Tucker Ellis LLP

GDPR UPDATE

YOUR QUESTIONS ABOUT GDPR – ANSWERED

JULY 2018

Much of the business community has been busy assessing whether and how to comply with the European Union's (EU) sweeping data privacy and security law, the General Data Protection Regulation (GDPR). If you have questions about whether and how your company needs to comply, the quick reference guide below will give you some direction.

WHAT IS THE GDPR?

The GDPR is an EU law governing how the personal data of EU residents is handled. It is designed to establish and enforce standards for the privacy and security of individuals' personal data.

DOES THE GDPR APPLY TO MY COMPANY?

Typically, companies become subject to the GDPR if they either 1) offer goods or services to residents of the EU; or 2) conduct some activities through a stable arrangement in the EU. If your company collects or uses the personal data of EU residents, then your company will likely be deemed either a "data controller" or a "data processor" under the GDPR. Data controllers direct the collection, use, storage, disclosure, retention, and deletion of personal data (such as retail and commercial websites that solicit information directly from customers), whereas data processors merely handle the data at the direction of the data controller (such as third-party marketing and analytics companies that receive customer information from a retailer). Both are subject to the GDPR, although they have different responsibilities, even if they are located or processing personal data outside of the EU.

WHAT IS PERSONAL DATA?

"Personal data" is information "relating to an identified or individual person" who is referred to in the GDPR as a "data subject." This broad definition includes information such as a person's name, address, email address, telephone number, and payment information, as well as less obvious identifiers such as a person's IP address, photographs, cookies, and log-in information that are often not covered by many privacy and security laws in the United States.

WHAT ARE MY COMPANY'S OBLIGATIONS UNDER THE GDPR?

- **You must have a lawful basis for processing personal data.** Typically, you can process personal data if the individual is already a customer of your company or to perform a contract, comply with the law, protect the interests of an individual or the public at large, or with the express consent of the individual. This "express consent" requirement prohibits the "pre-checked" boxes that have become the norm and which assume that an individual consents to a website's terms of use, to receive offers from third parties, etc. Rather, individuals must now engage in a deliberate action to express their consent, such as checking an unchecked box.

- **You must implement safeguards to facilitate compliance with the GDPR's requirements.** The GDPR requires organizational safeguards to limit how personal data is processed and to provide a level of security commensurate to the risks it poses.
    - **You must cull personal data you no longer need for the purpose for which you collected it.** You may store personal data only for as long as necessary for the purpose for which it was processed. For example, information collected for marketing purposes may be considered to be stale after a certain number of years; therefore, this information should not be maintained indefinitely, but should be deleted after a designated period of time.
    - **You must contract in writing with third parties with whom you share personal data to guarantee that they take sufficient steps to comply with the GDPR.** You may not share personal data with other entities, such as third-party marketing and analytics companies, without a written assurance that those companies utilize the requisite technical and organizational measures to protect personal data. Data processors may not process data contrary to a data controller's instructions.
    - **You must notify a supervisory authority generally within 72 hours of learning of a data breach.** If and when a data breach occurs, you must notify the appropriate supervisory authority "without undue delay and, where, feasible, not later than 72 hours after having become aware of it." Data processors also have a duty to report a breach to data controllers "without undue delay."
- **You must document your data processing activities.** You must have records of who is responsible for your record retention systems, how and why data was collected and disclosed or transferred, and when such data will be destroyed.
- **You must be prepared to comply with GDPR's grant of certain rights to EU residents.** At the time that personal data is collected, EU residents have a right to know who handles their data, how long it will be held, and whether the data collector intends to share the information. They also have the right to demand the correction, supplementation, or deletion of their personal data without undue delay in certain circumstances.

DO I NEED A DESIGNATED REPRESENTATIVE OR A DATA PROTECTION OFFICER?

