RSA

SOLUTION BRIEF

Helping Prepare for Risk Assessment & Compliance Challenges for GDPR with RSA Security

Addressing the ticking clock of GDPR compliance

The European Union (EU) General Data Protection Regulation (GDPR) that takes effect in May 2018 will bring changes for organizations that handle personally identifiable information (PII) of European residents. This regulation is intended to strengthen the protection of PII within the EU, and anywhere it is transferred outside of the EU. The scope of the GDPR encompasses all businesses based in the EU as well as any business that controls or processes personal data related to individuals in the EU. These requirements apply regardless of where the organization is based, making GDPR a truly global compliance requirement.

Non-compliance with GDPR requirements carries with it the potential for significant negative impacts; failure to achieve and maintain compliance 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 might prematurely exhaust available human and capital resources and take an unnecessarily long time to prepare for the impending regulation.

GDPR, and privacy legislation and directives in general, create specific challenges for organizations. All major compliance initiatives require a comprehensive approach to identifying control requirements (whether explicitly or implicitly stated in the legislation), marshalling resources to implement controls and then a strategy to measure and report on the ongoing compliance to those requirements. The challenge for most organizations is that, individually, compliance obligations are manageable. But as more and more requirements are placed on the organization, the strain of meeting these requirements can impact business operations.

Article 32 of the GDPR regulation lays out appropriate elements of a security risk assessment process to ensure controls are appropriately designed and implemented. In general, an effective risk assessment process helps accelerate the identification of the linkage between risks and internal controls. These processes help reduce GDPR compliance gaps and improve risk mitigation strategies. Closely related to the risk assessment process is the ongoing compliance efforts related to ensuring controls are designed and operating effectively to meet the organizational and technical controls needed by GDPR.

A compliance program management should provide the framework for establishing a scalable and flexible environment to document and manage your organization's policies and procedures to help demonstrated compliance with the GDPR. This includes documenting policies and standards, assigning ownership, and mapping policies to key business areas, objectives and controls. By implementing a GDPR policy program, organizations are empowered to effectively manage the entire policy development lifecycle process in addition to handling policy exceptions, policy reaffirmation and acknowledgement and demonstrating how your control environment correlates with your established policies and procedures.

With an organized, managed process to identify risks, coordinate compliance efforts and escalate issues, you get visibility into risks and efforts that can close and address risks to PII, and ultimately demonstrate GDPR compliance activities, in a timely manner. Organizations will see quicker reaction to emerging issues, creating a more proactive and resilient environment while helping to reduce the cost of compliance to GDPR.

RSA: Supporting a holistic approach to addressing risk assessments and compliance

RSA offers business-driven security™ solutions that link business context with security processes to help organizations manage risk and protect what matters most. RSA solutions are designed to help organizations effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk - all essential steps in helping organizations develop a holistic strategy for responding to GDPR.

With GDPR requirements as context, let's take a closer look at the RSA product and service portfolio, and how these offerings can help organizations prepare for GDPR.

RSA Archer Suite

The RSA Archer® Suite is an industry leading Governance, Risk & Compliance (GRC) solution that is engineered to empower organizations to manage multiple dimensions of risk with a solutions built on industry standards and best practices on one configurable, integrated software platform. It offers a wide variety of use cases designed to play a key part in helping an organization to establish and maintaining GDPR compliance.

RSA Archer Data Governance

RSA Archer Data Governance is designed to provide a framework to help organizations identify, manage, and implement appropriate controls around personal data processing activities. RSA Archer Data Governance helps empower organizations to maintain an accurate inventory of processing activities, establish and apply documented controls around the usage of PII, and manage data retention requirements.

Preparation for GDPR is essential

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

- Adopting policies and procedures to ensure and demonstrate that PII is handled in compliance with the regulation
- Maintaining documentation of 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
- Performing data protection impact assessments on planned processing of highly sensitive personal data
- Providing transparent notice to EU residents at the time information is collected, upon later inquiry
- If engaged in large scale monitoring of individuals, or processing special categories of personal data, appointment of a Data Protection Officer charged with the responsibility of monitoring the organization's compliance with the EU GDPR requirements

RSA Archer Privacy Program Management

RSA Archer Privacy Program Management is designed to enable organizations to group processing activities for the purposes of performing data protection impact assessments and tracking regulatory and data breach communications with data protection authorities. Chief Privacy Officer, Data Privacy Officers (DPO) and privacy teams are also enabled to benefit from a central repository of information needed to demonstrate commitment to GDPR compliance around the organization's privacy program.

Issues Management

RSA Archer Issues Management is designed to play an important role for an organization's GDPR program by helping to manage issues generated from risk and control assessments and audits. Organizations 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.

IT Risk Management

RSA Archer IT Risk Management helps organizations comprehensively catalog organizational hierarchies and the business processes and IT assets involved in the handling, processing, storage, and transmittal of EU resident data. This is designed to help organizations to ensure all business critical connections are documented and understood in the proper context of the organization's regulatory obligations, and establishes the structure to document applicable IT risks. Streamlined assessments can help to accelerate the identification of IT risks, and the linkage between risks and internal controls can help to ease communication of IT control requirements, helping to reduce GDPR compliance gaps and improving risk mitigation strategies. This agile framework is designed to empower 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 is designed to provide the framework to help organizations to establish a scalable and flexible environment to document and manage an organization's policies and procedures to help comply with the GRPR. This includes documenting policies and standards, assigning ownership, and mapping policies to key business areas, objectives, and controls. Implementing an GDPR policy program can help organizations effectively manage the entire policy development lifecycle process in addition to handling policy exceptions, policy reaffirmation and acknowledgement and demonstrating how your control environment correlates to your established policies and procedures.

IT Controls Assurance

RSA Archer IT Controls Assurance is designed to provide a framework and taxonomy to help organizations systematically document the GDPR control universe, enabling organizations to assess and report on the performance of controls at business hierarchy and business process levels. With streamlined processes and workflow for testing IT controls, organizations can deploy standardized assessment processes for manual controls and integrate testing results from automated systems. Issues identified during compliance assessments can be centralized, with the ability to track and report compliance gaps and remediation efforts. By improving the linkage between compliance requirements and internal controls, organizations can better communicate and report on GDPR compliance obligations using a common taxonomy and language.

RSA risk and cyber security practice

RSA offers a range of strategic services designed to help you craft a business-driven security strategy, build an advanced security operations center and revitalize your governance, risk and compliance (GRC) program. To complement our robust product offering, we also provide implementation and post-implementation support so that you can maximize your investment in our products.

RSA Risk Management Practice

A great place to start with the assessment of your organization relative to security best practices is the RSA Risk Management Practice. This practice is designed to deliver a variety of strategic consulting services to help you optimize your organization's governance, risk and compliance program. It also offers staff augmentation and support services to help you plan, implement, deploy and upgrade RSA products and services, including the RSA Archer Governance, Risk and Compliance solution.

Conclusion

Globally, organizations are actively assessing the impact of the GDPR on their business and data privacy and management operations. The deadline of May 2018 is looming, and any organization doing business in the EU or processing PII from EU residents needs to working through the deployment of additional processes, policies and technologies to avoid the significant fines posed by the regulation. By first implementing a standardized approach to risk assessment and then establishing a compliance program designed to protect PII of EU residents, your organization can establish the necessary framework to comply with this regulation. With a strong scope of products and services designed to address risk assessment and compliance processes, RSA can act as a strategic partner to help in any organizations' journey towards GDPR compliance.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.
For more information, go to **rsa.com**.