Why Your Small U.S. Business Should Care About GDPR

PUBLISHED ON
March 19, 2018

You're not alone if your small business hasn't been paying close attention to the fact that the General Data Protection Regulation (GDPR) goes live May 25. You may think the new European standard for cybersecurity doesn't apply to you because you don't do enough business in Europe to fall under the new regulation. Maybe you think your business is too small to be affected by the new regulation.

Maybe you're wrong?

GDPR is the European Union's (EU's) sweeping and comprehensive data security regulation. Its primary goal is to create more consistent protection of consumer and personal data across all EU nations. The bad news for businesses is that GDPR's requirements are strict. Stricter, in fact, than the already strict patchwork of U.S. data security laws and regulations. GDPR's definition of "personal data" is much broader than the one we often use under U.S. laws and regulations and includes IP addresses, social media handles and other pieces of information that a business might collect about a person. It also provides EU citizens and residents a "right to erasure" and "data portability" - meaning that a person has a right to have their personal data completely eliminated or transmitted to another controller. GDPR violations can be steep - up to $20 million. The real intimidating news for U.S. businesses is that GDPR's jurisdiction extends well beyond the borders of the EU and allows both its citizens (wherever residing) and its residents to pursue legal action against violating businesses even if those businesses are outside of Europe.

How does a U.S. business determine if the GDPR applies to them? Start by conducting a data security risk assessment - one that includes an evaluation of whether your business is regularly marketing to or doing business with customers who have some connection to the EU. Review your business's web presence and determine if your business is monitoring and collecting IP addresses of those using your website. Pay particular attention if those IP addresses originate in the EU. If your business is doing any of these things, it could be violating GDPR. The bottom line is that your business needs to become familiar with GDPR regulation and its requirements.

It will certainly be interesting to observe the nature and breadth of enforcement actions U.S. businesses may see under GDPR, as each EU country is going to be able to enforce GDPR on behalf of its own citizens. Ultimately, advance preparation will be key for U.S. businesses looking to steer clear of enforcement actions.If you have any questions about GDPR, please reach out to me.

:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com