RSA

SOLUTION BRIEF

HELPING ADDRESS DATA GOVERNANCE FOR GDPR WITH RSA

ADDRESSING THE TICKING CLOCK OF GDPR COMPLIANCE

EARLY PREPARATION FOR GDPR IS ESSENTIAL ACROSS THE GLOBE

The EU GDPR imposes interrelated obligations for organizations handling personal data of EU citizens, regardless of where they are incorporated, including:

- *Adopting policies and procedures to ensure and demonstrate that PII 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*
- *Performing data protection impact assessments on planned processing of highly sensitive personal data*
- *Providing transparent notice of processing activities, retention policies, data subject rights and other matters to EU residents at the time information is collected and upon later inquiry*
- *For some organizations, appointment of a Data Protection Officer charged with the responsibility of ensuring 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 to organizations that handle personally identifiable information (PII) of European residents. This regulation is intended to strengthen privacy rights and the security of such PII of individuals within the EU, whether that data is stored inside or outside of the EU. The scope of the GDPR encompasses all businesses established in the EU as well as any business outside the EU that controls or processes personal data related to individuals in the EU, making the GDPR a truly global compliance requirement.

Noncompliance 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 worldwide 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.

The GDPR specifies many actions organizations must take—institute a data protection officer, report a breach in 72 hours, acquire specific consent, and much more. However, at the core of the GDPR is the underlying requirement to implement data governance best practices to secure and protect PII by May 2018.

While all of the details of how organizations must implement Data Governance are not specifically dictated, the regulation places a lot of emphasis on implementing "…technical and organizational measures for ensuring the security of the processing" (Article 32 GDPR—Security of processing https://gdpr-info.eu/art-32-gdpr/). The regulation further requires controls, testing and documentation of these practices as part of compliance.

Organizations must protect PII in a number of different ways, and must be able to demonstrate due diligence in keeping 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, as well as ensuring that only authorized users have access to the data.

DATA GOVERNANCE FOCUS AREAS

Data governance fall into three key areas. While not new, these focus areas provide a foundational framework for organizations to focus on strengthening their GDPR compliance posture.

- Establishing controls and policies around data collection and usage
- Ensuring access to PII is proper and controlled
- Ensuring PII is properly processed and protected

Organizations need to establish and apply effective controls around the usage of PII, establish and manage retention requirements and maintain a record of processing activities of PII. By improving the framework and controls around the usage of PII, the organization is better able to address security risks, control access and meet reporting requirements for the management of PII.

To manage access to the data, organizations should institute an Identity and Access Management (IAM) solution to protect sensitive and personal information. Identity management has several components—authentication at the time of accessing the data as well as the overall governance of identities and levels of access across the organization. Multi-factor authentication can help organizations answer the question are my users who they claim they are? Having confidence in the answer is vitally important when protecting PII to only allow authorized users access. Working in concert with authentication, identity governance and lifecycle management allows organizations to answer the critical questions does the user have the right level of access? and is the access in compliance with policies? Proving that the access is appropriate, aligned with policies and auditable can help support overall compliance.

When access to data is managed and policies and controls are put in place, organizations then have greater confidence that PII in the organizations is being used for the proper reasons and access is limited only to authorized users. These data governance best practices support the GDPR by providing additional protection against accidental destruction, loss, alteration, unauthorized disclosure or access to personal data.

RSA: SUPPORTING A HOLISTIC APPROACH TO ADDRESSING DATA GOVERNANCE

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 an organization develop a holistic strategy for responding to the 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 the GDPR.

RSA SECURID® SUITE

At the heart of data governance specific to the GDPR is the need to manage who has access to PII, including auditing how they received that access, and ensuring that users who do access actually are who they say they are. Access assurance is key to preventing breaches resulting from unauthorized use of the data.

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 and is 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, these products can play a critical role in helping organizations to address the fundamental need for identity and access assurance.

RSA ARCHER® SUITE

The RSA Archer® Suite is an industry-leading Governance, Risk and Compliance (GRC) solution that includes specific use cases that are designed to play a key part in helping organizations to establish and maintain data governance for 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.
- 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 Officers, Data Privacy Officers 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.
- RSA Archer IT & Security Policy Program Management—RSA Archer IT & Security Policy Program Management is engineered to provide the framework for establishing a scalable and flexible environment to document and manage an organization's policies and procedures to help organizations comply with the GRPR. This includes documenting policies and standards, assigning ownership and mapping policies to key business areas, objectives and controls. By implementing the RSA Archer IT & Security Policy Program Management use case as part of an organization's GDPR program, organizations are empowered to effectively manage the entire policy development lifecycle process to align your control environment with privacy and data governance requirements.
- RSA Archer IT Controls Assurance—RSA Archer IT Controls Assurance is designed to provide a framework and taxonomy to systematically document the GDPR control universe, enabling organizations to assess and report on the performance of controls. Through RSA Archer IT Controls Assurance, organizations can deploy standardized assessment processes for controls and integrate testing results from automated systems. By improving the linkage between compliance requirements and internal controls, organizations are enabled to better communicate and report on GDPR compliance obligations using a common taxonomy and language.

RSA RISK AND CYBERSECURITY 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 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 Identity Assurance Practice—The RSA Identity Assurance Practice can support an organization in addressing the GDPR's prohibitions on unauthorized access to PII. 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.

RSA Risk Management Practice—The RSA Risk Management 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 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 needs to be working through the deployment of additional processes, policies and technologies now, in order to avoid the significant fines posed by the regulation. Maintaining data governance—through proper access and identity management policies and controls—will be critical in ensuring PII is properly cataloged and protected. With a unique scope of products and services targeting the critical areas of identity and access management and GRC, RSA can act as a strategic partner to help any organization in its journey towards GDPR compliance.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.