The General Data Protection Regulation (GDPR)

BUCKINGHAM

NEW STRICT PRIVACY REGULATIONS FOR US-BASED COMPANIES

targeting European Union Customers

A significant increase in personal data protection requirements for European Union (EU) members will take effect on May 28, 2018. Businesses may be fined up to 4% of global revenue or €20 million (whichever is greater) for violations. The standards affect any US company that solicits EU consumers regardless of whether they maintain a physical presence there. This includes companies using third-party firms such as marketing or e-commerce companies for EU operations.

The GDPR will affect businesses that market and sell goods or services in the EU or collect or process EU consumer personal information.

What data is protected: Personal data of individuals located in the EU is protected. The location or country of the entity holding or processing the data is now irrelevant. Personal data is broadly defined "as any information relating to an identified or identifiable natural person." This will include information such as: names, addresses, phone numbers, email addresses, IP addresses, vehicle identification numbers, and other data that would allow for identification of an individual directly or indirectly. Special categories of data further include information related to race, gender, genetic data, political affiliation, social, and cultural information.

Obligations for US businesses: This represents a significant increase in data privacy and security requirements for affected businesses, along with significant penalties for non-compliance. Companies must provide detailed disclosures to EU customers when collecting personal data, including obtaining "affirmative explicit consent to collect the data through a clear affirmative act freely given that is specific and informed" in some instances. New strict 72 hour notification requirements of a data breach will now apply. Additionally, EU residents have the right to have their personal data deleted "without undue delay" and to have personal data deleted once a business transaction is completed.

Immediate Action Items:

Ask yourself: Do I have customers, employees or potential customers in the EU?

If so, please consider taking the following actions immediately:

1. Review current data collection activities to understand what data you hold, where it comes from, and the obligations regarding the data.
2. Review any public facing privacy policies and practices.
3. Review current user consent policies and practices.
4. Review standard contract terms and provisions related to e-commerce or data collection.
5. Determine whether you need to appoint a data-protection officer to oversee GDPR compliance.
6. Consider applying for US Department of Commerce Privacy Shield Certification.

Are you in compliance? Contact **Paul Filon** (pfilon@bdblaw.com) to discuss today.