Organizations around the world have been watching anxiously as the General Data Protection Regulation (GDPR) approaches, bringing with it the potential for tremendous upheaval. Those who haven’t made a priority of preparing for this monumental shift in how private data is collected, stored and protected—which amounts to about half of US multinational companies, according to a PwC survey\(^1\)—face a very real risk of damage as GDPR blows in on May 25, 2018. With the potential for fines for noncompliance to reach in the millions of euros, the financial hit could be enough to shut some entities down. There’s still time to prepare, but with just months to go, it’s important to act quickly. This paper sets out five basic steps organizations may want to consider to help set up a framework for managing GDPR risk.

1. **KNOW WHAT’S COMING**

   It may sound obvious, but the first step in being prepared for GDPR is developing a clear awareness and understanding of the regulation and its requirements, particularly with regard to how those requirements apply to your organization. In brief, GDPR 1) applies to all companies that handle personal data of citizens of the EU, regardless of whether those companies are located in the EU, and 2) requires privacy controls to be implemented around processes for data collection, storage and protection. What does that mean precisely? There’s no getting around it: the only way to fully grasp its implications for your organization is to review the regulation itself (yes, all 99 articles) in detail, preferably with the guidance of legal and regulatory experts.

2. **SURVEY CURRENT CONDITIONS**

   Before you can strive towards meeting GDPR requirements for how to handle private data, you need to know what you’re dealing with—what data in your organization is subject to the privacy protections GDPR mandates, as well as where it’s stored and how it’s being used. If that sounds like a lot to track, it is. And the process is made even more challenging by the fact that data today is as likely to be in the cloud as in an on-premises data center. While automated tools can help meet the challenge of accurately identifying the type and amount of data residing in the IT infrastructure, much of this challenge will depend on data governance processes you implement regardless of whether the data is on-premises or in the cloud.

3. **CHECK YOUR STATE OF READINESS**

   Once the data that flows through the organization has been fully inventoried, it’s time to look at the ways in which data privacy is already being protected. Most organizations are likely to have measures in place to safeguard data, such as encryption processes, and these measures may have an important role to play in meeting some of the GDPR requirements for protecting the

---

\(^1\) PwC GDPR preparedness pulse survey, December 2016
privacy of data the organization collects and stores. Other existing measures organizations are likely to already have instituted that relate to safeguarding data include privacy impact assessments, formal data governance policies and data backup and retention policies and tools.

4. MANAGE THIRD-PARTY RISK
Any organization that operates in the public cloud—whether in part or entirely—or that maintains relationships with vendors and contractors that involve data sharing will find its GDPR risk complicated by the presence of third parties. Documenting third-party engagement, evaluating the level of risk the parties pose and optimizing third-party governance are all important and necessary aspects of managing GDPR risk.

5. BE PREPARED TO MOVE FAST
One key GDPR requirement is the 72-hour breach reporting rule, which mandates that any data breach must be reported no more than 72 hours after the organization that’s been breached becomes aware of it. To be prepared to act that quickly when the law goes into effect, planning needs to start now. That means thinking about what capabilities you will have in place to determine the scope and impact of a breach within 72 hours. This is especially critical given that there is evidence today that while breaches may take just minutes to happen, they can take months to discover.²

In the months remaining before GDPR takes effect, organizations can do a lot to plan and prepare for the impact, so that the effect on operations is minimized. To learn more about how RSA Archer can help with implementing GDPR governance, risk and compliance solutions in your organization, visit rsa.com/gdpr.

ABOUT RSA
RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, visit rsa.com.
Content and Liability Disclaimer

This White Paper is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Mention of RSA products or services is provided for informational purposes only. RSA Security LLC, EMC Corporation, Dell, Inc. and their affiliates (collectively, “RSA”) make no express or implied warranties with respect to the accuracy or completeness of the information contained herein. RSA shall not be responsible for any errors or omissions contained in this White Paper, and reserves the right to make changes anytime without notice. No contractual obligations are formed either directly or indirectly by this White Paper. All RSA and third-party information provided in this White Paper is provided on an “as is” basis. RSA DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, WITH REGARD TO ANY INFORMATION (INCLUDING ANY SOFTWARE, PRODUCTS, OR SERVICES) PROVIDED IN THIS WHITE PAPER, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. In no event shall RSA be liable for any damages whatsoever, and in particular RSA shall not be liable for direct, special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue or loss of use, cost of replacement goods, loss or damage to data arising out of the use or inability to use any RSA website, any RSA product or service. This includes damages arising from use of or in reliance on the documents or information present on this White Paper, even if RSA has been advised of the possibility of such damages. This White Paper may not be reproduced without RSA’s prior written consent.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, RSA and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA 7/17 H16472.

EMC2, EMC, the EMC logo, RSA, Archer, FraudAction, NetWitness and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other products or services mentioned are trademarks of their respective companies.