TUGGLE DUGGINS

ATTORNEYS AT LAW

March 21, 2018

Why North Carolina Companies Need to Prepare for Europe's New Privacy Rules

In just over two months, on May 25, 2018, the European Union (EU)'s newest privacy regulation, the General Data Protection Regulation (GDPR), will go into effect after years of drafting, debating and preparation. For business owners in North Carolina, this news may initially be met with a shrug; but the GDPR could have far reaching consequences well beyond the physical boundaries of the European Union. While companies based in Europe and major multinational corporations have been carefully preparing for this new regulation, many small-to-medium businesses in North Carolina and elsewhere in the United States continue to be unaware of the direct impact this new regulation could have on their business—even if those companies do not have a physical presence or employees in Europe. Being unprepared for the GDPR could leave many unsuspecting North Carolina businesses facing stiff financial penalties.

What is Protected by the GDPR and Who is Subject to the New Regulation?

The GDPR is designed to create uniform privacy laws across Europe and to better protect the personal data of EU citizens, including how that data is collected, stored, processed, used, and destroyed. The GDPR defines "personal data" to include any information related to a natural person that can be used to directly or indirectly identify that person. This broad definition can encompass anything from a person's name or photo to bank details, IP addresses, or posts on

social networking websites. Under the GDPR, companies will be required to implement more robust protections for personal data that they collect on EU citizens.

The GDPR is not limited to only European companies; rather it applies to any company which processes the personal data of EU citizens residing in the EU, regardless of the company's location. For example, a furniture manufacturer in High Point, North Carolina who regularly advertises or sells its merchandise online to consumers in Belgium or Germany would be subject to enforcement under the GDPR if that company is processing personal data, such as bank account details, of EU citizens in the course of those transactions.

What is Required Under the GDPR?

The GDPR introduces a number of new mandates, including revised conditions for consent, a narrow time frame for notifying authorities in the event of a data breach, and what is known as the "right to be forgotten."

While many company websites have long buried their terms and conditions in difficult-to-find locations or load the terms and conditions with a box prechecked for accepting them, the new regulation will require companies to stop using long privacy disclosures filled with difficult to understand legalese. Requests for consent to process an individual's data must be presented in an easily accessible form, using clear and plain language. Additionally, it must be as easy for the person to later withdraw consent as it is for the person to give it initially. Finally, parental consent will be required to process personal data of any EU citizen under the age of 16.

Likewise, under the GDPR, a company that is exposed to a data breach must notify the proper authorities in any European country where such a breach is "likely to result in a risk for

the right and freedoms" of EU citizens residing within that country within 72 hours of first becoming aware of the breach. Additionally, the customers whose personal data was subject to the breach must be notified without undue delay after becoming aware of the breach. These tight notification deadlines will require companies to have a clear action plan in place so they are not left unprepared and scrambling to try to meet the 72 hour deadline.

EU citizens also have what is known as the "right to be forgotten" under the GDPR. This means that EU citizens have the right to request that a company erase any personal data concerning themselves, and that the company must do so upon request without undue delay under various circumstances, including where the original purpose for collecting the personal data is completed or where the individual withdraws their consent. Returning to the example of the furniture manufacturer in High Point, this means that once the transaction is complete, the EU customer would have the right to request that the furniture manufacturer erase any personal data it may have retained about the customer.

In addition to these overhauls, the GDPR mandates a host of other changes, including requiring companies whose "core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale" to hire a data protection officer to help protect consumer personal data. To put that in simpler terms, a second example is helpful: a cloud-based data storage company based out of Durham, North Carolina providing services to clients in Europe may very well have to hire a data protection officer who meets all of the required qualifications listed in GDPR in order to be in compliance with the regulation.

What is the Penalty for Not Complying?

The GDPR does not just include many new rules; it also comes with serious teeth to enforce those rules. A company in breach of the GDPR can be fined up to four percent (4%) of its annual global gross revenue or €20 million (roughly $25 million), whichever is greater. While a maximum fine would be imposed for only the most serious violations of the GDPR, the threat of significant financial penalties still looms large for companies of all size doing business with EU citizens.

There remain several open questions and some confusion as to how the GDPR will be enforced outside of Europe. For some non-EU based companies processing or controlling EU citizens' personal data, the GDPR could require the company to appoint a representative within the EU to act as a point of contact for data protection regulators. For most companies, which are not required to appoint a representative under the rule, the EU member country whose citizens are impacted by a non-EU company's violation of the GDPR will need to rely on current international law to attempt enforcement. Thus, if a European country has a treaty with the United States allowing such, that country may be more likely to attempt enforcement than a country without such a treaty. The result is that there will likely remain a fair degree of ambiguity as to how enforcement of the GDPR will actually function in practice until it goes into effect and new standards begin to emerge.

A more likely scenario could arise where EU-based companies are reluctant to do business with non-EU based companies that are not in compliance with the GDPR. A fear of

running afoul of EU regulators could very well incentivize European companies to seek out business relationships with companies that are in compliance, ultimately resulting in U.S.-based companies having to come into compliance with the GDPR even if the threat of governmental enforcement remains low.

Conclusion

With the GDPR set to go into effect on May 25, 2018, companies doing business with citizens of the EU should not sit idly by and be caught off guard. Enactment of the GDPR can be an opportunity to take some time to review your company's data protection policies or to talk with an attorney about what steps should be taken now to prevent serious financial consequences down the road. As Benjamin Franklin once famously advised, an ounce of prevention is worth a pound of cure.

For more information, contact Ross Hamilton at rhamilton@tuggleduggins.com or (336) 271-5279 or contact Daniel Stratton at dstratton@tuggleduggins.com or (336)271-5240.