# 4 Things to Know
# —Today—
## About Ensuring GDPR Readiness and Compliance

WHITE PAPER

The General Data Protection Regulation (GDPR) may be the most important compliance and privacy initiative facing any organization accessing, storing or sharing personal information of European Union residents. As enterprises scramble to ensure their systems and processes are in place when the "go-live" date arrives, it's important to keep in mind four essential steps to take now.

On May 25, 2018, one of the widest-ranging and most stringent mandates on protecting personal data goes into effect—the General Data Protection Regulation (GDPR). This regulation—which spans the entire European Union (EU)—strengthens and unifies privacy laws in place for the EU's 28 member nations.

But GDPR is much more than a way to align data protection laws. It represents a dramatic expansion of the very definition of data protection as it relates to maintaining the privacy of personal data of European residents. And, in the increasingly global economy, that makes it relevant not only for EU-based organizations, but also for any enterprise doing business in an EU member nation, or controlling or processing personal data on any EU resident.

GDPR, which builds on the earlier 1995 Data Protection Directive, carries a strict and extremely costly set of penalties for violations. The fines range up to 20 million euros or 4% of gross annual revenues—whichever is greater. Fines can be levied for a variety of issues including, in certain circumstances, failure to notify supervisory authorities and, if relevant, individuals whose personal data was breached, within 72 hours after the breach was discovered. Even the very nature of a data breach has been re-scoped to include accidental destruction or alteration of personal data, or not having adequate processes in place to prevent unauthorized access to personal data.

RSA

TechTarget | Custom Media

As is often the case with the adoption of new governmental mandates—even one as wide-ranging and impactful as GDPR—not all organizations have proceeded with the proper sense of urgency in putting in place the necessary systems and processes to ensure compliance. A recent study from Osterman Research indicated that 64% of respondents' organizations were not ready to comply with GDPR requirements.[1] Yet another study pointed out that 60% of EU-based organizations and 50% of US-based enterprises say they face serious challenges in being GDPR compliant.[2]

Business and IT executives all need to be clear about a few things relating to GDPR:

- Compliance is not optional, and there is no "grace period" to allow a gradual achievement of compliance after May 25.
- This is a global initiative, affecting a very large percentage of enterprises based outside of the EU.
- The GDPR is written in a non-prescriptive way. That is, it does not include a lot of very specific "you must do things this way" guidelines, but rather requires organizations to take a risk-based approach.
- GDPR compliance is evidence based, in that it requires strict and clear documentation of processes and steps done to demonstrate compliance.

Fortunately, even though many organizations still find themselves playing catch-up on meeting the GDPR compliance deadline, there are some specific things enterprises can and should do now in order to get prepare for the May 25. Here are four steps you should take in order to help prepare for GDPR compliance and avoid operational, financial and reputational problems.

## 4 Steps to GDPR Compliance

GDPR compliance demands a risk-based approach in order to achieve the many goals of individual privacy and rock-solid data protection. This requires a highly collaborative effort among business executives, IT and security professionals, chief data officers, legal and compliance teams.

It also necessitates a multi-part framework that covers all the bases in building the design, deployment and ongoing management of technology designed to help with GDPR compliance.

There are four key steps in this journey toward GDPR compliance that all organizations—regardless of industry, company size, technology profile or business risks—should take:

1. **Risk assessment.** This is where everything starts, because without a full, open and frank assessment of potential risk factors, GDPR compliance is difficult to achieve. Organizations must have a full and current inventory of all data assets and a thorough understanding of what EU resident personal data they collect and store. This is where gaps are identified between risks and internal controls, and initial steps can be planned for bridging the gaps. In this phase, a process is developed that allows appropriate controls to be identified, designed and implemented to improve risk mitigation strategies.

2. **Data governance.** In order to prepare for GDPR mandates, organizations must know where EU resident personal data resides and who has access to that data. This is the starting point to putting in place proper controls—ensuring that the user's access to that personal data is relevant to their job responsibilities. Credentials can be hacked and privileges may go out of date, which means that secure authorization must be constructed in the context of business-aware and role-aware governance throughout the entire lifecycle of the personal data in question. Unless organizations know if a user has the proper access to personal data, and that the right access controls are in place and governance policies are updated as circumstances change, GDPR compliance is at risk.

3. **Breach response.** Once data breaches are identified, rapid response is essential in order to maintain compliance with GDPR's stringent guidelines for timely notification. This means that organizations must be able to detect breaches quickly—and ideally before they have a chance to take hold throughout the network and affect personal data. Full visibility is a must-have function across your full infrastructure, global data architecture and range of data assets. Typically, the proper supervisory authorities must be notified without undue delay, as must be any data subject where the breach is likely to result in a high risk to the rights and freedoms of such data subject.

1 "A practical guide for GDPR compliance," Osterman Research, July 2017
2 "Countdown to GDPR: Challenges and concerns," Varonis, October 2017

4. **Compliance management.** GDPR compliance is not just about passing an annual audit; in fact, the concept of continuous compliance requires a commitment to ongoing compliance monitoring and management. Also, compliance management should be engineered to help organizations prioritize different compliance issues as they arise, in order to put the right resources against the right problem at the right moment. At the same time, compliance processes, systems and tools must be designed in order to avoid disrupting essential business operations. Demonstrating that you actually have the proper safeguards in place, and a process to continually monitor compliance can go a long way toward convincing regulators that your organization has done its due diligence in meeting both the letter and the spirit of the regulation.

## Taking a Platform Approach to Comprehensive, Ongoing GDPR Compliance

As organizations have strived to implement the necessary technical and organizational measures required under GDPR, some have deployed numerous different solutions designed for individual use cases. This approach—rather than using a comprehensive framework to avoid data protection gaps—is inefficient, difficult to manage and more costly than using a tightly integrated GDPR platform.

By adopting and implementing a multifunctional GDPR platform, organizations not only can meet the mandate's guidelines faster, but they also can align the compliance initiatives with key daily operating processes.

A platform approach to GDPR compliance helps to ensure that technical tools and solutions enable continuous compliance monitoring and management, without unnecessary duplication and overlap, as well by minimizing the potential for gaps in functionality and data protection coverage. Ideally, the platform should help organizations identify business risks such as regulatory obligations, misalignment in risk management and data priorities, and imprecise modeling of potential financial impact of data breaches.

At the same time, the platform should account for important technology risks, including infrastructure and application protection, security event identification and rapid response, sifting out "false positives" in event identification and guarding against technology obsolescence as technical risks evolve.

This platform approach helps reduce—and ideally eliminate—the gap between what you already have in place to enable GDPR compliance and what you actually need. Solutions need to be engineered from the start to enable continuous compliance management, privacy by design and adherence to the other GDPR articles. This means your platform must deliver:

- Full data visibility, across location, devices and architecture
- Rapid insight into activity that may signal a potential data breach
- Proper business context that helps align threats with their business impact
- Efficient, comprehensive response capabilities to mitigate the potential for hefty financial fines prompted by a breach and insufficient or delayed acknowledgement

## Conclusion

GDPR is an unavoidable challenge in in doing business with any EU resident or any organization or entity located in or controlling or processing personal data of a European Union resident. Compliance is not optional, and violations carry the very real risk of hefty fines, unwanted publicity and loss of customer confidence.

IT and business decision makers working toward GDPR compliance should focus on each of the four steps identified in this paper—risk assessment, data governance, breach response and compliance management. This synergistic, comprehensive approach will enable more efficient implementation and continuous compliance management and coupled with a platform approach can enable full visibility, rapid insight, business context and efficient response.

## ABOUT RSA

RSA, a Dell Technologies business, 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/gdpr.