Luxury Daily®

The News and Intelligence You Need on Luxury

LEGAL AND PRIVACY

Most common misconceptions about GDPR and data processing

October 23, 2018

Eric V. Holtzclaw is chief strategist at PossibleNow

By Eric V. Holtzclaw

The General Data Privacy Regulation (GDPR) passed in the European Union (EU) in May and is one of the most popular topics of discussion amongst businesses that may or may not conduct business on an international level.

Time and time again, businesses and even media publications have stated that GDPR is not important to them, simply because they are either "not affected" or "not governed" by these regulations.

Many hold the perception that GDPR only applies to those in the EU, or those who manage business directly in the EU.

There is a misconception that the GDPR does not apply to businesses that do not offer goods or services to EU consumers, or process personal EU data. However, in all these scenarios, the GDPR rules and regulations still apply.

Here are three of the most common misconceptions about GDPR and businesses:

1. My organization does not process EU personal data

One of the first misconceptions about GDPR results from an organization's belief that it does not process personal data from the European Union.

However, many people do not understand the full scope of the GDPR definition of personal data.

The definition as allocated in the GDPR defines personal data as "anything that can directly or indirectly identify a natural person." This is in reference to any identifier such as name or identification number, location data or any online identifier such as IP address.

Additionally, many fail to realize the definition of processing as defined by the GDPR actually applies to any set of operations performed around data. This includes collecting information on customers, recording, alteration, retrieval of this information, consultation, use, erasure or destruction.

Combine the far-reach of modern technology and the number of people living abroad, and there is likely

information stored somewhere that affects EU citizens.

2. My organization does not have an EU presence

GDPR applies to “controllers” and “processors.”

A controller determines the purposes and means of processing personal data.

In other words, the controller is the business that is selling a good or service.

If an organization processes any sort of data for a controller, it is thus considered a “processor” under the GDPR.

Any size enterprise that processes data on behalf of its controllers is subject to governance, whether or not the organization in question has a physical presence in the EU.

Additionally, any company that is located outside of the EU is still subject to the law if the organization is operating an online business that EU customers can access, interact with or purchase products.

3. My organization does not offer goods or services to EU customers

Whether or not an organization offers goods or services to the EU does not matter if the organization is again processing for its controllers. This labels the organization as a legal “processor.”

Data processors include software providers such as Salesforce and Microsoft, call centers, payroll, accounting and market research firms, to name a few.

All of these functions within any company are considered departments that store or analyze data in some way.

If an EU citizen is affected, he or she is protected under the GDPR and the company must comply with the legalities surrounding that individual.

What is more, many companies that do not believe GDPR impacts them do, in fact, process data of EU data subjects.

More specifically, GDPR has created a groundswell of countries and states that have decided to update or create new regulations that mirror GDPR.

It is more important than ever for privacy to be a top priority.

It is recommended to establish a proactive practice of collecting country-of-residence of the prospects and customers with whom an organization conducts business.

Then, as appropriate, collect consent and communication preferences for each data subject.

Today, “unsolicited email” in the EU is an easy target for class action lawsuits, especially as it seems that consumer opinion on data protection has become increasingly negative.

ORGANIZATIONS MUST NOW reconsider whether or not they are governed under the laws of GDPR, as it is likely that they are.

The best defense is a good offense.

Considering ways to collect, store and easily change consent and privacy information should be a top concern for all companies.

Eric V. Holtzclaw is chief strategist at PossibleNow, Duluth, GA. Reach him at eholtzclaw@possiblenow.com.