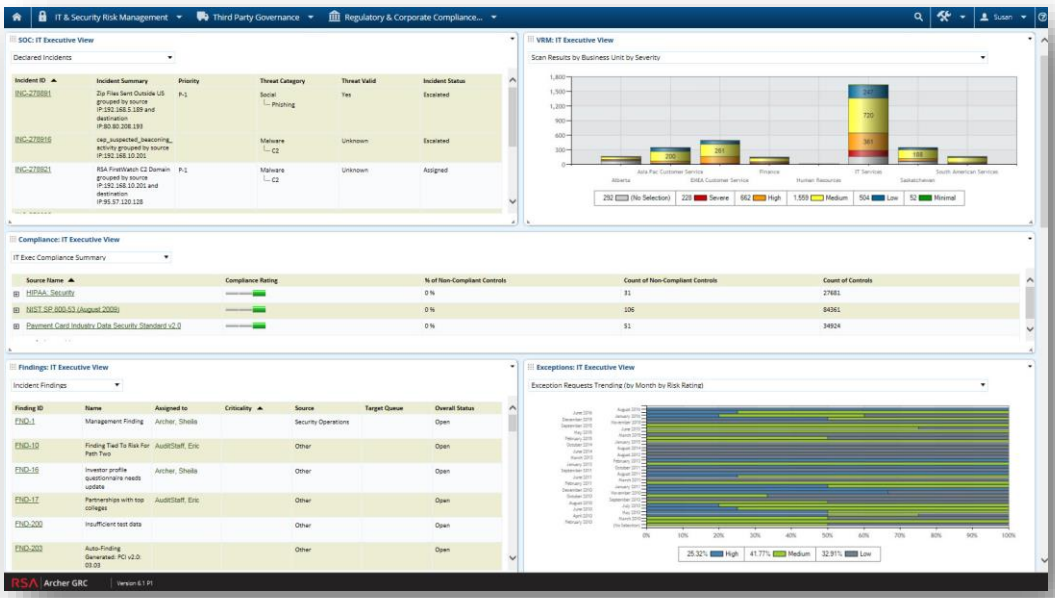
Issues Management
RSA Archer Issues Management lays the foundation for your EU GDPR program to manage issues generated from risk and control assessments and audits. You can create a consolidated view and workflow for managing findings, remediation plans, and exceptions. Issues Management also establishes business hierarchy to establish corporate structure for accountability. With an organized, managed process to escalate issues, you get visibility into risks and efforts to close and address those risks in a timely manner. Workflow for proper sign-off and approval of issues, remediation plans, and exceptions ensures identified issues are managed and mitigated. Your organization will see quicker reaction to emerging issues, creating a more proactive and resilient environment while reducing the cost of compliance to GDPR.

IT Risk Management
With RSA Archer IT Risk Management, you can comprehensively catalog organizational hierarchies and the business processes and IT assets involved in the handling, processing, storage, and transmittal of EU citizen data. This is done to ensure all business critical connections are documented and understood in the proper context of the regulatory obligations, and establishes the structure to document applicable IT risks in the Risk Register. Pre-built IT risk assessments, threat assessment methodology, and an IT control repository allow you to document and assess the design and effectiveness of applicable IT controls. Streamlined assessments accelerate the identification of IT risks, and the linkage between risks and internal controls eases communication of IT control requirements, reducing GDPR compliance gaps and improving risk mitigation strategies. This agile framework allows your organization to keep up with changing requirements and focus resources on the most impactful IT risks.

IT & Security Policy Program Management
RSA Archer IT & Security Policy Program Management provides the framework for establishing a scalable and flexible environment to document and manage your organization's policies and procedures to comply with the EU GRPR. This includes documenting policies and standards, assigning ownership, and mapping policies to key business areas, objectives, and controls. By implementing an EU GDPR policy program, you can effectively manage the entire policy development lifecycle process in addition to handling policy exceptions, policy reaffirmation and acknowledgement and demonstrating how your control environment complies with your established policies and procedures.

IT Controls Assurance
RSA Archer IT Controls Assurance provides a framework and taxonomy to systematically document the EU GDPR control universe. You can assess and report on the performance of controls at business hierarchy and business process levels. With streamlined processes and workflow for testing IT controls, you can deploy standardized assessment processes for manual controls and integrate testing results from automated systems. Issues identified during compliance assessments are centralized, with tracking and reporting of compliance gaps and remediation efforts. By improving the linkage between compliance requirements and internal controls, your organization can better communicate and report on EU GDPR compliance obligations using a common taxonomy and language across the organization.

