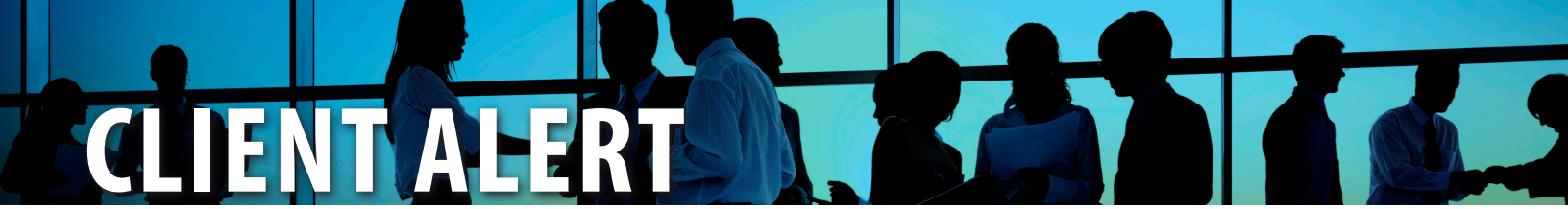


DATA PRIVACY AND CYBERSECURITY

WHAT US-BASED COMPANIES NEED TO KNOW ABOUT THE GDPR, AND WHY NOW?

by Sara H. Jodka

If you are a US-based or multinational company, you may have noticed that in the past few months you have started to see a significant increase in the number of vendor (or other) agreements that you have been asked to modify or verification forms that you have been asked to execute. If you have not yet, you probably will. The reason for this up-tick is simple, the European Union (EU) General Data Protection Regulation (GDPR) goes effect on May 25, 2018, and companies you work with must be GDPR compliant, which, in turn, puts obligations on you.

The Reach of the GDPR

If you have nothing to do with the EU, *i.e.*, no physical presence in the EU, no employees, no nothing, you are probably wondering why the GDPR impacts you at all. The answer to that comes down to how far the GDPR reaches, which includes its application to US-based companies and what that means for those companies. While the GDPR is the most significant change to European data privacy and security in over 20 years, and that is certainly true, it is also the most significant change to US data privacy security since HIPAA (as it impacted the healthcare industry) as many US-based companies will fall within the GDPR's reach, one way or another.

The GDPR reaches into US-based companies because the GDPR is designed to protect the "personal data" of individuals. Despite what you might have read in other sources, the GDPR does not say EU "residents" or EU "citizens", it says it applies to the processing of "personal data of data subjects" but controllers and processors who are in the EU, but also to "processing activities" related to: (1) offering goods or services; or (2) monitoring data subject behavior that takes places in the EU. See GDPR Article 3(2).

The GDPR replaces the 1995 EU Data Protection Directive which generally did not regulate businesses based outside the EU. However, now even if a US-based business has no employees or offices within the boundaries of the EU, the GDPR may still apply.

Privacy and Personal Data: EU v. US

Stepping back for a second, to understand the GDPR, it is important to understand that most of the world views privacy very differently than the US. Where many Americans put a lot of their personal information online via social media right down to what they ate for breakfast, privacy is a very tightly-held right in other parts of the globe and the definition of privacy is far more robust.

For example, where "personal data" is typically defined by US breach notification laws as an individual's name accompanied by some other type of identifying information, such as a social security number or financial account information, "personal data" under the GDPR goes much further and includes, "information related to an identified or identifiable natural person." This means that, if you can use any piece of information for learn or otherwise identify a natural person, the information is "personal data" under the GDPR, and the processing of that data is protected by the GDPR. This type of information includes an individual's name, ID number, location data, online identifier or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. It also includes, religion, trade union association, ethnicity, marital status, IP addresses, cookie strings, social media posts, online contacts, and mobile device IDs.

Am I a "Controller" or a "Processor" … or both?

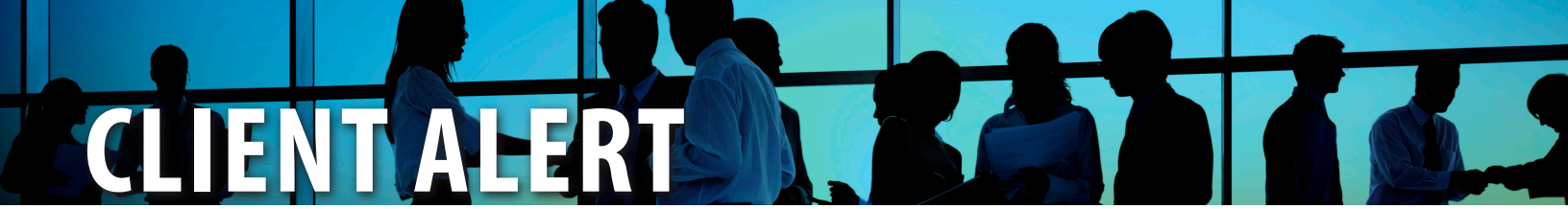
Stepping back for a second to understand the GDPR, it is important to understand that most of the world views privacy very differently than the US. Where many Americans put a lot of their personal information online via social media right down to what they ate for breakfast, privacy is a very tightly-held right in other parts of the globe, and the definition of privacy is far more robust.

