June 27, 2018 | Business, Corporate & Securities, Insights

Why you should care about complying with the GDPR even if you don't have customers in the European Union

By: Rich May, Arvid von Taube

You have probably noticed over the past month that most of the websites that you use have notified you that they are updating their privacy policies and terms of use and that by continuing to use the website, you provide certain consent to their use of cookies and the data they may collect from you.

These updates are all in response to the European Parliament's adoption of the **General Data Protection Regulation** ("GDPR") that became enforceable on May 25, 2018. The companies that operate these websites scrambled to become compliant with the GDPR's requirements and if you operate a website, you should pay attention to compliance as well, even if you don't have many customers in, or visitors from, the European Union. In fact, according to a recent study, more than two-thirds of U.S. companies believe that the GDPR will impact them.

WHO DOES THE GDPR APPLY TO?

The GDPR applies to the collecting and processing of personal data of individuals in the European Union ("EU"). This data includes a person's name, address, identifying internet data such as IP address, location and typical browsing data and website preferences stored in cookies. The GDPR affects U.S. companies because any company that stores or processes such personal data about citizens or residents of the EU, regardless of where that company is located, must comply with the GDPR. Although cookies do not necessarily have personal data stored in them, the European Parliament believes that cookies can be used—with other data—to uniquely identify someone, and therefore are subject to the GDPR.

KEY REQUIREMENTS OF THE GDPR

The GDPR allows companies to store personal data subject to certain requirements, including:

Related Services

Business, Corporate & Securities

Related Attorneys

Arvid von Taube

- The data may only be stored for as long as it is necessary for the purposes that it was collected.
- The data must be able to be transferred from one company to another.
- The data may only be collected with the consent of the person and such consent must be freely and affirmatively given. As noted in the lawsuits described below, this calls into question the typical practice of clauses like, "If you do not agree with the terms of our new Privacy Policy you must cease use of our website immediately" and "Your continued use of our website means you agree with our updated Privacy Policy and consent to the collection of data."
- Consent may be revoked by the person who gave it at any time, effectively requiring the company to keep track of all consents given. In other words, it is no longer sufficient to just have a click-through screen or notice on your website, but you must store and manage consents on your backend.
- The person has the "right to be forgotten", meaning if the person revokes consent, the person can request that all data tracked and stored be deleted. However, this right would not supersede any existing legal requirements in the U.S. (or abroad) that requires a company to maintain certain data, such as HIPAA requirements for healthcare records.

WHAT CHANGES SHOULD I MAKE?

Your website may already (and should) have a privacy policy and terms of use, but if it doesn't, those are the first things you should create. The privacy policy should clearly and plainly describe what kind of data is collected, for what purpose it is stored and for how long. If your website uses cookies, which most modern ones do, your policy should outline their purpose as well. Your website must display a cookie banner and ask a user for specific consent to the use of cookies and the collection of data. This information should be tracked in order to comply with the "right to be forgotten" requirements under the GDPR. Included in this tracking should be evidence that you obtained specific consent from the website user (e.g., that they clicked "I agree", "Yes" or "OK" on your cookie banner and personal data collection notice). Take special care not to prefill or prepopulate any answers for the user so that their consent is freely and affirmatively given.

You should also consider how third parties handle the data you collect from your website users. For example, ensure that any vendors or other third parties with whom you may share this data also comply with the requirements of the GDPR, which may necessitate a review of your standard form contracts or one-off contracts with third parties.

Finally, although a lot of the talk involving the GDPR centers on websites as they are the predominant means of collecting electronic data and use of cookies, don't forget about

your mobile app! Mobile use is quickly surpassing traditional web browsing on computers and your mobile app is subject to the same requirements as your website with respect to data collection under the GDPR. Any use of such app should be subject to written policies, explicit consent and tracking of collected data.

RISKS OF NON-COMPLIANCE

Depending on your business, location of website visitors and risk assessment, there are a number of options available to you in order to comply with the GDPR. First, you can take the approach of a number of large U.S.-based businesses and simply block all visitors from the EU (approx. 500 million people), including any U.S. citizens that may be visiting the website from the EU or if their home internet connection is run through a proxy/VPN in an EU member nation. At the end of May 2018, The Los Angeles Times, The Chicago Tribune, The New York Daily News and A&E Television Networks are a few examples of companies that simply blocked connections from the EU until such companies could figure out how to become fully compliant with the GDPR. It is unlikely that this blocking will be permanent but it highlights the risk and cost analysis for businesses.

Alternatively, assuming you have determined that it is not cost-prohibitive to comply with the GDPR, you should evaluate each piece of your data collection and retention and ensure that your documentation, including privacy policy, cookie policy and third party contracts, complies with the GDPR.

Regardless of which avenue you choose, even basic steps should be taken to ensure some compliance as failure to comply comes with steep penalties: up to €20 million or 4% of global annual turnover, whichever is higher. Recent examples of this are lawsuits filed against Google, Facebook and WhatsApp, accusing them of forcing users to choose between accepting new terms of use for compliance with the GDPR or stopping use of the websites, which may be considered coerced consent and therefore not freely given. However, these are high profile examples of Fortune 100 companies, and local mom and pop internet presences shouldn't garner immediate enforcement action. In fact, Andrea Jelinek, the EU's new chief regulator of data privacy, appears to be taking a measured approach to enforcement, noting that although regulators "have legal procedures to fulfill", they also "have to give [businesses] the opportunity to talk with us too. We are at the beginning of a journey, which we're going to make together through the field of data protection."

All of this may sound daunting, especially reviewing existing documentation for compliance. We're here to help! Give us a call if you have any questions.

Disclaimer: This summary is provided for educational and information purposes only and is not legal advice. The websites and companies mentioned herein are for illustrative purposes only, and the author and Rich May, P.C. do not recommend any services or products that they may offer. Any specific questions about these topics should be directed to attorney Arvid von Taube.