RSA

SOLUTION BRIEF

HELPING ADDRESS GDPR CHALLENGES WITH RSA

ADDRESSING THE TICKING CLOCK OF GDPR COMPLIANCE

RSA

PREPARATION FOR GDPR IS ESSENTIAL ACROSS THE GLOBE

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

- *Adopting policies and procedures to ensure and demonstrate that EU residents' personal data 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 PII that may be "high risk"*
- *Communication with EU citizens at the time information is collected, upon directed inquiry, and delivery of responses*
- *If engaged in large scale monitoring of individuals, or processing special categories of personal data, appointment of a Data Protection Officer charged to monitor the organization's compliance with the EU GDPR requirements*

The European Union (EU) General Data Protection Regulation (GDPR) that takes effect in May 2018 will bring changes for organizations that handle European residents' personally identifiable information (PII). This regulation is intended to strengthen and unify data protection for 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 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 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 exhaust available human and capital resources and take an unnecessarily long time to prepare for the impending regulation.

Successfully managing GDPR compliance requires organizations to utilize a risk-based approach. To demonstrate compliance, organizations should consider:

- 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

By taking a holistic approach to GDPR compliance, organizations 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.

FOUR KEY AREAS OF FOCUS FOR ADDRESSING GDPR

While GDPR has very specific articles defining particular steps to be taken, many aspects of GDPR compliance can be achieved through leveraging established data security and compliance management best practices. Based on extensive experience helping global organizations with implementation of security best practices, RSA has developed a four-part focus intended to assist organizations in moving towards GDPR compliance. It is important to recognize that ultimately GDPR compliance is a combination of technical requirements, legal analysis, process definition, documentation and human oversight. As such, organizations should consult with their legal experts on their individual compliance requirements.

The four key focus areas RSA sees as best practice and practical steps for GDPR are: Risk Assessment, Breach Response, Data Governance, and Compliance Management.

RSA

RISK ASSESSMENT

Article 32 of the regulation outlines appropriate elements of a security risk assessment process to ensure controls and risk are appropriately designed and implemented. An effective risk assessment process accelerates the identification of the linkage between risks and internal controls, reducing GDPR compliance gaps and improving risk mitigation strategies.

BREACH RESPONSE

Article 33 of the GDPR regulation outlines specific requirements for notification of a personal data breach to the supervisory authority. Obviously, the goal of any security team is to prevent these kinds of breaches, but breaches can still occur. As a result, many regulatory requirements focused on consumer data protection are turning their focus to breach response and reporting. In the case of GDPR, some of the specifics relate to having a full understanding of the details and impact of a data breach. Additionally, GDPR requires the ability to manage notification to regulators, generally within 72 hours of becoming aware of the breach. Accomplishing this objective will require a combination of processes and technical capabilities including security incident management, security operations and breach management, as well as tools for deep monitoring and analysis of system related security data, such as system events, coupled with strong forensics capabilities.

DATA GOVERNANCE

The GDPR regulation highlights that data governance is crucial in controlling who has access to data in organizations. Organizations must protect PII in a number of different ways, and must be able to demonstrate due diligence in keeping accurate records of processing activities, including the categories of personal data processed, the purposes of processing, categories of recipients of PII, transfers to third countries, and the relevant technical and organizational security measures. These requirements are in keeping with Identity and Access Management (IAM) and Data Governance best practices which would leverage an IAM solution to protect sensitive and personal information. Authentication solutions can add additional layers of data protection to ensure that only the correct users have access to the data. Additionally, an identity governance and lifecycle solution allows organizations to answer two critical questions; do they have the right level of access and is the access in compliance with policies. Audit trails can show regulators how organizations are complying with GDPR and appropriately managing data governance and data access.

COMPLIANCE PROGRAM MANAGEMENT

Compliance 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 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 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 correlates with your established policies and procedures. With an organized, managed process to escalate issues identified during control testing, you get visibility into risks and can address the risks in a timely manner. Organizations will see quicker reaction to emerging issues, creating a more proactive and resilient environment while reducing the cost of GDPR compliance.

RSA: SUPPORTING A HOLISTIC APPROACH TO ADDRESSING DATA PRIVACY

RSA offers business-driven security solutions that uniquely 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 solutions built on industry standards and best practices on one configurable, integrated software platform. RSA Archer offers a wide variety of use cases designed to play a key part in helping an organization in establishing and maintaining GDPR compliance.