For example, where "personal data" is typically defined by US breach notification laws as an individual's name accompanied by some other type of identifying information, such as a social security number or financial account information, "personal data" under the GDPR goes much further and includes, "information related to an identified or identifiable natural person." This means that, if you can use any piece of information for learn or otherwise identify a natural person, the information is "personal data" under the GDPR, and the processing of that data is protected by the GDPR. This type of information includes an individual's name, ID number, location data, online identifier or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. It also includes, religion, trade union association, ethnicity, marital status, IP addresses, cookie strings, social media posts, online contacts, and mobile device IDs.

This leads to the next set of logical questions: (1) what is processing of personal information? And (2) what is a "controller" and a "processor"?

The concepts of "controller", "processor" and "processing of personal data" are part of the new lexicon that US-based companies falling under the GDPR are going to have to get familiar because they are not terms that have much impact in the US, until now.

Simply put, "processing" personal data is basically collecting, recording, gathering, organizing, storing, altering, retrieving, using, disclosing, other otherwise making available personal data by electronic means. A "controller" is the entity that determines what to do with the personal data. Take for example, a company collects personal information from its customers in order to sell them products. In turn, the company provides that data to its shipping vendors and payment vendors to ship



the products to the customers and to bill and collect payment from the customers. The company/seller is the controller, and the shipping company and the payment company are processors.

With this example, the scope of the GDPR to US-based companies also becomes a little clearer as you can start to see where US-based companies would fall somewhere in that controller processor chain as far as they are selling to customers located in the EU.

The GDPR even applies if no financial transaction occurs if the US company sells or markets products via the Internet to EU residents and accepts the currency of an EU country, has a domain suffix for an EU country, offers shipping services to an EU country, provides translation in the language of an EU country, markets in the language of an EU country, etc.

The GDPR also applies to employee/HR data to the extent the individual employee is a data subject with rights in the EU.

As such, US-based companies with no physical presence in the EU, but in industries such as e-commerce, logistics, software services, travel and hospitality with business in the EU, etc., and/or with employees working or residing in the EU should be well in the process of ensuring they are GDPR compliant as should US-based companies with a strong Internet presence.

Why is this an issue now?

Why this is becoming even more of an issue for US-based companies now is that many companies that are required to be GDPR compliant have obligations that require them to take certain steps with their vendors. As such, many US-based companies that otherwise might not have any GDPR-compliance obligations are finding themselves Googling "GDPR" because they received an updated vendor contract that includes GDPR language or a verification request with similar references.

US-based companies should get prepared for these types of contract modification negotiations and verification requests and be ready to speak on the issues at hand; know what they are signing; know what they are agreeing to; know what they should not be agreeing to; know that they are in required compliance or will be in compliance by May 25, 2018; and know what the penalties are if they do not.

The fines and penalties are significant and many US-based companies will likely fall into the categories of controller and processor. While the GDPR provides for certain liability for each of those roles, some liability can be transferred by contract so contract review and GDPR understanding is critically important.

At a minimum, what should I know?

At a bare minimum, you should understand that if a company you work with is asking you to revise an agreement, sign off on a verification, or something similar, it might be related to their obligations under the GDPR and, in turn, yours.

One of the keys to the GDPR is that data subjects must be fully informed about what is happening to their data, why it is being collected, how it will be used, who will be processing it, where will it be transferred, how they can erase it, how they can protect it, how they can stop its processing, etc. The bulk of the consent and notification responsibility falls on the controller, but the processor and the controller have to work together to ensure the data subject's rights are protected and this will happens in two separate but distinct steps:

The first step is in the overall physical compliance process, which takes the most time as it requires reviewing data collection and processing; ensuring there is a legal right to have the data and process it; gaining a fundamental understanding of what is going on with the data and where it is going; building security protocols around the data; etc.

Controllers

Controllers specifically must, at a minimum:

1. Review data processing activities and conduct an Impact Assessment.
2. Identify their data processing activities for which it is a controller and ensure it understands its responsibilities.
3. Ensure that, in respect of each processing activity for which it is a controller, it has implemented appropriate technical and organizational measures to ensure compliance with the GDPR; and ensure it has appropriate processes and templates in place for identifying, reviewing and (and to the extent required) promptly reporting data breaches.

Processors

Processors must, at a minimum:

1. Review all data processing activities.
2. Ensure there is a lawful basis for each processing activity (or that there is consent or that an exemption or derogation applies).
3. Where consent is the basis for processing, review existing mechanisms for obtaining consent, to ensure they meet GDPR.
4. Where a legitimate interest is the basis for processing, maintain records of the organization's assessment of that legitimate interest, to show the organization properly considered the rights of the data subjects.
5. Update privacy policies.
6. Train employees who process personal data to quickly recognize and appropriately respond to requests from data subjects to exercise their rights.

The second step is in contracting between the controller and processor to ensure their contracts meet all the legal specifications of the GDPR. The GDPR outlines a number of contractual requirements between

controllers and processors including: identifying the subject matter and duration of the processing; identifying the nature and purpose of the processing; structuring the obligations and rights of the controller; acting only upon the written instructions of the controller; ensuring those processing data are doing it under written confidentiality agreement; assist the controller in meeting breach notification requirements.

Unlike US breach notification laws that allow more time to notify the appropriate individuals and authorities of a data breach, the GDPR requires notification be made within 72 hours of a breach.

There is a lot to take in and think about when it comes to the GDPR. This is a law that we have been reviewing, analyzing, and working with for almost two years. The hardest thing about the GDPR is changing your perspective and realizing it probably does have some applicability to your business; changing your lexicon to include words like "controller", "processor", and "data subject"; and learning to break the GDPR down to its manageable chunks so compliance stops being overwhelming and starts getting done, piece by piece.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of data privacy and cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.