WARD AND SMITH, P.A.
ATTORNEYS AT LAW

New Year, New Data Protection Law: Is Your Company Ready for the GDPR?

Written By **Angela P. Doughty, CIPP-US** (apd@wardandsmith.com)
January 8, 2018

The countdown has officially begun.

On May 25, 2018, the European Union's ("EU") General Data Protection Regulation ("GDPR"), a sweeping data privacy and security regulation resulting from years of regulatory and political negotiations, will officially go into effect. Because EU enforcement will begin promptly on the effective date, compliance must begin before May 25th.

Many U.S. companies and business people, including sole proprietors (all business entities such as corporations and limited liability companies, as well as individual sole proprietors are collectively referred to as "U.S. Businesses") who obtain data regarding EU subjects are either doubting or are in denial about the applicability of the GDPR to their business practices—after all, the United States still doesn't have an over-arching data protection law.

However, the new GDPR requirements make the cybersecurity world a lot smaller by substantially broadening the reach of the EU's data privacy compliance requirements, and the effects of the GDPR will ripple across the pond and impact many U.S. Businesses. The complexity and scope of the GDPR leave U.S. Businesses that are more accustomed to the patchwork of U.S. data privacy laws with more questions than answers. U.S. Businesses are also vulnerable to possible business disruptions and significant financial penalties.

GDPR Purpose

The GDPR was enacted to give EU subjects more control over their "personal data," and at its core, directs how such personal data may be collected, stored, transmitted and destroyed (collectively, "processed").

GDPR Jargon

Personal data can include almost any information relating to an EU subject. This definition is purposefully broad and includes even non-sensitive information such as a name, identification number, telephone number, email address, financial information, location, online identifier or screen name, or IP address, as well as certain special categories of personal data such as genetic, political, or religious information.

GDPR Applicability

The GDPR imposes new requirements not only on those organizations or individuals located in the EU, but also on organizations or individuals located anywhere in the world that process personal data of EU subjects in connection with either the offering of goods or services to EU subjects or the monitoring of behavior of EU subjects. The GDPR requirements apply

no matter the size of the business processing the information or the amount of information being processed. This means that any company—from a large U. S. based corporation to a small family-owned business located in Johnston County, North Carolina—could subject itself to GDPR requirements by selling its products online to EU subjects, if during that transaction it collects personal data from an EU subject. Again, for purposes of GDPR applicability, this personal data can be as innocuous as a name, email, or mailing address.

GDPR Requirements

The new GDPR framework will mean an overhaul in many U.S. Businesses' data privacy programs, even for those that already have robust data privacy programs in place. The following GDPR provisions will likely produce the most significant impacts for U.S. Businesses that are required to comply with the GDPR:

- *Lawful Processing* – The GDPR requires a valid legal basis for processing the personal data of any EU subject and lists a limited, specific set of instances that will qualify and provide that legal basis. These include instances such as processing in the performance of a contract, to protect a vital interest of the EU subject, or processing pursuant to an EU subject's consent. If processing is based on consent, that consent must be "freely given, specific, informed, and unambiguous," which implies that any consent forms must be written in plain language and easily accessible. Any consent form that contains legalese or illegible terms and conditions will likely not pass muster. Additionally, a person's consent cannot be contingent on the receipt of any good or service and the person must be allowed to withdraw consent at any time. There are additional consent requirements when the person is a child under the age of 16. The determination of whether there is a legal basis for the processing of an EU subject's personal data can be complex and must be done prior to processing the data.
- *Privacy Notices* – A business must, at the time of, or prior to, the processing of personal data, provide a detailed list of all the personal data that will be processed, the business's contact information, the purposes for which the personal data will be collected, whether the business intends to transfer the personal data to another party, and any other information related to the individual's rights regarding the personal data and how those rights can be exercised.
- *Breach Notification* – The GDPR's breach notification structure is far more rigorous than many of the breach laws adopted by individual states in the United States. Specifically, the circumstances requiring businesses to notify individuals affected by a breach and EU officials are much broader and more liberal, and the time frame for the required notifications much shorter.
- *Data Protection Officer* – One of the more controversial requirements of the GDPR is the requirement that a business appoint a Data Protection Officer" ("DPO") if the business will engage in certain activities, such as monitoring EU subjects on a large scale, processing special categories of personal data, or processing data relating to criminal offenses.
- *Rights in Personal Data* – The GDPR enumerates a number of fundamental rights that belong to all persons whose personal data is processed. These include the right to access the personal data (called the "Right to Access"), the right to request the deletion of personal data (called the "Right to be Forgotten"), and the right to receive personal data concerning the EU subject and transmit that data (called "Data Portability"). No matter how a business implements the GDPR, the business should design its privacy programs with these rights in mind.
- *Personal Data Security* – Businesses are required to implement the "appropriate level of security" for the personal data they process, including protection against loss, destruction, damage, or unauthorized access. Businesses will also have to maintain records of their personal data processing activities.
- *Cross-Border Data Transfer* – Perhaps the most significant impact for many U.S. Businesses will be the GDPR's requirements on the permissible transfer of personal data from the EU to non-EU countries. "Cross-Border Data Transfer" requirements are complex, extremely onerous, country specific, and include certain Codes of Conduct and certifications that should be reviewed and understood prior to transferring any EU subject's personal data.

GDPR Penalties

The monetary penalty for non-compliance with the GDPR can be astronomical. Fines will generally be based on factors such as the nature, gravity, and duration of the violation, whether the business took steps to mitigate the damage, prior infringements, the types of personal data involved, and whether the violation was intentional or negligent. Businesses found in violation of the GDPR may also face substantial business disruptions and become subject to periodic audits to ensure future compliance.

Conclusion

The GDPR is over 100 pages long and presents complex, stringent, and potentially expensive requirements for U.S. Businesses that process EU subjects' personal data or provide goods or services to EU subjects. U.S. Businesses should consider the types of data they have, and from whom they receive that data, to determine whether the new GDPR requirements will apply to their business practices.

--