RSA



Third Party Risk Management
RSA Archer Third Party Risk Management enables you to assess the inherent and residual risk to third parties as it relates to your GDPR obligations. It employs a series of risk assessment questionnaires to be completed by a third party to assess the vendor's internal control environment applicable to the EU GDPR and collect relevant supporting documentation for further analysis. The results are factored into a determination of the organization's residual risk across several risk categories, including compliance/litigation, financial, information security, reputation, resiliency, strategic, sustainability, and fourth party risk. Risk results are depicted for each product and service engagement provided by the third party and rolled up on an "aggregated" basis to depict your overall risk to the third party. In addition, you can assess contracts you have drafted with third parties to ensure they fulfill the third party's GDPR obligations and provide adequate risk transfer for your organization. Risk assessment findings can be automatically captured and managed as exceptions, and remediation plans can be established, assigned to the responsible individuals, and monitored to resolution.

Permission to Process and Be Forgotten
The EU GDPR requires organizations to obtain permission from EU citizens to process their personal data. It also requires organizations to manage and respond to EU citizen inquiries about if and how they process the citizen's personal data, as well as providing individuals the "right to be forgotten." Using RSA Archer on-demand applications, organizations can configure workflow and repositories to collect, document, and process these requirements to ensure permissions are obtained, and inquiries and responses are executed accurately, completely, and in a timely manner.

Maturing Your GDPR Program

Once your organization has mastered the initial GDPR program requirements, you can apply additional RSA Archer use cases to mature your program to address more specific risk and compliance elements, including:

- **Security Incident Management** - Implement a structured process for investigating, escalating and resolving cyber incidents.

- **IT Security Vulnerabilities Program** – Proactively manage cybersecurity risks by combining actionable cyber threat intelligence, security vulnerability assessment results, and business context on the criticality of IT assets.

- **Security Operations & Breach Management** - Centrally catalog IT assets for incident prioritization based on business context, monitor key performance indicators, measure control efficacy, and manage the overall security operations team, and focus on the most impactful incidents to lower overall security risk and react promptly and appropriately to data breaches.

- **Business Continuity and IT Disaster Recovery Planning** – Ensure you have the established resiliency required by the EU GDPR by documenting and testing business continuity and IT disaster recovery plans for business processes, locations, IT applications and infrastructure, and information assets, thereby enabling you to respond swiftly in crisis situations to minimize disruptions and protect your ongoing operations.

- **Key Indicator Management** - Establish and monitor key indicators associated with EU GDPR compliance. Associate indicators with risks, controls, strategies and objectives, products and services and business processes to monitor quality assurance and performance

- **Third Party Catalog** - Catalog your suppliers, partners, service providers and other third parties related to your EU GDPR compliance obligations.

- **Third Party Engagement** - Capture important details related to the products and services delivered by third parties, including contracts, perform risk assessments and monitor performance to SLAs.

"The best thing for me about working with RSA is the fact that, as a control and compliance officer, I have access to all data I need. I can see what's happening, and where the organization has deficiencies I can see what is done to cope with them. I can see whether or not management has accepted things correctly at the right levels and I can execute my control tasks much easier than in the past."

Jans Jans
Control & Compliance Officer
Rabobank

Organizations employ a third line of defense to independently validate the design and effectiveness of their internal control frameworks. RSA Archer Audit Management solutions alongside the above use cases offer a mechanism to validate that your organization has fulfilled its EU GDPR obligations.

- **Audit Engagements and Workpapers** - Efficiently perform audit engagements, maintain workpaper documentation, and provide consistent and timely reporting on audit results.

- **Audit Planning & Quality** – Plan your GDPR audits by identifying, defining and assessing the risk of your auditable entities across the organization. Automatically integrate management risk and control information to ensure audit objectives are aligned with your risk and compliance priorities.

CONCLUSION

EU GDPR compliance to protect personal information of EU citizens will be a complex and time consuming undertaking for most organizations. RSA Archer can help your organization establish the necessary framework to comply with this regulation by implementing a business-driven approach to security, ensuring your risk and control framework is accurate, complete, and protected from theft, destruction, or interruptions.