Three Things Tech Companies Should Do to Get GDPR Compliant

04.19.18

This article originally appeared in the May 1, 2018 issue of the San Francisco Business Times. To view the original article, click here.

Everyone has different standards for privacy online. Some people are happy sharing their every thought with the world, while others actively avoid any social media presence. Similarly, some consumers don't mind sharing personal data with businesses, while others are more protective of their information.

But while individuals may differ in terms of what they want to share online, nobody wants the data they do share to be misused or mishandled – that's what the European Union's new General Data Protection Regulation (GDPR) is all about. Though unprecedented in the digital realm, GDPR ultimately goes back to a society's right to set limits on what methods of information collection are acceptable.

The result is that many data-driven businesses accustomed to traditional methods of gathering, storing and sharing customer and consumer data will find that GDPR is more demanding than what they're used to. Most "opt-outs," for example, will now need to be replaced with affirmative "opt-ins." GDPR also introduces the idea of a new kind of personal information, "pseudonymized" data, which makes connecting the data to an individual almost impossible. Because pseudonymized data is less rigorously guarded, organizations will be highly incentivized to store data in this format.

These examples represent just a sample of the changes brought about by GDPR, so it's not surprising that even with the deadline for implementation looming, many organizations don't feel prepared. Thankfully, there are some strategic decisions companies can make to lessen the pain of transition.

To help you get started with your company's transition to GDPR, here are three initial steps you should take to ensure that complications relating to compliance don't hurt your business.

1. Focus on Preventative Measures

Article 25 of GDPR specifies that companies must protect customer data "by design and by default." Adhering to this regulation requires companies to essentially forget about data protection as a discrete department of the organization and instead incorporate it as a central principle of business process design from the ground up. For example, to stay in compliance with GDPR privacy requirements, personal data should only be processed in cases where it is absolutely necessary.

As you may have guessed, adhering to these kinds of regulations requires a solid understanding of both your data security policies and your current business processes. If you find that you don't have a grip on the latter, then consider GDPR an opportunity for a bit of important housekeeping.

2. Get Certified Now

Because GDPR is far broader in scope than U.S. regulations, American companies that do business globally may find themselves subject to regulation for the first time since incorporation. Thankfully, GDPR isn't drastically different from certain U.S. regulations, meaning that there are plenty of resources to help companies get close to full compliance.

One thing all digital businesses not explicitly subject to U.S. regulations should be doing is getting ISO-certified before doing business in the EU, if at all possible. It's also important to note that if your organization is already compliant with HIPAA, PCI and the like, then the transition will be significantly smoother.

The lesson here is that the more regulatory certifications your organization earns, the easier it will be to demonstrate your commitment to data privacy – whether for GDPR or for some future regulatory change.

3. Embrace the Spirit of Cooperation

Even if you've been preparing for GDPR for months, you might be worried about how it's all actually going to work. Business and IT leaders aren't the only ones, though. Until it happens, regulators, too, won't know exactly how certain provisions will work in practice. They'll be learning just as much as you are, initially.

In this transition phase, dedication to the spirit of cooperation may be the best asset. Ignoring or resisting requests from regulators will only make things more difficult for everyone involved. Don't forget that GDPR gives regulatory bodies the ability to heavily penalize organizations who fail to take reasonable steps.

As GDPR comes into effect on May 25, 2018 it is critical that companies adhere to the application penetration test as part of their due diligence. Learn how BPM's information security assessment practice can help you get compliant. Contact David Trepp at dtrepp@bpmcpa.com *or 541-687-5222.*

BPM's Information Technology Audit and Compliance Group (IT Assurance), *provides comprehensive IT counsel to emerging growth, late stage, private and public companies. BPM is the only company headquartered in California accredited to perform ISO 27001 certifications, FedRAMP assessments, and SOC 1/SOC 2 examinations.*

David Trepp *is a partner in the IT Assurance Practice at BPM and leads its Information Security Assessment Services Group. A technology entrepreneur since 1989, Trepp has led over 1,100 information security penetration test engagements for clients across all major industries throughout the United States and abroad.*