- RSA Archer Security Incident Management is designed to enable processes to address the flood of security alerts and implement a managed process to escalate, investigate and resolve security incidents.
- RSA Archer Security Operations and Breach Management is engineered to extend the security incident process by adding workflow for data breaches and management of the overall security operations team.
- RSA Archer Issues Management is intended to play an important role for an organization's GDPR program by helping organizations managing issues generated from risk and control assessments and audits.
- RSA Archer IT Risk Management is designed to help organizations accelerate the identification of IT risks related to GDPR compliance and improves an organization's risk mitigation strategies.
- RSA Archer IT & Security Policy Program Management provides the framework to help organizations establish a scalable and flexible environment to document and manage an organization's policies and procedures to help comply with the GRPR.
- RSA Archer IT Controls Assurance provides a framework and taxonomy to assist organizations to systematically document the GDPR control universe, enabling organizations to assess and report on the performance of controls at business hierarchy and business process levels.

RSA NETWITNESS® SUITE

The RSA NetWitness® suite is a threat detection and response platform that is designed to allow security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. RSA NetWitness directly helps organizations address GDPR requirements for user data protection in the threat discovery and response activity itself. RSA NetWitness is designed to scan your entire infrastructure for indications, often subtle or obfuscated, that exploits are active. The system is engineered with behavioral analysis and machine learning designed to correlates indicators and assigns risk scores that identify anomalies that warrant investigation.

Unlike traditional prevention systems, RSA NetWitness Suite helps your organization hunt for the threats that have successfully invaded your organization. Undetected, such exploits can wreak havoc on your infrastructure and intellectual property, and can create the types of data breaches that the GDPR specifically targets.

Additionally, the platform is engineered with a range of controls, such as obfuscation, that security analysts can leverage to help protect privacy-sensitive data, without reducing analytical capability. RSA NetWitness Suite can be configured to limit exposure of privacy-sensitive metadata and raw content (packets and logs) using a combination of techniques, including:

- Data Obfuscation – Privacy-sensitive metakeys can be obfuscated for specified analysts/roles
- Data Retention Enforcement – Retain privacy-sensitive data only as long as needed
- Audit Logging – Audit trail for privacy-sensitive activities, e.g., attempts to view/modify data.

For GDPR, timeliness will be absolutely critical in meeting the 72-hour breach notification requirement. RSA Netwitness can help speed up the process of understanding the scope and nature of a breach with improved visibility into the attack sequence.

RSA SECURID® SUITE

At the heart of GDPR is the need to establish data governance practices (technical and organizational) to secure access to PII. This means implementing identity and access management (IAM) technology and policies to ensure that users accessing PII are authorized to do so. Access governance allows you to know at any time who has access to what applications and data, what level of access they have, who approved the access as well as have an audit trail to prove who approved and how they received that access.

The RSA SecurID® Suite including RSA SecurID® Access and RSA® Identity Governance and Lifecycle is designed to enable organizations of all sizes to minimize identity risk and deliver convenient and secure access to their modern workforce. The RSA SecurID Suite leverages risk analytics and context-based awareness designed to ensure the right individuals have the right access, from anywhere and any device. Given the data governance

and identity management requirements within the GDPR regulation, these products can play a critical role in helping organizations to address the fundamental need for identity and access assurance.

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.

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 suite.

Obviously, a major requirement within GDPR is the efficient and effective management of incidents when they do occur. When organizations discover a security breach, they need to quickly determine exactly what happened, how it happened, the scope and impact of the compromise, and the steps needed to contain and remediate it. The RSA Incident Response team can help organizations quickly understand the details and the necessary steps to take during a breach. Paired with other RSA Archer solutions, the *RSA Incident Response Practice* can tailor those next steps to help organizations meet the unique requirements of GDPR.

The *RSA Advanced Cyber Defense Practice* can help security organizations develop the processes, procedures, workflows and automation that facilitate a prompt, decisive response to data breaches and other cyber incidents.

The *RSA Identity Assurance Practice* can support an organization in addressing the identity management requirements within GDPR by helping organizations pursue growth objectives while reducing identity-related security risks. Our services are designed to help improve your organization's ability to bridge the "islands of identity" that have popped up across your organization that create complexity and risk.

CONCLUSION

Globally, organizations are actively assessing the impact of 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 work through the deployment of additional processes, policies and technologies to avoid the significant fines posed by the regulation. Establishing and maintaining compliance designed to protect PII of EU citizens will be a complex and time consuming undertaking for most organizations.

RSA

RSA can help your organization establish the necessary framework to prepare yourself for this regulation by implementing a business-driven approach to security, ensuring your risk and control framework is accurate, complete, and prepared for today's regulatory challenges and business risks. With a unique scope of products and services spanning risk assessment, security controls deployment and management, and ongoing compliance management, RSA can act as a strategic partner to help any organization in its journey towards GDPR compliance.