NEWS ALERT

PRIVACY & CYBERSECURITY

Three Important Considerations For All Businesses in Light of GDPR

By Dena M. Castricone | May 25, 2018

Today, the European General Data Protection Regulation ("GDPR") takes effect. The GDPR is the most comprehensive and complex privacy regulation currently enacted. The GDPR can apply to a business or organization (including a non-profit organization) anywhere in the world and its potential financial impact is huge; fines can reach up to € 20 million Euros (over $23 million USD) or 4% of an entity's total revenue, whichever is *greater*. Not surprisingly, the potential for this type of penalty has caused concern and chaos leading up to the May 25, 2018 effective date. In light of this significant international development, all organizations should consider the following:

1. Does the GDPR Apply?

If your entity "processes" the "personal data" of anyone within the European Union, then the GDPR may apply. "Personal data" under the GDPR is any information that could identify an individual, directly or indirectly, like a name, email address or even an IP address. The GDPR also broadly defines "processing" to include activities such as collecting, storing or using the personal data. For more information on how to determine if the GDPR applies to your entity, watch our 3-minute video on the subject.

2. If the GDPR Does Apply, What is the Compliance Strategy?

You need a plan. Yes, it would have been ideal to have it in place by today but if the GDPR applies to your entity, do not delay any further in creating a GDPR compliance strategy. A GDPR compliance strategy starts with a detailed examination of your entity's data collection and use practices. Those practices must comply with the GDPR requirements and your entity may need to implement new or revised policies to address specific compliance requirements. This process is specific to the particular practices of each entity – there is no one-size-fits-all GDPR compliance program. You can find the regulatory language here.

3. Even If the GDPR Does Not Apply, How Do You Handle the Data You Collect?

Even if the GDPR does not apply to your entity, there are significant risks and liability surrounding the data collection and processing practices of any business. Data breaches happen every day. No business is immune. Each organization should closely examine its data collection and use practices and determine if it absolutely needs all of the data it collects. Then, the organization must determine whether the steps it is taking to protect the data it collects are reasonable in today's environment. In Massachusetts, businesses must undergo this process and create a written information security plan. In Connecticut, having such a plan may help avoid a government enforcement action if you experience a data breach. In addition, the Federal Trade Commission and states' Attorneys General are actively pursuing companies with questionable privacy practices

We have helped many clients with privacy projects including GDPR compliance and creating written information security plans. If you have any questions or need assistance with any privacy or cybersecurity matter, please contact:

Dena M. Castricone at dcastricone@murthalaw.com or 203-772-7767 or
Daniel J. Kagan at dkagan@murthalaw.com or 203-772-7726

Also, subscribe to our blog at www.privacyandcybersecurityperspectives.com.