BrownWinick
ATTORNEYS AT LAW®

GDPR is Here – Is Your Business Ready?

By **Brian McCormac, Caitlin Andersen, and Thomas Story**, BrownWinick Attorneys
mccormac@brownwinick.com / andersen@brownwinick.com / story@brownwinick.com

When you think of Black Friday, you may cringe about stampeding customers seeking bargains the day after Thanksgiving. However, Friday, May 25, 2018 brings an entirely different source of dread for businesses: compliance with the EU's General Data Protection Regulation ("GDPR"). You are not alone if your business is not ready for GDPR, as a recent study indicated that 85% of US and EU companies were not fully prepared for GDPR's effective date of May 25.

What Is GDPR?

GDPR replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy, and reshape the way organizations approach data privacy. GDPR is brand new and with a length of 261 pages in English (much of which is still being ironed out) there are questions remaining about how it will be implemented. However, some of the key provisions of GDPR include:

- *Increased Transparency/Notice.* Companies are required to notify data subjects of the information they collect, how and why they use it, and with whom they share the data, all in clear, easily understandable language.
- *"Privacy by design."* GDPR requires that companies implement appropriate technical and organizational measures to protect the rights of data subjects.
- *"Data Minimization."* Companies must hold and process only the data that is "absolutely necessary" and limit access to personal data to only those who need it.
- *Penalties.* Fines for violations can be in amounts up to 4 percent of annual global turnover or €20,000,000, whichever is greater.
- *Clear and Revocable Consent.* Requests for consent to gather information must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. It must be as easy to withdraw consent as it is to give it.
- *Breach Notification.* With any data breach likely to result in a risk for the rights and freedoms of individuals, companies must notify customers within 72 hours of becoming aware of the data breach.
- *Right to Access.* Data subjects may request whether a company is processing their personal data and for what purpose. Companies must provide a copy of the personal data upon request.
- *Right to be Forgotten.* In certain circumstances, data subjects have a right to require companies to erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing activities.

Does GDPR Apply to Your Business?
If your company has information about EU residents, GDPR likely applies to you. The GDPR applies to all companies, regardless of location, who are processing personal data of EU residents, with a few exceptions. However, GDPR does not extend to businesses' information. It only applies to real people.

Do We Need Consent from EU Residents?
Consent is not necessarily required for all data processing activities. The GDPR sets forth several alternate reasons for data processing that do not rely on consent. Among these are: (a) compliance with a legal obligation, (b) performance of a contract, (c) vital interest of a person, (d) public interest, or (e) the company's legitimate interest. Consent is generally required for the processing of sensitive information, such as race, religion, political opinions, health information, and biometric data. If consent is required, it must be clear, unambiguous, and revocable.

What Should Your Business Do?
If it appears that GDPR applies to your business, the first step is to identify a person in your organization to take the lead on data privacy. That person should ask the following questions:

- What information does our company collect about European residents?
- How does our company collect and use this information?
- Do we share this information with third parties, and for what purpose?
- For how long will we need this information?

The answers to these questions will help inform a review and update of your privacy policies and practices. It is advisable to consult with counsel knowledgeable about global data privacy as you work toward compliance with GDPR and other data privacy regulations.

For more information regarding GDPR and how it may impact your business, please feel free to contact Brian McCormac, Thomas Story, Caitlin Andersen.

666 Grand Avenue, Suite 2000
Des Moines, IA 50309
515-242-2400
www.brownwinick.com