You may need a Designated Representative if you are not based in the EU and you consistently process the personal data of EU residents. In that case, you must appoint a representative who is located in one of the EU member states where you process data or offer goods or services. You will need a Data Protection Officer if: 1) you submit personal data to a public authority; 2) your core activities necessitate regular, systematic large-scale monitoring of individuals; or 3) your core activities require large-scale processing of highly sensitive personal data. If you process the personal data of approximately 5,000 or more EU residents or derive revenue directly from data analytics or advertising, you should consider this question closely.

GDPR UPDATE

WHAT STEPS SHOULD I TAKE TO START MY COMPANY'S COMPLIANCE EFFORTS?

Although the GDPR imposes many requirements, addressing the following essential issues will go a long way toward compliance with GDPR's fundamental privacy and data security mandates.

- **Data mapping and inventory** – Prepare and maintain a summary of what personal data you collect and store, in-points and end-points of this data, how it is used, and where it is stored. Review and document how you seek, record, and manage consent and whether you need to make any changes.
- **Lawful basis for data processing** – Determine and document any lawful basis for your processing of personal data and notify individuals of those bases in your Privacy Policy.
- **Data retention and destruction policies** – Document and maintain any policies governing how you retain and destroy personal data in your possession.
- **Identify your governance structure** – Identify those individuals who are responsible for privacy and data security governance within your organization and their responsibilities.
- **Privacy and security program** – Assess your internal privacy and data security policies. Have you adequately conducted privacy and security risk assessments, and if so, do they need to be updated? Evaluate the administrative, physical, and technical measures you have in place for protecting personal data, your data backup process to ensure integrity and availability of data, and testing done to assess the effectiveness of your security measures.
- **Sharing personal data with third parties and vendors** – Summarize how and with whom you share personal data, including your use of contracts with third parties regarding privacy and data security practices, protecting personal data, breach notification procedures, and risk allocation for breaches. Assess your policies governing your vetting and managing these third parties.
- **Document privacy and data security efforts** – Do you have a system in place for documenting your efforts to comply with privacy and security standards and requirements? Do you have procedures in place to address individuals' rights under the GDPR, including a designated contact person for individuals to contact to exercise their rights?
- **Staff training** – Evaluate the staff training you have done on your company's data protection policies and practices and determine what additional training is necessary, particularly if staff have not been trained on the GDPR.
- **Cyber insurance** – Assess whether you have cyber insurance and whether your coverage is adequate to meet the ever-growing risks you face. Know what notification and breach response requirements you have under the terms of your policy.
- **Incident response planning** – Prepare and maintain a written incident response plan that details how your organization will act in the event of a data breach. Engage the members of the response team and practice your response using real-world scenarios.

- **California privacy requirements** – California recently passed comprehensive privacy legislation closer in scope to the GDPR than anything previously seen in the United States. If your company does business in California, even if not physically located there, the new law potentially applies to you. While the new California law does not go into effect until January 2020 and is likely to undergo changes over the next year, you should take steps now to determine its applicability to your business and familiarize yourself with its expected requirements. Tucker Ellis has issued a July 2018 Client Alert providing more information about California's new law.
- **Get expert help** – You must determine what personal data is collected; how and when it is used or shared; how it is stored, secured, accessed, corrected, and deleted; and what changes you must make to comply with the GDPR and other laws, including California's. You may also need assistance crafting data retention, privacy, data security, and incident response policies, as well as evaluating your risk assessments and data security measures. You may also need to review contracts with third-party vendors who process personal data on your behalf and update your staff training. It is important to put together a team of management, information technology, and legal experts to assist you with GDPR compliance.

ADDITIONAL INFORMATION

For additional information, please contact:

Dan Messeloff | 216.696.5898 | daniel.messeloff@tuckerellis.com
Bill Berglund | 216.696.2698 | william.berglund@tuckerellis.com
Avril Love | 213.430.3306 | avril.love@tuckerellis.com
Emily Knight | 216.696.4893 | emily.knight@tuckerellis.com

This Client Alert has been prepared by Tucker Ellis LLP for the use of our clients. Although prepared by professionals, it should not be used as a substitute for legal counseling in specific situations. Readers should not act upon the information contained herein without professional guidance.

©2018 Tucker Ellis LLP. All rights reserved.