ARE YOU READY FOR GDPR?

04/17/2018

GDP What?

Personal data is currency in the new world, and while the United States uses a sectoral approach to data privacy, the European Union (EU) treats privacy as a fundamental right of its citizens. Therefore, where U.S. regulations are based on the categorization of information, the EU model covers all categories of data. With an ever-evolving digital market, the EU adopted a new set of rules, the General Data Protection Regulation (GDPR), in April 2016 to streamline the protection of its citizens' personal data. GDPR will make the biggest change to European data security in 20 years and is scheduled to go into effect in the European Union on May 25, 2018.

But I Don't Do Business in the EU, So This Doesn't Apply to Me, Right?

Nope. Any U.S. company that has a web presence and markets their products online may come under scope of GDPR. A U.S. company does not have to have a physical presence in the EU to be subject to GDPR. The impact of this regulation depends upon whether personal data of EU citizens are collected or processed by a company. Personal data, as defined by GDPR, includes any information that relates to an individual, such as names, email address, other personally identifying information, and technical information, such as an IP addresses, cookie strings, social media posts, online contacts and mobile device IDs.

Some points of note on GDPR's scope:

- GDPR does not require a financial transaction to occur to come under its scope.
- GDPR applies if a data subject (individual) is in the EU when the data is collected. Therefore, GDPR does not apply when data is collected on an EU citizen while they are outside the EU.
- When collecting data on an individual via an online interface, a business would have to target a data subject in an EU country. Generic marketing is not intended to come under the scope of GDPR, but it is easy to blend the lines from generic to targeted marketing. Some examples of this include marketing materials are in the native language of a user in a European Union country, or reference EU users in marketing materials or accepting foreign currency or maintaining a domain suffix for another country.

Why Should I Care About GDPR?

Penalties, penalties, penalties. GDPR sets forth two tiers of severity for violations to its regulations. A lower tier infraction may result in a maximum penalty of the greater of up to 2% of worldwide annual revenue for the prior financial year or 10 million Euros. A more severe infraction penalty can be up to the greater of 20 million Euros or 4% of worldwide annual revenue for the prior financial year.

What's The Big Deal About GDPR?

Some of the important elements of GDPR include:

- *Requiring consent of data processing to ensure rights of EU citizens:* For U.S. companies, EU-directed online marketing interactions will need to obtain explicit consent. This consent must be freely given, specific, informed and unambiguous.
- *Requiring parental consent for processing children's data*: Parental consent is required to process personal data of children under the age of 16. Verification of an individual's age should be part of the collection process.
- *Protecting EU citizen's rights to erasure of their personal data*: If an EU citizen's data is no longer needed for the reasons it was originally collected, then that citizen has the right to be forgotten.
- *Safe handling of cross-border data transfers*: In order to be allowed to transfer data to a country that is not subject to GDPR, then business sending the information must ensure that the business receiving the data is in a country that has equal or better data protection laws in place. This does not currently include the United States. The European Commission has adopted the EU-US Privacy Shield to allow the Commission to conduct periodic reviews to determine whether an adequate level of protection exists for cross-border transfers.
- *Preventing data breaches*: Data protection compliance must be adhered from inception to delivery in the lifecycle of a service or product. Businesses must be able to prove their compliance as well. GDPR also requires the designation of a data protection officer: (1) for all public authorities; (2) where the core activities of the controller or processor require regular and systematic monitoring of data subjects on a large scale and (3) core activities of the controller or processor involve large-scale processing of special categories of sensitive personal data for the purpose of uniquely identifying a natural person or concerning a person's health.
- *Providing guidance for data breach notification*: One of the most noticeable changes of GDPR is the 72-hour rule. Upon a breach, companies IT resources will need to analyze whether the exposure of data can cause a risk to the rights of EU data subjects. Notification to an EU regulator or supervising authority is required within 72 hours of a large exposure of email addresses, medical or financial information or identifiers related to children. If there is a substantial risk to an individual's privacy rights, then individuals must also be notified.

What Does This Mean for My US Company?

It's a good time to:

- *Update Consent Notices*: Consent communication must be clear, to the point and easy to understand. Do individuals understand the legal basis for processing their data? Do they understand the intended use of their information? Their right to complain if they believe their data is being mishandled? Long terms and conditions and boxes checked by default are no longer acceptable forms of consent.
- *Inventory Data*: Businesses should map and document all personal data they maintain. Can you provide documentation as to where personal data came from? Where it is held? Why it is processed? Who is it shared with?
- *Update Retention Policy*: With the right to be forgotten, data controllers must now ensure personal data is stored for a strict minimum time and that such data is deleted once it is no longer being used for the purpose it was collected. What is your current deletion cycle? How long do you hold data? For what purposes?
- *Update Breach Preparedness*: Companies who experience a breach of EU citizen personal data must now comply with the 72 hour rule. Will your procedures and third party service provider requirements allow you to adhere to this new timeframe and other GDPR breach response rules?
- *Structure for Successful Compliance*: Under GDPR, companies must prove they have effective policies and procedures in place to comply with GDPR data protection principles. Do you have updated policies in place? Have you performed your third party due diligence with GDPR in mind? Do you have a data protection officer designated? Do you meet all the requirements? An overarching review of your privacy program will help ensure conformity.

- *Consider Cross-Border Data Transfers*: If you operate on an international scale, consideration must be given to which data protection supervisory authority you are subject to. These transfers are only allowed when GDPR requirements are met, and related violations will result in the highest fines.

As May 25 approaches, U.S. companies should bear in mind that one of the main objectives of GDPR was to expand its territorial scope. Companies must ensure they are compliant prior to the effective date or be subject to penalties.